ANUÁRIO DA PROTEÇÃO DE DADOS

2019

COORDENAÇÃO

FRANCISCO PEREIRA COUTINHO

GRAÇA CANTO MONIZ

CEDIS

CEDIS CENTRO DE I&D
SOBRE DIREITO E SOCIEDADE

ANUÁRIO
DA PROTEÇÃO DE DADOS
2019

ANUÁRIO DA PROTEÇÃO DE DADOS

2019

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CEDIS CENTRO DE I&D
SOBRE DIREITO E SOCIEDADE

ANUÁRIO DA PROTEÇÃO DE DADOS 2019

COORDENAÇÃO

Francisco Pereira Coutinho
Graça Canto Moniz

SECRETÁRIA EXECUTIVA

Izabel de Albuquerque Pereira

EDIÇÃO

Universidade Nova de Lisboa. Faculdade de Direito.
CEDIS, Centro de I & D sobre Direito e Sociedade
Campus de Campolide, 1099-032 Lisboa, Portugal

SUPORTE: ELETRÓNICO

Maio, 2019

ISSN 2184-5468

CATALOGAÇÃO NA PUBLICAÇÃO

PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.). Anuário da Proteção de Dados 2019. Lisboa: CEDIS, 2019

Nota introdutória

O Anuário da Proteção de Dados é uma revista jurídica de livre acesso, disponível em linha no sítio http://protecaodedados.ue.cedis.fd.unl.pt/, que pretende divulgar estudos doutrinários sobre o direito da proteção de dados pessoais. A revista é editada desde 2018 pelo Observatório para a Proteção de Dados pessoais, um grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da Faculdade de Direito da Universidade Nova de Lisboa.

Os nove artigos publicado na edição de 2019 do Anuário resultam de uma chamada lançada em setembro de 2018 no sítio da internet do Observatório para a Proteção de Dados Pessoais. Os textos foram depois selecionados e revistos pelos coordenadores do Anuário. Aos autores foi permitido escreverem de acordo com a nova ou a antiga grafia.

O Anuário inicia-se com um texto da autoria de Sérgio Henriques e de João Luís sobre os fundamentos de licitude para o tratamento de dados pessoais no contexto laboral, em que é dado especial destaque ao consentimento.

Seguem-se dois textos sobre os direitos do titular dos dados, em particular o direito de não sujeição a decisões exclusivamente automatizadas e o direito ao apagamento; o primeiro, da autoria da Gabriela Caldas, é um contributo para o debate em torno da (in)existência de um direito do titular dos dados à explicação das decisões tomadas por algoritmos sem qualquer intervenção humana; o segundo, da autoria de Francisco Lima e de Mateus Carvalho, problematiza a hipótese da aplicação global do direito ao apagamento.

A compatibilidade com o RGPD de algumas tecnologias e respetivas aplicações foi um dos tópicos que ocupou parte significativa do debate académico mais recente do direito da proteção de dados pessoais. É o caso

dos *Smart Tourist Destinations*, cuja conformidade com os princípios do RGPD é discutida por Manuel David Masseno e Cristiana Santos. O mesmo acontece com a *blockchain* e a videovigilância, analisadas, respetivamente, por Maria Rebelo e Lurdes Alves.

O Anuário termina com uma visão crítica dos regimes especiais de proteção de dados (Inês Oliveira), a análise da Diretiva (UE) 2016/681e da respetiva proposta de lei de transposição para o direito nacional (Ricardo Rodrigues de Oliveira) e com uma discussão sobre a lei das secretas e a imperatividade constitucional como dilema às novas ameaças num contexto global de defesa e segurança (Sérgio Azevedo).

Esta obra não teria sido possível sem o patrocínio da SRS Advogados e da FUTURA, a quem agradecemos, nas pessoas do Luís Neto Galvão (SRS Advogados) e do Rodrigo Adão da Fonseca (FUTURA), o apoio que têm prestado desde a primeira hora a este projeto. Igualmente devidos são agradecimentos à Izabel de Albuquerque Pereira e ao Matheus Passos Silva, pelo auxílio prestado na revisão do Anuário, bem como a todos os autores que participam nesta edição do Anuário.

Lisboa, 15 de abril de 2019

Graça Canto Moniz
Francisco Pereira Coutinho
Coordenadores do Observatório para a Proteção de Dados Pessoais

Lista de Abreviaturas

AIPD – Avaliação de Impacto sobre Proteção de Dados
AR – Assembleia da República
art. – Artigo
arts. – Artigos
CC – Código Civil
CDFUE – Carta dos Direitos Fundamentais da União Europeia
CE – Comissão Europeia
CEE – Comunidade Económica Europeia
CNIL – Comission Nationale de L'informatique et des libertés
CNPD – Comissão Nacional de Proteção de Dados
COM – Comunicação
CP – Código Penal
CRP – Constituição da República Portuguesa
CSM – Conselho Superior da Magistratura
DCIAP – Departamento Central de Investigação e Ação Penal
DLT – Distributed Ledger Technology
DPA – Data Protection Authority ou Autoridade de Proteção de Dados
DPIA – Data Protection Impact Assessment
DPO – Data Protection Officer
EDPS – European Data Protection Supervisor
ENISA – European Networks and Information Security Agency
EPD – Encarregado de Proteção de Dados
EUA – Estados Unidos da América

G29 ou Grupo de Trabalho – Grupo de Proteção de Dados do Artigo 29º.
GDPR – General Data Protection Regulation
GNR – Guarda Nacional Republicana
GPS – Global Positioning System
ICO – Information Commissioner's Office
ICTs – Information and Communication Technologies
IoT – Internet of Things
IP – Internet Protocol
JO – Jornal Oficial
n.º – Número
NATO – North Atlantic Treaty Organization / Organização do Tratado do Atlântico Norte
NUIPC – Número Único de Identificação do Processo Crime
OLP – Organização para a Libertação da Palestina
OPCs – Órgãos de Polícia Criminal
p. – página ou páginas
para. – Parágrafo
P2P – Peer-to-Peer
PbD – Privacy by Design
PIDE/DGS – Polícia Internacional e de Defesa do Estado/ /Direção-Geral de Segurança
PNR – Passenger Name Record
PSP – Polícia de Segurança Pública
RGPD – Regulamento Geral sobre a Proteção de Dados Pessoais
SIED – Serviço de Informações Estratégicas de Defesa
SIM – Serviços de Informações Militares
SIRP – Sistema de Informações da República Portuguesa
SIS – Serviço de Informações e Segurança
ss. – seguintes
STD – Smart Tourism Destination
STJ – Supremo Tribunal de Justiça
TC – Tribunal Constitucional
TIJ – Tribunal Internacional de Justiça
TJ ou TJUE – Tribunal de Justiça da União Europeia
TPJI – Tribunal Permanente de Justiça Internacional

TRP – Tribunal da Relação do Porto
UE ou EU – União Europeia / European Union
UIP – Unidade de Informação de Passageiros
v. – volume
WP 29 – Working Party Article 29

Índice Sumário

Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral

Sérgio Coimbra Henriques*
João Vares Luís*

Resumo: O progresso tecnológico possibilita novas formas de prestação e de controlo da actividade laboral, num contexto de hiperconexão em que, cada vez mais, a linha que divide o trabalho e a vida pessoal é ténue. Na vigência do Regulamento Geral sobre a Proteção de Dados Pessoais e sob a égide constitucional dos direitos fundamentais dos indivíduos, assegurar um nível adequado de proteção da privacidade e dos dados pessoais dos trabalhadores no âmbito do seu vínculo laboral coloca desafios que não devem ser desconsiderados. Desenvolvemos, portanto, quais os fundamentos de licitude para o tratamento de dados pessoais dos trabalhadores pelas entidades empregadoras, designadamente a necessidade do tratamento para a execução do contrato de trabalho no qual o trabalhador é parte, a realização de operações de tratamento de dados pessoais necessárias ao cumprimento de obrigações legais e os interesses legítimos daquelas, aos quais se encontra inerente a garantia da necessária proporcionalidade entre a prossecução de uma finalidade de tratamento de dados lícita e o respeito pelas liberdades e direitos fundamentais dos trabalhadores.

Palavras-chave: *Fundamentos de licitude; consentimento laboral; interesses legítimos da entidade empregadora; privacidade no local de trabalho.*

---

* Advogado. Licenciado em Direito pela Faculdade de Direito da Universidade Nova de Lisboa (FDUNL), Mestre em Ciências Jurídicas Empresariais pela FDUNL e Doutorando em Direito Privado pela FDUNL. Investigador do Centro de Investigação & Desenvolvimento sobre Direito e Sociedade (CEDIS).

** Advogado. Licenciado em Direito pela Faculdade de Direito da Universidade Nova de Lisboa (FDUNL) e Pós-Graduado em Ciências Jurídicas Empresariais pela FDUNL. Frequentou a 2.ª edição do Curso Breve sobre Proteção de Dados Pessoais organizado pela Associação da FDUNL (Jurisnova). Dedica-se, em especial, às áreas de prática de Direito do Trabalho e de Propriedade Intelectual e Tecnologias de Informação.

Abstract: Technological advancement allows for new ways of performing and supervising labour-related activities, in a context of hyper-connectivity in which, ever more so, the line dividing work and personal life is faint. Under the EU General Data Protection Regulation and the constitutional nature of fundamental rights, ensuring an adequate level of privacy and data protection within the employment relationship is a challenge that must not be taken lightly. Therefore, it's important to determine when the processing of personal data of employees by the employers is lawful, namely when the processing is necessary for the performance of a employment contract to which the employee is party, the performance of data processing activities necessary for compliance with legal obligations and the legitimate interests pursued by employers, to which are ineherent the need to ensure the proporcionality between said legitimate processing purposes and the fundamental rights of employees.

***Keywords**: Legal basis; worker consent; legitimate interests pursued by the employer; privacy at the place of work.*

Introdução

A proteção da privacidade dos trabalhadores perante a entidade empregadora, exercício tantas vezes necessário como forma de responder, no plano jurídico, à eventual incapacidade do trabalhador de salvaguardar os seus direitos fundamentais numa situação de subordinação jurídica e eventual dependência económica, constitui um elemento ontológico do direito do trabalho moderno. O vínculo laboral conhece limites e contornos que não se subsumem apenas à autonomia privada das partes contratantes. A entidade empregadora e, também, os trabalhadores, conhecem, por imperativo legal, um grande conjunto de direitos, deveres e obrigações que procuram assegurar um resquício de equilíbrio numa relação contratual em que as partes, regra geral, se apresentam em planos diametralmente distintos. Da mesma forma que o indivíduo goza, no âmbito do seu direito de personalidade, de uma expectativa jurídica de proteção e tutela da sua privacidade e de uma esfera de vida privada que se deve considerar impenetrável, também o trabalhador, na sua necessária qualidade de pessoa singular[1], merece semelhante proteção, ainda que adaptada às

[1] Art. 11.º do Código do Trabalho.

exigências da convivência laboral. A realidade laboral deseja e admite o controlo do empregador de determinados aspetos da rotina laboral de cada trabalhador, mas também exige a proibição de qualquer entrada abusiva, por desnecessária, na esfera privada de um trabalhador.

Os requisitos impostos pelo RGPD no domínio da proteção dos dados pessoais dos indivíduos constituem apenas mais uma refracção, ainda que com contornos muito próprios e uma relevância crescente, deste percurso de reconhecimento da individualidade de cada pessoa singular e da necessidade de um domínio de proteção em que esta se possa manifestar de forma livre. Não surpreende, neste contexto, que o respeito pela privacidade dos trabalhadores e a proteção dos seus dados pessoais perante a eventualidade de tratamento destes pelo empregador seja de cabal importância. A generalidade das pessoas passa uma quantidade considerável do seu tempo no local de trabalho ou, pelo menos, a desempenhar funções laborais. Sendo o direito à privacidade e à proteção dos dados pessoais direitos fundamentais, não é menos do que essencial que seja assegurado um nível adequado de proteção da privacidade dos trabalhadores no âmbito do seu vínculo laboral. Ademais, as novas tecnologias e os avanços no domínio digital oferecem às entidades empregadoras e aos próprios trabalhadores novas formas de prestação da sua atividade laboral, possibilitando a melhoria do seu desempenho ou, até, a opção de trabalhar a partir de casa. Esta realidade caracterizada pela hiperconexão, consequência das referidas novas tecnologias e outros avanços, veio perturbar a linha que antes dividia o trabalho e a vida pessoal, criando um desafio muito relevante à assumida pretensão legal de proteção da privacidade e dos dados pessoais das pessoas singulares.

Aqui chegados, é nosso intuito desenvolver quais os fundamentos que legitimam o tratamento de dados pessoais dos trabalhadores pelo empregador, assim como compreender qual o juízo interpretativo a realizar para esse efeito. Ainda que seja de reconhecer, à partida, a relevância de uma entidade empregadora poder proceder ao tratamento de dados pessoais dos seus trabalhadores com a pretensão de detectar ou prevenir a perda de dados pessoais relevantes (como seja a informação sobre clientes), de detectar ou prevenir a perda ou até o roubo de bens e propriedade intelectual, ou, ainda, de potenciar a produtividade e desempenho desses trabalhadores, não é de conceder, de forma imediata, a admissibilidade de tais operações de tratamento. Como sempre acontece no caso de colisão de direitos,

o interesse legítimo da entidade empregadora, como veremos, deve ser sopesado perante outros elementos relevantes (nos quais são de incluir os direitos fundamentais dos trabalhadores), num juízo de proporcionalidade.

1. Dados pessoais e contrato de trabalho

A evolução das tecnologias informáticas permite que a recolha, partilha e tratamento de dados pessoais[2], com fins económicos, seja hoje realizada a uma escala sem precedentes. Simultaneamente, as pessoas singulares disponibilizam, cada vez mais, as suas informações pessoais de uma forma pública e global. É esta contraposição que fundamenta a intervenção legislativa a nível europeu no domínio da proteção dos dados pessoais de cada um, enquanto reflexo, em grande medida, do direito fundamental à reserva da intimidade da vida privada, também previsto no ordenamento jurídico nacional, desde logo no art. 26.º da CRP. Não obstante, a proteção dos dados pessoais das pessoas singulares entronca em liberdades e princípios que enformam o direito da UE, como o respeito pela vida privada e familiar, a liberdade de pensamento, consciência e de religião, a liberdade de expressão, a liberdade de empresa e a diversidade cultural e religiosa. Assim, é pacífica a conclusão de que o direito à proteção de dados pessoais não é absoluto e deve ser equilibrado com outros direitos fundamentais em conformidade com o princípio da proporcionalidade, tal como previsto no número 2 do art. 18.º da CRP. Subjacente à proteção dos dados pessoais das pessoas singulares surge não só a proteção do direito à autodeterminação informativa (também este direito merecedor de consagração constitucional no art. 35.º da CRP) mas, também, o direito à proteção da privacidade de cada um[3]. A autodeterminação informativa,

---

[2] O tratamento de dados pessoais é "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*". (art. 4.º, número 2 do RGPD, destaque nosso).

[3] Não será, portanto, de estranhar que o art. 2.º da Lei n.º 67/98, de 26 de Outubro (vulgo Lei da Proteção de Dados Pessoais) determine que o tratamento de dados pessoais processa-se "de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.".

ao visar assegurar o controlo do particular sobre os seus dados pessoais, permitindo-lhe limitar o tratamento, acesso e divulgação destes, contribui no sentido da proteção da privacidade, inserindo-se no âmbito da tutela jurídica do direito fundamental à privacidade e do desenvolvimento da personalidade[4].

Visa-se a proteção direta de interesses individuais de pessoas singulares, pelo que a tutela legal das situações de não cumprimento de obrigações relativas a proteção de dados ou da violação do dever de sigilo relativamente a estes (prevista, nomeadamente, nos arts. 43.º e 47.º da Lei de Proteção de Dados), constitui uma parte do leque de normas de proteção da esfera privada do indivíduo, as quais carecem de conjugação com a tutela geral da personalidade consagrada no art. 70.º do CC, a qual, por sua vez entronca no princípio constitucional da dignidade da pessoa humana[5].

Com a aplicação do RGPD a partir do dia 25 de maio de 2018, e na ausência da publicação de qualquer legislação nacional portuguesa que viesse coartar o âmbito de aplicação das suas normas na medida admitida pelo próprio RGPD como opção de cada Estado-Membro, o conteúdo deste tornou-se diretamente aplicável em todos os Estados-Membros da UE e, consequentemente, no nosso ordenamento jurídico. Esta vigência traduziu-se na alteração do paradigma vigente no que diz respeito à proteção de dados pessoais. Passando-se de um sistema de controlo externo, o qual era efetuado pelas Autoridades Nacionais de cada Estado-Membro[6], para

---

[4] Será assim de entender que este conjunto de direitos relacionados com o tratamento de dados pessoais soçobra de "alguns 'direitos-mãe' em sede de direitos, liberdades e garantias. É o caso do direito à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa". Em conjunto "todo este feixe de direitos tende a densificar o moderno direito à autodeterminação informacional, dando a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em 'simples objeto de informação'" (Canotilho, José Joaquim Gomes e Moreira, Vital. *Constituição da República Portuguesa Anotada*, 4.ª ed., v. 1, Coimbra: Coimbra Editora, 2007, p. 550-552).

[5] Tal como plasmado no art. 1.º da CRP e nas decorrências desse princípio que aqui surgem como diretamente relevantes: A inviolabilidade da integridade física e moral das pessoas, e os direitos ao respeito pelo seu bom nome e reputação, à proteção da sua imagem, à palavra, à reserva da intimidade da vida privada e familiar e ainda ao direito à proteção legal contra quaisquer formas de discriminação (arts. 25.º e 26.º da CRP).

[6] Que autorizavam as atividades de tratamento de dados pessoais pelos agentes económicos e, posteriormente, fiscalizavam essas mesmas atividades (cfr. Sarmento e Castro,

um sistema de responsabilização (*accountability)* das próprias empresas, no pressuposto de que os agentes económicos responsáveis pelo tratamento de dados devem assegurar, por sua conta e risco, o cumprimento das disposições do RGPD[7].

São já conhecidos os inúmeros aspetos em que o RGPD veio implicar a alteração ou aperfeiçoamento de procedimentos e formas de atuação já enraizadas na prática comercial diária relativamente às atividades de tratamento de dados pessoais, assim como o exigente entorno sancionatório que foi associado ao incumprimento destas regras. Um dos assuntos que, a este respeito, mais tem suscitado debate na doutrina e jurisprudência nacionais é a questão do consentimento dos trabalhadores como fundamento de licitude para o tratamento de dados pessoais dos trabalhadores por parte das entidades empregadoras.

Nos termos do RGPD, o consentimento é um dos fundamentos de licitude para o tratamento de dados pessoais, pois, entre outros critérios, o tratamento "*só é lícito se e na medida em* que" (...) "[o] *titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas*" (art. 6.º, n.º 1, alínea a) do RGPD)[8]. Refira-se que o consentimento, tal como definido pelo n.º 11 do art. 4.º do RGPD, tem de corresponder a uma manifestação de vontade livre, específica e informada[9].

Catarina. *Direito da informática, privacidade e dados pessoais*, Coimbra, Almedina, 2005, p. 68-70 e Guerra, Amadeu. *A privacidade no local de trabalho*, Coimbra, Almedina, 2004, p. 90-91). A título de exemplo, a CNPD continua a supervisionar a efetiva aplicação das normas legais, mas os mecanismos de notificação prévia deixaram de estar em vigor em 25 de maio de 2018. A partir desta data as próprias empresas passaram a assegurar, sob pena de sanção, a conformidade com as disposições legais aplicáveis.

[7] Terá interesse indicar algumas formas de tratamento de dados: a recolha e registo de dados; a organização e estruturação de dados (por exemplo, em bases de dados), a conservação de dados, a criação de perfis (i.é., de clientes), o *machine learning* (i.é., algoritmos preditivos de tendências que funcionam com base nos dados), divulgação ou a transmissão de dados, assim como a comparação ou interconexão de dados.

[8] Não abordaremos as especificidades da obtenção do consentimento para o tratamento de dados pessoais cujo titular seja menor (i. é, considerando 38 e art. 8.º do RGPD), sem prejuízo de reconhecermos a possibilidade da existência de vínculos laborais em que tomem parte trabalhadores que não gozem de forma plena dos seus direitos por motivo de idade poder suscitar questões interpretativas relevantes.

[9] Mais exatamente: "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os

Pressupostos de difícil concretização no contexto de uma relação de trabalho, onde a autonomia privada do trabalhador se encontra sujeita, de forma legítima, ao poder directivo do empregador[10] e, igualmente relevante, muitas vezes coartada pela dependência económica do trabalhador relativamente ao seu vínculo laboral (e à remuneração resultante deste). Situação que o pode colocar especialmente fragilizado e, até, incapaz de manifestar a sua vontade de forma livre[11]. Esta construção abstracta de putativa sujeição do trabalhador perante a sua entidade empregadora é especialmente relevante perante o entendimento jurisprudencial sustentado pela generalidade dos tribunais portugueses no sentido de que o vínculo laboral é caracterizado pela subordinação jurídica do trabalhador perante a entidade empregadora[12]. Não poucas vezes, numa relação

---

dados pessoais que lhe dizem respeito sejam objeto de tratamento". E, como acrescenta o considerando 32 do RGPD, o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro, por exemplo uma declaração escrita ou oral, mesmo que essa declaração seja providenciada por aquele que pretende encetar atividades de tratamento de dados, na medida em que o conteúdo da declaração seja inteligível e de fácil acesso (cfr., sobre o assunto, considerando 42 do RGPD). Por sua vez, o silêncio, opções pré-validadas ou a omissão de declaração não constituem um consentimento.

[10] Aliás, a posição de poder e autoridade da entidade empregadora mais não é do que o reverso da própria subordinação a que o trabalhador se acomete por efeito do contrato de trabalho. Sobre os poderes da entidade empregadora no âmbito da relação de trabalho, vd., por todos, Fernandes, António Monteiro. *Direito do Trabalho*, Coimbra: Almedina, 15.ª ed., 2010, p. 272-293 e Xavier, Bernardo da Gama Lobo *et al. Manual de Direito do Trabalho*, Lisboa: Verbo – Babel, 2.ª ed., 2014, p. 445-474.

[11] Esta tensão é assumida e declarada pela própria CRP, que parte de um conceito humanista da relação de trabalho, assente na necessidade de achar soluções que possam garantir tanto a liberdade de empresa como os direitos dos trabalhadores (cfr., para maiores desenvolvimentos, Abrantes, José João. "A Constituição e as Reformas Laborais em Curso", in *Congresso Europeu de Direito do Trabalho*, Coimbra: Almedina, 2014).

[12] Aliás, a distinção entre o contrato de trabalho e o contrato de prestação de serviço, tal como feita pelos Tribunais portugueses, assenta nas diferenças quanto ao objeto e à verificação de subordinação jurídica: enquanto que o objeto do contrato de trabalho consiste na prestação pelo trabalhador de atividade intelectual ou manual, colocando este à disposição da entidade empregadora a sua capacidade de trabalho; o objeto do contrato de prestação de serviço consiste precisamente no resultado da atividade da pessoa que presta o serviço (importando o resultado e não tanto a atividade em si). Apenas por efeito de um contrato de trabalho aceita o trabalhador ficar sob a direção do empregador, que pode, dentro do que lhe é admitido pelas normas legais, fiscalizar e disciplinar o trabalhador – esta é a noção de subordinação

laboral, a divergência de opinião constitui um luxo que simplesmente não se encontra ao dispor do trabalhador. Mesmo que este manifeste o seu consentimento de forma expressa e explícita, sempre serão de se suscitar dúvidas quando à liberdade dessa manifestação[13].

Ora, face ao debate em torno da problemática do consentimento no âmbito das relações laborais, o RGPD constituía uma oportunidade única para, por um lado, resolver as divergências até aqui existentes, e, por outro, prever um regime tendencialmente uniforme em todos os Estados-Membros da UE. Não foi esse o caso, pois, de acordo com o art. 88.º do RGPD, a definição de normas mais específicas para garantir a defesa dos direitos e liberdades dos trabalhadores, nomeadamente a sua dignidade e direitos fundamentais, no que respeita ao tratamento de dados pessoais no contexto laboral, é uma opção deixada a cargo de cada Estado-Membro, caso estes entendam estipular tais regras. Sobre o tema, o RGPD apenas

---

jurídica (ainda que a mesma seja de considerar necessariamente variável, por forma a abarcar a variabilidade de situações a que correspondem vínculos laborais na realidade social), que se contrapõe, por exemplo, à ausência de verdadeiros poderes de autoridade sobre o prestador de serviço daquele que o contrata. Claro está. Pelo que a dependência e subordinação jurídica são características essenciais ao contrato de trabalho: "pode haver subordinação jurídica sem haver dependência/subordinação económica e que pode, também, haver subordinação/ /dependência económica sem haver subordinação jurídica. (...) Deste modo, a subordinação jurídica consiste no poder que a entidade empregadora tem de algum modo orientar, dirigir e fiscalizar a atividade em si mesma, de outra pessoa, submetida à sua autoridade." (Acórdão do STJ, Proc. 1175/14.7TTLSB.L1.S1, 26 de outubro de 2017). Ver também Acórdão do STJ, Proc. n.º 1156/04.9TTCBR.C2.S1, 15 de dezembro de 2015, disponível em www.dgsi.pt. A própria imperatividade do regime da cessação do contrato de trabalho, por exemplo, é determinada por razões de coerência sistemática, "cuja última *ratio* será proteger os trabalhadores do desequilíbrio económico existente entre as partes, assegurando simultaneamente o direito dos trabalhadores à compensação, por um lado, e a salvaguarda da competitividade das empresas, por outro lado." (Acórdão do STJ, Proc. 3301/17.5T8LSB.S, 11 de janeiro de 2018, – todos disponíveis em www.dgsi.pt. Ainda que, como é sabido, na prática, nem sempre a dependência económica exista, pois uma faixa reduzida de trabalhadores, pelas especiais características da sua função ou profissão, retêm muito relevante poder negocial perante o seu empregador.

[13] Relembre-se que é precisamente por esta razão que o Código do Trabalho veio positivar a defesa da esfera privada do trabalhador. Nesta sede, cfr., por exemplo, o Acórdão do TC, n.º 306/03, 25 de junho de 2003, proferido em sede de fiscalização preventiva do art. 17.º, n.º 2, segundo segmento, do Código do Trabalho, no qual se afastou uma solução legislativa que implicaria excessiva intromissão na esfera privada do trabalhador ou do candidato ao emprego, com violação das disposições conjugadas dos arts. 26.º, n.º 1 e 18.º, n.º 2, da CRP.

veio prever que, tal como descrito no seu considerando 43[14], em situações de alegado ou pressuposto desequilíbrio, o consentimento não deverá constituir fundamento de licitude válido para o tratamento dos dados pessoais, implicitamente restringindo o leque de fundamentos de licitude para o tratamento de dados pessoais caso se verifique entre as partes qualquer desequilíbrio na sua relação. Dado o desequilíbrio próprio aos intervenientes do vínculo laboral, que se verifica em regra e é admitido e afirmado pelas normas que regulam o contrato de trabalho, a existência de consentimento por parte do trabalhador não poderá constituir fundamento de legitimidade para o tratamento dos dados pessoais deste. Todavia, as diversas normas do RGPD não procuram resolver, pelo menos de forma direta, qual o tratamento de dados pessoais dos trabalhadores por parte da entidade empregadora que seja de entender como lícito, antes meramente aflorando a existência deste problema, por via do já referido considerando[15].

---

[14] Com importância para a problemática, consta desse considerando que *"[a] fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento*, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução." (destaque nosso).

[15] Quanto a esta questão, o considerando 54 do RGPD adianta um interessante elemento para a teleologia subjacente a esta divisão. Ao mesmo tempo que o RGPD determina expressamente que "[o] tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, *sem o consentimento do titular dos dados*", vem igualmente restringir o acesso a esses mesmos dados de saúde pública, estipulando que essas atividades de tratamento motivadas por razões de interesse público "*não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores* ou as companhias de seguros e entidades bancárias" (destaque nosso). Relembre-se que os nossos tribunais já sustentaram, na vigência da Lei de Proteção de Dados Pessoais, que, na falta de consentimento do visado para a recolha de imagens, quando as mesmas estejam enquadradas em lugares públicos, o tratamento de dados pessoais é lícito na medida em que visem a realização de interesses públicos ou que hajam ocorrido publicamente (como decidiu o Tribunal da Relação de Lisboa: "Imagens captadas em local de acesso público, mesmo na falta de consentimento do visado, não correspondem a qualquer método proibido de prova, por não

2. A licitude no tratamento pela entidade empregadora de dados pessoais de trabalhadores

Na ausência de soluções alternativas constantes do texto do RGPD, soçobra uma dúvida interpretativa relevante, a qual poderá originar nas entidades empregadoras e nos demais responsáveis pelo tratamento de dados pessoais[16] um elevado grau de incerteza quanto aos procedimentos adequados a implementar. Nomeadamente, no que diz respeito à redação a adotar nas cláusulas relativas ao tratamento de dados pessoais constantes dos contratos individuais de trabalho celebrados com os seus trabalhadores, de modo a cumprir com as exigências previstas no art. 13.º do RGPD.

Sob a epígrafe "*Informações a facultar quando os dados pessoais são recolhidos junto do titular*", o RGPD estipula que aos titulares dos dados pessoais

---

violarem o núcleo duro da vida privada, avaliado numa ideia de proporcionalidade e por existir uma justa causa na sua obtenção e utilização, que é a prova de uma infracção criminal. Num mundo que se pretende cada vez mais transparente, em que se aceita como normal que o sigilo de operações financeiras seja cada vez menos protegido em nome de interesses patrimoniais, como sejam o do efectivo cumprimento por todos das obrigações fiscais, não seria compreensível a proteção do direito a não serem utilizadas, perante o tribunal, imagens de um particular a circular em locais públicos, quando essa utilização visa, apenas, contribuir para a eficiência do sistema de justiça" (Acórdão do Tribunal da Relação de Lisboa, Proc. 12/14.7SHLSB.L1.L1-5,10 de maio de 2016, disponível em www.dgsi.pt). Este é um percurso já trilhado pelo STJ, que decidiu no sentido de que "[a] instalação de sistemas de videovigilância nos locais de trabalho envolve a restrição do direito de reserva da vida privada e apenas poderá mostrar-se justificada quando for necessária à prossecução de interesses legítimos e dentro dos limites definidos pelo princípio da proporcionalidade" (Acórdão do Tribunal da Relação de Lisboa, Proc. 05S3139, 8 de fevereiro de 2006, disponível em www.dgsi.pt). Sendo isso certo no caso de verificação de interesse público no tratamento, contrapõe-se que a entidade empregadora poderá utilizar meios de vigilância à distância quando tenha por finalidade a proteção e segurança de pessoas e bens. Contudo, essa possibilidade circunscreve-se a locais abertos ao público ou a espaços de acesso a pessoas estranhas à empresa, em que exista um razoável risco de ocorrência de delitos contra as pessoas ou contra o património. Traduzindo-se, assim, numa forma de vigilância genérica, destinada a detetar factos, situações ou acontecimentos incidentais, e não numa vigilância diretamente dirigida aos postos de trabalho ou ao campo de ação dos trabalhadores (cfr., neste preciso sentido, Acórdão do STJ, Proc. 05S3139, 8 de fevereiro de 2006, disponível em www.dgsi.pt).

[16] É responsável pelo tratamento de dados pessoais "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras" que "*determina as finalidades e os meios de tratamento de dados pessoais*." (art. 4.º, número 7 do Regulamento, destaque nosso).

deve ser facultada informação relativa às finalidades de tratamento a que se destinam os dados pessoais, bem como o fundamento jurídico para o tratamento de tais dados. Note-se que os requisitos agora previstos nos arts. 13.º e 14.º do RGPD, referentes ao cumprimento do direito de informação dos titulares dos dados pessoais, são mais densos e exigentes face ao enquadramento legal anterior e plasmado no art. 10.º da Lei de Proteção de Dados Pessoais, impondo às empresas uma necessária revisão de procedimentos já existentes e/ou a criação de novos mecanismos, de modo a que as mesmas possam demonstrar e provar o cumprimento com as novas regras impostas pelo RGPD[17,18].

Tal como já referido, o RGPD não adianta uma solução concreta para esta questão, antes remetendo os possíveis caminhos para a sua resolução para a esfera decisória de cada Estado-Membro. Com efeito, de acordo com o disposto no art. 88.º do RGPD, estes poderão estabelecer, através de legislação laboral específica ou em instrumentos de regulamentação coletiva de trabalho, normas destinadas a garantir a tutela de direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, designadamente para efeitos de recrutamento ou de execução do contrato de trabalho (incluindo o cumprimento das obrigações previstas em lei ou em instrumentos de regulamentação coletiva de trabalho, de gestão, planeamento e organização do trabalho, entre outros). Este dispositivo legal remete então para o legislador nacional a opção de adotar normas especiais que reflitam medidas adequadas, necessárias e proporcionais para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais dos titulares dos dados pessoais, no contexto da competitividade das empresas portuguesas no quadro da União Europeia,

---

[17] A exigência acrescida quanto ao direito de informação dos titulares constitui uma manifestação clara do sistema de responsabilização ou de *accountability* das próprias empresas, em detrimento de um sistema de controlo externo por parte de uma autoridade de controlo, no caso português a CNPD.

[18] A título exemplificativo, a entidade empregadora terá de informar adequadamente os trabalhadores sobre como a informação será tratada, o porquê de o tratamento ser necessário e quais os direitos que o trabalhador tem para proteger a sua privacidade. Neste contexto, por exemplo, qualquer tratamento de dados pessoais realizados em segredo, ou seja, sem que o trabalhador seja informado previamente, atenta contra os direitos fundamentais do trabalhador, sendo de considerar, em geral, proibido (sem prejuízo de poderem existir excepções, nomeadamente no caso de suspeita da prática de crime ou prática ilícita relevante).

com especial relevo para a transparência do tratamento dos dados, a transferência de dados pessoais num determinado grupo empresarial e os sistemas de controlo no local de trabalho (como, por exemplo, a adopção de mecanismos de videovigilância e de geolocalização ou a implementação de sistemas de controlo da assiduidade e da pontualidade dos trabalhadores)[19].

Nesta sequência, é de antecipar que o governo Português apresentou à AR a Proposta de Lei n.º 120/XII[20] que visa assegurar a execução, na ordem jurídica interna, do RGPD, também contendo uma norma relevante no âmbito do art. 88.º do RGPD. Nesta sede, a referida Proposta de Lei estabelece que as entidades empregadoras, na qualidade de responsáveis pelo tratamento dos dados pessoais dos seus trabalhadores, podem tratar estes dados, não só nos termos definidos no Código do Trabalho e respetiva legislação complementar, mas, também, respeitando as especificidades a esse tratamento estabelecidas no art. 28.º da Proposta de Lei n.º 120/XIII.

Umas das especificidades previstas neste artigo é a de que, nas situações em que do tratamento dos seus dados pessoais resultar, para o trabalhador, uma vantagem jurídica ou económica, o consentimento deste não constitui requisito para o tratamento[21]. Além disso, o n.º 3 do art. 28.º da Proposta

---

[19] Importa mencionar que esses sistemas deverão observar como princípio a proteção de dados desde a concepção e por defeito (cfr. considerando 78 e art. 25.º do Regulamento), pelo que os próprios sistemas adoptados tenderão a assegurar que os dados pessoais são tratados apenas na medida do necessário, de acordo com um juízo de proporcionalidade.

[20] https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368. A Proposta de Lei n.º 120/XIII foi objeto de discussão na generalidade no dia 03 de Maio de 2018, tendo a sua aprovação sido recusada. Nesta sequência a Proposta de Lei voltou a baixar à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da AR.

[21] A este propósito, através do seu Parecer n.º 20/2018, a CNPD levantou reservas à redação da alínea a) do n.º 3 do art. 28.º da Proposta de Lei n.º 120/XIII. Com efeito, a referida Comissão admitiu que a redação poderá decorrer "de um qualquer lapso que torna, na realidade, o preceito incompreensível.", na medida em que, na opinião desta, apenas não deverá relevar o consentimento do trabalhador, como condição de licitude do tratamento de dados pessoais pelo empregador, quando existe uma situação de desequilíbrio entre as Partes "precisamente porque a natureza não paritária da relação laboral não permite assegurar a liberdade da manifestação de vontade do trabalhador, requisito imprescindível de relevância jurídica do consentimento". *A contrario*, quando do tratamento resulte "uma vantagem jurídica ou material para o trabalhador é que o seu consentimento pode relevar, sendo essa circunstância a única exceção.". Neste sentido, a CNPD emitiu parecer negativo quanto à redação deste dispositivo legal, pois, no seu entendimento, o mesmo "restringe excessivamente a relevância do consentimento do trabalhador, com isso eliminando qualquer margem de livre arbítrio

de Lei n.º 120/XIII estabelece que o consentimento do trabalhador não constituirá fundamento bastante de legitimidade para o tratamento dos dados pessoais, se esse mesmo tratamento estiver também abrangido pelo disposto na alínea b) do n.º 1 do art. 6.º do RGPD, ou seja, se o tratamento dos dados pessoais for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do respetivo titular, o consentimento não deverá constituir o fundamento que legitima o tratamento dos dados pessoais dos trabalhadores[22-23].

---

dos trabalhadores mesmo quando há condições para a sua manifestação.". Também o GT29 para a Proteção dos Dados da Comissão Europeia se debruçou sobre a problemática do livre arbítrio dos trabalhadores para a manifestação de consentimento, afirmando que: "Contudo, isto não significa que os empregadores nunca possam utilizar o consentimento como fundamento legal para o tratamento. Pode haver situações em que seja possível ao empregador demonstrar que o consentimento foi dado livremente. Atendendo ao desequilíbrio de poder entre empregadores e empregados, estes só podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas". A denominação deste grupo de trabalho resulta do facto de ter sido instituído pelo art. 29.º da Diretiva 95/46/CE. O GT29 é um órgão consultivo europeu independente em matéria de proteção de dados e privacidade.

[22] Neste sentido, veja-se o Parecer 2/2017 adotado em 08 de Junho de 2017 pelo GT29: "O GT29 sublinhou anteriormente no Parecer 8/2001 que, quando um empregador tenha de proceder ao tratamento de dados pessoais dos seus empregados, *é enganoso partir da suposição de que o tratamento pode ser legitimado através do consentimento dos empregados*. Nos casos em que um empregador afirme que é necessário o consentimento e exista um efetivo e potencial prejuízo que decorre do não consentimento do empregado (que pode ser altamente provável no contexto laboral, especialmente no que se refere ao acompanhamento por parte do empregador do comportamento do empregado ao longo do tempo), *o consentimento não é válido,* uma vez que não é, nem pode ser dado livremente. Assim, relativamente à maioria dos casos de tratamento de dados dos empregados, *o fundamento jurídico de tal tratamento não pode, e não deve ser o consentimento dos empregados, sendo necessária uma base jurídica diferente*. Além disso, mesmo nos casos em que o consentimento pudesse ser considerado como constituindo uma base jurídica válida de tal tratamento (ou seja, se puder ser, sem qualquer dúvida, concluído que o consentimento é dado livremente), a manifestação de vontade do empregado tem de ser específica e informada. Os valores predefinidos nos dispositivos e/ou a instalação de software que facilitem o tratamento eletrónico de dados pessoais não podem ser qualificados como consentimento dado pelos empregados, uma vez que o consentimento exige uma manifestação ativa de vontade. A falta de ação (ou seja, não alterar os valores predefinidos) não pode, em geral, ser considerada como um consentimento específico para permitir tal tratamento." (destaque nosso).

[23] O GT29 também adoptou em 28 de novembro de 2017 um conjunto de entendimentos, cuja última revisão ocorreu a 10 de abril de 2018, denominados *Guidelines on consent under*

Não partindo para a análise desenvolvida e pormenorizada das possíveis consequências da redação adotada na referida Proposta de Lei[24], parece-nos que esta, em caso de aprovação em votação final global do diploma na AR, resolve, em grande medida, as dúvidas que circundam o tema do consentimento dos trabalhadores[25]. Aqui chegados, sempre importará ponderar quais as implicações práticas do afastamento do consentimento enquanto fundamento de legitimidade para o tratamento de dados pessoais de trabalhadores.

3. Problemas práticos suscitados pelo tratamento de dados pessoais de trabalhadores por parte do empregador

Neste contexto, com que fundamentos poderão as entidades empregadoras proceder ao tratamento de dados pessoais em contexto laboral? Na medida em que o consentimento não deverá constituir fundamento legítimo para o tratamento dos dados pessoais dos trabalhadores se esse tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais, cumpre abordar as implicações práticas dessa limitação, analisando com que outros fundamentos poderão as entidades empregadoras proceder ao tratamento de dados pessoais em contexto laboral.

À partida importa salientar que, de acordo com aquela que foi a prática mais usual, pelo menos até à data de aplicação do RGPD, entendemos que a larga maioria das operações de tratamento de dados pessoais dos

---

Regulation 2016/679, onde aborda esta precisa problemática, concluído que o consentimento livre do trabalhador dificilmente pode ser conseguido, pelo que o fundamento de licitude para o tratamento de dados pessoas dos trabalhadores não deve ser a obtenção dos consentimento destes (“*[t]herefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee*”).

[24] Os moldes concretos dessa norma aquando da futura aprovação da mesma são, à data da feitura do presente texto, ainda uma incógnita.

[25] Nesta linha, é de apontar não ser imediatamente aparente qual a consequência danosa para a proteção dos dados pessoais dos trabalhadores desta opção da legislação nacional, excepto a implícita redução da discricionariedade do trabalhador na gestão destes.

trabalhadores foi baseada na obtenção do consentimento destes para o tratamento, normalmente através da previsão de uma cláusula de tratamento de dados pessoais nos respetivos contratos de trabalho, nos quais o trabalhador expressamente autorizava e consentia que a sua entidade empregadora tratasse os dados por aquele fornecidos, no âmbito da relação laboral, com a assinatura do contrato de trabalho que o vinculava a esta. Relativamente ao tratamento de dados pessoais recolhidos anteriormente com base no consentimento dado, nos termos do disposto da Diretiva 95/46/CE, transposta para o nosso ordenamento jurídico pela Lei da Proteção de Dados Pessoais, não será necessário obter, novamente, o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no RGPD, para que o responsável pelo tratamento prossiga essa atividade após a data de aplicação do presente regulamento[26]. Não obstante, sempre impenderá sobre as entidades empregadoras o dever de cumprir com o disposto nos arts. 13.º e 14.º do RGPD, consoante os dados pessoais sejam ou não recolhidos junto do respetivo titular, o que implica a necessidade de informar – agora sim novamente – os seus trabalhadores dos seus direitos, designadamente através da revisão de políticas internas de tratamento de dados pessoais, de aditamentos aos contratos de trabalho já celebrados e da adoção de novas cláusulas de tratamento de dados pessoais nos contratos de trabalho a celebrar[27].

---

[26] Esta limitação da aplicabilidade do RGPD a situações que se encontravam regularizadas nos termos da legislação aplicável pretérita pode operar uma desproteção dos trabalhadores relativamente às expectativas quanto ao consentimento estabelecidas pelo RGPD. No entanto, essa concessão é de entender justificada quer pela manutenção das relações jurídicas já estabilizadas, quer pelos consideráveis custos económicos associados à renovação da obtenção do consentimento de todos os trabalhadores (cfr., sobre o assunto, considerando 171 do RGPD).

[27] Sobre o tema, no plano da dilucidação desta problemática, a CNPD publicou no seu site a seguinte resposta-tipo à questão de saber se é necessário o consentimento dos trabalhadores no âmbito da gestão administrativa ou de processamento de remunerações: "Não. Os tratamentos de dados pessoais, no âmbito da gestão dos recursos humanos, têm como fundamentos de legitimidade a execução do contrato de trabalho e a lei. O consentimento dos trabalhadores não é de uma maneira geral considerado válido, pois raramente poderá ser dado em condições de liberdade, atendendo ao desequilíbrio entre as partes." (https://www.cnpd.pt/bin/faqs/faqs.htm, página consultada pela última vez a 15/09/2018). Sem contribuir ativamente para a determinação da forma mais adequada para a resolução do problema, este elemento interpretativo traça uma linha clara entre os tratamentos de dados pessoais que são do foro estrito (e necessário) da execução do contrato de trabalho (*in casu*, a gestão de recursos

Este conjunto de obrigações legais a que se encontram adstritas as entidades empregadoras exigirá das mesmas a adoção de mecanismos internos e eficazes de controlo e cumprimento com os normativos legais (*compliance*[28]), evitando, por conseguinte, o quadro sancionatório previsto no RGPD[29]. Neste sentido, e tendo em conta o enquadramento acima descrito relativo à exclusão do consentimento enquanto fundamento de legitimidade para o tratamento de dados pessoais de trabalhadores, é de fulcral importância debruçarmo-nos sobre alguns fundamentos que, dependendo da operação de tratamento em causa, poderão legitimar o tratamento dos dados pessoais em contexto laboral por parte das entidades empregadoras.

Numa primeira análise dir-se-á que o fundamento mais imediato para o desenvolvimento de operações de tratamento de dados pessoais dos trabalhadores é a necessidade deste para a execução do contrato de trabalho no qual o trabalhador é parte, ao abrigo da alínea b) do número 1 do art. 6.º do RGPD. O tratamento de dados relativos ao trabalhador, tais como o nome completo, idade, data de nascimento, morada, endereço de correio eletrónico, número de identificação fiscal e de beneficiário da segurança social, número do Cartão de Cidadão e respetiva validade, remuneração e local de trabalho, é indissociável da gestão corrente de recursos humanos no seio empresarial, nela incluindo-se, designadamente, o processamento e pagamento das retribuições e complementos remuneratórios aos trabalhadores, o registo de tempos de trabalho e de assiduidade e pontualidade,

---

humanos), os quais encontram fundamento no próprio contrato de trabalho entre as partes; e outros tratamentos de dados pessoais, que, à partida, não se encontrem legitimados pela mera existência do contrato de trabalho e relativamente aos quais, no entendimento da CNPD, o consentimento dos trabalhadores não deve ser entendido, de uma maneira geral, como válido.

[28] Sobre a matéria, com especial enfoque na relevância de assumir, no domínio das atividades financeiras, a necessidade de minimizar o risco de incumprimento por via de sistemas de controlo, vd. Labareda, João. "Contributo para o Estudo do Sistema de Controlo e da Função de Cumprimento ('Compliance')", in *Estudos do Instituto de Valores Mobiliários*, 2014, p. 28-35, disponível em http://www.institutovaloresmobiliarios.pt/.

[29] Que, em caso de violação das disposições referentes, designadamente, aos princípios básicos do tratamento ou aos direitos dos titulares dos dados, prevê a aplicação de coima até € 20.000.000,00 ou, no caso de uma empresa, até 4% do seu volume de negócios anual, caso este valor seja superior ao limite anteriormente indicado. Cfr. art. 83.º do RGPD.

a gestão e marcação de períodos de férias, bem como o cumprimento de outras obrigações decorrentes dos contratos com aqueles celebrados[30].

A legislação laboral portuguesa impõe às entidades empregadoras uma multiplicidade de obrigações que implicam, necessariamente, a realização de operações de tratamento de dados pessoais dos seus trabalhadores. A título de exemplo, elenquemos algumas das principais obrigações legais aqui relevantes: (i) nos termos conjugados do art. 8.º da Lei n.º 70/2013, de 30 de agosto e do art. 3.º da Portaria n.º 294-A/2013, de 30 de setembro, a adesão da entidade empregadora ao Fundo de Compensação de Trabalho é obrigatória (com exceção da possibilidade de opção por adesão a Mecanismo Equivalente), devendo ser comunicada a esse Fundo a admissão de cada trabalhador que venha a ser admitido até à data do início da execução do respetivo contrato, para efeitos da sua inclusão. Para esse efeito são obrigatoriamente comunicados ao Fundo diversos dados de identificação do trabalhador (art. 5.º da referida Portaria n.º 294-A/ /2013, de 30 de setembro); (ii) de acordo com o disposto no art. 29.º do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social, aprovado pela Lei n.º 110/2009, de 16 de Setembro, "*a admissão de trabalhadores é obrigatoriamente comunicada pelas entidades empregadoras à instituição de segurança social competente*, no sítio na internet da segurança social" (destaque nosso); (iii) o número 3 do art. 457.º Código do Trabalho estabelece que o "empregador *pode proceder ao tratamento informático de dados pessoais dos trabalhadores referentes a filiação sindical,* desde que, nos termos da lei, sejam exclusivamente utilizados para cobrança e entrega de quotas sindicais" (destaque nosso).

Acresce que os arts. 281.º a 284.º do Código do Trabalho impõem um conjunto de obrigações às entidades empregadoras em matéria de segurança e saúde no trabalho, designadamente a obrigação do empregador transferir a responsabilidade pela reparação de acidentes de trabalho e doenças profissionais para entidades legalmente autorizadas a realizar este tipo de seguros, operação que implica, pela sua própria natureza, o

---

[30] Neste sentido, veja-se o Parecer 2/2017 adotado em 08 de junho de 2017 pelo GT29: "As relações de trabalho baseiam-se frequentemente num contrato de trabalho entre o empregador e o empregado. Quando se cumprem as obrigações nos termos deste contrato, tais *como o pagamento do empregado, o empregador é obrigado a proceder ao tratamento de determinados dados pessoais*." (destaque nosso).

tratamento de dados pessoais dos seus trabalhadores. Também em matéria referente ao poder disciplinar, o empregador deve ter um registo atualizado das sanções disciplinares "feito por forma que permita facilmente a verificação do cumprimento das disposições aplicáveis, nomeadamente por parte das autoridades competentes que solicitem a sua consulta." (art. 332.º do Código do Trabalho). O conteúdo desse registo disciplinar individualizado são dados pessoais de cada trabalhador, tratados de acordo com as disposições do RGPD e com fundamento no artigo citado. Por último, recai também sobre as entidades empregadoras o dever de manter o registo dos tempos de trabalho, incluindo dos trabalhadores que estão isentos de horário de trabalho, em local acessível e por forma que permita a sua consulta imediata, conforme o disposto no art. 202.º do Código do Trabalho, dados individualizados respeitantes a cada trabalhador, relativamente aos quais o RGPD exige os mesmos cuidados no seu tratamento[31].

Em todas estas situações a base jurídica para o tratamento dos dados pessoais dos trabalhadores residirá, nos termos da alínea c) do número 1 do art. 6.º do RGPD, no cumprimento das obrigações legais a que estão sujeitas as entidades empregadoras.

Assim, a necessidade do tratamento para a execução do contrato de trabalho constituirá o mais importante fundamento de legitimidade a que as entidades empregadoras podem recorrer para habilitar a generalidade das operações de tratamento dos dados pessoais dos seus trabalhadores. Embora este seja, em nosso entender, o principal fundamento de licitude

---

[31] A este propósito, cumpre convocar a decisão do TJUE no Acórdão datado de 30 de maio de 2013 (Acórdão do TJ, C-342/12, *Worten*, ECLI:EU:C:2013:355), no qual, na vigência da Diretiva 95/46/CE, foi declarado que o conceito de dados pessoais abrange o registo dos tempos de trabalho no qual se inclua a indicação, para cada trabalhador, das horas de início e de termo do tempo de trabalho, assim como quaisquer interrupções ou intervalos. Também nos termos desse Acórdão, tal natureza do registo dos tempos de trabalho não impede o acesso a estes pela autoridade nacional com competência para a fiscalização das condições de trabalho, na medida em que essa obrigação seja necessária para o exercício, por essa autoridade, da sua missão de fiscalização da aplicação da legislação em matéria de condições de trabalho, nomeadamente, no que respeita ao tempo de trabalho (em Portugal, a ACT). Pelo que o empregador não só deve manter o registo dos tempos de trabalho plenamente disponível para consulta imediata por parte das autoridades competentes, como simultaneamente tem de garantir a proteção desse registo em moldes adequados com a natureza do seu conteúdo (por se tratarem de dados pessoais).

para o tratamento de dados pessoais em contexto laboral, a necessidade do tratamento para a execução do contrato de trabalho não será fundamento único de legitimidade para o tratamento dos dados pessoais de trabalhadores[32].

A invocação de um interesse legítimo para o tratamento pela entidade empregadora, nos termos da alínea f) do número 1 do art. 6.º do RGPD, implica que a própria finalidade do tratamento de dados pessoais[33] deve ser também legítima[34], o tratamento deve ser realizado mediante métodos ou tecnologias específicas que, por referência à finalidade de tratamento, sejam de considerar estritamente necessários, adequados, proporcionais e aplicados da forma menos intrusiva possível para a privacidade e respeito de outros direitos fundamentais da pessoa singular. Este crivo[35], demarcadamente apertado, coloca sobre as entidades empregadoras o ónus de assegurar que se encontram aptas a demonstrar que tomaram as medidas adequadas a garantir o necessário equilíbrio entre a prossecução de uma finalidade (legítima) de tratamento de dados e o respeito pelas liberdades e direitos fundamentais dos trabalhadores e as expectativas razoáveis destes na relação com as suas entidades empregadoras[36]. Ora, o alcançar de tal

---

[32] Neste mesmo sentido, veja-se o Parecer 2/2017 do GT29 sobre o "tratamento de dados no local de trabalho". Este Parecer completa o Parecer 8/2001 sobre este tema, também publicado por este grupo de trabalho, em 13 de setembro de 2001.

[33] São exemplos gerais de finalidades de tratamento dos dados pessoais a comercialização direta, a vídeo vigilância, a análise de perfis de consumo de clientes, o desenvolvimento de novos produtos e serviços ou a adaptação de produtos e serviços, a gestão de contactos, informações, pedidos, reclamações, pagamentos ou faturação, a gravação de chamadas para prova de transação comercial ou para controlo de qualidade ou mesmo o marketing de produtos e serviços.

[34] A finalidade de tratamento corresponderá, na prática, a uma qualquer necessidade concreta da entidade empregadora. Mas esta finalidade não será de considerar, apenas por essa razão, legítima.

[35] No qual o trabalhador se pode apoiar para invocar o direito de oposição ao tratamento por fundamentos legítimos, nos termos do art. 21.º do RGPD.

[36] Os interesses legítimos das entidades empregadoras podem constituir um fundamento de licitude para o tratamento, desde que não prevaleçam indevidamente sobre os direitos e liberdades fundamentais dos trabalhadores, tomando em conta as expectativas razoáveis destes baseadas na relação com o responsável pelo tratamento de dados. A existência de um interesse legítimo requer uma avaliação minuciosa, nomeadamente quanto à hipótese de o trabalhador poder prever, numa escala razoável e adequada, no momento e no contexto em que os dados são

equilíbrio adivinha-se de difícil aferição. A composição deste vai revelar-se especialmente dependente da concreta situação verificada.

Verificando-se uma situação em que a entidade empregadora monitoriza os perfis de redes sociais de antigos colaboradores com o intuito de aferir, através do histórico profissional disponibilizado nestas redes, se estes cumprem, designadamente, com as cláusulas de não concorrência ou de confidencialidade constantes dos seus contratos de trabalho, cujas referidas cláusulas continuam em vigor mesmo após a cessação dos respectivos vínculos laborais, a finalidade desse tratamento pode ser entendida como, em abstrato, legítima. O tratamento de dados pessoais decorrentes dessa monitorização pode ser fundamentado na necessidade do mesmo para a tutela dos interesses legítimos da entidade empregadora – i. é, a não transferência de *know-how*, técnicas e métodos de antigos trabalhadores para empresas directamente concorrentes com a atividade por esta exercida – desde que tal monitorização seja realizada da forma menos intrusiva possível para os direitos e liberdades desses antigos trabalhadores[37], respeitando, tanto quanto possível, a sua privacidade.

Já no caso de aplicação ou emprego de medidas de controlo da utilização feita dos meios e equipamentos informáticos ou de comunicação da titularidade de entidade empregadora, que, por força da prestação da atividade laboral pelos trabalhadores, são colocados à disposição destes, o tratamento de dados pessoais decorrente da adoção de tais medidas também poderá encontrar justificação nos interesses legítimos prosseguidos pela entidade empregadora. Por exemplo, quer o aumento da produtividade e/ou da rentabilidade da força de trabalho, quer a pretensão de salvaguarda da integridade e conservação dos equipamentos,

---

recolhidos, se esses mesmos dados poderão vir a ser tratados pela sua entidade empregadora com uma determinada finalidade (cfr., sobre o assunto, considerando 47 do RGPD).

[37] O GT29 adianta um exemplo concreto sobre a matéria: "Um empregador monitoriza os perfis de antigos empregados no LinkedIn que estão envolvidos durante a vigência das cláusulas de não concorrência. A finalidade desta monitorização consiste em controlar a conformidade com essas cláusulas. A monitorização é limitada a estes antigos empregados. Enquanto o empregador puder provar que tal monitorização é necessária para proteger os seus interesses legítimos, que não existem outros meios menos invasivos disponíveis e que os antigos empregados tenham sido devidamente informados da extensão da observação regular das suas comunicações públicas, o empregador pode invocar o fundamento jurídico do art. 7.º, alínea f), da Diretiva (cfr. ponto 5.2 do Parecer 2/2017 do GT29).

podem constituir fundamento legítimo para o tratamento de dados. No entanto, as entidades empregadoras não devem simplesmente assumir que a demanda da melhoria do desempenho dos trabalhadores justifica, sem mais, a intromissão desregrada na privacidade e outros direitos fundamentais destas pessoas. O tratamento de dados pessoais com essa finalidade é legítimo apenas na medida em que os métodos adoptados sejam adequados, necessários e proporcionais face aos direitos dos trabalhadores, garantindo um equilíbrio entre os interesses e direitos em presença. De igual forma, também no caso de adopção pela entidade empregadora de sistemas que possibilitem o controlo da pontualidade e da assiduidade dos trabalhadores[38] com o intuito de monitorização das entradas e saídas nas suas instalações, é óbvio que o tratamento de dados pessoais resultantes da implementação de tais sistemas é suscetível de contender com a privacidade dos trabalhadores[39]. Daí a necessidade da adopção de medidas adequadas de controlo. Posto isto, as entidades empregadoras poderão legitimar o recurso a tais sistemas, bem como a necessidade do tratamento, nos seus interesses legítimos que, sendo diretamente relacionados com o controlo da pontualidade e assiduidade, se manifestem. A legitimidade do tratamento

---

[38] Como já referido, exigida por lei: art. 202.º do Código do Trabalho. O entendimento jurisprudencial dominante nos tribunais portugueses vai no sentido de que o controlo da assiduidade dos trabalhadores pela entidade empregadora constitui um direito desta, decorrente do poder de direção que lhe é conferido pela lei laboral. Não obstante, o controlo da assiduidade deve ser feito no respeito dos direitos dos trabalhadores. Vd., com relevância para esta temática, o Acórdão do TRP, Proc. 28801/15.8T8PRT.P1, 26 de junho de 2017, disponível em www.dgsi.pt, em que o Tribunal decidiu que "O 'toque do telefone' para controlo da pontualidade e da assiduidade do trabalhador é uma prática grotesca, face ao legalmente estatuído no art. 202.º do Código do Trabalho, e constitui uma ofensa à sua dignidade – art. 15.º do Código do Trabalho", a propósito de trabalhador que havia sido ordenado a registar a sua assiduidade da seguinte forma (que incumpriu): "não ligou nem deu toque à entrada e à saída, no período da manhã e da tarde, para o telemóvel do Dr. D..., como tinha sido ordenado".

[39] Ademais, mesmo que o tratamento de dados pessoais com essa finalidade possa ser legítimo, o empregador continua a ter de cumprir com a sua obrigação de informação. Esta abrange, por exemplo, se e quando existe vigilância dos trabalhadores, as finalidades desse tratamento de dados, os sistemas e meios utilizados para esse tratamento, que informação é guardada após o tratamento e durante quanto tempo, quem pode aceder aos dados pessoais e em que circunstâncias, como é que os dados são protegidos e, também, os direitos dos trabalhadores perante a circunstância do tratamento dos seus dados pessoais.

destes dados não confere à entidade empregadora, por exemplo, a faculdade de recorrer à informação daí resultante como elemento de avaliação dos seus trabalhadores[40].

Em todos os casos acima descritos, entendemos que os interesses legítimos das entidades empregadoras podem constituir fundamento jurídico bastante para o tratamento dos dados pessoais dos trabalhadores[41]. Não obstante, tal tratamento encontra limitações claras, devendo ser estritamente necessário para cumprir uma finalidade legítima e determinada e estar conforme com o princípio da proporcionalidade, nas suas vertentes de adequação, necessidade e proporcionalidade *stricto sensu*.

Em suma, a verificação da proporcionalidade das operações de tratamento face aos direitos e liberdades fundamentais dos trabalhadores deverá ser realizada em momento prévio à adopção de qualquer medida de controlo, de modo a, por um lado, permitir que seja averiguada a sua adequação face aos direitos fundamentais dos trabalhadores e às exigências próprias da concreta relação de trabalho (eventualmente reflectidas no conteúdo do interesse legítimo), e, por outro, determinar quais as medidas

---

[40] Exemplifica o GT29: "Um empregador mantém uma sala com servidores onde os dados empresariais sensíveis, os dados pessoais relativos aos empregados e os dados pessoais relativos aos clientes são armazenados em formato digital. A fim de cumprir as obrigações jurídicas para proteger os dados contra o acesso não autorizado, o empregador tinha instalado um sistema de controlo de acesso que regista a entrada e a saída dos empregados que têm a devida autorização para entrar na sala. Caso qualquer peça de equipamento venha a desaparecer ou os dados sejam suscetíveis de acesso não autorizado, perda ou furto, os registos mantidos pelo empregador não lhe permite determinar quem teve acesso à sala nessa altura. Dado que o tratamento é necessário e não prevalece o direito ao respeito da vida privada dos empregados, pode ser no interesse legítimo (...), se os empregados foram adequadamente informados sobre a operação do tratamento. *No entanto, a monitorização contínua da frequência e da entrada e da saída exatas dos empregados não pode ser justificada, se esses dados forem também utilizados para outros fins, como, por exemplo, a avaliação do desempenho dos empregados*." (cfr. ponto 5.5 do Parecer 2/2017 do GT29, destaque nosso).

[41] Assim se admitindo o tratamento de dados pessoais dos trabalhadores, o que não preclude os vários requisitos próprios ao tratamento, como seja o de transparência (os trabalhadores devem ser informados expressamente dos contornos do mesmo), respeito pelos direitos dos titulares dos dados pessoais (no caso, os trabalhadores), o armazenamento dos dados pessoais pelo período estritamente necessário ou a proteção adequada dos dados pessoais (mediante as medidas de segurança adequadas – sejam estas de cariz organizacional ou técnico).

que devem ser implementadas para garantir que eventuais violações desses direitos são limitadas ao mínimo estritamente necessário[42].

Conclusão

A pretensão de assegurar a constante compatibilização dos interesses da entidade empregadora com os direitos, liberdades e garantias fundamentais dos trabalhadores, incluindo os seus direitos à privacidade e à proteção dos dados pessoais, exige, sobretudo do responsável pelo tratamento de dados pessoais, que estes sejam tratados para finalidades determinadas, explícitas e legítimas, tendo por base um fundamento legal ou jurídico que garanta a licitude do tratamento. Neste sentido, dado o desequilíbrio próprio dos intervenientes típicos de uma relação laboral, e tendo em conta a referida necessidade de compatibilização dos interesses em conflito, o consentimento por parte do trabalhador não deverá, nem poderá, constituir fundamento de legitimidade para o tratamento dos dados pessoais deste.

No entanto, esse afastamento do consentimento enquanto fundamento de legitimidade para o tratamento de dados pessoais de trabalhadores, não impede as entidades empregadoras de procederem ao tratamento de dados pessoais em contexto laboral quando outros fundamentos de legitimidade se manifestem. A necessidade do tratamento dos dados para a execução do contrato de trabalho no qual o trabalhador é parte constitui um dos fundamentos de licitude mais expeditos, do qual as entidades empregadoras se poderão socorrer para proceder ao tratamento de dados pessoais intrinsecamente ligados com a execução e gestão da relação contratual, que poderá e deverá ser complementada pela realização de operações de tratamento de dados pessoais necessárias ao cumprimento das suas obrigações legais.

Perante interesses legítimos do responsável pelo tratamento, fundamento de licitude para o tratamento de dados pessoais em contexto laboral, encontra-se ainda assim inerente a obrigação de demonstração por parte daquele de que foram tomadas as medidas adequadas a garantir o exigível equilíbrio entre a prossecução de uma sua finalidade de tratamento de

---

[42] Nomeadamente, a eventual necessidade de avaliação de impacto sobre a proteção de dados ou de consulta prévia junto da autoridade de controlo (arts. 35.º e seguintes do RGPD).

dados e o respeito pelas liberdades e direitos fundamentais dos trabalhadores. A concretizar mediante a realização de um verdadeiro teste de verificação prévia e concreta da proporcionalidade das operações de tratamento de dados com os direitos, liberdades e garantias fundamentais dos trabalhadores, tais como estas se mostram absolutamente necessárias e justificadas pelo concreto fundamento de licitude em causa. Só assim se garante a justa composição dos interesses em presença no vínculo laboral.

O direito à explicação no Regulamento Geral sobre a Proteção de Dados

Gabriela Caldas*

Resumo: Os desafios da evolução tecnológica, incluindo novas formas de tratamento automatizado de dados pessoais, impõem a adoção de regulamentação apropriada, tanto do ponto de vista da proteção dos direitos fundamentais como da preservação da inovação. O Regulamento Geral sobre a Proteção de Dados situa-se nessa zona de compromisso marcada pela importância em dispor de regras flexíveis que, protegendo o essencial, mantêm validade numa perspetiva de futuro. O reforço do papel da interpretação associado a este modelo exigirá esforço acrescido por parte dos reguladores na consideração das diferentes questões técnicas e jurídicas evidenciadas no debate sobre o direito à explicação e na identificação das melhores formas de garantir a instrumentalização da inovação digital ao serviço dos indivíduos e da sociedade em geral.

Palavras-chave: *Regulamento Geral sobre a Proteção de Dados; decisões individuais automatizadas; direito à explicação; interpretação da lei.*

Abstract: The challenges of technological developments, including new forms of automated processing of personal data, require the adoption of appropriate regulations, from the point of view of protecting fundamental rights and preserving innovation. The General Regulation on Data Protection is located in this commitment area marked by the importance in having flexible rules that, while protecting the essential, maintain the validity in a perspective of future. The reinforcement of the role of interpretation associated with this model will require greater efforts by regulators to deal with the different issues addressed in the debate on the right to explanation identifying the best ways to ensure the exploitation of digital innovation is at the service of individuals and society in general.

Keywords*: General Regulation on Data Protection; automated individual decision-making; right to explanation; interpretation of the law.*

---

* Doutoranda em Direito e Segurança na Faculdade de Direito da Universidade Nova de Lisboa (FDUNL). *Licence Spéciale* em Direito Europeu no Instituto de Estudos Europeus da Universidade Livre de Bruxelas. Membro do Centro de Investigação & Desenvolvimento sobre Direito e Sociedade (CEDIS).

Introdução

A revolução digital a que assistimos desde meados do século passado acelerou de forma significativa nos últimos anos em resultado dos progressos tecnológicos verificados sobretudo na área das redes neurais e da *machine learning*[1]. Muito embora o impacto das tecnologias digitais não tenha ido, até agora, além da criação de novos produtos e serviços que introduzem melhorias qualitativas na nossa vida diária, certo é que o seu desenvolvimento faz antever alterações de fundo na organização da sociedade e do nosso modo de vida em geral. O potencial das tecnologias de inteligência artificial[2] é imenso, sendo-lhe reconhecida capacidade suficiente para gerar dentro de pouco tempo sistemas dotados de larga autonomia, aptos a substituírem a intervenção humana em praticamente todos os estádios da formação da vontade e da tomada de decisões. Daí a absoluta necessidade de salvaguardar o conjunto complexo de direitos fundamentais e princípios democráticos que serve de imprescindível pano de fundo à manutenção dos equilíbrios da nossa sociedade.

Para além das perturbações relacionadas com o emprego e a organização da economia de que se começa a falar insistentemente, importa referir que as novas tecnologias facilitam substancialmente uma vasta tipologia de meios de controle político e social, tanto por parte de autoridades públicas como de entidades privadas, sobre largas franjas da população, a custos reduzidos e com elevada eficácia. Os instrumentos utilizados, embora impercetíveis nalguns casos, podem mesmo assim ter um impacto significativo no comportamento das pessoas, levando-as não só a agir de determinada maneira, mas também a percecionar a realidade e a estruturar o próprio pensamento em função da informação que lhes é canalizada.

Acresce que as novas tecnologias da informação estimulam os indivíduos a disponibilizar publicamente cada vez mais dados pessoais e permitem que empresas privadas e autoridades públicas façam uso de tais dados

---

[1] A *machine learning* é o ramo da inteligência artificial que explora processos de fazer com que os sistemas autónomos melhorem o seu desempenho com base na experiência.

[2] O conceito de inteligência artificial é aplicado a sistemas que interagem com o seu ambiente e são capazes de atuar para atingir determinados objetivos.

no exercício das suas atividades numa escala sem precedentes através de procedimentos automatizados difíceis de controlar[3].

Estes fatores, aliados às divergências entre as regulamentações nacionais e à inconsistência das regras dos nossos principais parceiros externos, estão na base da atualização e reforço das normas europeias em matéria de proteção de dados que culminaram em abril de 2016, após mais de cinco anos de intensas negociações, com a adoção do RGPD[4].

Na exposição de motivos do RGPD é desde logo reconhecida a premência em dotar a União Europeia dum quadro jurídico de proteção dos dados pessoais mais consistente e rigoroso na sua aplicação, que permita à economia digital desenvolver-se no espaço interno e aos cidadãos controlar os seus próprios dados, num ambiente generalizado de segurança para os indivíduos, operadores privados e entidades públicas.

É com este propósito de aprofundamento e facilitação das regras de proteção de dados que, nomeadamente o art. 5.º do RGPD, acrescenta aos princípios anteriormente consagrados na Diretiva 95/46/CE, o princípio da transparência em relação ao titular dos dados, o da minimização de dados e o da responsabilidade por defeito do responsável pelo tratamento dos dados.

Das salvaguardas introduzidas pelo RGPD para reforçar o controle individual sobre os dados pessoais salientam-se as que se prendem com a tomada de decisões automatizadas. Entre elas inclui-se a obrigação de fornecer "informações significativas sobre a lógica envolvida", expressamente referida nos art. 13.º a 15.º, bem como o direito de "obter intervenção humana" mencionado no art. 22.º, a que se convencionou chamar "direito à explicação" com base na expressão "...obter uma explicação sobre a decisão tomada ..." utilizada no considerando 71.

---

[3] Bentley, Peter, Brundage, Miles, Haggström, Olle, Metzinger, Thomas. *Should we fear artificial intelligence?,* 2018, p. 15. Disponível em http://www.ep.europa.eu/stoa/ (acedido a 13/5/2018).

[4] Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, p. 1–88.

Uma parte dos autores[5] vê o "direito à explicação" como um instrumento imprescindível de promoção da responsabilidade e transparência dos sistemas de *machine learning* que o RGPD não pode deixar de contemplar dada a generalização e impacto do uso de tais sistemas, enquanto outros[6] se interrogam em que medida o "direito à explicação", a existir, poderá efetivamente ser posto em prática tal a falta de clareza dos mecanismos de proteção consagrados no RGPD nesta matéria a exemplo, de resto, do que acontece relativamente a outros direitos como o direito de retificação e o direito ao apagamento dos dados.

O presente artigo tem por objetivo analisar os contornos desta discussão para, no final, tecer algumas considerações sobre o papel da regulação na promoção do desenvolvimento digital em conformidade com os valores e princípios que moldam as nossas sociedades.

1. Breve análise do debate em torno do direito à explicação no RGPD

O debate gerado em torno do direito à explicação que aborda, entre outras, questões complexas sobre a interpretação dos algoritmos enquanto responsáveis pelo tratamento de dados pessoais segundo uma lógica compreensível para os humanos, tem atraído a atenção tanto da comunidade científica como de um número crescente de juristas interessados em investigar a exequibilidade do direito, bem como o valor normativo do termo "explicação" dentro do contexto da inteligência artificial.

No campo do debate jurídico as contribuições mais proeminentes provêm de dois trabalhos de investigadores de Oxford que apresentam, cada um, conclusões distintas sobre como interpretar as disposições relevantes do RGPD nesta matéria. O primeiro, de Bryce Goodman e Seth

---

[5] Malgieri, Gianclaudio, Comandé, Giovanni. 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation', in *International Data Privacy Law*, v. 7, Issue 4, 2017, p. 243–265. Disponível em https://doi.org/10.1093/idpl/ipx019 (acedido a 5/5/2018).

[6] Wachter, Sandra, Mittelstadt, Brent and Russell, Chris. "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", in *Harvard Journal of Law & Technology*, 31, 2018, p. 842-888. Disponível em http://dx.doi.org/10.2139/ssrn.3063289 (acedido a 18/1/2019).

Flaxman[7], conclui que o RGPD cria um direito à explicação, enquanto o segundo, de Sandra Wachter, Brent Mittelstadt e Luciano Floridi[8], afirma que atualmente tal direito não existe.

Bryce Goodman, do Oxford Internet Institute, e Seth Flaxman, do Departamento de Estatística de Oxford, não hesitam em considerar que, embora o texto do RGPD não inclua qualquer referência expressa a um direito à explicação, a sua existência não pode ser questionada face às disposições do RGPD em matéria de decisões automatizadas. A parte do artigo que se refere ao direito à explicação (a outra diz respeito à não discriminação) é, no entanto, reduzida e os argumentos são sucintos. Numa primeira versão, os autores baseiam a existência deste novo direito no considerando 71 do RGPD que, ao afirmar que o titular dos dados, no caso de tratamento automatizado, tem sempre "...o direito de obter uma explicação sobre a decisão tomada na sequência dessa avaliação...", seria suficientemente claro. Numa versão posterior[9], os autores referem que o direito resulta dos art. 13.º a 15.º, onde são especificadas as salvaguardas requeridas pelo art. 22.º no que toca à fundamentação das decisões individuais automatizadas.

Questionando-se sobre o significado da expressão "informações uteis relativas à lógica subjacente" empregue nas referidas disposições, Goodman e Flaxman relembram os três tipos de obstáculos à transparência algorítmica elencados por Burrell[10]: i) dissimulação intencional da informação por parte do responsável pelo tratamento; ii) informação que é ininteligível para as pessoas em geral; iii) discrepância entre os modelos matemáticos gerados por *machine learning* e as formas de raciocínio humano, sendo este último o principal desafio que se põe aos investiga-

---

[7] Goodman, Bryce & Flaxman, Seth. "EU Regulations on Algorithmic Decision Making and 'a Right to an Explanation'", *2016 ICLM Workshop on Human Interpretability in ML*, 2016, p. 1.

[8] Wachter, Sandra et al.. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", in *International Data Privacy Law*, 7, 2, 2017, p. 76.

[9] Goodman Bryce & Flaxman, Seth. "EU Regulations on Algorithmic Decision Making and 'a Right to an Explanation'", in *AI Magazine*, vol. 38, n. 3, 2017, p. 56 e 57.

[10] Burrell, J. "How the machine "thinks": Understanding opacity in machine learning algorithms", in *Big Data & Society*, 2016, p. 1.

dores e programadores, em especial com o aparecimento das técnicas de *deep learning*[11].

Sem deixar de relevar os obstáculos técnicos que se levantam atualmente, bem como as imprecisões do texto legislativo, Goodman e Flaxman insistem na importância de fundamentar decisões individuais automatizadas, sustentando que "qualquer explicação adequada deve, no mínimo, descrever como os dados recolhidos se articulam com as previsões",[12] o que pressupõe que o modelo algorítmico deva ser claro e compreensível para um ser humano desde a sua programação inicial, para o que é necessário que o trabalho dos especialistas na matéria seja encorajado e prossiga.

O segundo artigo, de Wachter, Mittelstadt e Floridi, investigadores do Oxford Internet Institute, é antes de tudo uma forte contestação não só à existência do direito à explicação no RGPD como à sua viabilidade. Os autores não deixam de reconhecer, no entanto, que a inexistência de um tal direito constitui uma lacuna importante na proteção dos dados pessoais no caso de decisões automatizadas, para o que recomendam a adoção de uma série de medidas, incluindo legislativas, destinadas a explicitar as ambiguidades e omissões de que o atual texto padece[13].

Para melhor compreensão da análise, o artigo distingue à partida dois significados para o termo "explicações": o da funcionalidade do sistema de processamento e o das decisões individuais específicas. A esta distinção acresce ainda a das explicações *ex ante* e *ex post* conforme sejam fornecidas antes ou depois da tomada de decisão automatizada[14].

Depois de examinar as diferentes disposições suscetíveis de fundamentar um direito à explicação no RGPD, ou seja os art. 22.º, 13.º, 14.º e 15.º, os autores concluem que nenhuma delas fornece uma base legal suficientemente forte para o que se convencionou chamar um "direito à explicação", determinando tão só um direito limitado à obtenção de informação por

---

[11] O *deep learning* é uma forma particular de *machine learning* que envolve o uso de redes neurais com capacidade de aprendizagem e de compreensão de grandes quantidades de dados de forma não supervisionada.

[12] Goodman, Bryce & Flaxman, Seth. "EU Regulations on Algorithmic Decision Making and 'a Right to an Explanation'", in *ICML Workshop on Human Interpretability in ML,* 2016, p. 6.

[13] Wachter, Sandra et al.. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *op. cit.*, p. 96 e ss.

[14] *Idem*, p. 81.

parte do titular dos dados sobre a lógica envolvida no processamento dos sistema automatizados de tomada de decisão que apelidam de "direito de ser informado".

Esperando que novos desenvolvimentos venham a introduzir o direito à explicação num futuro próximo, enumeram três cenários que lhes parecem plausíveis nesse sentido: i) a adoção de normas de direito nacional que vão além do RGPD e que criem um direito à explicação de decisões específicas (semelhantes às medidas legislativas alemãs tomadas ao abrigo da Diretiva de 1995); ii) uma iniciativa por parte dos responsáveis pelo tratamento de dados no sentido de incluir o direito à explicação de decisões específicas no conceito "salvaguarda adequada" tal como se encontra expresso no n.º 3 do art. 22.º; e iii) finalmente, decisões judiciais que vão no mesmo sentido, isto é, que interpretem amplamente as salvaguardas do art. 22.º ou então que estabeleçam que o direito de acesso inscrito no art. 15.º integra o direito à explicação no rol dos requisitos enunciados na alínea h) do seu nº 1.

O texto de Wachter e outros é, por sua vez, fortemente criticado num artigo de Andrew Selbst e Julia Powles[15], que o qualificam de "reação exagerada" ao artigo de Goodman e Flaxman e de contribuir para "distorcer o debate" em torno do direito à explicação no RGPD.

Através de uma análise do texto e do espírito da lei, que pretendem mais construtiva e direcionada para os seus reais objetivos, Selbst e Powels concluem que as "informações significativas sobre a lógica envolvida" exigidas no caso de decisões automatizadas, não podem deixar de conter "algo como" um direito à explicação para permitir que o titular dos dados exerça efetivamente os seus direitos relativamente a decisões que o afetem, direitos que lhe são conferidos não só pelo RGPD mas que resultam dos próprios direitos fundamentais [16].

Na defesa da existência deste direito os autores referem, por um lado, as obrigações dos responsáveis pelo tratamento de dados de prestar informações adicionais, em que se incluem elementos úteis sobre a lógica em causa, o significado e as consequências previsíveis para o titular dos dados, resultantes da alínea f) do n.º 2 do art. 13.º e da alínea g) do n.º 2

---

[15] Selbst, Andrew D. and Powles, Julia. "Meaningful Information and the Right to Explanation", in *International Data Privacy Law*, 7, 4, 2017, p. 234. Disponível em https://ssrn.com/abstract=3039125 (acedido a 5/5/2018).

[16] *Idem*, p. 242.

do art. 14.º e, por outro, o direito de acesso conferido ao titular dos dados pela alínea h) do n.º 1 do art. 15.º.

Este entendimento é, segundo eles[17], suportado pelo art. 22.º que, depois de estabelecer no n.º 1 o princípio geral de que "o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar", introduz no n.º 3 uma lista não exaustiva de medidas de salvaguarda dos direitos, liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana, de exprimir o seu ponto de vista e de contestar as decisões, caso estas sejam tomadas no âmbito das exceções enumeradas nos n.º 2 a 4 [18].

Na definição do que são as garantias adequadas, o considerando 71 introduz uma clarificação importante ao indicar que o titular dos dados tem o direito de obter intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. O considerando acrescenta, ainda, que "A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstancias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião politica, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos....".

Embora os considerandos não tenham natureza vinculativa certo é que assumem um papel determinante na interpretação do clausulado, como reconhecem Selbst e Pawels, que concluem, assim, pela existência de um direito à explicação no RGPD, resultante da alínea f) do n.º 2 do art. 13.º,

---

[17] *Idem*, p. 237.

[18] *Idem*, p. 236.

da alínea g) do n.º 2 do artigo 14, da alínea h) do n.º 1 do art.15.º e do art. 22.º, mesmo que a expressão não conste de nenhum destes artigos. Acrescentam que esta conclusão tem suporte na lógica subjacente ao conjunto das disposições do RGPD e nos objetivos que ele expressa de reforço da proteção dos direitos e garantias individuais no que toca ao controle dos dados pessoais, base sobre a qual o texto legislativo tem de ser interpretado[19].

Esta convicção de que o RGPD deve ser visto como um todo sustentável, em que a par de direitos específicos, como o direito de acesso e o direito de retificação e de apagamento, e de mecanismos de salvaguarda, tais como a avaliação de impacto e a certificação, estão presentes importantes objetivos transversais como o de explicar e tornar os algoritmos mais responsáveis e compreensíveis que têm de ser tidos em consideração, é partilhada por Lilian Edwards e Michael Veale[20].

Outra questão, segundo estes autores[21], refletida no debate sobre o direito à explicação, é a da exequibilidade das disposições do RGPD que, embora sejam claras quanto à existência legal do direito e das garantias em causa, não deixam de levantar inúmeros problemas sobre a sua operacionalidade no estado atual da evolução tecnológica. A este propósito chamam a atenção para os art. 17.º e 20.º, sobre o direito de retificação e apagamento e o direito à portabilidade dos dados, que, apesar da precisão do seu enunciado, de igual modo colocam questões de ordem técnica quanto à sua implementação.

2. A interpretação do RGPD à luz da metodologia clássica e da autorregulação

Para além da tecnologia envolvida, a questão da natureza dos algoritmos usados na tomada de decisões é, sobretudo, uma questão legal na medida

---

[19] Selbst, Andrew D. and Powles, Julia. "Meaningful Information and the Right to Explanation", *op. cit.*, p. 242.

[20] Edwards, Lilian and Veale, Michael. "Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for", in *Duke Law and Technology Review*, 2017, p. 81.

[21] *Idem*, p. 67 e ss.

em que os cidadãos têm, num Estado de Direito, de dispor de meios eficazes para preservar os direitos, liberdades e garantias de que são titulares e, se for caso disso, para contestar quaisquer decisões que os infrinjam. Os sistemas automatizados permitem hoje criar perfis e categorizar os indivíduos em níveis de alto ou baixo risco em matéria de saúde, crédito, emprego, classificá-los como potenciais infratores ou mesmo como potenciais criminosos ou terroristas, sendo que tais decisões têm impacto significativo na passagem de fronteiras, no acesso à segurança social, na assistência médica, na entrada em estabelecimentos de ensino, etc.

No entanto, o tratamento dos dados pessoais baseado em algoritmos é ainda caracterizado pela opacidade dos mecanismos operacionais e pela ininteligibilidade da lógica envolvida na preparação e obtenção dos *outputs*. A rede inextricável de algoritmos que se sucedem e se encadeiam resulta num imbróglio de decisões obscuras, que criam incerteza e desconfiança sobre como um ambiente controlado por máquinas irá interagir com o mundo real e interpretar e avaliar os nossos comportamentos[22]. Daí que tenhamos de criar novos meios de proteger a liberdade individual e os direitos de cidadania, num quadro jurídico de regras previsíveis e credíveis, capaz de assegurar o funcionamento dos mecanismos de impugnação das decisões individuais na base das quais se constrói a sua legitimidade. Nas palavras de M. Hildebrandt, "sendo certo que os remédios do passado já não são eficazes, é preciso repensar e reinventar o Estado de Direito, tornando o imbróglio algorítmico transparente e as suas decisões compreensíveis e contestáveis"[23].

Embora as opiniões divirjam sobre o conteúdo e interpretação das diferentes disposições, a doutrina tende a concordar em atribuir ao RGPD o objetivo de acionar os mecanismos de salvaguarda do direito fundamental à proteção de dados e do direito à transparência do perfil em todas as situações em que haja decisões automatizadas que afetem significativamente os indivíduos.

Em concreto, como resulta do RGPD, as decisões individuais automatizadas são sempre geradoras de obrigações e de direitos com determinada

---

[22] Hildebrandt, Mireille. "The New Imbroglio – Living with Machine Algorithms", in *The Art of Ethics in the Information Society*, 2016, p. 5. Disponível em https://works.bepress.com/mireille_hildebrandt/75/ (acedido a 7/8/2018).

[23] *Idem*, p. 2.

especificidade. Os artº 13.º e 14.º exigem que o titular dos dados, quer tenha sido ele ou não a facultar os dados pessoais, receba informações sobre a existência de tais decisões, sobre a sua lógica e sobre a importância e consequências previstas que possam ter, enquanto o art. 15.º atribui ao titular dos dados o direito de obter confirmação sobre o tratamento dos dados pessoais e de lhes aceder, bem como a informações específicas adicionais, designadamente sobre a lógica subjacente caso haja decisões automatizadas. Por sua vez, o artº 22.º proíbe decisões individuais tomadas exclusivamente com base no tratamento automatizado a não ser nos casos excecionais que enumera de forma taxativa, sendo que nestes casos as salvaguardas obrigatórias incluem, no mínimo, o direito de obter intervenção humana, de manifestar o seu ponto de vista e de contestar a decisão.

A asserção de direitos e obrigações no RGPD relativamente a decisões individuais automatizadas não é incompatível com o reconhecimento dos obstáculos científicos e técnicos que se põem quanto à efetividade do seu exercício. É antes a aceitação de que todas as decisões que afetam significativamente qualquer indivíduo são passíveis de contestação, pelo que se lhes exige, primeiro que tudo, que obedeçam aos princípios básicos da fundamentação e da transparência. Se isso não for possível, ou, desde que isso não seja possível, tais decisões devem ser tidas por incompatíveis com as normas vigentes.

Em grande parte, graças à investigação e publicação de trabalhos de relevo na matéria, tem-se notado nos últimos anos uma atitude menos complacente por parte da sociedade no que toca à "prepotência" algorítmica sem que tal atitude tenha, nem era isso o que se pretendia, impedido o desenvolvimento das técnicas de *machine learning*[24]. Nos setores mais diversos – das redes sociais à administração da justiça – é cada vez maior a presença de sistemas de *machine learning* devido à sua capacidade de melhorar exponencialmente a gestão dos dados a um custo e escala que seriam impraticáveis com recursos humanos. Esta é uma tendência que se irá acentuar, sendo unânime entre os especialistas o sentimento de que os

[24] Casey, Bryan, Farhangi, Ashkon and VOGL, Roland. "Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise", in *Berkeley Technology Law Journal*, 2018, p. 5 e ss. Disponível em https://ssrn.com/abstract=3143325 (acedido a 3/6/2018).

algoritmos de aprendizagem vão desempenhar um papel cada vez maior na organização da nossa vida. Como os deveremos então regular?

A responsabilidade algorítmica assenta na transparência. Questão que se tem posto é a de saber se essa transparência deve implicar a partilha do funcionamento dos algoritmos com os indivíduos cujos dados pessoais foram objeto de tratamento, ou se, por a informação se afigurar demasiado complexa, uma explicação sobre esse funcionamento será bastante. Embora reconhecendo as dificuldades práticas da primeira opção, autoridades nacionais como o ICO têm-na defendido sempre que os algoritmos em questão afetem os direitos e liberdades dos indivíduos[25].

A resposta a esta questão não resulta clara do RGPD. De resto, uma das características que alguns autores lhe atribuem é a de estabelecer um quadro normativo proativo que repousa, e bem, sobre o contributo da governação digital para agilizar políticas e procedimentos capazes a cada momento de melhor assegurar os equilíbrios entre a defesa dos direitos individuais e a preservação da inovação[26]. Parece, com efeito, razoável apontar o RGPD como um exemplo da solução Goldilocks[27], ou seja, de um compromisso entre a necessidade de resolver problemas específicos e a de deixar espaço para a investigação e criação.

A adoção de disposições tendencialmente flexíveis que deixem margem para acolher novos desenvolvimentos tecnológicos acarreta, no entanto, novos desafios para a interpretação e poderes acrescidos para quem as vai aplicar. Se, na verdade, a linguagem do RGPD deixa pairar alguma ambiguidade sobre conceitos como o do direito à explicação das decisões individuais automatizadas, afigura-se por outro lado importante atentar na significativa mudança introduzida pela regulamentação no sentido de ampliar e reforçar os poderes de execução conferidos às autoridades de proteção de dados, especialmente nos capítulos VI e VIII.

---

[25] *Guide to the General Data Protection Regulation* (GDPR). Disponível em https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (acedido a 9/8/2018).

[26] Floridi, Luciano. "Soft Ethics and the Governance of the Digital", in *Philosophy & Technology*., 31, 2018, p. 3.

[27] Princípio segundo o qual a solução ideal se situa no meio termo. "High-Level Hearing: a European Union Strategy for Artificial Intelligence", 27 março 2018, p. 24. Disponível em https://ec.europa.eu/epsc/events/high-level-hearing-european-union-strategy-artificial-intelligence_en (acedido em 10/5/2018).

A CE tem também incentivado a atividade de grupos de especialistas na elaboração e disponibilização de linhas de orientação em matéria de interpretação do RGPD para benefício das autoridades nacionais e do público em geral. É o caso do GT29 que, em outubro de 2017, publicou um conjunto de diretrizes sobre a tomada de decisões individuais automatizadas e a definição de perfis no contexto do RGPD[28].

O GT29, criado pela diretiva 95/46 CE e agora substituído pelo Comité Europeu para a Proteção de Dados, foi desde a sua constituição o principal órgão consultivo da CE em matéria de proteção de dados e de questões de segurança da informação. Embora as suas recomendações não sejam vinculativas, elas constituem um referencial para as diferentes autoridades dos Estados-Membros e são, portanto, cruciais para compreender como essas autoridades vão interpretar o RGPD[29].

As referidas diretrizes do GT29 relativas a decisões individuais automatizadas constituem, pois, um utilíssimo instrumento de clarificação na compreensão de alguns temas polémicos gerados em torno do direito à explicação, como sejam os da determinação do conteúdo do direito "a ser informado", de "obter intervenção humana" e de "aceder a informações úteis relativas à lógica subjacente".

Depois de identificar os princípios da transparência e da qualidade da informação enunciados nos art. 5.º e 12.º, como princípios essenciais para a compreensão do RGPD, o documento do GT29 sublinha, quanto ao "direito a ser informado", que a informação sobre o tratamento dos dados e objetivos pretendidos tem de ser clara e inteligível para o respetivo titular, ou seja, entenda-se, adequada às caraterísticas do interessado[30].

---

[28] "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/67*", adotadas em 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018. Disponível em http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826 (acedido a 9/8/2018).

[29] Cabe agora ao Comité Europeu para a Proteção de Dados, a funcionar desde maio de 2018, desempenhar essa importante tarefa de emitir orientações sobre a interpretação dos principais conceitos do RGPD e assim contribuir para uma aplicação uniforme e coerente da legislação europeia em matéria de proteção de dados de acordo com a Comunicação da Comissão ao Parlamento Europeu e ao Conselho "Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018", COM (2018) 43 de 24/1/2018, p. 11.

[30] GT29, *Guidelines*, *op. cit.*, p. 16 e ss.

Relativamente ao significado de "intervenção humana" nos termos nomeadamente do art. 22.º, refere que o mero envolvimento simbólico não é suficiente, sendo exigível que tenha um papel decisivo na tomada de decisão, para o que esta deve estar a cargo de alguém com autoridade e competência para a alterar, depois de revistos todos os fatos pertinentes[31].

Numa ótica de dar primazia ao princípio do controle dos dados pessoais pelo titular, o GT29 não deixa, no entanto, de equacionar as dificuldades decorrentes do desenvolvimento e complexidade das técnicas de *machine learning*, nem os legítimos interesses do responsável pelo tratamento dos dados[32].

Daí que o RGPD obrigue o responsável pelo tratamento a fornecer ao titular dos dados as informações sobre a lógica envolvida na tomada de decisão que sejam necessárias para que este exerça os seus direitos, mas que não o obrigue, no entanto, a uma explicação complexa dos algoritmos usados ou à sua divulgação completa. O direito à explicação pode pois não exigir a total abertura das "caixas pretas"[33], desde que o interesse individual do titular seja respeitado em todos as fases de tratamento dos dados, através de informação suficiente, atempada e adequada à sua efetiva proteção.

No sentido de facilitar o cumprimento dos requisitos legais do art.º 22, o GT29 faz ainda algumas sugestões de boas práticas[34] que, no fundo, correspondem a medidas de autorregulação por parte dos responsáveis pelo tratamento dos dados a ter em consideração em todas as fases do processo, desde o *design* do modelo até à sua efetiva utilização.

Finalmente, convém sublinhar que o dispositivo do art. 22.º não constitui para o GT29 um mero instrumento de contestação dependente da iniciativa individual, mas sim a afirmação de que são proibidas decisões individuais automatizadas que não se enquadrem em nenhuma das exceções taxativamente enumeradas[35].

---

[31] *Idem*, p. 21.

[32] *Idem*, p. 25.

[33] Conceito decorrente da ciência da computação que designa sistemas de que se conhecem apenas os dados de entrada e de saída sem acesso ao seu funcionamento interno.

[34] Por ex., verificações regulares da qualidade dos modelos e dos algoritmos usados e realização de auditorias independentes para garantir que os indivíduos são tratados de forma justa, correta e não discriminatória. GT29, *Guidelines*, *op. cit.*, p. 31 e ss.

[35] GT29, *Guidelines*, *op. cit.*, p. 19.

Esta interpretação corresponde à vontade do legislador de deslocar da esfera individual para o campo da autorregulação a efetiva proteção dos direitos conferidos ao titular dos dados pelo RGPD, com vista a minorar as inevitáveis dificuldades práticas do exercício de tais direitos se considerarmos a assimetria de recursos entre uns e outros que o RGPD não deixa de evocar.

Considerações finais

A previsão da irrupção de novas formas de inteligência artificial que, a curto prazo, vão não só melhorar a qualidade do nosso quotidiano, como transformar a realidade político-social em que vivemos, exige uma atenção especial no que toca à proteção das liberdades e garantias fundamentais do individuo em que se inclui o direito à proteção dos dados pessoais. O RGPD reflete a preocupação de adequar a proteção dos dados pessoais aos novos desafios da tecnologia, por forma a proporcionar ao titular dos dados os instrumentos necessários para supervisionar e controlar a utilização que deles é feita.

Entre os direitos que o RGPD atribui ao titular dos dados está o de contestar quaisquer decisões que o afetem significativamente desde que tomadas unicamente com base no tratamento automatizado dos seus dados pessoais, bem como o de obter informações úteis sobre tais decisões, a que se tem chamado direito à explicação e que resultaria, segundo alguns autores[36], em especial dos art. 13.º a 15.º e 22.º, como descrito anteriormente.

A polémica em torno da questão de saber se tal direito se encontra ou não inscrito no RGPD não se afigura verdadeiramente relevante.

O conhecimento dos fatos e da lei que nos rege, a possibilidade de exprimir outros pontos de vista e de contestar quaisquer decisões que nos afetem, o direito a um processo equitativo, são tudo parte integrante dos valores essenciais que o Estado de Direito tem de garantir e que nenhuma regulamentação pode desrespeitar e de que é inseparável o princípio geral da motivação das decisões, mormente das que limitem os direitos e liberdades individuais.

---

[36] Goodman, Bryce e Flaxman, Seth. "EU Regulations on Algorithmic Decision Making and 'a Right to an Explanation'", *op. cit.*, p.1.

A questão relevante do debate sobre o direito à explicação não é assim a de pretender que tal princípio, para ser atendível no quadro da proteção de dados, tenha de ser especificamente enunciado no RGPD.

O ponto central é que o legítimo exercício do direito à explicação ganha particular significado quando na base da decisão litigiosa se encontram tratamentos automatizados, incluindo a definição de perfis, obtidos por meio de algoritmos indecifráveis para o titular dos dados, colocando-se então a verdadeira questão de saber até que ponto a opacidade algorítmica e o receio de entravar a inovação poderão impedir o funcionamento do princípio da motivação das decisões.

Em abstrato ninguém duvida da necessidade de um direito à explicação de decisões automatizadas, a dúvida está em como o exercer enquanto os algoritmos forem inexplicáveis.

Face à imprecisão da legislação caberá à jurisprudência e aos reguladores manter um olhar atento sobre os caminhos da inovação por forma a assegurar que o desenvolvimento das tecnologias digitais não se faz em detrimento dos direitos e liberdades dos cidadãos, mas sim ao seu serviço.

No seu Parecer de 26 de julho de 2017 sobre o projeto de acordo entre o Canadá e a UE em matéria de transferência de dados PNR[37], o Tribunal de Justiça refere expressamente a necessidade de "prever que os modelos e os critérios utilizados no âmbito do tratamento automatizado dos dados dos registos de identificação dos passageiros serão específicos, fiáveis e não discriminatórios", sem o que tal tratamento não será compatível com as disposições da CDFUE.

Para ser legítimo, o tratamento de dados pessoais deve ser rodeado de medidas claras e precisas que permitam que os titulares dos dados disponham de garantias suficientes para proteger eficazmente os seus dados pessoais contra os riscos de abuso, sendo que "a necessidade de dispor de tais garantias é ainda mais importante quando os dados pessoais são sujeitos a tratamento automatizado"[38].

Tratando-se de uma decisão judicial que se prende com a proteção dos dados pessoais num contexto de cooperação policial por maioria de razão será de supor que o Tribunal, chamado a pronunciar-se sobre a matéria no

---

[37] Parecer 1/15 do TJ de 26 de julho de 2017, para. 172. Disponível em http://curia.europa.eu/juris/liste.jsf?pro=AVIS&num=C-1/15 (acedido a 24/10/2017).

[38] *Idem*, para. 141.

âmbito do RGPD, não tenha dúvidas em declarar a nulidade de decisões individuais automatizadas a que falte fundamentação consistente.

Importantes avanços no sentido de explicar a inteligência artificial estão em curso[39], sendo a própria CE a eleger a inteligência artificial explicável**,** na sua Comunicação de 25 de abril 2018 "Inteligência artificial para a Europa"[40], como uma das prioridades em matéria de investigação e inovação nesta área. Esse é, no entanto, um processo em desenvolvimento que não pode sobrepor-se à absoluta exigência de respeitar e proteger os direitos fundamentais no tempo presente, independentemente de eventuais avanços tecnológicos, como foi reconhecido por investigadores de diversas áreas na Declaração de Toronto de 16 de maio de 2018[41].

Até lá, se a explicação tem ou não de passar por abrir "caixas pretas" é algo que só deverá ser avaliado em função dos legítimos interesses dos cidadãos e nunca em função dos meios técnicos disponíveis.

---

[39] O programa "Explainable Artificial Intelligence" da *Defense Advanced Research Projects Agency* tem como objetivo criar um conjunto de técnicas de *machine learning* que produza modelos mais inteligíveis, mantendo um alto nível de aprendizagem (precisão de previsão) e que permita que os utentes humanos compreendam, confiem e controlem com eficácia a geração de novos parceiros artificialmente inteligentes.

[40] COM (2018) 237 de 25/4/2018, p. 19.

[41] Disponível em https://www.accessnow.org/cms/assets/uploads/2018/05/Toronto-Declaration-D0V2.pdf (acedido a 11/1/2019).

O Direito ao apagamento de dados como realidade global

Francisco Arga e Lima*
Mateus Magalhães de Carvalho**

Resumo: Num mundo cada vez mais informatizado e global, a proteção de dados pessoais tem ganho destaque a nível europeu. Em especial, a faculdade de apagar (ou "esquecer") dados de um motor de busca da *Internet* mostra evidentes dificuldades técnicas e jurídicas que importam descortinar, de modo a assegurar uma eficaz proteção dos dados pessoais, segundo os elevados padrões europeus. Propomo-nos, assim, discutir que titulares de dados se encontram protegidos pelo âmbito de aplicação do direito ao apagamento de dados, bem como em que moldes deverá tal apagamento lograr a maior eficácia possível, no respeito pelos normativos internacionais.

Palavras-chave: *RGPD; Apagamento; Ciberespaço; Extraterritorialidade; Geoblocking.*

---

* Francisco Arga e Lima encontra-se no quarto e último ano da sua licenciatura, na Faculdade de Direito da Universidade Nova de Lisboa (FDUNL). Frequenta igualmente o I Curso de Pós-Graduação em Proteção de Dados e Empresas, na Faculdade de Direito da Universidade de Lisboa. Participou em vários moot courts ao longo da sua formação académica, tendo sido vencedor da VII Edição do Moot Court Nacional de Direito Internacional Público, finalista na I edição do Moot Court Português de Direito da Concorrência e vencedor da V Edição do EUROPA Moot Court, em Kavala (este último versando sobre Proteção de Dados). Iniciou a sua produção científica em 2017, com o artigo "Direito a ser Esquecido: Um Conceito em Construção", o qual foi menção honrosa para o Prémio Pessoa Jorge, promovido pela SRS Advogados.

** Mateus Magalhães de Carvalho frequenta o quarto ano da Licenciatura em Direito, na Faculdade de Direito da Universidade Nova de Lisboa. Participou em diversos moot courts, tendo sido vencedor na VII Edição do Moot Court Nacional de Direito Internacional Público, bem como vencedor e melhor orador na V Edição do EUROPA Moot Court, em Kavala (este último subordinado à temática da Proteção de Dados). É, desde 2017, membro do Conselho Pedagógico da Faculdade de Direito da Universidade Nova de Lisboa.

Abstract: In a increasingly informatical and global world, personal data protection has gained the spotlight in the European Union. Especially, the power to erase (or "to forget") data from an Internet search engine shows clear technical and legal problems that must be uncovered, in order to ensure an effective data protection, according to the high European standards. Therefore, we seek to discuss which data subjects are protected by the scope of application of the right of erasure of personal data, as well as how such erasure should achieve effectiveness, in accordance with the international regulatory instruments.

Keywords: *GDPR; Erasure; Cyberspace; Extraterritoriality; Geoblocking.*

Introdução

Foi em maio de 2018 que se tornou aplicável na UE a mais recente ferramenta legislativa em matéria de proteção de dados pessoais: o RGPD[1]. Este novo diploma procura garantir um elevado e uniforme nível de proteção das pessoas singulares neste campo através de vários direitos subjetivos, como o direito ao apagamento dos dados postulado no art. 17.º, n.º 1, RGPD[2-3].

É propósito do presente artigo discutir o campo de aplicação deste direito quando uma sua pretensão se reporte a dados na posse de motores de busca, numa análise bipartida, realizada nos seguintes termos:

i) em primeiro lugar, tentaremos compreender quais os titulares de dados que poderão recorrer a esta figura, já que não pode, no nosso entender, a sua existência estar desligada de considerações territoriais relacionadas com os Estados terceiros cujos ordenamentos não contemplam o direito ao apagamento;
ii) em segundo lugar, iremos, ainda, procurar determinar quais as consequências territoriais de tal apagamento de dados. Para tal,

---

[1] Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[2] *Vide*, por exemplo, o Considerando 10 do RGPD.

[3] Este elevado padrão de proteção das pessoas singulares vem, por exemplo, reconhecido no artigo 8º da CDFUE.

apoiar-nos-emos no recente reenvio prejudicial que opõe a *Google, Inc.* à autoridade francesa de proteção de dados, a CNIL, em que é perguntado ao TJ quais as vestes que uma supressão de hiperligações deve assumir, se globais ou se circunscritas a um qualquer âmbito territorial menor. Sondaremos as questões suscitadas neste processo à luz do RGPD, assim procurando determinar qual o escopo territorial do apagamento de dados e já não da supressão de hiperligações, em função da normal sucessão de atos legislativos europeus que desembocou na entrada em vigor deste regulamento.

1. Breve síntese da evolução das concepções normativas do esquecimento e seu escopo aplicativo

Antes de mergulharmos no objeto do presente estudo, importa descrever os principais acontecimentos que se relacionam com a origem do direito ao apagamento de dados, bem como a clarificação do âmbito territorial dos atos normativos europeus relativos à proteção de dados. Em particular, cabe analisar o caso *Google Spain*, em que foi consagrado um direito à supressão de hiperligações e foi discutida a sua aplicação geral a entidades situadas fora da União Europeia. Este direito é, no mínimo, uma forma embrionária do direito ao apagamento, pelo que cumpre igualmente distinguir estes dois direitos já elencados.

1.1. Acórdão Google Spain

Em 2010, M. Costeja González apresentou uma reclamação à Agência Espanhola de Proteção de Dados contra o jornal *La Vanguardia Ediciones SL* e contra a *Google Spain* e *Google Inc*, procurando ocultar informação de plataformas dos demandados, relativa a dívidas suas à Segurança Social.

Nestes termos, M. Costeja González pediu a remoção dos seus dados da notícia do jornal, bem como a eliminação das referências à notícia no motor de pesquisa da *Google Inc*. A autoridade espanhola de proteção de dados, a *Agencia Española de Protección de Datos* considerou que apenas a *Google Spain* e a *Google Inc*. deveriam suprimir a informação controvertida (sob a forma de hiperligações). Estas interpuseram recurso para o Supremo Tribunal

de Justiça Espanhol, que remeteu três questões prejudiciais ao TJ, tendo sido emitido acórdão em 13 de maio de 2014[4].

Para o presente estudo, importa focar principalmente duas delas: será que a Diretiva 95/46/EC[5] consagra um "Direito a ser Esquecido", ou seja, um direito a partir do qual um sujeito possa exigir a um motor de pesquisa que suprima certos resultados de pesquisa? E será que o Supremo Tribunal de Justiça Espanhol pode aplicar as normas de proteção de dados europeias contra uma entidade sediada nos EUA (a *Google Inc.*)?

Começando pela primeira pergunta, importa analisar a Diretiva 95/46/CE, já revogada, e ver quais as disposições que podem ajudar a responder a essa questão. Neste diploma não se encontrava vertido, expressamente, um "Direito a ser Esquecido", mas eram previstos outros dois direitos bastante importantes: o direito de acesso (art. 12.º e 14.º) e de oposição (art. 14.º e 15.º). O primeiro dividia-se em dois outros direitos complementares: o direito de acesso aos próprios dados[6] e o direito de retificação, apagamento e bloqueio (art. 14.º)[7]. O segundo direito analisado pelo TJ dividia-se no direito de oposição a decisões automatizadas (art. 15.º), de oposição devido à situação particular da pessoa em causa (art. 14.º, al a)), e de oposição à utilização dos dados para efeitos de *marketing* direto (art. 14.º, al. b)).

No presente contexto, importa fundamentalmente definir o direito de retificação, apagamento e bloqueio. Na sua égide, podia um titular de dados pessoais, por "razões preponderantes e legítimas relacionadas com a sua situação particular", opor-se a que os dados que lhe dissessem respeito fossem objeto de tratamento.

O TJ decidiu conjugar os direitos de acesso e de oposição no sentido de o operador do motor de busca, a pedido de um titular de dados pessoais,

---

[4] Acórdão do TJ, C-131/12, *Google Spain*, ECLI:EU:C:2014:317.

[5] Diretiva 95/46/EC do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[6] Este direito permitia aos sujeitos em causa saberem, a cada momento, se os seus dados estão a ser alvo de qualquer tipo de tratamento e, se tal se verificar, para que fins estão a ser tratados que categorias de dados são objeto de tratamento, a que destinatários vão os mesmos ser comunicados e a origem dos dados pessoais, etc.

[7] Conferia aos titulares dos dados a faculdade de obterem do responsável pelo tratamento de dados a retificação, o apagamento, ou mesmo o bloqueio dos dados em causa, caso considerassem que o tratamento não ia de acordo com os cânones da Diretiva 95/46/EC.

ser obrigado a suprimir da lista de resultados, apresentada na sequência de uma pesquisa feita a partir do seu nome, as ligações que contenham informações sobre si. Concluiu, assim, pela existência de um direito à supressão de hiperligações na Diretiva 95/46/EC[8].

Contudo, o TJ não discutiu apenas a existência de um direito à supressão de hiperligações, mas também apreciou o escopo territorial da Diretiva no seu todo. De facto, foi perguntado ao TJ até que ponto poderia o Supremo Tribunal de Justiça Espanhol aplicar os direitos de acesso e oposição contra uma empresa com sede nos EUA (neste caso, a *Google Inc.*).

O TJ considerou que a Diretiva era aplicável à *Google Inc.*, apesar desta ser uma empresa americana, já que esta detinha um estabelecimento num Estado-Membro da UE: a *Google Spain*. Deste modo, o Tribunal conferiu à Diretiva um âmbito de aplicação particularmente amplo, extensível para fora da União, desde que cumpridas as condições do seu art. 4º, n.º 1, alínea a)[9].

1.2. Google Spain *vs. RGPD*

Procede da exposição anterior a sedimentação no ordenamento europeu de um direito à supressão de hiperligações ou à desindexação. Contudo, em maio de 2018, começou a produzir efeitos o RGPD. Este regulamento consagra um direito ao apagamento de dados pessoais (art. 17.º). Conforme o n.º 1 de tal artigo, pode o titular dos dados "obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada", caso se cumpra alguma das condições aí plasmadas, nomeadamente a ilicitude do tratamento (alínea d)).

Por questões de ordem prática relativas à economia do presente estudo, esta nossa análise incidirá sobre o direito ao apagamento, já que a Diretiva na qual o TJ se baseou para construir o direito à supressão de uma hiperligação se encontra, agora, revogada, em consequência da entrada em vigor do RGPD.

---

[8] *Vide* Acórdão do TJ, C-131/12, *Google Spain*, cit., para. 100; *Vide*, igualmente, Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, LSE Law, 2015, p. 8.

[9] Ver, em particular, Acórdão do TJ, C-131/12, *Google Spain*, cit., paras. 50 a 58.

Ora, os critérios de aplicação do RGPD, constantes do art. 3º, são, em termos gerais, similares aos estabelecidos no Acórdão *Google Spain* para o direito à desindexação, pelo que as variações de vulto entre os dois documentos legislativos consistirão nos direitos neles consagrados para assegurar o esquecimento das pessoas singulares. Deste modo, resta-nos distingui-los. Serão o direito à desindexação e o direito ao apagamento de dados um e o mesmo direito?

Podemos alvitrar do andamento do processo legislativo europeu (revogação da antiga Diretiva e sua substituição pelo RGPD) que foi intenção legiferante definir como única cláusula operativa da supressão de dados o art. 17.º do RGPD e o seu direito ao apagamento[10]. Confirmemos, então, a correção de tal asserção.

Ora, o direito à desindexação não se traduz em mais que a supressão de hiperligações dos resultados de buscas operadas com base no nome do titular dos dados. Não possibilita o apagamento da informação constante dos *websites* para os quais tais hiperligações remetem (cujos servidores são estranhos ao controlo do motor de busca), nem tão pouco, e mais decisivamente, o apagamento da informação pessoal do sujeito dos servidores de indexação[11] a partir dos quais os motores de busca geram os resultados das pesquisas realizadas. Com efeito, o direito à desindexação não possibilita

---

[10] Esta é, de facto, uma das interpretações possíveis do considerando n.º 66 do RGPD quando refere que, para "reforçar o direito ao esquecimento", o direito ao apagamento deve ser implementado com recurso ao disposto no art. 17.º, n.º 2, daqui se podendo retirar que tudo aquilo que compõe o direito ao esquecimento que não seja o apagamento de dados é, precisamente, a obrigação de notificação de tal pedido a responsáveis subsequentes. In Xanthoulis; Napoleon. "Conceptualising a Right to Oblivion in the Digital World: A human rights-based approach", disponível em: https://ssrn.com/abstract=2064503 ou http://dx.doi.org/10.2139/ssrn.2064503, p. 16. (acedido a 09/03/2019).

[11] Bases de armazenamento e organização dos dados utilizados para gerar resultados de buscas, governados segundo um modelo de otimização dessas tarefas, que visa promover uma maior latência dos resultados de busca apresentados em cada pesquisa. Estas são compostas, em constante mudança, por todos os dados recolhidos indiscriminadamente por um motor de busca na Internet, através de um processo denominado de web crawling. Os dados pessoais de um sujeito são, de forma muito sintética, tratados na sua recolha de toda a Internet, na sua organização em servidores de indexação e na sua submissão a algoritmos de produção de resultados de busca. Ver Brin, Sergey; Page, Lawrence. "The Anatomy of a Large-Sclae Hypertextual Web Search Engine; Stanford University", disponível em: http://infolab.stanford.edu/~backrub/google.html (acedido a 09/03/2019), bem como Patil, Yugandhara; PATIL,

a supressão de hiperligações geradas por qualquer outra combinação de palavras inseridas no motor de busca que não a dos nomes dos titulares de dados[12].

Por seu turno, no direito ao apagamento a impossibilidade de aceder à informação pessoal do titular de dados alcança-se, em teoria, mediante o verdadeiro apagamento dos dados pessoais dos repositórios onde estes estejam armazenados em cada motor de busca.

Podemos até concluir que a desindexação é, por inerência lógica, consumida nas suas utilidades pelo direito ao apagamento. Se os dados pessoais de um sujeito são apagados no seu lugar de armazenamento originário, então não podem ser transferidos para servidores de indexação e, consequentemente, organizados em hiperligações como resultado de buscas.

Torna-se, então, intuitivo, que o direito à supressão de uma hiperligação e o direito ao apagamento são dois direitos distintos, de naturezas e implicações práticas diferentes, mais não seja pelo facto de o primeiro permitir que um motor de busca mantenha os dados pessoais de determinado sujeito na sua posse, ao invés do direito ao apagamento.

É no direito ao apagamento que centraremos a nossa análise, discutindo: (i) os limites territoriais inerentes a uma sua aplicabilidade numa realidade transfronteiriça como a *Internet*; e (ii) as consequências que pode assumir por forma a assegurar a eficiência da proteção dos dados pessoais das pessoas singulares, quando compatibilizada com todos os outros interesses em jogo.

2. A extraterritorialidade do direito ao apagamento: titulares

No nosso entender será fundamental para o presente estudo a compreensão de que o direito ao apagamento de dados é, como todos os direitos previstos no RGPD, territorialmente limitado pela natureza das competências e poderes da União Europeia.

Sonal. "Review of Web Crawlers with Specification and Working", in *International Journal of Advanced Research in Computer and Communication Engineering*; v. 5, 2016, p. 220-223.

[12] É claro que este direito pode ser alargado a outras combinações introduzidas num motor de busca, mas existirão sempre outras possibilidades de obter, nos resultados de uma busca, as hiperligações que contêm os dados pessoais do seu titular.

É nessa senda que importa articular o art. 17.º com o art. 3.º, n.º 1 do RGPD, que versa sobre o âmbito territorial deste diploma, dizendo que o mesmo se aplica a todos os tratamentos de dados pessoais efetuados no contexto de atividades do responsável do tratamento que se manifestem no território da União, *independentemente de o tratamento ocorrer dentro ou fora da União*[13].

No entanto, não podemos deixar de notar o seguinte: uma coisa é a aplicação do RGPD (que se quer global), outra bem distinta é a extensão territorial dos direitos por ele criados (*maxime* o direito ao apagamento), que assumirá contornos variáveis em função das particularidades concretas da pretensão do titular dos dados[14].

Não há dúvida que, se interpretadas literalmente, as provisões do RGPD em análise podem ser potencialmente aplicadas a toda a *Internet*, estando, desse modo, ao dispor de todos os titulares de dados, em qualquer parte do mundo, como ferramenta jurídica de salvaguarda da proteção das suas informações pessoais.

Com efeito, tal entendimento de aplicação global das regras europeias de proteção de dados já brotava da jurisprudência europeia e, em especial, do caso *Google Spain*[15]. Entende-se do art. 3.º que a aplicação do RGPD não apresenta quaisquer limites territoriais ou relacionados com a nacionalidade do titular dos dados, sendo antes definida *ratione materiae*, em função de um tratamento de dados pessoais ter ocorrido no contexto de atividades que se manifestem na União.

Foi esta a intenção manifestada pelo legislador europeu, justificada pelo desejo de concretizar um direito fundamental dos cidadãos e de tornar

---

[13] Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, LSE Law, 2015, p. 12; Svantesson, Dan. "Extraterritoriality In The Context Of Data Privacy Regulation", in *Masaryk University Journal of Law and Technology*, v. 7 (1), 2012, p. 87-96.

[14] O antigo GT29 sublinhou a necessidade de avaliar as pretensões dos titulares de dados numa base casuística, *vide* GT29, "Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment In "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) And Mario Costeja González", 26 de novembro de 2014, p. 12.

[15] *Vide* Acórdão do TJ, C-131/12, *Google Spain*, cit., para. 60; ver também, entre outros, Acórdão do TJ, Proc. C-324/09, *L'Oréal e o.*, ECLI:EU:C:2011:474, para. 67.

a UE um padrão de referência global no que diz respeito à garantia da privacidade no mundo digital[16].

Mas será juridicamente aceitável que a União estenda, com base nesta norma, a sua competência extraterritorial de forma absoluta e incondicionada nos termos de uma leitura literal do art. 3º do RGPD quando articulado com o art. 17.º do RGPD? Esta questão terá de merecer uma resposta negativa da nossa parte, em face dos fundamentos apresentados em seguida.

2.1. Abrangência do direito ao apagamento de dados no direito internacional

2.1.1. Soberania territorial no ciberespaço

Em primeiro lugar, cabe olhar para o Direito Internacional e, especificamente, para as regras de soberania a que os Estados estão vinculados, de modo a averiguar qual pode ser a extensão do braço normativo europeu. Contudo, o âmbito do nosso estudo conduz-nos para um domínio que não se confunde com os tradicionais espaços de desenvolvimento humano (a terra, o mar, o espaço aéreo ou o espaço exterior).

Realmente, as questões relacionadas com a *Internet* estão intimamente ligadas a um novo domínio, que começa agora a ganhar importância na orla internacional: o ciberespaço. Este caracteriza-se por ser um domínio operacional diferenciado pelo uso de meios eletrónicos, através do espectro eletromagnético, que permitem a criação, armazenamento, modificação, troca e uso de informação, através de redes interdependentes e conectas, usando tecnologias de comunicação e informação[17]. Assim sendo, qualquer tipo de tratamento de dados realizado através da *Internet* implica a passagem pelo ciberespaço, na medida em que aquela utiliza meios eletrónicos e o espectro eletromagnético, para partilhar, alterar e criar informação, numa rede global.

---

[16] CE, *Press Release*: "European Commission sets out strategy to strengthen EU data protection rules", *IP/10/1462*, Brussels, 4 de novembro de 2010.

[17] Kuehl; Daniel T.. "From cyberspace to cyberpower: Defining the problem", in *Cyberpower and national security*, National Defense University Press, 2009, p. 27.

Ainda que não existam fontes normativas consolidadas em relação a este domínio, podemos vislumbrar certas produções doutrinárias que visam auxiliar na resolução dos problemas de conciliação da soberania estadual com o ciberespaço e, consequentemente, permitem determinar quando é que um sujeito se pode valer do art. 17.º RGPD.

Em 2013, o *Cooperative Cyber Defence Centre of Excellence* da NATO divulgou o *Tallinn Manual*[18], que consiste num compêndio de regras vistas como direito internacional costumeiro, aplicáveis ao ciberespaço e acompanhadas de comentários sobre a sua base legal e possíveis divergências entre os especialistas que as elaboraram[19].

Logo num ponto inicial, afirmam os autores do documento que nenhum Estado pode arrogar soberania sobre a totalidade do ciberespaço. Contudo, constatam também que os Estados podem exercer prerrogativas sobre qualquer ciberinfraestrutura situada no seu território, bem como sobre as atividades associadas a essas infraestruturas[20]. Assim, reconhecem os autores a aplicabilidade do princípio da soberania territorial ao ciberespaço, nos termos do qual um Estado exerce poderes soberanos plenos e exclusivos no seu território[21].

Com a aplicação deste princípio ao ciberespaço, as ciberinfraestruturas situadas no território de um determinado Estado estão sujeitas à soberania territorial desse Estado, pelo que este tem o poder de controlar entradas e saídas do seu território, até de quaisquer formas de comunicação e, transpondo este raciocínio para o nosso estudo, quaisquer tipos de dados[22]. Que conclusões podemos fazer da aplicação deste princípio ao ciberespaço?

---

[18] Schmitt; Michael N. (ed). *Tallinn Manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence*, Cambridge University Press, 2013.

[19] Schmitt, Michael N.. "International Law in Cyberspace: The Koh Speech and the Tallinn Manual" Justaposed, *Harvard International Law Journal,* v. 54, 2012, p. 15.

[20] *Idem*, p. 15 e ss.

[21] *Vide* Acórdão do TPJI, *S.S. Lotus (Fr. v. Turk.),* (ser. A) Nº. 10, 7 de Setembro de 1927, p. 18 e ss.; Acórdão do TPJI, *Free Zones of Upper Savoy and District of Gex (Fr. v. Switz.),* (ser.A/B) Nº. 46, 7 de junho de 1932, p. 166 e ss.; Heinegg, Wolff Heintschel von, "Legal implications of territorial sovereignty in cyberspace", *4th International Conference on Cyber Conflict (CYCON),* 2012, p. 8.

[22] Heinegg, Wolff Heintschel von. "Legal implications of territorial sovereignty in cyberspace", *4th International Conference on Cyber Conflict (CYCON)*, 2012, p. 8 e 11.

A primeira consequência que podemos retirar é a de que ciberinfraestruturas localizadas em locais cobertos pela soberania territorial de um Estado se encontram protegidas contra a interferência dos demais, independentemente da sua pertença ou por quem sejam utilizadas[23].

Aceitando este raciocínio, então parece ser evidente que, não obstante possíveis limitações por parte do corpo normativo internacional, as ciberinfraestruturas e ciberoperações exercidas dentro do território nacional de um Estado (ou da UE, no âmbito das competências que lhe foram atribuídas pelos Estados-Membros) estão sujeitas ao poder regulatório e sancionatório do Estado em causa. Transpondo isto para a realidade do direito ao apagamento de dados, então todos os dados pessoais tratados dentro da UE são, naturalmente, suscetíveis de conduzir à aplicação do art. 17.º do RGPD, por se traduzirem numa ciberoperação efetuada no território europeu.

A segunda conclusão que se retira da aplicação da soberania territorial ao ciberespaço, e a mais decisiva para o presente estudo, está relacionada com a grande abrangência do direito de um Estado a exercer a sua jurisdição sobre ciberinfraestruturas e ciberatividades.

Esta ideia segue o postulado no *Tallinn Manual*, de que um Estado pode exercer a sua jurisdição de três formas distintas: (i) sob agentes que fazem parte de operações cibernáuticas no seu território; (ii) sob infraestruturas do ciberespaço, baseadas no seu território ou (iii) extraterritorialmente, de acordo com o direito internacional. Daqui derivam potenciais bases para o exercício da jurisdição de um Estado, fora da sua circunscrição territorial, sobre operações no ciberespaço, como a nacionalidade do agente, nacionalidade da vítima, violação de normas de direito internacional ou motivos de segurança nacional.

Um outro princípio que permite o exercício da jurisdição de um Estado sobre atos praticados no estrangeiro, consubstancia-se na doutrina dos efeitos, a partir da qual um Estado pode exercer jurisdição sobre um facto que ocorreu no estrangeiro, mas produziu efeitos significativos no seu território[24].

---

[23] *Idem*.

[24] Nas palavras do Advogado-Geral do M. Darmon: "Dois fundamentos da competência dos estados são incontestados em direito internacional: a territorialidade e a nacionalidade. A primeira reconhece competência jurisdicional a um Estado desde que a pessoa ou o bem

2.1.2. O confronto com a extraterritorialidade do apagamento de dados

Com base nestas ideias, estamos em condições de formular o nosso primeiro argumento. Realmente, advém da ordem jurídica internacional a necessidade de o direito da UE cumprir um dos mais basilares princípios da ordem internacional: o princípio da não ingerência nos assuntos internos de Estados terceiros.

Surge então, de forma premente, a necessidade de desenhar o limite entre (i) a legítima aplicabilidade extraterritorial de direitos europeus (como o do apagamento), em função de um âmbito *ratione materiae* que vise salvaguardar direitos previstos na CDFUE; e (ii) a extensão de competências jurisdicionais para dentro de Estados onde tais direitos a salvaguardar não foram soberanamente criados, nem lograram o consenso axiológico-valorativo da respetiva comunidade.

Não é por acaso que o TIJ, em casos como o *Barcelona Traction*[25], impõe a todos os Estados a obrigação de darem provas de moderação e prudência quanto à extensão da competência dos seus órgãos, como bem relembra o Advogado-Geral Darmon, na sua opinião do caso *Ahlström*[26].

Ademais, uma aplicação incondicionada do RGPD a todo o globo poderia fazer grassar práticas de *forum shopping* junto de DPA e tribunais europeus. Por exemplo, como bem teoriza Kuner face aos comandos do caso *Google Spain*, não parecem existir quaisquer razões, à luz do RGPD, pelas

---

em causa nele estejam situados ou que o evento em questão nele se tenha desenrolado (...). A territorialidade, ela mesmo, gerou dois princípios de competência distintos: a territorialidade subjectiva, que permite sujeitar à competência de um Estado os actos que tenham origem no seu território, mesmo que a sua consumação tenha ocorrido no estrangeiro; a territorialidade objetiva, que lhe permite, inversamente, conhecer dos actos cujo início de execução tenha ocorrido no estrangeiro mas cujo cumprimento, pelo menos parcial, ocorreu no seu próprio território.". Heinegg, Wolff Heintschel von. "Legal implications of territorial sovereignty in cyberspace", *Cyber Conflict (CYCON)*, 2012, p. 14 e 15; Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, de 25 de maio de 1988, para. 19 e ss. A análise da Opinião do Advogado-Geral M. Darmon será desenvolvida nos pontos seguintes.

[25] Acórdão do TIJ, *Case Concerning the Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain)*, 5 de fevereiro de 1970.

[26] Ver Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, ECLI:EU:C:1988:258, p. 24.

quais um cidadão chinês que usasse um motor de busca estabelecido nos EUA com uma subsidiária na Hungria não pudesse reivindicar, por meio da agência de proteção de dados húngara, um seu direito ao apagamento contra tal motor de busca por forma a ter os seus dados pessoais eliminados em todo o globo e não só na União[27].

Existe, neste caso, um especial interesse europeu na salvaguarda da privacidade deste cidadão de um Estado terceiro? Existe algum fator suficientemente acutilante de ligação do sujeito ao fórum no qual ele pretende fazer valer os seus direitos? Pelo contrário, este alcançaria o absurdo de, nestes termos, demandar uma entidade americana com base no direito da União não tendo qualquer outra ligação à União que não fosse o uso de um serviço de *internet* igualmente acessível em território europeu; e de, logrando um acolhimento das suas pretensões, eliminar informação que lhe seja relativa não só na União Europeia como em toda a *Internet*.

Com base nestes pressupostos, parece ser mais correta a adoção de uma primeira coordenada genérica definitória da extensão do direito ao apagamento, que sustenta uma interpretação restritiva do art. 3.º, n.º 1 do RGPD quando articulado com o art. 17.º do RGPD: se o único interesse substancial do titular dos dados é o de evitar o acesso à informação de cidadãos de um Estado terceiro sem qualquer conexão à União Europeia, então este não poderá invocar o direito ao apagamento. Flui do que foi dito que, ainda que o RGPD tenha um âmbito de aplicação potencialmente global, a União Europeia só deve proceder à concretização do direito ao apagamento por ele criado naquilo que consistir um interesse substantivo e merecedor de tutela à luz do ordenamento europeu.

Deste modo, o RGPD, por meio do art. 17.º, será aplicável a todas as ações, independentemente da nacionalidade dos sujeitos envolvidos ou do território onde tais ações tenham lugar, que produzam efeitos significativos em espaço europeu, ao serem disruptivos dos valores e direitos fundamentais que a União, através dos arts. 7.º e 8.º da CDFUE, pretende assegurar em matéria de privacidade e proteção de dados.

Procede-se assim à corporização da teoria dos efeitos, delimitadora das competências extraterritoriais dos vários Estados. Este princípio permite aos Estados regular comportamentos que ocorram fora do seu território,

---

[27] Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, 2015, LSE Law, p. 12 e 13.

desde que estes produzam efeitos substanciais nesse mesmo território[28]. E, sem dúvida, a disponibilização de certos tipos de resultados em motores de busca, mesmo que tal processamento afete titulares não europeus ou que se dê fora da UE, pode produzir um efeito substancial em território europeu, pondo em causa objetivos europeus nesta matéria[29].

2.1.3. A teoria dos efeitos aplicada ao apagamento de dados: o auxílio interpretativo do TJ

Não podemos ignorar, contudo, que estes efeitos de que falamos constituem uma realidade imaterial e transfronteiriça, algo que pode ser um óbice à aplicação desta teoria neste campo. Torna-se, nesta altura, urgente convocar alguma jurisprudência europeia, referente a ramos de direito análogos, em que a teoria dos efeitos é pressuposto do exercício de competências normativas por parte das autoridades europeias (neste caso, jurisdicionais). E, neste sentido, pode a aplicação do RGPD beneficiar em muito dos ensinamentos do TJ em matéria concorrencial.

Vejamos, por exemplo, o caso *Ahlström*[30], começando pela opinião do Advogado-Geral Marco Darmon, na sequência da apensação de uma série de processos condenatórios concorrenciais relativos a práticas concertadas no setor industrial da pasta papel, em função da contestação, em todos eles, da competência da União em matéria de aplicação das regras europeias deste ramo de direito a empresas de Estados terceiros.

Ora, com base numa análise à jurisprudência do TJ, à jurisprudência do TIJ e até numa viagem comparativa aos ditames do direito norte-americano em matéria de competência extraterritorial, o Advogado-Geral concluiu que: (i) a jurisprudência do TJ não rejeita a aplicação da teoria dos efeitos em matéria de competência extraterritorial da União; (ii) tal exercício de competência baseada num efeito qualificado manifestado no domínio europeu é conforme às normas e princípios do Direito Internacional; e que

---

[28] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten", *KU Leuven Centre for IT & IP Law*, 2015, p. 23.

[29] *Vide* considerandos 1, 7, 9, 10 e 13 do RGPD.

[30] Acórdão do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, *Ahlstrom Osakeyhtio and Other/Comission*, ECLI: EU:C:1993:120.

(iii) a teoria dos efeitos deveria ser adotada como critério da competência comunitária[31].

Com efeito, é curioso notar que as conclusões do Advogado-Geral se arrimam em conceitos originários da doutrina e jurisprudência norte-americanas, onde é já traquejada, em campos como a responsabilidade civil, a prática de limitar a jurisdição de algum fórum quando a controvérsia ou as partes não apresentam com ele uma conexão suficiente[32]. São convocados conceitos como o da *rule of reason* ou o do *judicial interest balancing* para defender o caráter razoável do exercício de competências pelo qual a União também se deve pautar[33].

Não deixa de ser sintomático do acerto das conclusões de Marco Darmon que o Tribunal tenha seguido o critério de competência por ele proposto, tendo, em decisão posterior, rejeitado os argumentos das empresas de Estados terceiros relacionados com a incompetência da União, com base nesta ideia de que as autoridades da União deveriam impor as regras europeias às empresas de Estados terceiros cujas ações, mesmo que praticadas fora de território europeu, tivessem um efeito qualificado (e, por isso, digno da reivindicação de competência comunitária) no mercado interno, realidade imaterial que não deixa de integrar o conceito de efeitos interterritoriais[34]. É, ainda, de extrema valia estudar a jurisprudência do TJ referente à propriedade intelectual no contexto de motores de busca de fins comerciais, *maxime* o caso que opôs a *L'Oréal* ao *eBay* (Caso *L'Oréal*)[35].

Neste processo era discutida a aplicação do direito europeu às atividades comerciais e de marketing desenvolvidas pela plataforma eletrónica *eBay*

---

[31] Ver Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, ECLI:EU:C:1988:258, para. 14, 27, 53 e 58.

[32] Christopher Kuner advoga, aproveitando tais ensinamentos do ordenamento norte-americano, que: "similar action may be needed to limit the right to suppression", referindo-se à desindexação, num raciocínio que não deixa, no entanto, de se revelar pertinente em sede do direito ao apagamento. *Vide*, igualmente Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 13.

[33] Ver Opinião do Advogado-Geral (Marco Darmon) do TJ, Proc. Apensos 89/85, 104/85, 114/85, 116/85, 17/85 e 125/85 a 9/85, ECLI:EU:C:1988:258, paras. 38, 40, 41 e 48.

[34] *Idem*, paras. 14, 16, 18 e 19.

[35] Acórdão do TJ, Proc. C-324/09, *L'Oréal e o.,* ECLI:EU:C:2011:474.

(que contém um motor de busca de produtos), por forma a apurar se direitos de propriedade intelectual da *L'Oréal* teriam sido violados, algo que fluiria da aplicação das regras europeias[36].

Embora reconheça que o efeito útil das normas europeias seria posto em causa se a sua aplicação fosse precludida pelo simples facto do prevaricador das mesmas operar num Estado-terceiro, e que tal dê força a uma aplicação que não se norteie por barreiras territoriais, o Tribunal deixa claro que o mero facto de a plataforma eletrónica ser acessível em território europeu não constitui base suficiente para a aplicação do direito da União Europeia[37].

Afirma, igualmente, que deve ser feita uma análise casuística da existência de fatores de conexão suficientemente relevantes entre as práticas *sub judice* e o domínio europeu para determinar a aplicação àquelas das regras europeias em matéria de propriedade intelectual[38].

É, assim, míster transpor esta última ideia para o direito da proteção de dados, corporizando outra coordenada genérica da extensão do direito ao apagamento, no contexto da sua sujeição à teoria dos efeitos. Qualquer Estado, e por isso também a União Europeia, quando fazendo cumprir as suas normas no ordenamento internacional, não está munido de qualquer *carte blanche*, devendo sempre assegurar que a pretensão de uma implementação extraterritorial das suas normas é razoável, numa análise casuística[39].

Devem assim as DPA sondar, em cada pretensão de apagamento dos titulares de dados, fatores de conexão do quadro factual de cada processo ao ordenamento europeu, *i. e.*, um efeito do processamento controvertido que seja significativamente disruptivo dos interesses europeus e que, por isso, torne razoável a aplicação das suas normas legais de proteção de dados, nomeadamente, do artigo 17.º, RGPD. Este processo de indagação é mais premente em casos em que tal conexão não é tão clara, como aqueles em

---

[36] Para um maior detalhe do quadro factual, *vide Idem* paras. 26-50.

[37] *Idem*, paras. 63-64.

[38] *Idem* paras. 65-66, onde o Tribunal afirma esta ideia e conclui pela existência de fatores de conexão suficientes entre as atividades do eBay e a UE.

[39] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 23-25.

que o titular dos dados ou a entidade por ele demandada (ou ambos) não sejam europeus[40].

É defendido por alguns autores que um desses fatores de conexão pode ser a harmonização normativa entre os ordenamentos jurídicos relevantes[41]. Por exemplo, se a norma europeia que prevê a possibilidade de apagamento de dados pessoais encontrar uma norma similar, por exemplo, no ordenamento jurídico japonês, tornar-se-á menos problemática uma demanda extraterritorial das entidades europeias. Tal já não será o caso se tal norma não se encontrar replicada, por exemplo, no ordenamento norte-americano.

2.2. As autoridades de proteção de dados no plano global

Suponhamos que o direito ao apagamento de dados assumiria um escopo global de aplicação, desprovido de limites territoriais ou de razoabilidade do exercício da jurisdição da União. Qual seria a legitimidade jurídico-política da União para o aplicar, "criando" autênticos "direitos ao apagamento" em ordenamentos estrangeiros como efeito direto da aplicação de uma norma europeia? Torna-se esta questão ainda mais bizarra se considerarmos a força que uma resposta positiva atribuiria às entidades administrativas encarregadas de fazer cumprir o RGPD: as DPA.

Por um lado, é clara a falta de recursos (humanos e financeiros) destas agências para lidar com o enorme volume de pedidos de apagamento vindos de todo globo, expectável num quadro como o descrito *supra*, o qual é potencialmente catalisador de práticas de *forum shopping*[42]. Se uma DPA se encontrar obstruída com pedidos de apagamento de indivíduos que não apresentem qualquer conexão relevante com a União, como irá lidar efetivamente com aqueles pedidos cujo tratamento consubstancia um interesse substantivo do ordenamento europeu, fruto da clara conexão dos casos ao domínio europeu?

---

[40] Não podemos deixar de sublinhar o cariz meramente indiciário destes fatores face à aplicação *ratione materiae* do RGPD.

[41] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, p. 26 e 27.

[42] Ver *supra*, p. 66.

Por outro lado, se existem requisitos exigentes a ser cumpridos antes de uma DPA de um Estado-Membro aplicar direito da União num outro Estado-Membro, como o TJ avança no Acórdão *Weltimmo*[43], não deveriam existir requisitos ainda mais exigentes no que concerne a extensão dos poderes de uma tal agência em relação a Estados terceiros? E não seria o cumprimento de tais ditames ainda mais imperativo (ou até inibidor da atuação de uma DPA) quando o pedido de apagamento não apresenta qualquer conexão relevante ao Estado-Membro no qual dada DPA opera? O art. 55.º, n.º 1, RGPD diz que as DPA são competentes no território do seu próprio Estado-Membro, algo que exclui liminarmente a sua competência extraterritorial.

Efetivamente, e transpondo as palavras de Kuner do direito à desindexação para o direito ao apagamento, é necessário tornar o âmbito deste direito proporcional à sua aplicabilidade prática, impedindo que se torne tão abrangente ao ponto de se tornar insignificante[44]. É do maior interesse da União Europeia que o direito ao apagamento assuma, no plano global da sua aplicação que a ubiquidade da *Internet* exige, o escopo que, realisticamente e em consonância com os princípios do Direito Internacional, pode, na prática, assumir. Só deste modo se poderá assegurar o seu efeito útil (bem como do regulamento que o encerra) evitando que um instrumento legal com o potencial de inspirar desenvolvimentos extremamente positivos no campo da proteção de dados seja fragilizado pelas críticas daqueles que apontam à União a imposição dos seus valores em jurisdições não-europeias[45].

Fazemos nossas as palavras do Conselho da Europa quando defende que "*as medidas adotadas pelas autoridades estatais europeias no combate a conteúdo e atividades ilegais na Internet não devem resultar num impacto desnecessário e desproporcionado para lá das fronteiras desse Estado*"[46].

---

[43] Acórdão do TJ, Proc. C- 230/14, *Weltimmo,* ECLI:EU:C:2015:639, paras. 56 e 57.

[44] Kuner, Christopher. "EU Judgment on Internet Data Protection and Search Engines", in *Society and Economy Working Papers*, LSE Law, 2015, p. 23.

[45] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 3.

[46] Ver Conselho da Europa, Committee of Ministers to member States on the free, transboundary flow of information on the Internet, CM/Rec(2015)6, de 1 de Abril de 2015.

Cabe, por fim, sinalizar, em matéria já estritamente referente ao direito da proteção de dados, alguns casos em que se descortina a apologia da necessidade de aferição de fatores de conexão relevantes entre o pedido de apagamento e a UE como ponto prévio da aplicação das respetivas normas europeias.

Por exemplo, o GT29 pareceu deixar implícita a necessidade do estabelecimento de limites em relação a quem pode se socorrer do apoio das DPA, ao afirmar que, na prática, estas ir-se-iam concentrar nos pedidos que apresentassem uma conexão clara entre o titular dos dados pessoais e a UE[47]. No entanto, e até por uma questão de honestidade intelectual, não podemos deixar de sublinhar que a ideia transmitida pelo GT29 é tão-somente uma de *prioridade* e não tanto de *exclusividade* da alocação de recursos das DPA aos pedidos que manifestem uma ligação clara com a União; até porque tal afirmação é precedida da asserção de que o artigo 8º da CDFUE reconhece a todos o direito à proteção de dados[48].

Mas aquilo que é uma subliminar referência deste grupo à maneira como os óbices de natureza prática da aplicação deste direito podem acabar por concorrer para a determinação do seu escopo, é posteriormente confirmada por um dos seus membros, a *Agencia Española de Protección de Datos*, no quadro de um pedido de apagamento, efetuado por um cidadão paraguaio, de hiperligações de domínios exteriores à União.

Com efeito, em 2015, a *Agencia Española de Protección de Datos* considerou inadmissível o pedido de apagamento do mencionado cidadão, por considerar que este não mantinha nenhuma vinculação clara com um Estado-Membro[49]. Esta decisão foi judicialmente confirmada em 2017 por um tribunal espanhol, um órgão judicial europeu vinculado à aplicação de

---

[47] Grupo de Trabalho do Artigo 29, *Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment In "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) And Mario Costeja González"*, 26 de novembro de 2014, para. 19; Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"", *KU Leuven Centre for IT & IP Law*, 2015, p. 15.

[48] É utilizada a expressão *"DPA's will focus on claims (...)"*; ao invés de, por exemplo, *"DPA's will only focus on claims"*.

[49] *Agencia Española de Protección de Datos*, Procedimiento Nº: TD/01176/2015, Resolución Nº.: R/01976/2015, p. 8.

direito europeu, o mesmo que realizou o pedido de reenvio para o TJ no Caso *Google Spain*[50].

Ainda que tais decisões (administrativa e judicial) tenham sido tomadas à luz da antiga Diretiva, não deixa de ser elucidativa a afirmação da necessidade de limitar a extensão dos direitos dos cidadãos em matéria de proteção de dados, quando não estão em causa quaisquer interesses relevantes da União.

3. A extraterritorialidade do direito ao apagamento: consequência e modo do apagamento

Todo o raciocínio feito na secção anterior refere-se aos limites de aplicação do direito ao apagamento de dados, proveniente da articulação entre os artigos 3.º n.º 1, e 17.º do RGPD. Porém, todos estes fundamentos concorrem, igualmente, para a determinação do âmbito do apagamento de dados quando as pretensões do seu titular são acolhidas.

Ora, encontra-se presentemente diante do TJ um processo prejudicial que opõe a *Google Inc.* e a CNIL[51]. Esta, face a pedidos fundamentados no direito à supressão de uma hiperligação, resultante do acórdão *Google Spain*, exigiu à *Google Inc.* que suprimisse os resultados referentes aos dados em causa, não apenas dos domínios europeus (como a *Google.fr*), mas também dos domínios exteriores à UE, como a *Google.com*, de modo a salvaguardar o efeito útil deste direito.

Apesar de a Google ter apresentado recurso, a CNIL reiterou a sua posição, insistindo na supressão de resultados a nível global, já que, caso contrário, o direito a ser esquecido poderia ser facilmente contornado e esvaziado de efeitos práticos[52]. Não tendo a *Google* acatado a ordem, a autoridade francesa iniciou um processo judicial contra a empresa.

---

[50] *Vide* http://cyberlaw.stanford.edu/blog/2017/12/right-be-forgotten-and-global--desindexação-some-news-spain (acedido a 09/03/2019)

[51] Acórdão do TJ, C-507/17, pedido de decisão prejudicial apresentado pelo *Conseil d'État* (França) em 21 de agosto de 2017.

[52] No mesmo sentido, entre nós, Marques, João. "Direito ao Esquecimento: A aplicação do Acórdão Google pela CNPD", in *Fórum de Proteção de Dados*, n. 3, 2016, p. 55.

Nesta senda, a *Google* implementou um sistema de bloqueio geográfico, alargando o suprimento de resultados a qualquer extensão do motor de busca, desde que tal extensão esteja a ser operada por um utilizador situado no Estado-Membro da UE onde o pedido foi aprovado[53].

A CNIL, contudo, considerou a medida insuficiente para garantir a proteção dos utilizadores franceses, impondo uma coima de €100.000 à *Google*[54]. Afirmou que o suprimento dos resultados com base num sistema de geolocalização seria insatisfatório, já que os resultados continuariam acessíveis fora de França. Por outro lado, e mais decisivamente, seria igualmente possível aos utilizadores contornarem este sistema, utilizando um endereço estrangeiro, mesmo estando em território francês[55].

Insatisfeita, a *Google* recorreu para o *Conseil d'État*, estando, à data do presente estudo, o processo suspenso face a um reenvio prejudicial para o TJ[56].

As três questões prejudiciais colocadas ao Tribunal, lidas de acordo com o RGPD conforme nos propusemos fazer, podem unir-se sob a seguinte questão de fundo: que extensão deve ser dada ao direito ao apagamento dos dados? Deve este levar a um apagamento global e absoluto dos dados controvertidos; deve tal apagamento ser restringido aos domínios europeus de um motor de busca (*vide Google*.pt ou *Google*.es); e ainda, e independentemente da resposta às questões anteriores, deve ser adotado, pelos motores de busca, um sistema de *geoblocking* em articulação com um dos anteriores modelos?

Qual a opção que deve tormar o TJ à luz do RGPD?

---

[53] Kulk, Stefan; Borgesius, Frederik Zuiderveen. "Privacy, freedom of expression, and the right to be forgotten in Europe", in *Cambridge Handbook of Consumer Privacy*, 2017, p. 29 e 30. Ver, igualmente, *infra,* Ponto 4.3.

[54] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000032291946&fastReqId=273825503&fastPos=1 (acedido a 09/03/2019)

[55] *Idem*.

[56] Acórdão do TJ, Proc. C-507/17, pedido de decisão prejudicial apresentado pelo *Conseil d'État* (França) em 21 de agosto de 2017; Lomas, Natasha. "Google's right to be forgotten appeal heading to Europe's top court", *TechCrunch*, 2017, p. 21.

3.1. Apagamento global

Começando pela primeira pergunta feita ao TJ, relativa ao alegado escopo global do apagamento de dados, teremos de regressar ao Direito Internacional e averiguar se tal abordagem não interfere com o princípio da não ingerência nos assuntos de Estado terceiro, ou seja, se é permitida à luz da soberania territorial no ciberespaço.

De facto, aquando de um apagamento de informação na *Internet*, entramos novamente no ciberespaço, pelo uso de meios eletrónicos e através de redes interdependentes e conectas. Assim sendo, para que o apagamento seja global, teremos de responder a uma questão de vital importância: poderá a UE, respeitando as normas e princípios do Direito Internacional, exigir aos motores de busca o apagamento de informação em domínios não europeus?

Primeiramente, podemos vislumbrar que as estruturas que acedem ao ciberespaço (por exemplo, computadores pessoais) e, neste caso, a um motor de busca, são objeto do poder soberano do respectivo Estado onde se localizam. Ora, conforme a teoria da soberania territorial, pode um Estado criar e aplicar regras às ciberinfraestruturas que se encontrem no seu território. Por exemplo, os EUA podem regular o acesso dos computadores situados no seu território, e a UE poderá regular o acesso dos computadores localizados na UE.

Por outro lado, não são só as ciberinfraestruturas situadas num certo Estado que são alvo da soberania desse Estado, mas também as ciberopeações que ocorram no seu território. O que é, então, uma ciberoperação? Tal conceito prende-se com a criação, modificação, armazenamento e transmissão de informação, através do espectro eletromagnético, em conjugação com aparelhos eletrónicos[57]. Assim sendo, qualquer tipo de transmissão de informação entre uma infraestrutura, situada num Estado terceiro, que suporte um motor de pesquisa e, por exemplo, um computador pessoal situado na UE (ou outra qualquer ciber-infraestrutura), será merecedor de poderes soberanos da União[58].

---

[57] Kuehl; Daniel T.. "From cyberspace to cyberpower: Defining the problem", in *Cyberpower and national security*, National Defense University Press, 2009, p. 28 e 29.

[58] Por esta razão se justifica, por exemplo, que o acórdão Google Spain não infrinja o Direito Internacional. Muito embora o tratamento de dados tenha sido feito nos EUA, os dados

Já as situações contrárias, em que a UE exerce poderes soberanos sobre as ciberinfraestruturas situadas em Estado terceiros, que conduzam ciberoperações sem interferência no território europeu, parecem ser mais difíceis de conceber, pelo facto daquelas não se encontrarem no espaço europeu, nem estas se intersetarem com a UE. Encontramos, assim, como grande obstáculo a um tal apagamento de dados o princípio da não ingerência em assuntos de Estados terceiros.

Contudo, e como concluído anteriormente, poderá um Estado aplicar as suas normas a entidades ou atividades localizadas fora do seu território, em certas situações, *maxime* de acordo com a teoria dos efeitos. Cabe assim perguntar: será que o armazenamento, criação e modificação de informação, num Estado terceiro, bem como a transmissão de informação, através da *Internet*, entre Estado terceiros poderão ser submetidos ao braço normativo europeu, com base nestes princípios?

Ora, uma resposta a esta questão não é, de todo, fácil. Situações podem existir em que, por exemplo, por motivos de pura segurança nacional, é argumentável que um Estado possa exigir o apagamento global de informação disponível na *internet*, mesmo que essa não chegue a ser transmitida no seu território, até face ao dever de toda a comunidade internacional de evitar que as suas ciberinfraestruturas e ciberoperações causem danos a outros Estados.

Contudo, estas situações são excepcionais, pelo que, por regra, dar-se-á uma resposta negativa à anterior questão. Realmente, se as ciberoperações não penetram no território europeu, nem estão as ciberinfraestruturas que as conduzem sob o domínio de aplicação do direito da UE, então só se estiver em causa uma situação que justifique a invocação dos outros princípios de soberania para lá da territorialidade se poderá arguir a possibilidade de a UE exigir o apagamento global. Assim sendo, exigir um apagamento global como regra geral da aplicação do art. 17.º do RGPD violaria os princípios da independência e igualdade entre Estados e o da não ingerência em assuntos internos de Estados terceiros.

Por último, também poderão estar em causa problemas na compatibilização entre direitos fundamentais de Estados diferentes. Realmente, grande parte dos Estados não europeus (*maxime* EUA) ainda não consagraram um

---

eram transmitidos em espaço europeu, pelo que a União Europeia podia aplicar o normativo de proteção de dados a essa ciberoperação.

direito ao apagamento de dados, pelo que, se se recorrer ao apagamento global, estar-se-á a eliminar informação sem que tal mecanismo esteja previsto no ordenamento jurídico do Estado em causa. Pode até ser colocada a seguinte pergunta: será que a aplicação de requisitos europeus a uma escala global afeta, em grande medida, a liberdade de expressão em Estados terceiros?

3.2. Apagamento baseado no domínio

A segunda metodologia de apagamento de dados possível é a baseada nos domínios utilizados para as pesquisas realizadas num motor de busca (uma *domain-based erasure*). Esta abordagem ao processo de apagamento permite modificar os resultados de uma pesquisa em função da extensão utilizada para aceder ao motor de busca (por exemplo, se esta for .pt, .es, .fr, .us ou .com)[59], ou seja, proceder a operações de apagamento em relação às versões europeias do motor de busca e não o fazer em relação às demais.

Na senda do caso *Google Spain* e da operacionalização do direito à desindexação, esta metodologia fundada no domínio foi advogada pelos vários motores de busca demandados por titulares de dados pessoais, com destaque para a *Google Inc*. Esta decidiu limitar a remoção de resultados de busca decorrente da aplicação do direito europeu de proteção de dados às suas versões europeias, permanecendo inalteradas as restantes, como por exemplo a *Google.com*.

Esta solução mereceu, de imediato, críticas das autoridades europeias de proteção de dados, pela ausência de medidas suplementares de limitação de acesso a dados cuja supressão fosse ordenada[60]. Foi por estas entidades observado que o efeito útil da supressão de uma hiperligação seria posto em causa se dados removidos dos domínios europeus de um dado motor de busca pudessem ser consultados através de uma simples mudança da extensão utilizada para aceder a tal plataforma de

---

[59] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten", *KU Leuven Centre for IT & IP Law,* 2015, p. 16 e ss.

[60] *Idem*, p. 4.

pesquisa[61-62]. Esta mesma posição foi seguida por inúmeros tribunais nacionais, como por exemplo o *Tribunal de Grande Instance de Paris* que, num caso que opôs dois cidadãos franceses à *Google*, rejeitou tal abordagem baseada no domínio, considerando-a insuficiente[63].

Não podemos deixar de seguir tais opiniões, transpondo-as para o contexto do apagamento de dados. Uma *domain-based erasure* encontra como óbice a sua (in)eficiência, ao não permitir assegurar o efeito útil de um apagamento de dados, em relação a qualquer pesquisa realizada por qualquer sujeito, constatada a facilidade que o utilizador normal tem de mudar a extensão do *site* do motor de busca, assim consultando informação removida por meio deste modelo de apagamento. Com efeito, a proteção de qualquer conjunto de dados pessoais nunca poderá ser eficiente e completa se os expedientes utilizados para a assegurar forem facilmente contornáveis, como é o caso de um método exclusivamente baseado no domínio[64].

3.3. Apagamento híbrido fundado na geo-localização: o "modelo Youtube*"*

Chegamos, por fim, à última metodologia de apagamento a discutir que se compatibiliza com a técnica do "bloqueio geográfico", ou seja, que conforma os resultados de uma pesquisa (revelando ou não dados cujo

---

[61] Grupo de Trabalho do Artigo 29; *Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment In "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) And Mario Costeja González"*, 26 de novembro de 2014, para. 20.

[62] Por exemplo, bastaria a um cidadão português que não conseguisse, através da google.pt aceder a uma notícia sobre M. González (em função da supressão de links ordenada no processo Google Spain) mudar a sede da sua pesquisa para a google.com para consultar tal informação e esvaziar o efeito da supressão de hiperligações já realizada.

[63] "It is in vain that Google France asks (...) that the injunction be limited to links on Google.fr, seeing as it does not establish the impossibility to connect from French territory to other domain name extension of Google's search engine.", tradução inglesa de um extrato retirado do Acórdão do Tribunal de Grande Instance de Paris, *M. et Mme X et M. Y v. Google France*, 16 de setembro de 2014, disponível em http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291. (acedido a 09/03/2019)

[64] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten"*, KU Leuven Centre for IT & IP Law*, 2015, p. 4 e 5.

apagamento foi ordenado) com a localização do IP utilizado para a fazer[65]. Deixamos já patente que este é o método por nós preconizado como consequência, por defeito, de um pedido para apagamento bem-sucedido. A nossa tese baseia-se na convicção de que esta abordagem dá resposta às falhas apontadas quer ao apagamento global quer ao apagamento baseado no domínio, surgindo como complemento imprescindível a este último.

Em primeiro lugar, um apagamento mediante *geoblocking* permitiria (regra geral) um exercício razoável e moderado da competência normativa da UE em direção a Estados-terceiros onde o direito ao apagamento não existe, assim cumprindo todos os crivos do Direito Internacional Público, da jurisprudência da União e dos pareceres das DPA europeias já avançados anteriormente, que tornam criticável uma extensão global do apagamento de dados[66].

Ora, tendo, por via da regra, a UE apenas a possibilidade de controlar ciberoperações que interfiram com o seu território, então, através do *geoblocking* tal seria respeitado, permitindo às autoridades europeias estender a sua jurisdição sobre processamentos externos e, ao mesmo tempo, confinar o impacto da sua atuação ao espaço europeu[67]. De facto, a partir do momento em que dada informação seja transmitida, através de qualquer domínio, para uma ciberinfraestrutura situada na UE, terá esta o poder de aplicar as suas normas a essas transmissões de dados. Caso estas não passem pelo espaço europeu então, por via da regra, tal aplicação parece violar o Direito Internacional. Nesta senda, o *geoblocking* apresenta-se como um meio termo razoável, em que a UE apaga os dados de todos os domínios acedidos através de uma ciberinfraestrutura situada na UE, sendo respeitados os princípios internacionais da soberania estatal.

Em segundo lugar, este método cumpriria a exigência de uma fórmula eficiente (porque onerosa de contornar) de garantia dos direitos dos titulares de dados pessoais, formulada pelas DPA e tribunais na crítica à *domain-based approach* posta em prática pela *Google*. E, neste campo, não

---

[65] Um Endereço de Protocolo da Internet (endereço IP), é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utilize a Internet para comunicação. Um endereço IP serve, sobretudo, uma função de localização do seu respetivo dispositivo.

[66] Ver, genericamente, Capítulo 3 deste artigo.

[67] Alsenoy, Brendan van; Koekkoek, Marieke. "The extra-territorial reach of the EU's "right to be forgotten", *KU Leuven Centre for IT & IP Law*, 2015, p. 19.

podemos ignorar que as técnicas de *geoblocking* utilizadas pela *Google* foram, de facto, consideradas inadequadas porque ineficientes para garantir o efeito útil das normas europeias de proteção de dados (na instância do direito à desindexação)[68]. Cumpre sinalizar que a abordagem deste motor de busca consistiu numa utilização cumulada de um suprimento de informação em função do domínio e do denominado *soft geoblocking*.

Ora, a abordagem da *Google* faz com que, tendo sido ordenado um suprimento de informação no espaço europeu, quaisquer utilizadores a operar a partir de tal território que queiram consultar domínios exteriores à União (*i.e. Google.com*) são automaticamente redirecionados para a versão do motor de busca específica do país onde se localiza o IP da infraestrutura utilizada na pesquisa (como um computador pessoal)[69]. O *geoblocking* presente neste modelo corresponde a este redirecionamento, mas é facilmente contornável visto que podem os utilizadores reverter tal procedimento: (i) clicando numa opção disponibilizada de "mudar para *Google.com*"; ou (ii) voltando a escrever a versão *.com* do motor de busca na barra de pesquisa.

Tal facilidade de contornar este expediente de geo-localização valeu-lhe o epíteto de *soft geoblocking*[70], por oposição ao *hard geoblocking*, em que tal possibilidade de reverter a filtragem de resultados de busca baseada na localização geográfica de quem os pretende produzir não existe. É um tal modelo de *hard geoblocking* aquele cuja transposição para a realidade do apagamento de dados defendemos, cumulado com as outras abordagens acima explicadas, como passamos a descrever.

Quando seja realizado um apagamento de dados, este restringir-se-á, por princípio, ao espaço europeu. Como? Ainda que não detalhando as vicissitudes tecnológicas que encerrariam tal operação (ao pretendermos somente focar as questões jurídicas da temática subjacente), não podemos deixar de reconhecer que a mesma implicaria, com a maior das probabilidades, uma alteração da estrutura de funcionamento dos motores de busca no processo de armazenamento e tratamento de dados, uma vez que exigiria a separação dos servidores de indexação utilizados para o espaço

---

[68] *Idem*, p.15.

[69] *Idem*, p.18.

[70] Outra expressão possível para designar tais realidades é *soft geofiltering tools*.

europeu e fora dele[71]. Uma vez tendo procedido a tal apagamento, os resultados modificados em conformidade com a legislação europeia seriam disponibilizados exclusivamente em domínios europeus (em articulação com a *domain-based approach*), domínios esses que seriam os únicos. Estes, tendo sido identificada a sua localização, não conseguiriam ter acesso, por nenhuma das vias possíveis acima identificadas, às versões não-europeias do motor de busca usado.

Semelhantes abordagens são realizadas em plataformas como o *Youtube* ou a *Comedy Central*, em que alguns dos seus conteúdos só estão disponíveis para utilizadores americanos, estando os restantes utilizadores – cuja geolocalização extravase aquele âmbito – impedidos de o consultar ou de contornar o seu suprimento.

Um óbice significativo a estas técnicas não deixa de ser a impossibilidade de uma completa eficácia das mesmas, que podem ser contornadas, por exemplo, através da utilização de *proxy servers* que obnubilem o IP utilizado numa pesquisa. No entanto, é nossa convicção de que a eficácia destas técnicas não implica uma *impossibilidade de circunvenção*, mas antes uma *onerosidade de circunvenção*. Fazendo nossas as palavras de Schultz, um expediente informático nesta matéria será eficiente se tornar a ação que visa evitar substancialmente mais difícil de executar, onerando significativamente quem a deseje levar a cabo[72]. Tal ónus parece-nos existir na necessidade de utilização de um *proxy server*, uma vez que este é uma ferramenta não conhecida pelo utilizador médio, que é aquele que não possui conhecimentos especiais de informática.

Em suma, o modelo acima descrito oferece o complemento necessário à *domain-based approach* por forma a concretizar o art. 17.º do RGPD no mundo da *Internet*, que tanto exige em matéria de conformidade e coordenação interjurisidicional. Deve, por isso, constituir o modelo-regra aquando da aplicação do RGPD. Não podemos deixar, no entanto, de avançar que este

---

[71] Muito provavelmente, funcionando em *data centers* (locais onde estão concentrados os sistemas computacionais de uma qualquer empresa, como por exemplo, sistemas de telecomunicações ou de armazenamento de dados) exclusivamente para operações dentro da UE.

[72] Schultz; Thomas. "Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", in *European Journal of International Law*, v. 19, n. 4, 2008, p. 822.

modelo não pode deixar de contemplar exceções em que um apagamento global se justifica quando seja a única forma de assegurar o efeito útil do direito em análise.

3.4. A opinião do advogado-geral M. Szpunar

No âmbito do processo C-507/17 (Google v. CNIL), foi muito recentemente divulgada a opinião do Advogado-Geral M. Szpunar sobre a extensão territorial do direito à desindexação, cujas conclusões podemos transpor para o presente estudo, muito embora se baseiem na interpretação da Diretiva 95/46/EC[73].

Como ponto de partida, afirma o Advogado-Geral que nem o art. 4.º da Diretiva nem o Acórdão *Google Spain* tratam especificamente a questão do âmbito territorial do direito à desindexação, ainda que delimitem o âmbito territorial do diploma no qual este se insere. Estando estas orientações vertidas no art. 3.º RGPD, não se nos afigura nenhuma razão para não transpor, também, este raciocínio para o direito ao apagamento (art. 17.º RGPD)[74].

Assim, considera o Advogado-Geral que, aquando da definição da extensão territorial do direito à desindexação, devem ser distinguidas as buscas, conforme sejam feitas dentro ou fora da EU. Em relação às segundas, não devem os respetivos resultados ser afetados pela supressão de hiperligações[75]. Neste sentido, propõe um modelo em que os motores de busca não têm de levar a cabo a supressão em todos os seus domínios, afastando, por isso, uma extensão global do direito à desindexação[76]. No entanto, afirma que, uma vez efetuada a desindexação nas versões europeias de um dado motor de busca, devem ser adotadas todas as medidas necessárias para assegurar a efetividade de tal direito, nomeadamente através do *geoblocking*[77].

---

[73] Opinião do Advogado-Geral (M. Maciej Szpunar) do TJ, Proc. C-507/17, *Google*, ECLI:EU:C:2019:15.

[74] *Idem*, para. 45.

[75] *Idem*, paras. 45 e 46.

[76] *Idem*, paras. 62, 63 e 79.

[77] *Idem*, paras. 71, 74 e 78.

Para fundamentar as suas conclusões, o Advogado-Geral argumenta que (i) uma desindexação global seria desconforme ao Direito Internacional Público[78] e que (ii) poderia abrir um precedente a práticas de restrição de acesso à informação, nomeadamente por parte de regimes autoritários[79].

Como é fácil de observar, a proposta do Advogado-Geral vai de encontro ao modelo de apagamento híbrido fundado na geolocalização defendido no presente artigo, ainda que se refira ao direito à desindexação. No entanto, não nos parece incorreto aplicar a mesma lógica ao direito ao apagamento de dados.

Por fim, o Advogado-Geral equaciona a possibilidade de, em casos excecionais, conferir à desindexação um âmbito global, à luz do que já é prática quanto a atividades exteriores à UE que afetem o mercado interno europeu. No entanto, pela imaterialidade inerente à Internet, considera difícil efetuar uma analogia entre ela e o mercado interno, cujas fronteiras estão já estabelecidas[80]. No nosso entender, tal analogia será possível para plenamente aplicar a teoria dos efeitos ao apagamento de dados, se recorrermos às teses da soberania no ciberespaço já por nós abordadas *supra*.

Conclusão

Cumpre, por fim, sistematizar as soluções defendidas no presente artigo, assentando tal raciocínio no normal *ictus* de um pedido para o apagamento de dados.

Primeiramente, devem as DPAs avaliar, caso a caso, se o apagamento de dados requerido corresponde a um interesse significativo da UE, quando comparado com os interesses de outros Estados terceiros com os quais a querela *sub judice* se relacione. Tal acontecerá se uma ciberoperação for realizada na União ou, tendo sida realizada fora dela, tenha um efeito manifestamente disruptivo no ordenamento europeu em matéria de proteção de dados. Se não se verificar esta conexão relevante do pedido ao fórum europeu, então tal demanda não deve ser admitida perante as DPAs.

---

[78] *Idem*, paras. 47 a 49.

[79] *Idem*, paras. 60 e 61.

[80] *Idem*, paras. 48 a 53.

Se, pelo contrário, tal ligação ao ordenamento europeu se verificar, deve o apagamento proceder e devem as autoridades atender a uma segunda camada de compatibilização de interesses, as relativas à extensão extra-europeia do apagamento. Por defeito, consideramos que em relação à informação disponibilizada fora da União prevalecerá o interesse do Estado terceiro em mantê-la acessível aos seus cidadãos. Além do mais, o apagamento global tem como obstáculo direto a sua difícil compatibilização com o princípio da não ingerência em assuntos internos de outros Estados.

Assim, num confronto teórico entre o apagamento global e o baseado nos domínios, é o segundo modelo aquele que permite à União controlar condutas externas de tratamento de dados sem interferir na soberania de Estados terceiros. Mas este modelo, por si só, mostra-se ineficaz na proteção dos direitos fundamentais dos titulares de dados. Nesse sentido, será de aplicar um modelo híbrido fundado num *hard geoblocking*, nunca fugindo à possibilidade de arguir um apagamento global, quando os interesses da UE se sobreponham àqueles de Estados terceiros no que diz respeito ao apagamento extraterritorial de dados de um certo titular.

Deste modo, pode a UE assegurar a verdadeira eficácia das disposições do RGPD, mais concretamente do seu art. 17.º, através de um exercício de competências jurisdicionais – dos tribunais e DPA – moderado e razoável no espaço internacional que, por não se pretender estender até onde não terá a devida legitimidade (sempre atento às nuances da natureza global da *Internet*), se torna incomparavelmente mais eficaz.

Assuring Compliance of European Smart Tourist Destinations with the Principles of the General Data Protection Regulation: a roadmap* *

Manuel David Masseno***
Cristiana Santos****

---

* Paper accepted, following a Call for Papers, and presented at the *2nd UNWTO World Conference on Smart Destinations*, convened by the United Nation World Tourism Organization and the Government of the Kingdom of Spain, at Oviedo, the 26th June 2018.

** This paper was drafted within the framework of the Research Project: "*Big Data, Cloud Computing* y otros retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico" – DER2015 – 63595 (MINECO/FEDER). Coordinated by Professor Apollònia Martínez Nadal at the *Universitat de les Illes Balears*, Spain.

*** Professor Adjunto no Instituto Politécnico de Beja, onde também integra a Coordenação do Laboratório UbiNET – Segurança Informática e Cibercrime e do Mestrado em Engenharia de Segurança Informática. Membro do Grupo de Estudos Temático em Direito Digital e *Compliance* da FIESP – Federação das Indústrias do Estado de São Paulo, Brasil, desde 2016. Investigador no IJI – Instituto Jurídico Interdisciplinar da Faculdade de Direito da Universidade do Porto, desde 2005, Investigador no Projeto I+D "*Big Data, Cloud Computing y otros nuevos retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico*" (DER2015-63595-R MINECO/FEDER), coordenado pela *Universitat de les Isles Balears*, desde 2016. Assessor Jurídico Independente no Projeto da União Europeia (Horizonte 2020) PoSeID-on – Protection and control of Secured Information by means of a privacy enhanced Dashboard (ID: 786713), desde 2018.

**** Mestre em Direito dos Contratos e da Empresa pela Universidade do Minho (2012), Doutora em Direito, Ciência e Tecnologia pelo *Joint International Doctoral Program* (LAST-JD) – ERASMUS MUNDUS, das Universidades de Bolonha, Turim, Luxemburgo e Autónoma de Barcelona, e em Informática, pelas Universidades de Bolonha e do Luxemburgo (2017). Investigadora colaboradora no Centro de Investigação em Justiça e Governança – JusGov da Universidade do Minho, desde 2013; Advogada, desde 2011.

Abstract: This paper aims to provide a consistent answer to the concerns regarding privacy and data protection within the framework of Smart Tourism Destinations (STD) that tourism science has given rise to, given the applicability of the new General Data Protection Regulation of the EU (GDPR). Our main result provides a roadmap for compliance of STD design and management with the core principles embodied in the GDPR, providing guidelines both for public and private sectors and for other stakeholders, namely for citizens-tourists. With this work we intend to help achieve fully privacy-compliant STD, in Europe and elsewhere.

Keywords: *Privacy and Data Protection, GDPR, Regulation, Smart Tourism Destinations*

Resumo: Este estudo pretende dar uma resposta consistente às preocupações relativas à privacidade e à proteção de dados no contexto dos Destinos Turísticos Inteligentes (DTIs), as quais foram postas em evidência pela ciência do turismo, tendo em mente o novo Regulamento Geral sobre Proteção de Dados da UE (RGPD). O nosso principal resultado consiste em enunciar um esboço de roteiro para aferir da conformidade da conceção e gestão dos DTIs com os princípios fundamentais do RGPD, facultando orientações tanto ao setor público quanto ao privado e a outros interessados, como os cidadãos-turistas. Com este trabalho pretendemos ajudar a alcançar uma plena conformidade das STDs com a privacidade e a proteção de dados, na Europa e não só.

Palavras-chave: *Privacidade e Proteção de Dados, RGPD, Regulação, Destinos Turísticos Inteligentes*

Introduction

STD are an offspring of the technological foundations of *Smart Cities*. They benefit from the interplay between other technological environments based on the IoT and the *Cloud*, as enabled by *Big Data Analytics*. However, the connections between STD and Privacy & Data Protection did not receive significant attention within legal research[1],

[1] For the legal theoretical framework of this paper, see our recently published articles, such as Masseno, Manuel David; Santos, Cristiana. "Between Footprints: Balancing Environmental Sustainability and Privacy in Smart Tourism Destinations", in *Unitedworld Law Journal*, v. 1-II, 2017, p. 96-118, accessed 30/07/2018 <https://www.unitedworldschoollawjournal.com/wp-content/uploads/2018/05/Between-Footprints-Balancing-Environmental-

even if it was perceived and identified as an overlooked issue by tourism science[2].

Basically, these technology-enhanced tourism services allow tourists to get more from their travel and helps them to fulfil the experiential potential of their destination.

However, ICT embedded within STD also permit the collecting and analysis of large amounts of data (for example, to enable the identification of attitude patterns and to predict the behavior of tourists or travelers). This is achieved by identifying their potential needs and desires even at an unconscious level. Hence, these experiences are achieved through intensive personalization, context-awareness and real-time monitoring, which involve processes of information management that entail legal risks, demanding a careful analysis of the data protection framework. As a large spectrum of user-generated content processed in a STD concern personal data and human interaction, there is a direct impact on individuals and their rights regarding the processing of personal data.

Moreover, the application of the GDPR, which came into effect on 25 May 2018, renders urgent a review of the current conceptions and practices regarding privacy concerns STS to ensure compliance.

Nevertheless, while realizing the benefits of using big data analytics and being a competitive STD, addressing data protection issues supports good practice in information governance that organizations utilizing STD should closely assess. Therefore, data protection compliance should be

---

Sustainability-and-Privacy-in-Smart-Tourism-Destinations-by-Manuel-David-Masseno-and-Cristiana-Santos-1.pdf,> and Masseno, Manuel David; Santos, Cristiana. "Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations", *MediaLaws – Rivista di Diritto dei Media*, 2018, n. 2, p. 251-266, accessed 30/07/2018 <http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of--smart-tourism-destinations/>.

[2] Namely, Anuar, Faiz I.; Gretzel, Ulrike. "Privacy Concerns in the Context of Location-Based Services for Tourism", in *ENTER 2011 Conference. Accessibility of ICTs and Accessible Travel Information*, Innsbruck, Austria, 2001, accessed 30/07/2018 <http://agrilifecdn.tamu.edu/ertr/files/2013/02/13.pdf>; Buhalis, Dimitrios; Amaranggana, Aditya. "Smart Tourism Destinations", *Information and Communication Technologies in Tourism 2014 – Proceedings of the International Conference in Dublin, Ireland*, Heidelberg: Springer, 2014, pp. 553-564; or Gretzel, Ulrike; Sigala, Marianna *et al.* "Smart tourism: foundations and developments", *Electronic Markets*, v. 25, n. 3, 2015, p. 179–188.

an enabler of the success of STD and not a regulatory or administrative burden.

The paper is organized as follows. Section 2 outlines some of the most important risks attributable to STD regarding privacy and data protection. Section 3 describes the obligations of the organizations processing personal data, according to the GDPR[3], which constitute the current basis of the EU-wide legal obligations regarding privacy and data protection. Section 4 refers to the compliance tools which confirm to the above-mentioned legal obligations. Section 5 concludes the paper.

1. The Risks of Smart Tourism Destinations for Privacy and Data Protection

In this section we explain some of the potential risks STD technologies entail for privacy and data protection. As is increasingly appreciated, the use and combination of advanced techniques of *Big Data Analytics*, which include machine learning, data mining techniques, etc., enhance the common risks to privacy and data protection. The following are enhanced when information (*e.g.* mobility data) is connected and matched with data from other sources of publicly available information (e.g., *Facebook* or *Twitter* postings, reviews at *Booking* or at *TripAdvisor*, blogs entries, etc.) and analysis revealed users' social interactions and activities, as is the case with smart tourist travel cards.

1.1. Identification and re-identification of individuals from allegedly anonymized or pseudonymized data

These concerns stem from the fact that integrating large collections of data from distinct sources of available tourism datasets, even with

[3] Regulation (EU) 2016/679, of the EP and of the Council of 27/04/2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), accessed 30/07/2018 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG>.

apparently innocuous, non-obvious or anonymized resources, may enhance a jigsaw of indirect correlation of identification and re-identification; this scenario could escalate if massive information resources via the web are available[4]. Thereby, personal information set through re-identification intrinsically conforms with legal requirements, as identification not only means the possibility of retrieving a person's name and/or address, but also includes potential identifiability by singling out, *linkability* and inference[5].

As data collected by the ubiquitous computing sensors is, in principle, personal data[6] or personally identifiable information, the processing of non-sensitive data can lead, through data mining, to data that reveals personal or sensitive information, thus blurring the conventional categories of data.

1.2. Covert profiling of individuals and non-transparency of the processing

Profiling is an important feature in tourism destinations. Tourism service providers are adapting their approach to service by meeting the personalized expectations of customers. Data-processing scenarios collect user's input and feedback which are used to build fine-grained premium services and recommender systems in the form of trail packages. The richer the user profile, the higher the temptation for operators to target a user with unsolicited advertising or to engineer a pricing structure

---

[4] ART 29 WP – Article 29 Working Party of the European Union: Opinion 7/2003, on the re-use of public sector information, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf>; Opinion 3/2013, on purpose limitation, accessed 30/07/2018<http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>; and, Opinion 6/2013, on open data and public-sector information (PSI) reuse, accessed 30/07/2018<http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf>.

[5] ART 29 WP Opinion 05/2014, on anonymization techniques, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

[6] ART 29 WP Opinion 4/2007, on the concept of personal data, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>, consulted on 15/06/2018.

designed to extract as much surplus from the user as possible[7]. Notably, "[...] analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behavior patterns."[8]. However, as a norm, the GDPR prohibits automated individual decision-making that significantly affect individuals in Art. 22 (1).

Indeed, development of consumer-tourist automated profiles, facilitated by Big Data Analytics, can *significantly affect* data subjects[9]. Covert profiling, in certain cases, may lead to unintended consequences: i. when based on incomplete data, profiling can lead to false negatives, depriving individuals from benefits that they would be entitled to; ii. the so called, "*filter bubbles*" effect, according to which data subjects will only be exposed to content which confirms their own preferences and patterns, without any door open to serendipity and casual discovery; iii. isolation and/or discrimination.

Besides, within a STD, machine learning decisions and profiling can lead to direct or indirect discrimination through the exclusion/denial of services/goods (e.g. denial of insurance, exclusion from the sale of tourist services or high-end products, shops or entertainment complexes of certain profiles of tourists and even decisions that impact upon health, creditworthiness, recruitment, insurance risk, etc). It can even lead to discrimination in relation to essential utilities for those unwilling to share personal data. As indicated, tourists may be discriminated against if they belong to a certain social group, but also this categorisation might be based on factors, identified by the analytics, that they share with members of that group. Therefore, to ensure a fair and transparent processing (as determined by the principle of fairness and transparency), automated

---

[7] ENISA – European Networks and Information Security Agency. 2015 Report on Privacy and Data Protection by Design – from policy to engineering, accessed 30/07/2018 <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport>, .

[8] ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

[9] EDPS – European Data Protection Supervisor. Opinion 3/2015, Europe's big opportunity, EDPS Recommendations on the EU's options for data protection reform, accessed 30/07/2018 <https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_en.pdf>.

decisions should take account of all the circumstances concerning the data and not be based on merely de-contextualized information or on data processing results[10]. Moreover, the data controller should find ways to build discrimination detection into their machine learning systems, to prevent inaccuracies and errors being assigned to labeled profiles, as referred in Recital 71 of GDPR[11].

1.3. Repurposing of data

Data analytics can mine data for new insights and find correlations between apparently disparate datasets. Hence, automatic capture of big data can be frequently reused[12] for secondary unauthorized purposes, profiling, or for abusive marketing activities, undermining the purpose specification principle, which states that the purposes for which data is collected must be specified and lawful (Art. 5(1) (b)). As for repurposing, personal data should not be further processed in a way that the data subject might consider unexpected, inappropriate or otherwise objectionable[13] and, therefore, unconnected to the delivery of the service.

1.4. Surveillance under the disguise of service provision and its desensitizing effect

On the other hand, the data subject's interactions within a STD will be increasingly mediated by or delegated to (smart) devices and apps. Most of

---

[10] ART 29 WP Guidelines on Transparency under Regulation 2016/679, accessed 30/07/2018 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227>.

[11] ART 29 WP Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, accessed 30/07/2018 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

[12] ART 29 WP Opinion 3/2013, on purpose limitation, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> .

[13] COE – Council of Europe Guidelines on the Protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD, 2017, accessed 30/07/2018 <https://rm.coe.int/16806ebe7a>.

the destinations are using video-surveillance systems as sensors to supply real-time information on public transportation, traffic (also in relation to emergency and personal safety), navigation, and access to tourist information on the go, all of which provide value to the user: safety, convenience, and utility in daily lives, as well as on vacation.

This information is transmitted via, for e.g., smart remote controllable digital Closed-Circuit Television cameras that can zoom, move and track individual pedestrians, Automatic Number Plate Recognition, GPS, Wi-Fi network tracking reliable facial recognition software, and location-based service apps.

It has been argued that such devices desensitize users to providing location-based information because of the ease with which it happens and the "coolness" factor that comes with it.

1.5. Failed consent

Within this sort of intelligent environment, it is problematic to give, or withhold, our prior consent to data collection, as it seems to be absent by design. These ubiquitous sensors are so embedded in the destination that there is little awareness of them, or none at all; thus, they literally "disappear" from the users' sight. Users will not even be conscious of their presence and hence the notion of consent to the collection of data is problematic. We may, at least to some extent, concede that obtaining such consent, in STD contexts, would be achieved in a mechanical or perfunctory manner, or as a "routinization".

We also perceive with regard to Closed-Circuit Television, Automatic Number Plate Recognition and Webcams whilst tracking and sensing that notice in the form of information signs in the area being surveilled, or on related websites, would not conform to the consent requirements. Thus, the main issue of the *IoT* embedded in STD is that its sensorization devices are explicitly designed to be unobtrusive and seamless, invisible in use and imperceptible to users and thereupon, users do not have the opportunity to give their unambiguous, informed, specific, explicit, and granular consent[14].

---

[14] ART 29WP Opinion 15/2011, on the definition of consent, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/

Therefore, the data controller might have difficulty in demonstrating that consent was given, and the data subject is not able to withdraw that consent. Still, consent is not yet part of a function specification of *IoT* devices, and thus, they do not have the means to "provide fine-tuned consent in line with the preferences expressed by individuals," because smart roads, trams, tourist office devices are usually small, screenless and lack an input mechanism (a keyboard or a touch screen)[15].

1.6. Imbalance

Smart technologies often produce situations of imbalance, where data subjects are not aware of the fundamental elements of data processing and related consequences, are unable to access and manage their information, which leads secondarily to an enhanced information asymmetry as consumers.

1.7. Tendency to collect and analyze all data

The tourism industry is inherently based on data-exchange: to generate massive databases, it is necessary to optimally exploit all information available and thus, datasets need to be as exhaustive and varied as possible in order to faithfully reflect tourist activity within a territory.

In substance, smart technology undertakes the extensive collection, aggregation and algorithmic analysis of all the available data for various reasons, such as understanding customer purchasing behaviour and patterns or remarketing based on intelligent analytics, hampering the data minimization principle (Art. 5 (1)(c)). In addition, irrelevant data is also being collected and archived, undermining the storage limitation principle (Art. 5 (1) (e)).

---

wp187_en.pdf> ; updated by its Guidelines on Consent under Regulation 2016/679, accessible at <http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>.

[15] ART 29 WP Opinion 8/2014, on the recent developments on the Internet of Things, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

1.8. Inaccurate data

Where information sources are not trustworthy, results drawn from data analysis may also not be representative or accurate (*i.e.*, analysis based on social media sources are not necessarily representative of the whole population at issue).

Besides, machine learning itself may contain hidden bias which lead to inaccurate predictions and profiles of individuals. In any case, profiling involves creating derived or inferred data, occasionally leading to incorrect decisions (discriminatory, erroneous and unjustified), regarding their behaviour, health, creditworthiness, recruitment, insurance risk, etc.

Even exercising the "*right to be forgotten*", where data subjects have the right for their data to be erased in several situations (e.g., when the data is no longer necessary for the purpose for which it was collected, or based on inaccurate data (as set by the accuracy principle depicted in Art. 5 (1) (d)), it may in reality be difficult for a business to find and erase someone's data if it is stored across several different systems and jurisdictions.

2. The obligations of organizations while processing personal data within a STD

While realizing the benefits of using big data analytics and being a competitive STD, addressing data protection concerns supports best practices in information governance. Accordingly, it is in the interests of organizations intending to become an STD should pay careful attention to these issues. Data protection compliance should hence be viewed as an enabler of the success of an STD and not as a regulatory or procedural burden. As is by now widely known, infringement or non-compliance with the Regulation may lead to fines up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher.

As stated in the tourism literature, tourism, by definition, is a service--intensive industry with a "*business network*", since it relies on a number of stakeholders for its ability to deliver products and services. In this network, each of the actors involved in the transportation, accommodation, gastronomy, attractions and ancillary services, potentially process personal data.

For a STD, the public or private organisations that decide the "whys" and "hows" by which the personal data is to be processed are called "data controllers". They may use other parties that process personal data on their behalf, called "data processors". Both data controllers and data processors must abide by the GDPR obligations.

However, Big Data Analytics can make it difficult to distinguish between controllers and processors; further, within the modern data value chain, organizations outsourcing analytics and artificial intelligence to specialized companies need to consider carefully who has control over the processing of any personal data (Art. 4 (7) (8)).

Therefore, if an organization chooses to store its customer data in the cloud, then the cloud provider is likely to be a data processor, as it is acting on the original organization's behalf, and it is not determining the purpose of the processing.

Hence, if an organization purports aims to conduct its analytics outsourcing in a data controller-data processor relationship, it is important that the contract includes clear instructions about how the data can be used and the specific purposes for which it is being processed. However, it does not follow from the existence of a contract of this type that the sub--contracted company performing data analysis is a data processor; if this company uses its discretion and expertise to decide what data to collect and how to apply its analytic techniques, then it is very likely to be a data controller as well; in fact a co-controllership[16] (Art. 24).

Under the accountability principle (Art. 24), data controllers shall be responsible for, and be able to demonstrate compliance with, all the obligations and principles contained in the regulation. Some of its most important obligations are explained below.

2.1. Appointing a Data Protection Officer

The GDPR mandates the appointment of a DPO within the organization whose responsibilities include: monitoring data governance and privacy,

---

[16] ICO, "Guide on Big Data, Artificial Intelligence, Machine Learning and Data Protection", 2017, accessed 30/07/2018 <https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/>.

providing advice, monitoring data protection impact assessments, and acting as the point of contact with any supervisory authority. This is mandatory where the processing is carried out by a public authority or body, except for the courts; their core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or processing on a large scale of special categories of data (Articles 37 to 39)[17].

2.2. Algorithmic accountability

Organizations should also check "algorithmic accountability", which means being able to check that the algorithms used and developed by machine learning systems are actually doing what we think they are doing and are not producing discriminatory, erroneous or unjustified results. Organizations using machine learning techniques in STD are obliged to assure data quality by checking the sources of the data, the accuracy of the data, whether is sufficiently up to date, how securely it is kept, and whether there are restrictions on how it can be used (anonymized data).

2.3. Fair, lawful and transparent processing obligations

STD organizations must process personal data "fairly, lawfully and in a transparent manner in relation to the data subject", i.e., when the data is collected, it must be clear as to why that data is being collected and how the data will be used. Whether the data is volunteered, observed, inferred, or collected from accessible sources, individuals are fully entitled to know what it is, from where and from whom the controllers obtained it, and how automated decisions were taken in relation to it. The GDPR prohibits automated individual decision-making that significantly affect individuals (Art. 22 (1)). Therefore, in order to ensure fair and transparent processing, automated decisions should take account of all the circumstances

[17] ART 29 WP Guidelines on Data Protection Officers ('DPOs'), accessed 30/07/2018 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44100>.

surrounding the data and not be based on merely de-contextualized information or on data processed results. The controller should furthermore build discrimination detection into their machine learning systems, to prevent inaccuracies and errors being assigned to labeled profiles.

2.4. Lawfulness of processing

Processing personal data should be based upon certain conditions, namely: the consent of the tourist, a contract, a public interest, a legitimate interest, etc. In these intelligent environments, our ability to give or withhold our prior consent to data collection is questionable, as it seems to be absent by design. Within STDs, it should be acknowledged that ubiquitous sensors are so embedded in the destination that they literally "disappear" from the users' sight, meaning that users will not even be conscious of their presence and hence, by definition, do not consent to the collection of data. So, at least to some extent, the obtaining of consent in STD contexts can at best be mechanical, perfunctory, or routinized.

With reference to the remaining legal criteria, processing personal data relies on "public interest", which can sidestep the need for consent (health, national governmental agencies gather data – for e.g. e-Government systems, e-Health). Nevertheless, this possibility should not conceal any eventual "third-party interest".

Most commercial systems rely on the "legitimate interests" ground, even if they consist of "the vaguest ground for processing". This offers considerable scope for industry to process data by claiming any purportedly necessary "legitimate interest". In fact, the processing must be "necessary" for legitimate interests and not just *potentially* interesting for the operator. It follows that the processing is unnecessary if there is any other means of meeting that legitimate interest which interferes less with public privacy.

As for the contractual condition, it may be difficult to show that big data analytics in STD are strictly necessary for the performance of a contract, since the processing goes beyond what is required to sell a product or deliver a service.

2.5. Purpose limitation

The principle of purpose limitation is to ensure that the purpose for which the data is collected is specified and lawful. This principle also prevents arbitrary re-use, which means that personal data should not be further processed in a manner that the data subject might considered unexpected, inappropriate or otherwise objectionable and therefore unrelated to the delivery of the service. In other words, exposing data subjects to different/greater risks than those contemplated by the initial purposes may be considered to amount to the further processing of data in an unexpected manner[18].

2.6. Data Minimization, Collection and Retention obligations

Data minimization means that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*" (Art. 5 (1) (c)). This obligation means that STD entities should minimize the amount of data they collect and process, and the length of time they keep the data. Even if in practice, smart technology envisages the massive collection, aggregation and algorithmic analysis of all the available data to understand customer buying behavior and patterns, or remarketing based on intelligent analytics, organizations need to be clear about which data is deemed to be *necessary, excessive* and *relevant* for processing purposes.

As for data storage, personal data shall not be kept (stored) longer than necessary for the purpose for which it is being processed, as prescribed by the storage limitation principle **(**Art. 5 (1) (e)). This obligation is part of the lifecycle governance strategy retention policies of companies that defensibly dispose of irrelevant data rather than keeping data archived forever.

Regarding retention timeframes, retention schedules allow unnecessary data to be disposed of, as it is no longer of business value or needed to meet

---

[18] ART 29 WP Opinion 3/2013, on purpose limitation, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

legal obligations. Data mapping techniques may permissibly identify where and what type of data is stored within an organization. Data management segmentation can also help to segregate EU data from data coming from other data subjects.

2.7. Accuracy and up to date processing obligations

If sources of data are reliable, accurate and representative, so too must be the results drawn from big data analysis employed in a STD environment (Art. 5 (1) (d)). For example, analysis based on social media sources are not necessarily representative of the population as a whole[19].

Organizations employing machine learning algorithms need to consider the distinction between correlation and causation[20], *i.e.*, when there is no *direct cause and effect* between two phenomena that show a close correlation. In these cases there is a risk of drawing inaccurate, but also – and when applied at the individual level – potentially unfair and discriminatory conclusions[21]. The potential accuracy (or inaccuracy) of any resulting decisions might cause discriminatory, erroneous and unjustified decisions regarding the data subject´s behavior in relation to their health, creditworthiness, recruitment, insurance risk, etc. The quality of the profiles and of the personal data upon which they are built, again, seem to matter for the prosperity of the industry.

2.8. Data breach reporting

EU data protection law requires controllers to promptly notify the relevant supervisory authority and the data subjects of potential data breaches in the event of causing a high risk to data subjects. The notification must include at least: the name and contact details of the DPO (or other relevant point of contact); the likely consequences of the data breach; and

---

[19] ICO, Guide on Big Data, cit.

[20] ICO, Guide on Big Data, cit.

[21] EDPS, Opinion 7/2015 on Meeting the challenges of big data, accessed 30/07/2018 <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf>.

any measures taken by the controller to remedy or mitigate the breach. However, the controller may be exempt from this requirement if the risk of harm is remote because the affected data are protected (e.g., due to strong encryption). Most importantly, if the risks associated with the breach have been effectively resolved, then the organization may be exempt from the notification requirements[22].

2.9. Processing activities records

EU data protection law requires organizations involved in STD to keep records (written or electronic) of their data processing activities (art. 30). Examples of records to be kept include the purposes of the processing; the categories of data subjects and personal data processed; and the categories of recipients with whom the data may be shared. Upon request, these records must be disclosed to DPAs.

2.10. Codes of conduct and certification mechanism

In order to enhance transparency and compliance with this Regulation, associations and other institutional bodies representing both controllers and processors are obliged to elaborate codes of practice specifying how the GDPR should be applied. These bodies must then submit their draft codes of conduct to the relevant supervisory authority for approval. The GDPR introduced certification mechanisms and data protection marks, allowing data subjects to quickly assess the level of data protection employed by the products and services in question. A list of certified organizations will thus be publicly available. Codes of conduct and approved certification mechanisms will also assist controllers in identifying the risks related to their type of processing and in adhering to best practices.

---

[22] ART 29, Guidelines on Personal data breach notification under Regulation 2016/679, accessed 30/07/2018 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

3. Compliance tools at the GDPR

Compliance tools enable STD organizations to meet their data protection obligations while protecting people's privacy rights in a STD context. These are: anonymization and pseudonymization techniques, privacy policies, DPIA, personal data stores, algorithmic transparency, privacy seals/certification, and PbD measures to mitigate identified legal risks and implications. STD managers may demonstrate commitment to compliance through internal documentation and employee training in relation the GDPR-related mandates, such as via written internal policies.

3.1. Anonymization

As a stated principle, when data is rendered *anonymous* (Recital 26 of the GDPR) all identifying elements have been irreversibly eliminated from a set of personal data, and allows no possibility to re-identify the person(s) concerned. Consequently, it is deemed to be no longer personal data. Later, anonymised data might be aggregated in order to be analysed and to gain insights about the population, as well as combined with data from any other sources. At this stage, *IoT* developers can analyse, share, sell or publish the data without any data protection requirements.

Conversely, de-anonymization strategies in data mining techniques entails that anonymous data is cross-referenced with other sources to re-identify the anonymous data. Thus, the processing of datasets rendered anonymous may never be absolutely ensured.

In what refers to *pseudonymized* personal data, identifiers are replaced by a pseudonym (through encryption of the identifiers). In turn, pseudonymized data continues to allow an individual data subject to be singled out and linkable across different datasets and therefore stays inside the scope of the legal regime of data protection[23].

[23] ART 29, WP Opinion 05/2014, on anonymization techniques, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

3.2. Privacy policies

Privacy policies consist of documents which set forth an organization's data practices on processing activities of personal data to its users, such as collection, use, sharing, and retention. They serve as a basis for decision-making and as a "tool for preference-matching" for consumers, as consumers tend to place a higher value on a product/service, after learning more about its attributes and tradeoffs. As such, Privacy Policies constitute the *locus* where consequences are produced, the "technically most feasible place to protect privacy and personal data"[24].

The GDPR states that information addressed to the data subject should be "concise, easily accessible and easy to understand, and that clear and plain language, and additionally, where appropriate, visualization is used" (Article 12(7) and Recital 60).

However, in a STD scenario, these requirements can be problematic, and it has been suggested that privacy notices are not feasible when Big Data Analytics are entailed, given that: travelers engaged in tourism are unwilling to read lengthy legalese such as privacy notices, since it would take significantly more time than they spend using the content or the app itself; the context in which data is collected (e.g., destination apps, wearable watches and glasses or IoT devices) is difficult to provide the information.

Regarding the amount and type of these interactions, it is just too onerous for each data subject to assess their privacy settings across dozens of entities in order to ponder the non-negotiable trade offs of agreeing to privacy policies without knowing how the data might be used now and in the future, and to assess the cumulative effects of their data being merged with other datasets. On the other hand, information can be delivered in a user-friendly form, namely by: videos or in-app notices; cartoons and standard icons applied to privacy notices, explaining their content. As for wearable devices, privacy information could be provided on the device itself, or by broadcasting the information via Wi-Fi or making it available through a QR code[25].

---

[24] President's Council of Advisors on Science and Technology, Big Data and Privacy: a Technological Perspective. Executive Office of the President, USA (2014), accessed 30/07/2018 <https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf>.

[25] ART 29, WP Opinion 8/2014, on the recent developments on the Internet of Things, accessed 30/07/2018 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>.

3.3. Data protection impact assessment

A DPIA is a tool that can help to identify and mitigate privacy risks before the processing of personal data. This assessment involves description of the envisaged processing operations, an evaluation of the privacy risks and the measures contemplated to address those risks.

Art. 35 of GDPR indicates that when a type of processing which uses a systematic and extensive evaluation of individuals based on automated processing and profiling is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged operations on the protection of personal data. It is likely that general big data applications within an STD involving the processing of personal data will fall into this category[26].

3.4. Privacy by design

PbD is an approach in which IT system designers seek to adopt preemptive *technological* and *organizational* measures to protect personal data, when designing or creating new products and services. By design solutions are necessary at the early development stage (planning and implementation) of any new product or service that affects personal data. It aims to address privacy concerns attached to the very same technology that might create risks (Art. 25).

Besides anonymization techniques, PbD involves other engineering and organizational measures, including: security measures such as access controls, audit logs and encryption; data minimization measures, to ensure that only the personal data that is needed for a particular analysis or transaction is processed at each step (such as validating a customer); purpose limitation and data segregation measures so that, for example, personal data is kept separately from data used for processing intended to detect general trends and correlations; as well as sticky policies which

[26] ART 29, WP Guidelines on Data Protection Impact Assessment (DPIA), accessed 30/07/2018 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

record individual preferences, and corporate rules within the metadata that accompanies data.

Within a STD scenario, controllers and processors should test the adequacy of the above-mentioned solutions by design on a limited amount of data by means of simulations before they are used on a larger scale. Such a learn-from-experience approach makes it possible to assess the potential bias inherent in using different parameters in analyzing data, and provides a rational for minimising the use of information. However, there is a lack of a privacy mindset in IT system designers. As stated by ENISA: "[...] privacy and data protection features are, on the whole, ignored by traditional engineering approaches when implementing the desired functionality. This ignorance is caused and supported by limitations of awareness and understanding of developers and data controllers as well as lacking tools to realize PbD. While the research community is very active and growing, and constantly improving existing and contributing further building blocks, it is only loosely interlinked with practice."[27]

3.5. Personal data spaces

The European Data Protection Supervisor suggested that one way to increase an individual's control over the use of their data is through what are usually called personal data spaces, vaults or stores, which are often provided by personal information management services[28].

These are third-party services (intermediaries) that collect, manage and store people's personal data on their behalf and make it available to organisations as and when the individuals wish to do so. This tool aims to address criticisms related to the lack of control over how personal data is used in a big data environment, as tourists are not aware of how data is being collected or how it is used, and do not have the time to read privacy notices.

---

[27] ENISA, 2015, Report on Privacy and Data Protection by Design, cit.

[28] EDPS, Opinion 7/2015, cit.

3.6. Algorithmic transparency

The following suggestions concerning algorithmic transparency are reflected in the research findings of the ICO[29]: techniques for algorithmic auditing can be used to identify the factors and make transparent the algorithm step-by-step development that influence an algorithmic decision and assure public trust; interactive visualization systems can help individuals to understand why a recommendation was made and give them control over future recommendations; and ethics boards can be used to help shape and improve the transparency of the development of machine learning algorithms.

3.7. Privacy seals and certification

Certification schemes (Arts. 42, 43, Recital 100) can be used to help demonstrate data protection compliance of STD big data processing operations. They encourage the "establishment of data protection certification mechanisms and of data protection seals and marks" to demonstrate that processing operations comply with the Regulation. These are awarded by data protection authorities or by accredited certification bodies[30].

Conclusions

The preceding analysis emphasizes that smart tourism is becoming a big contributor to, and benefactor of, ubiquitous, always-on data capture about customers, aimed at enhanced tourism experiences, and increasing competitiveness. This extensive collection and processing of personal data in the context of STD using algorithm-driven techniques has given rise to serious privacy concerns, especially relating to the wide-ranging electronic surveillance, profiling, and disclosure of personal data. The concern is to

---

[29] ICO, Guide on Big Data, cit.

[30] ENISA, Recommendations on European Data Protection Certification, 2017, accessed 30/07/2018 <https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport>.

understand if the capacities created by the technology – personalized services and enhanced experiences – can be reconciled with data protection obligations. As we have seen, Smart Tourism raises significant issues with respect to information governance and as to how to legitimately derive "added" value from information in an open and ubiquitous info-structure. At a minimum, GDPR will be a real game changer, and European SDT confronts challenges in being compliant with it, whether at the EU or national level.

Os desafios do Regulamento Geral de Proteção de Dados diante da nova tecnologia blockchain

Maria Paulo Rebelo*

Resumo: A criação e o surgimento de novos *softwares* baseados em tecnologia *blockchain*, caracterizada por ser altamente decentralizada, transparente e imutável, lançam desafiantes perguntas ao novo Regulamento Geral de Proteção de Dados, criticado por ter sido criado tendo apenas em vista realidades virtuais centralizadas de controlo de dados. Sem prejuízo de quer o Regulamento europeu, quer a *blockchain* desejarem objetivos comuns, como o aumento da transparência e da confiança na troca de dados *online*, demonstraremos que, na verdade, em vários aspectos os desentendimentos entre ambos são reais. Em todo o caso, é possível adequá-la ao Regulamento: identificando a figura do responsável pelo tratamento ou subcontratante; reajustado certos direitos, como o direito ao apagamento, à realidade da *blockchain*, entre outros. O trabalho fez uso de metodologia bibliográfica e documental, de cunho dogmático-jurídico.

Palavras-chave: *blockchain; Regulamento Geral de Proteção de Dados*

Abstract: The creation and emergence of new software based on blockchain technology, characterized by their highly decentralized, transparent and immutable systems, challenge the recent General Data Protection Regulation to new questions, as it is severely criticized for bearing in mind only virtual realities based on centralized data control. Despite both the General Data Protection Regulation and blockchain share common interests in increasing transparency and confidence in online data exchange, the truth is that in several ways misunderstandings between the two are real. Nonetheless,

* Doutoranda em Direito Público pela Universidade Federal da Bahia; Investigadora Convidada pelo Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law; Mestre em Direito Intelectual, Pós-Graduada em Direito do Trabalho e Licenciada em Direito pela Faculdade de Direito de Lisboa; Pós-Graduada em Direito Empresarial pela Faculdade de Direito da Universidade de Coimbra. Professora de Pós-Graduação em Direito Processual Civil na UNIFACS (Brasil). Auditora de Justiça.

adjustments are feasible to adapt it to the Regulation: it is possible to identify the data controller and processor, to readjust; certain rights, such as right to erasure, among others. This work made use of bibliographical and documentary methodology of juridical and dogmatic nature.

Keywords: *blockchain; General Data Protection Regulation*

Introdução ao problema

O presente artigo vem questionar a articulação que uma das mais badaladas tecnologias dos últimos anos enfrenta com a chegada do novo RGPD.

A tecnologia *blockchain* tem vindo a assumir grande protagonismo nos últimos anos, no contexto de técnicas de computação em rede. Tem, inclusivamente, sido referenciada como uma das principais tecnologias integrantes da quarta revolução industrial[1]. Com efeito, os utilizadores da *blockchain* operam com base na lógica *P2P* (entre si), acabando por possuir uma cópia de toda a *DLT* (tecnologia de *distributed ledgers*, i.e., de dados/ /registos distribuídos/descentralizados) no seu próprio computador.

A principal questão que aqui se coloca, então, é a de saber qual o nível de impacto que esta tecnologia tem em áreas como a da proteção de dados, tradicionalmente voltadas para uma regulação analógica; ou se existe potencial para aplicar a *blockchain* ao serviço daquela mesma proteção. Entre outras coisas, torna-se relevante perceber se a *blockchain* pode ser considerada, *ab initio,* como um *software* que realiza tratamento de dados e perceber se os dados armazenados na *blockchain* são dados pessoais. Se considerarmos que a tecnologia implica a recolha de dados pessoais e o respectivo tratamento, uma terceira questão coloca-se na identificação do *responsável pelo tratamento (data controller)* e do *subcontratante (data processor)* que atuam na cadeia de blocos. Por último, depois de percebermos quais os

[1] A título de exemplo, Aste, Tomaso, Tasca, Paolo, Matteo, T Di. "Blockchain Tecnologies: foreseeable impacto on industry and society", disponível em http://discovery.ucl.ac.uk/10043048/1/Aste_BlockchainIEEE_600W_v3.3_A.doccceptedVersion.x.pdf, (acedido a 20/01/2019) ou Xing, Bo; Marwala, Tshilidzi. "Blockchain and Artificial Intelligence", disponível em https://arxiv.org/pdf/1802.04451.pdf (acedido a 20/01/2019).

principais direitos postos em causa por esta tecnologia, é preciso enfrentar o problema de garantir que eles sejam cumpridos.

1. A emergência de novas "economias digitais": controlo de dados e blockchain

Apesar de a *internet* ter sido originalmente concebida como um fenómeno de livre interligação entre redes a nível mundial, um espaço virtual onde todos os usuários se apresentassem de forma igualitária, a verdade é que, nos dias de hoje, o ciberespaço é uma verdadeira plataforma eletrónica de transação onde os dados pessoais dos seus utilizadores se convertem num dos maiores ativos económicos do mundo *online*, transformando-se na nova "moeda" digital. A grande quantidade, complexidade e variabilidade de informações que hoje circula *online* é inclusivamente apelidada de *Big Data*[2] e tem levantado algumas inquietações, não pela sua própria existência, mas pelo uso que grandes prestadores de serviços *online* como a *Google*, *Amazon*, *Apple* e *Facebook* fazem dela. Hoje em dia, grandes empresas controlam facilmente a forma como cada um de nós pesquisa, compra e se relaciona com terceiros; tudo graças à informação gratuita que lhes passamos e eles armazenam, processam e monitorizam. Para a grande maioria das empresas que estão *online* e para os prestadores de serviços em rede, a troca de serviços e produtos aparentemente gratuitos é feita à custa da

---

[2] Não existe uma informação unívoca em torno da expressão. Como reporta Mauro, Greco e Grimaldi, podem ser identificados vários grupos de posicionamentos na forma como a ideia é concebida: (i) um que se foca nas principais características, a saber, os três V's (Volume, Velocidade e Variedade); (ii) outro que dá ênfase às necessidades tecnológicas exigidas para processar grandes quantidades de informação; (iii) e um terceiro que recorre ao impacto que este tipo de informação tem na sociedade. Por todos, Mauro, Andrea De, Greco, Marco, Grinaldi, Michele. "What is Big Data? A consensual definition and a review of key research topics", in *AIP Conference Proceedings 1644,* 97 (2015), disponível em http://big-data-fr.com/wp-content/uploads/2015/02/aip-scitation-what-is-bigdata.pdf (acedido a 20/01/2019). Uma proposta de definição que agregue todos os traços acima apontados é possível. Nestes termos, *Big Data* pode ser compreendido como uma mais valia económica, sob a forma de informação, que, pelo seu significativo volume, pela velocidade com que são processadas e pela variedade do seu teor, demandam plataformas tecnológicas adequadas ao seu processamento em valor económico (p. 103).

entrega de informação pessoal, que serve de "pagamento" para a obtenção de acessos e serviços *online*. Por ser assim, a partilha de informação e dados pessoais tornou-se algo inevitável no mundo virtual. A centralização deste tipo de informações em poucos provedores *online* tem gerado grandes preocupações[3], já que técnicas de mineração de dados tornam possível a identificação de padrões de consumo e a construção de bancos de dados sobre consumidores, não-raro sem que os cidadãos tenham disso ciência.

Paralelamente a esta "monetarização" da informação e do controlo sobre dados *online*, outra grande "moeda" digital que surgiu em 2008/2009 foi a criptomoeda conhecida como *Bitcoin*. Desenhada por Satoshi Nakamoto[4], funciona através de um sistema de protocolos que operam *P2P*, oferece um sistema financeiro de pagamento *online* sem a intervenção de uma entidade central que gerencie todas as operações. Ao operar desta forma, a *Bitcoin*, que é construída sobre a técnica da *blockchain*, chama à atenção pela transparência com que promove entre privados (*peers*) comunicações e transações. A sua arquitetura descentralizada tem sido apontada como uma das maiores valias desta tecnologia, permitindo a redistribuição do poder a todos os navegadores da comunidade digital e impedindo o processamento e armazenamento de dados em servidores centrais localizados.

As atividades desenhadas em rede entre indivíduos são, assim, efetuadas puramente com base no consenso de todos os seus intervenientes e a correspondente transparência e publicidade de toda essa informação devolve-lhes o poder sobre si mesmos e a confiança que resgatam dos servidores *online*, para depositar no funcionamento imparcial dos algoritmos matemáticos.

É neste ponto que a tecnologia *blockchain* e a regulamentação europeia revelam os seus interesses comuns: tal como aquela *DLT* promete a descentralização do tratamento de dados, garante a confiança e transparência nas redes *P2P*, a eliminação do domínio dos grandes blocos sobre dados

---

[3] Filippone, Roberta. "Blockchain and individuals' control over personal data in European data protection law", 2017, disponível em http://arno.uvt.nl/show.cgi?fid=143638 (acedido a 20/01/2019).

[4] Depois do domínio "bitcoin.org" ter sido registado online em 2008, um artigo da autoria de Satoshi Nakamoto foi publicado poucos meses depois (Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System", disponível em https://bitcoin.org/bitcoin.pdf (acedido a 20/01/2019), com as bases daquilo que seria a tecnologia *Bitcoin* e o fenómeno das criptomoedas. O nome Satoshi Nakamoto, porém, foi um pseudónimo usado para esconder a(s) sua(s) verdadeira(s) identidade(s), que permanece(m) até aos dias de hoje desconhecida(s).

pessoais dos usuários e a devolução desse controlo aos próprios, também o RGPD compartilha ideias paralelas de devolução do controlo sobre os dados aos seus titulares, para os quais consagra uma série de direitos, entre os quais o direito ao apagamento (art.º 16º e 17º do RGPD)[5].

Todavia, por mais tentador que pareça ser esta devolução de controlo aos titulares dos dados sobre as suas informações, importa não perder de vista que a *blockchain* é uma tecnologia que tem como mais-valia garantir, precisamente, a autenticidade de informações mediante a sua imutabilidade, pelo que, só por si, e enquanto desacompanhada de ferramentas (*rectius,* tecnologias *by desin*) complementares que as compatibilizem com os direitos dados pelo RGPD aos titulares, o seu uso é minimamente comprometedor[6].

2. A tecnologia *blockchain*

A tecnologia *blockchain*, tal como a terminologia sugere, é uma concatenação de "blocos", cada um deles composto por um certo número de *data* (dados), relacionados entre si de tal modo que cada novo bloco que se acrescenta à sequência contém uma imagem criptográfica do anterior. Por outras palavras, é uma base de dados digital, partilhada, descentralizada e sincronizada que se mantém à base de um algoritmo consensual e armazenado em diversos *nodes* (computadores individuais/usuários). Por ser assim, esta tecnologia tem a particularidade de não poder ser manipulada a partir do momento em que a informação é armazenada no bloco, pois assim que

---

[5] EDPS, Parecer 9/2016 "EDPS Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data", 2016, disponível em https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf (acedido a 20/01/2019); Ramsay, Sebastian. "The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR", Tese de Mestrado apresentada à Universidade de Estocolmo, 2018, p. 6, disponível em http://www.diva-portal.org (acedido a 20/01/2019).

[6] Fabiano, Nicola. "Internet of Things and Blockchain: legal issues and privacy. The challenge for a privacy standard", in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017, p. 730, disponível em https://ieeexplore.ieee.org (acedido a 20/01/2019).

entra neste é anexada à sequência já pré-existente. Apesar do termo ser por vezes usado para identificar qualquer *DLT*, independentemente de armazenar ou não dados em blocos, a verdade é que a noção de *blockchain* pode apenas designar a modalidade de *DLT* que efetivamente armazena informação em blocos, que por sua vez são "acorrentados" ou "ligados" (*hashed*) uns aos outros numa cadeira ininterrupta (*chained*).

Basicamente esta *DLT* funciona por um processo de dois momentos: cada utilizador tem uma chave pública (sequência alfanumérica) que o representa e à sua conta, e que é a que partilha com terceiros para poder celebrar transações; e uma chave privada (também alfanumérica) que representa basicamente uma senha/*password* própria que mantem sigilosa perante terceiros. As chaves relacionam-se através de operações matemáticas, que basicamente permitem à privada desencriptar dados através da chave pública.

O teor da informação que entra na sequência tem ainda a sua integridade salvaguardada graças a um mecanismo de "consenso" que subjaz a esta tecnologia. Como é que isto é possível? Cada bloco contém aspectos fundamentais da transação que ocorreu no bloco anterior e o respetivo *hash*[7]; se toda a rede e todos os *nodes* chegarem a consenso sobre a validade de uma nova transação, então um novo bloco será cronologicamente agrupado ao precedente, naquilo que se tornará uma cadeia de históricos validados. Uma vez adicionados, os blocos não podem ser removidos. E assim é porquanto a *blockchain* funciona numa rede descentralizada de computadores que periodicamente se sincronizam por forma a confirmar, repetidas vezes, que todos partilham das mesmas bases de dados, assegurando e

---

[7] O *hash*, que é uma técnica que solidifica praticamente todo o funcionamento da *blockchain*, é basicamente uma cadeia/código alfanumérico que permite a qualquer pessoa verificar que determinada informação digital é idêntica à informação que foi objecto de um *hash*; o que facilita em muito, por exemplo, a autenticação de documentos, i.e., a prova de que determinado documento é idêntico ao que foi atribuído um *hash*. Todavia, esta técnica só funciona num sentido, o que passa do documento original para o *hash*; já não no sentido contrário, i.e., do *hash* para o documento original. Ou seja, o *hash* não permite a chamada retroengenharia (*reverse-engineering*) para encontrar o documento original. Ainda assim, não deixa de ser possível estabelecer uma ligação entre o documento inserido na *blockchain* pelo *hash* e o titular do mesmo; desta forma, mesmo que em si mesmo não permita *reverse-engineer*, o *hash* de um documento de identidade, de um título de propriedade, ou de um plano de saúde do seu titular pode ser considerado dado pessoal.

veracidade das informações contidas no *ledger* que circula em toda a rede. São os mineiros (*miners*) que ficam encarregues de resolver os problemas matemáticos que transformam as informações (texto) contidas em cada bloco em sequências alfanuméricas designadas de *hashes*; que mais não são do que uma impressão digital única que confirma a correspondência de informação registada no *ledger* ou na *blockchain*. Desta forma, quanto mais usuários (*nodes*) integrarem a rede, menos os utilizadores precisam de confiar uns nos outros ou em terceiros intermediários para garantir transações seguras. Isto quer dizer que, na *blockchain*, a prova criptográfica e os algoritmos digitais substituem a confiança tradicional depositada em intermediários.

A tecnologia *blockchain* costuma dividir-se em duas principais classificações: as *public blockchains*, sempre que qualquer usuário lhe pode aceder e fazer uso para efeitos transacionais[8]; e *private blockchains*, sempre que a cadeia de blocos é controlada por uma determinada entidade e o acesso é autorizado apenas a determinados *nodes*[9]. Para exemplificar, podemos tomar em consideração a *Bitcoin*: como o seu sistema foi pensado para permitir que qualquer cidadão que entre na rede possa celebrar transações *online*, ele é, naturalmente, um sistema amparado numa *public blockchain*. Em sentido contrário, as *blockchain* autorizadas ou privadas processam-se como uma rede privada tipo *Intranet*, com um administrador centralizado de cuja autorização/permissão é necessária para poder passar a operar na *blockchain*. Pense-se na gestão de um setor de recursos humanos por um sistema de *private blockchain*, que faz uso desta tecnologia precisamente para obter um registo auditável de todos os seus dados sem que o público, em geral, e os funcionários, em particular, possam ter acesso. Estas tecnologias de *blockchain* privadas em pouco se distinguem de bases de dados privadas; a verdadeira revolução que esta tecnologia trouxe para o plano digital centra-se, verdadeiramente, nas cadeias de blocos públicas e na possibilidade de tornar qualquer registo imutável.

---

[8] Segundo os dados do Relatório elaborado pela *EU Blockchain Observatory and Forum* ("*Blockchain and the GDPR;* disponível em https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (acedido a 20/01/2019) 80% de todas as aplicações *blockchain* existentes são públicas.

[9] Ainda existem outras variações possíveis, como *blockchains* públicas, mas sujeitas a autorização.

Na *blockchain,* é possível armazenar qualquer tipo de dados (documentos, arte, registos, etc.) no *ledger* de três formas diferentes: texto, de forma criptográfica ou por *hashing.* A forma mais fácil de o fazer é com recurso a texto corrente; de resto, só não será a forma mais desejável do ponto de vista da privacidade já que qualquer pessoa pode arbitrariamente ler esses dados (no caso de *public blockchains*).

Em vez disso, o conteúdo lançado em blocos no *ledger* pode ser encriptado. A maioria dos *DLT*'s acaba por abarcar dois tipos de dados/informações: a) o *header* (cabeçalho) que contem o registo da data e hora, a fonte dos dados (a identidade é representada normalmente por um endereço IP) e o *hash* do bloco anterior; b) o conteúdo da transação em si, i.e., os dados a serem efetivamente armazenados na *blockchain* (designado por *payload*). A diferença entre um e outro prende-se com o fato de o *header* normalmente não ser encriptado, ao contrário do *payload*[10]. Alternativamente à encriptação do texto lançado no *ledger*, os usuários também podem transformar esse conteúdo em *hashes* e depois lançar estas (e não o próprio texto/informação) na *DLT*. Os *hashes*, que são sequências criptográficas unidirecionais, não podem ser objeto de retroengenharia (*reverse engineering*), pelo que não podemos recorrer a chaves privadas para os desencriptar; aquilo que permitem, pelo contrário, é verificar se determinado documento com certas características foi armazenado ou não num banco de dados e atestar a sua correspondência.

Várias têm sido as aplicações possíveis desta tecnologia. Além da já aqui mencionada crucial importância no funcionamento de *criptomoedas*, a blockchain foi ainda mote para desassossegar o mundo dos contratos civis com a criação da figura dos *smart contracts*[11] e, além de muitas outras, pode

---

[10] Sempre que os dados são encriptados, só o utilizador que tenha a chave privada poderá desencriptar os mesmos. A criptografia surge, assim, como técnica para garantir uma assinatura digital única que permite a reversão dos dados ao estado anterior e o desbloqueamento do documento. Pessoas que não tenham esse acesso autorizado, deixam de poder ter acesso à informação encriptada.

[11] Costuma atribuir-se a Nick Szabo a autoria da criação destes "contratos inteligentes" (*smart contracts*), nos anos 90. Szabo quis reformular a forma como pensamos os contratos e fê-lo através da criação de um software de computador semelhante a cláusulas contratuais que se baseassem na confiança de protocolos criptográficos. O uso de contratos inteligentes amparados na tecnologia blockchain permite, hoje em dia, aos seus usuários celebrar relações jurídicas vinculantes com recurso a códigos criptográficos e fazendo uso daquele software

vir a ter significativa relevância no setor dos registos públicos, apesar das questões que a temática já tem levantado[12].

3. O novo Regulamento Geral de Proteção de Dados

Como acima mencionado, o debate em torno do problema aqui colocado não pode ser deslocado do novo RGPD, que entrou em vigor no espaço europeu em Maio de 2018[13].

---

para garantir o cumprimento do contrato. Em determinada medida, não podemos dizer que os contratos tal como os conhecemos hoje sejam significativamente diferentes *smart contracts*, já que antes da execução deste, também lhe precede um momento de negociação prévio entre os contraentes para registar o seu teor em *smart contract* code. A grande mais-valia desta tecnologia e que faz dos contratos inteligentes um marco no mundo digital e novas tecnologias, prende-se com a sua força autoexecutória, i.e., na capacidade que este tem de vincular o cumprimento de obrigações contratuais. O código presente no *smart contract* é executado diretamente, sem necessidade de recorrer a quaisquer intermediários para o efeito, tais como ações declarativas, executivas, recurso a advogados, etc. Enquanto programas digitais formatados sob a tecnologia do consenso blockchain, quaisquer mudanças não autorizadas na sua estrutura encontram-se necessariamente inviabilizadas e todas as condições previamente acordadas são objeto de uma implementação e controlo estritos, automatizados pelo código computacional trazido pelo software. Ambas as partes sabem destas condições e aceitam-nas. O comprador sabe que o não pagamento do preço no prazo acordado implica a imediata perda de controlo sobre o bem; o credor sabe que se o mesmo não for efetuado, a verificação da *compliance* é imediata e automático o procedimento executório de cessação contratual, sem custos adicionais relacionados (*v.* Belo, José. "Smart Contracts: Possível Solução Para A Relutância Em Entrar Num Contrato Em Ambiente Online?", *Cyberlaw,* v. 1, n. 5, 2018, disponível em https://www.academia.edu/36701400/Smart_contracts_poss%C3%ADvel_solução_para_a_relutância_em_entrar_num_contrato_em_ambiente_online (acedido a 20/01/2019).

[12] Assim, e apenas a título de exemplo, discute-se como compatibilizar a blockchain com serviços de cartório, já que (i) o funcionamento *P2P* da *blockchain* seria incompatível com a necessária a presença de funcionários que façam a leitura e análise da documentação apresentada pelas partes, qualifiquem os títulos etc.; (ii) a vantagem da consensualidade que a tecnologia traz nada acrescentaria ao princípio do trato sucessivo (coerência na cadeia de transmissões) que já existe no sistema de registos; (iii) além de que a imutabilidade da *blockchain* seria também supostamente incompatível com a necessidade de introduzir retificações aos registos.

[13] A nível internacional, destaco ainda (i) a modernização da Convenção 108 de 1981 (Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal) levada a cabo desde Maio de 2018 pelo Conselho da Europa e já assinada

Porque o nosso propósito não é o de fazer uma análise exaustiva deste diploma, vamos apenas referenciar alguns aspectos relevantes que desafiam a temática da *blockchain*[14]: (i) os principais conceitos-chave envolvidos, (ii) os princípios que maior potencial têm de ser afetados, (iii) que direitos atribuídos aos titulares dos dados pessoais poderão ser ofendidos.

À imagem e semelhança das boas práticas europeias, o RGPD veio adotar como técnica legislativa o uso de definições para esclarecer noções fundamentais à compreensão do documento. Entre outras, destacam-se os conceitos de (i) *dados pessoais*: qualquer informação/dado que se relacione com uma pessoa identificável (art.º 4º, n.º 1 do RGPD); (ii) de *dados pseudonimizados*: o tratamento de dados que, apesar de à partida não poder ser atribuído a um titular específico, admite essa hipótese com recurso a informações suplementares (art.º 4.º, n.º 5 do RGPD); (iii) *responsável pelo tratamento*: entidade que decide a finalidade do tratamento (art.º 4º, n.º 7 do RGPD), (iv) *subcontratante:* entidade que procede ao tratamento de dados por conta do responsável do tratamento (art.º 4.º, n.º 8 do RGPD), (v) *tratamento de dados*: qualquer operação que se faça com uso de dados pessoais, que vão desde a simples recolha/coleta, passando pelo seu processamento, armazenamento, transferência ou mesmo eliminação (art.º 4º, n.º 2 do RGPD).

Relativamente aos princípios previstos no RGPD, destacam-se (i) o princípio da *limitação das finalidades*: qualquer dado pessoal só pode ser

---

por Portugal desde Outubro desse ano (modificações que vieram adequar a Convenção aos diplomas internacionais existentes e, assim, (i) reajustaram conceitos e incorporaram as noções de *data controller* e *data processor*, (ii) reforçam-se princípios como o da proporcionalidade e da minimização do uso de dados; (iii) acrescenta-se disposição específica para regulamentação do consentimento do titular dos dados; (iv) alarga-se o catálogo de dados considerados sensíveis, (v) reforçam-se as exigências em matéria de segurança e proteção de dados; (vi) novos direitos são atribuídos aos titulares dos dados, (vii) criam-se novas obrigações etc.); e (ii) a Lei 13.709, de 14 de Agosto (Lei Geral de Proteção de Dados), que instituiu as novas regras brasileiras em matéria proteção de dados pessoais, ainda que este venha apenas a entrar em vigor em 2020 (18 meses após a sua promulgação) redigida sob notória influência daquilo que já se professava nas regulações europeias nesta matéria e, portanto, sem grandes novidades jurídicas regulatórias,).

[14] Como os principais problemas de compatibilização desta tecnologia com o RGPD não se colocam em abstrato para todas as técnicas *blockchain*, mas sobretudo quando o tipo de sistema *blockchain* é de acesso público; a análise aqui efetuada parte desta premissa e dirige-se sobretudo à análise destes, e não de outros (v.g. privados) sistemas.

recolhido e tratado com propósitos legítimos, concretos e determinados, que sejam devidamente comunicados ao respetivo titular, e sem que possam ser usados para outras ou além das finalidades recolhidas (art.º 5º, n.º 1, al. b) do RGPD); (ii) princípio da *minimização dos dados*: o tratamento tem que ser compatível com as finalidades declaradas para a sua recolha e limitadas ao necessário para a sua prossecução (art.º 5º, n.º 1, al. c) do RGPD); (iii) princípio da *transparência*: que garante ao titular dos dados que todas as informações são dadas e de forma clara e precisa (art.º 5º, n.º 1, al. a) e 12º do RGPD); (iv) o princípio dos *limites da conservação:* que visa garantir que todos os dados são conservados adequadamente, por forma a permitir sempre a identificação e acesso dos seus titulares (art.º 5º, n.º 1, al e) do RGPD); (v) princípios da *integralidade e confidencialidade*: acompanhados de medidas técnicas de proteção desses mesmos dados, que impeçam o acesso não autorizado, a perda, etc., sob pena de responsabilidade administrativa ou mesmo penal (art.º 5º, n.º 1, al f) do RGPD).

Por último, destacamos ainda alguns direitos atribuídos ao titular dos dados que o RGPD veio revisitar e/ou incorporar: (i) direito de *acesso* aos dados (art.º 15º do RGPD), que poderá ser efetuado sem quaisquer constrangimentos e a qualquer tempo desde que efetuado mediante requerimento prévio; (ii) direito de *retificação e apagamento*, que se traduz no direito do titular dos dados a, por ex., ver revogado o seu consentimento, exigir do responsável pelo tratamento a destruição dos seus registos no banco de dados, a sua a total exclusão, a mera oposição ao tratamento, ou correção (art.º 16º e 17º do RGPD); (iii) direito à *portabilidade dos dados* (art.º 20º do RGPD), i.e., o direito solicitar ao responsável pelo tratamento a transmissão dos seus dados pessoais para outra entidade.

4. Âmbito de aplicação do RGPD, dados pessoais e tratamento de dados

Saber se a tecnologia blockchain deve passar pelo crivo das restrições das leis de proteção de dados exige a resposta a duas perguntas: (i) será que os dados armazenados na cadeia de blocos se configuram dados pessoais?; (ii) se assim for, será que a *blockchain* realiza tratamento de dados de alguma forma?

4.1. Dados pessoais

Sabemos que dados pessoais constituem qualquer tipo de informação associada a uma pessoa identificada ou identificável (nome, número de identificação fiscal, agência e conta bancária, escola que frequentou, notas que tirou, idade, etc.)[15]. Sabemos também que (i) o RGPD só se aplica caso estejamos perante um dado considerado como "pessoal" e não a qualquer tipo de dado; e que (ii) dados anónimos não entram no escopo da regulamentação europeia. Para saber se a *blockchain* lida com dados pessoais, precisamos perceber que dois são os tipos de dados que nela interagem: aquilo a que se chama de *transactional data*[16] e as *public keys*.

Dados financeiros, médicos, de identificação, comportamento de consumo *online* são informações pessoais que se costumam designar por *transactional data* e sobre os quais costumam girar as transações *online*. Como vimos acima[17], há três formas de armazenar dados na *blockchain*: texto, criptografia ou *hashing*; pelo que a resposta a esta pergunta exige uma apreciação sob todas estas alternativas. A primeira hipótese não levanta grandes dúvidas: quando os dados são armazenados na *DLT* sob a forma de texto simples, estão necessariamente em causa dados pessoais que permitem identificar uma pessoa, pelo que colhe aplicação o RGPD. Já relativamente aos dados armazenados sob a forma criptográfica, como permanece possível o seu acesso mediante o uso de uma chave privada, o seu rastreamento até ao respetivo titular permanece viável e, portanto, não podem ser considerados como anónimos, mas pseudonimizados.

---

[15] Nos termos do artigo 4.º, n.º 1 do RGPD, deve entender-se por dado pessoal uma "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".

[16] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper,* n. 18-01, p. 9 e ss., disponível em https://papers.ssrn.com (acedido a 20/01/2019).

[17] *Supra*, 3. II.

Por último, e com as necessárias reservas[18], se os *transactional data* forem transformados em *hashes*, ainda poderão ser considerados como dados pessoais. É verdade que o nível de privacidade oferecido por um *hash* é significativamente maior que a mera criptografia, pois este não pode ser objeto de retroengenharia. Todavia, não é outra a conclusão que se pode extrair do parecer do Grupo de Trabalho sobre o Artigo 29 (GT29)[19], ao concluir que também os *hashes* são formas de pseudonimização (e não de anonimização) de dados pessoais, na medida em que uma pessoa pode ainda ser rastreada e identificável[20].

As chaves públicas (*public keys*) não são dados transacionáveis, mas um conjunto alfanumérico que identifica de forma pseudonimizada um usuário que pretende fazer transações ou comunicações[21]. Vimos acima a noção de dados *pseudonimizados*. Ora, as transações/comunicações na *blockchain* que são efetuadas através da publicação de uma chave pública estão irremediavelmente associadas a um endereço de *IP*. Todavia, se por um lado é certo que esta chave pública se encontra criptografada para que se consiga um certo anonimato na operação *online*, não menos certo é ser possível identificar indiretamente a entidade/sujeito que representa

---

[18] Nomeadamente, se, com o tempo, avanços tecnológicos no mundo da criptografia revelarem ser efetivamente possível tornar estes dados anónimos, como promete o SHA-256 ou SHA-3. Por outro lado, e como se dirá *infra*, algumas técnicas têm permitido que estes dados transacionais não sejam diretamente lançados na *blockchain*, das quais é maior exemplo o armazenamento de dados fora da *blockchain* vinculados à cadeia de blocos por meio de um *hash* (*cf.* Finck, Michèle. *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, pág. 11, disponível em https://papers.ssrn.com (acedido a 10/01/2019).

[19] GT29, Parecer 05/2014 sobre técnicas de anonimização, disponível em https://www.gpdp.gov.mo (acedido a 10/01/2019). Como se pode ser no Parecer: "a utilização de uma função *hash* com uma variável criptográfica (em que um valor aleatório, designado por 'variável criptográfica', é adicionado ao atributo a ser dividido [*hashed*]) é passível de reduzir a probabilidade da determinação do valor de entrada mas, ainda assim, continua a ser possível de efetuar, mediante os meios razoáveis, o cálculo do valor original do atributo escondido por detrás do resultado de uma função *hash* com uma variável criptográfica" (cit. pág. 22).

[20] Neste sentido, Finck, Michèle. *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 11, disponível em https://papers.ssrn.com (acedido a 10/01/2019).

[21] Ramsay, Sebastian. *The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR*, Tese de Mestrado apresentada à Universidade de Estocolmo, 2018, p. 41, disponível em http://www.diva-portal.org (acedido a 10/01/2019).

aquele usuário pela reutilização daquela chave-pública e correspondente associação a determinado endereço de *IP*[22]. A não ser assim e mal se conceberia um sistema que usa precisamente a técnica da cadeia de blocos para garantir a unicidade da operação entre determinados sujeitos, i.e., para garantir que aquela operação em concreto foi efetivamente realizada por aqueles indivíduos em particular.

Sendo então possível associar aquela chave pública – leia-se, aquele dado pessoal (realização de uma transação, promoção de um registo, realização de uma operação de voto, etc.) – a determinado usuário, então teremos de concluir que também as chaves públicas se qualificam como dados pessoais para efeitos da aplicação da regulamentação europeia de dados pessoais[23].

Também paralela a esta discussão, encontra-se o acórdão C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* de 19 de Outubro de 2016, relacionado a endereços de *IP* dinâmicos (*dynamic IP addresses*); e isto porque aqui o TJ vem discutir o conceito de "dados pessoais" de forma muito relevante para o contexto da *blockchain*. Não obstante o acórdão ser anterior ao RGPD, como o conceito de dados pessoais deste se manteve inalterado, a referência mantém a sua pertinência.

---

[22] Reid, Fergal; Harrigan, Martin. "An analysis of anonymity in the bitcoin system", *arXiv:1107.4524v2*, 2011; e Biryukov, Alex; Khovratovich, Dimitry; Pustogarov, Ivan, "Deanonymisation of clients in Bitcoin P2P network", *arXiv:1405.7418v3*, 2014, ambos disponíveis em https://arxiv.org (acedido a 10/01/2019).

[23] Como clarifica Finck, uma chave pública é um dado que não pode ser imputado a determinado titular excepto se complementado com informações adicionais (tal como nome, endereço IP etc.). Quando essas informações se reúnem a identificação de usuários torna-se possível pelo que chaves públicas não podem ser consideradas dados anónimos. Para além dessas informações serem, não-raro, divulgadas voluntariamente pelos próprios usuários, a Autora também reporta que estudos académicos já demonstram que chaves públicas podem ser usadas para localizar endereços de *IP* se levar em conta informação adicional (cf. Finck, Michèle. *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 13, disponível em https://papers.ssrn.com (acedido a 10/01/2019). No mais, diz-nos De Filippi que "While good privacy norms would require people to constantly generate a new address before performing a new transaction, only a minority of people actually engage in these practices. In the Bitcoin space, most non-tech savvy people simply reuse their Bitcoin address without realizing that, by doing so, they are publicly disclosing valuable personal information" (Primavera, De Filippi. "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies", in *Journal of Peer Production*, v. 9, 2016, p. 11, disponível em https://papers.ssrn.com (acedido a 10/01/2019).

Alguns *sites* de serviços federais alemães para se protegerem de ataques *online* e permitir ações penais, guardam em registo todas as consultas de usuários que acedem aos seus sítios (sessão, nome do sítio, ficheiro consultado, dados transferidos, endereço *IP* do computador do utilizador etc.). P. Breyer, um desses usuários, deu entrada de uma ação contra a República Federal Alemã alegando que a conservação do seu endereço *IP* era desnecessária para os propósitos alegados. Ora, os *IP's* são conjuntos numéricos que permitem identificar computadores ligados à *internet* e que são transmitidos ao servidor do *site* visitado para que os dados consultados possam ser transferidos ao destinatário. Entre esses *IP's*, encontra-se uma modalidade designada "IP dinâmico" que, ao contrário do "IP estático", muda a cada nova conexão à *internet* e, assim, impede que, por ficheiros públicos, se consiga encontrar diretamente determinado computador sem antes recorrer ao respetivo fornecedor de acesso à *internet*. Em resposta à questão prejudicial colocada ao TJ sobre saber se esse *IP* dinâmico poderia ou não ser considerado dado pessoal, foi considerado que a noção de dado pessoal da então Diretiva 95/46 deveria ser interpretada no sentido de incluir esse endereço, mesmo quando careça de informações de terceiro (neste caso o fornecedor de acesso à *internet*) para prestar informação complementar necessária à identificação do computador usuário (§31); entendendo que um dado pessoal pode ser assim considerado mesmo que nem todas as informações necessárias para identificar o seu titular se encontrem na posse da mesma pessoa (§44) e desde que "não seja proibido por lei ou inexequível" (§46) a um fornecedor de serviços transmitir diretamente ao prestador aquelas informações suplementares necessárias à identificação do titular dos dados.

Algumas tentativas têm sido postas em prática para ultrapassar esta situação e retirar estes dados da alçada do RGPD. Relativamente aos *transactional data*, caso os dados sejam armazenados fora da cadeia pública), mas vinculados ao *ledger* através de um *hash*, seria possível encriptar os dados de forma segura, já que protegidos por um *hash* irreversível. No *ledger* apenas um dado aleatório alfanumérico ficaria visível enquanto os verdadeiros dados a que o *hash* se referia ficariam armazenados fora da cadeia de blocos. O principal risco associado a esta alternativa prende-se com a necessária implicação de um terceiro na gestão desse banco de dados editável fora da cadeia. Nesta situação, um dos potenciais motivos que teria conduzido à opção pela *blockchain* – a descentralização de informação

– seria diretamente afetada pela reunião do controlo/confiança dos dados numa entidade centralizada.

Ao contrário daqueles, porém, as *public keys* não podem ser transferidas para fora da cadeia por serem parte integrante do funcionamento da própria *blockchain* e necessárias para que a validação de transações ocorra. Apesar de a tarefa ser mais árdua, algumas tentativas têm, não obstante, se destacado na doutrina mais recente[24].

4.2. Tratamento de dados

Nos termos do art.º 4, n.º 2, do RGPD, o tratamento de dados é considerado como qualquer operação que é executada com dados pessoais, "(...) 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".

---

[24] Em particular, a criptomoeda *Monero* (que logrou esconder o endereço dos seus usuários, mudando-lhes o endereço e gerando chaves secretas) e as também designadas *zero knowledge proofs ou ZKP* (provas de conhecimento zero) que, sem fornecerem dados concretos, funcionam numa lógica binária de verdadeiro/falso e permitem atestar um acontecimento sem fazer referência a informações sobre o mesmo. Basicamente este ZKP limita-se a atestar se uma transação em que determinada chave pública foi usada teve lugar, sem mencionar dados sobre ela. Ainda numa outra hipótese, mencionam-se as chamadas *ring signatures,* que encontraram uma forma de omitir dados da *key* ao ocultar a transação realizada dentro de outras tantas; basicamente esta *ring signature* atesta que o usuário tem uma chave privada que corresponde a um conjunto de chaves públicas, mas sem revelar qual. Por último, destacam-se ainda técnicas que procuram dispersar a informação disponível, incorporando "ruído" ou "excesso de informação desnecessária": a ideia é garantir que de um ponto de vista externo seja impossível identificar os destinatários/remetentes das transações, tantas são e de forma tão agrupada que se apresentam. Por todos, Primavera De Filippi. "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies", in *Journal of Peer Production*, v. 9, 2016, p. 14, disponível em https://papers.ssrn.com, (acedido a 11/01/2019). O próprio GT29 já veio reconhecer esta última técnica como uma possível medida aceitável de anonimização. Para uma explicação clara das várias opções cfr. Relatório elaborado pela *EU Blockchain Observatory and Forum* (*Blockchain and the GDPR,* 2018, p. 19-23, disponível em https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (acedido a 11/01/2019).

Resta saber que ações são levadas a cabo nos dados que são lançados para a *blockchain* como dados pessoais. Aqui a análise uma vez mais ponderará quer as *public keys* e *transactional data*, quer os próprios *nodes*.

A cada *chave pública* corresponde uma determinada chave privada que é entregue a todos os usuários da cadeia de blocos, pelo que todos os usuários de uma chave pública se podem controlar mutuamente e verificar a autorização de novas transações. Essas verificações de validade são automatizadas segundo um algoritmo da tecnologia *DLT*. Tendo em conta a amplitude do termo de tratamento de dados no RGPD, mesmo que o tratamento seja autonomizado e se processe pela via de um algoritmo matemático, é possível qualificar como tal esta operação de verificação da validade de transações através de chaves públicas.

No que respeita aos *transactional data*, os dados são validados também através de certos algoritmos: são armazenados num determinado bloco, que é posteriormente anexado à *blockchain* e distribuído por todos os outros usuários. Isto implica que operações de uso e armazenamento são necessariamente realizadas, pelo que também quanto a estes dados se deve considerar existir tratamento de dados para efeitos do art. 4.º, n.º 2, do RGPD.

Quanto aos *nodes*/usuários e respetivo endereço, também vimos que cada um mantém cópia e registo com todos os outros *nodes* com os quais comunica, o que faz com que também eles mantenham uma rede de armazenamento de dados pessoais que possa ser qualificada como tratamento de dados[25].

5. Potenciais conflitos com princípios do RGPD

Como é característico das *blockchain* públicas, os participantes da cadeia normalmente desconhecem que dados (pessoais ou não; sensíveis ou não) estão a ser lançados no *ledger*. Por isso se diz no Relatório apresentado pelo EU *Blockchain Observatory and Forum* que o problema entre *blockchain* e o

---

[25] Ramsay, Sebastian. "The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR", *Tese de Mestrado apresentada à Universidade de Estocolmo*, 2018, p. 43-44, disponível em http://www.diva-portal.org (acedido a 12/01/2019)

RGPD não respeita à tecnologia em si, mas ao uso que dela é feito, o que implica uma análise casuística[26]. Isto porque, e como mencionámos acima, a *blockchain* apenas se revela através de *hashes* (códigos alfanuméricos). Um sistema público *blockchain* será usado por uma grande diversidade de usuários e para registar qualquer tipo de documentos, transações, registos, envolvendo indistintamente dados pessoais, dados não pessoais, dados sensíveis, etc. Dada a grande diversidade de usos possíveis, as *public blockchain* acabam por ter grande dificuldade em conseguir construir medidas de proteção do tipo requerido pelo RGPD (art. 25.º). Para fazer face a este problema, muitos talvez procurem transportar o encargo da *compliance* para os próprios utilizadores (proibindo o *upload* de certo tipo de dados, exigindo que os usuários prestem consentimento etc.), o que, claramente, não dá uma resposta satisfatória à situação.

A elaboração do RGPD foi levada a cabo num momento em que o revolucionário sistema descentralizado da *blockchain* se começava ainda a desenvolver, pelo que as principais preocupações a que precisava dar resposta centravam-se sobretudo nos serviços em *cloud* e nas redes sociais, organizadas essencialmente por sistemas centralizados com que os usuários interagem[27]. A chegada de *blockchains* públicas trazem consigo um sistema que foge a este mundo centralizado. Nestes sistemas onde toda a informação é partilhada e replicada por toda a rede, a eliminação de dados e a tutela da privacidade podem representam um problema para os seus titulares. Ora, como em princípio os dados armazenados numa cadeia de blocos se tornam invioláveis, excluí-los dificilmente se torna uma opção e a afetação do direito ao apagamento torna-se uma realidade. Por outro lado, o fenómeno da descentralização que tanto caracteriza o funcionamento desta tecnologia, implica a ausência de um controlo único e centralizado da informação numa entidade concreta, o que dificulta a compreensão dos sujeitos obrigados às regras previstas no Regulamento, o apuramento de responsabilidades e a aplicação das respetivas sanções.

---

[26] Relatório *Blockchain and the GDPR;* p. 16, disponível em https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (acedido a 11/01/2019).

[27] Eichler, Natalie, et. Al. "Blockchain, data protection and GDPR", in *Blockchain Bundesverband,* disponível em https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf (acedido a 28/01/2019).

É inegável a existência de uma grande tensão entre a arquitetura descentralizada desta tecnologia e o novo RGPD, que acaba por refletir um conflito idêntico de objetivos entre, por um lado, a necessidade de proteger dados pessoais e acautelar os direitos dos seus titulares e, por outro, a vontade de promover a inovação tecnológica.

5.1. Direito ao apagamento e retificação

Nestes sistemas de *blockchain* públicas, assim que transações são registadas na cadeia, deixam de poder ser modificadas ou apagadas: uma transação subsequente que anule ou modifique os termos da anterior pode sempre ocorrer, mas fá-lo-á mediante a adição de um novo bloco ao *hash* original que, além de registar a nova transação onde ratifica os dados da anterior, ainda a reproduz. A forma de garantir que a cadeia não é alterada e editável encontra-se na referência que cada bloco subsequente tem necessariamente que fazer do anterior, através de *hash* criptográfico; desta forma, se a informação contida nesse bloco anterior for alterada, assim também o será o respetivo *hash* o que permitirá a detetar a falsificação. Quer isto dizer, então que, em princípio, todos os dados lançados na *blockchain* seriam tendencialmente indestrutíveis, imutáveis e impassíveis de modificação, o que claramente representa um problema na óptica do RGPD.

Veja-se que já desde Maio de 2014, no processo C-131/12 que opôs *a Google Spain* e *Google Inc.* à Agência Espanhola de Proteção de Dados e a Mario González, o TJ determinou que este último, reclamante nos autos que moveu contra a Google, tinha direito a remover dos motores de busca qualquer conteúdo recuperável nos índices de resultados de pesquisa. Na sua justificação, o TJ considerou que esse direito é independente de saber se a manutenção dessa informação em resultados de pesquisa causa, ou não, qualquer prejuízo ao titular dos dados (§96); e que, nos termos dos direitos fundamentais plasmados no art. 7º e 8º da Carta, esse direito se sobrepõe não só sobre qualquer interesse económico do operador do motor de busca, como também de qualquer interesse público em encontrar essa informação em resultados de pesquisa, excepto em circunstâncias muito excepcionais (§97). Amparado no direito ao apagamento e de oposição da Diretiva 95/46 (art.os 12.º, b) e 14.º, a), respetivamente) o TJ veio consolidar o "direito ao esquecimento" no espaço informático, o qual, por sua vez,

foi igualmente reforçado em rúbrica própria pelos art.os 17º e 5.º, n.º 1, al. d) do RGPD.

Naturalmente que o direito ao apagamento não é de natureza absoluta. As circunstâncias em que os titulares dos dados podem fazer uso deste direito restringem-se, entre outras, às situações em que: (i) deixem de ser necessários à finalidade que motivou a recolha (art.º 17º, n.º1, al. a) do RGPD); (ii) o titular retire o seu consentimento (art.º 17º, n.º1, al. b) do RGPD); (iii) o titular oponha-se ao tratamento sem que haja interesses legítimos prevalecentes que o justifiquem (art.º 17º, n.º 1, al. c) do RGPD); ou (iv) tenham sido tratados ilicitamente (art.º 17º, n.º 1, al. d) do RGPD). Mas independentemente disto, outros problemas práticos poderiam advir desta situação. Desde logo, o titular dos dados que pretendesse fazer valer este direito não tinha como reclamar perante todos os outros *nodes* da rede os seus direitos, já que não tinhe como os identificar. Por outro lado, mesmo que o conseguisse, esses *nodes* não teriam como, eles mesmos, conseguir modificar ou apagar qualquer dado armazenado no *DLT*.

Além deste âmbito limitado, também caberá perguntar o que efetivamente constitui a noção de "apagamento" ("*erasure*"), já que o próprio RGPD não o especifica. Será que representa o total desaparecimento dos dados do mundo real e/ou virtual, ou basta que haja técnicas de proteção que tornem os mesmos criptografados de forma irreversível? Já vimos que no âmbito do sistema *blockchain* um apagamento é tecnicamente muito difícil porquanto o sistema foi criado precisamente com o propósito de impossibilitá-lo. No entanto, a criação de alternativas tecnológicas que limitem o processamento dos dados[28], ou que façam referência a dados anteriores como não sendo mais consideráveis, poderá ser questionável como sendo suficiente para efeitos de acautelar este direito.

Já têm sido desenvolvidas ideias que permitem ultrapassar este problema. Mas mais uma vez a análise passa por uma distinção entre *transactional data* e *public keys*[29].

Quanto aos primeiros, basta que os mesmos sejam armazenados num banco editável e criptografado de dados fora da cadeia, para poder

---

[28] Finck, Michèle. "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation and Competition Research Paper,* n. 18-01, p. 24, disponível em https://papers.ssrn.com (acedido a 20/01/2019).

[29] *Idem,* p. 24.

corresponder com as exigências do RGPD e permitir a eliminação dos dados sem interferir com a *blockchain*. Todavia, estas modificações ao *software* sempre acarretarão consequências indesejáveis, nomeadamente no plano da integralidade de teor e autenticidade dos documentos registados na *blockchain*, requerendo a nomeação de entidades responsáveis para as administrar. Por outro lado, certas características apontadas como grandes vantagens desta tecnologia, tal como a descentralização de dados *P2P*, deixarão de poder subsistir, para que se permita a compatibilização da mesma com o RGPD. Alternativamente, e como já vimos acima, surge ainda a possibilidade de armazenar dados num banco de dados encriptado e introduzir um *hash* desse mesmo banco na cadeia de blocos; técnica que mantém a integralidade e integridade do teor dos dados sem os tornar visíveis no *ledger*. Esta é, de resto, uma tendência nesta indústria: evitar enviar dados pessoais diretamente na cadeia de blocos, para os armazenar em bancos de dados fora da cadeia, com apenas um e unidirecional *hash* dos dados armazenados na própria *blockchain*; é esse *hash* que servirá de ponto de referência e link para o banco de dados fora da cadeia de blocos.

No que respeita às *public keys*, há quem mencione procedimentos realizados em ambientes supervisionados e seguros onde o próprio titular dos dados possa eliminar a sua chave privada, inviabilizando simplesmente o acesso àqueles dados, já que ela seria a única responsável por desencriptar a respetiva informação[30]. Em alternativa, há quem fale nos chamados *chameleon-hashes* ("*hashes* camaleão") que reescreveriam o teor dos blocos armazenados na *blockchain*, sob determinadas restrições e supervisão de autoridades autorizadas e com transparência[31]. Esta solução, porém, ao

---

[30] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper,* n. 18-01, p. 24, disponível em https://papers.ssrn.com (acedido a 20/01/2019). No mesmo sentido, também a a *Comission Nationale Informatique & Libertés* (CNIL) reconhece que "(...) la suppression de la clé secrète de la fonction de hachage qui aura un effet similaire. Il ne sera plus possible de prouver ou de vérifier quelle information avait été hachée. L'empreinte ne présentera plus, en pratique, de risque sur la confidentialité. L'information devra, ici aussi, être supprimée des autres systèmes où elle aura été stockée pour le traitement" (p. 10, disponível em: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf , acedida a 22/01/2019).

[31] Giuseppe Ateniese et al, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends", pág. 2, disponível em https://eprint.iacr.org/2016/757.pdf (acedido a 23/01/2019): "(...) we argue that an immutable ledger is not appropriate for all new applications

confiar numa terceira autoridade/árbitro para realizar o serviço, acaba por voltar ao mesmo problema da própria essência da *blockchain* ser posta em causa.

5.2. Transferência de dados

Nos termos do disposto no art.º 3.º, n.º 1 e 2 (após a correção linguística levada a cabo pelo Conselho da UE n.º 8088/18[32]), o RGPD aplica-se a tratamentos de dados independentemente da residência do seu titular, desde que este se encontre em território da União. Por outro lado, nos termos do art.º 44º do RGPD, as transferências de dados para países terceiros só são possíveis quando respeitado um conjunto de condições, nomeadamente a existência de um nível de proteção adequado (a definir pela própria Comissão) e de uma autorização específica do titular dos dados.

E é aqui que chegam as perguntas: como podemos determinar em que país determinado *node* se encontra? Como é que na *blockchain* podemos garantir que as transferências de dados se processam com níveis adequados de proteção? No âmbito da contratação digital, será possível estabelecer cláusulas contratuais padronizadas para salvaguardar estes direitos na *blockchain*?

Sucede, porém, que quando estão em causa *blockchain* públicas uma presunção quanto à existência de *nodes* situados – ou de tratamentos

---

that are being envisaged for the blockchain. Whether the blockchain is used to store data or code (smart contracts), there must be a way to redact its content in specific and exceptional circumstances. Redactions should be performed only under strict constraints, and with full transparency and accountability"); Ibáñez Luis-Daniel, O'Hara, Kieron; Simperl, Elena. "On Blockchains and the General Data Protection Regulation", p. 8, disponível em https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf (acedido a 09/01/2019).

[32] Documento do Conselho da UE, n.º 8088/18, de 19 de abril de 2018, disponível em http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf (acedido a 22/01/2019). Sobre a problemática linguística que antecedeu esta revisão Moniz, Maria Graça, "Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD", *UNIO – EU Law Journal*, v. 4, n. 2, 2018, disponível em http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Graça%20Canto%20Moniz.pdf (acedido a 18/01/2019).

realizados – fora do território da União torna-se fácil de extrair. Além disso, os *miners* (mineradores) – que resolvem os problemas matemáticos que permitem o lançamento de dados para o *ledger* –, são sempre escolhidos aleatoriamente para a tarefa, podendo encontrar-se em qualquer lugar do mundo[33]. Na falta da decisão tomada ao abrigo do art.º 45º, dispõe o art.º 46º que os dados sempre poderão ser transferidos para terceiros, desde que apresentadas "garantias adequadas e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas" eficazes. Ora, apesar de em teoria se poderem conceber alterações ao protocolo do *software* o se compatibilizar com estas condições, dificilmente tal será possível. Por ser assim, a doutrina tem vindo a apontar a necessidade de consentimento explícito para a transferência dos dados a terceiros, com informação prévia acerca dos possíveis riscos envolvidos[34].

5.3. Controlo sobre os dados

Outro problema de compatibilização que encontramos entre *blockchain* e o RGPD prende-se com a identificação do responsável pelo tratamento (*data controller*), *i.e.*, aquele que determina as finalidades do tratamento de dados e assume a responsabilidade originária por qualquer violação[35]) e do subcontratante (*data processor*), *i.e.,* aquela entidade que efetivamente realiza o tratamento de dados conforme instruções do responsável pelo tratamento. E este problema é tanto mais complexo no contexto digital da *blockchain*, quanto mais nos apercebermos de que as mesmas entidades podem assumir, simultaneamente, mais do que um papel. Apesar de ambos os papéis desempenhados não serem livres de obrigações e responsabilidades pelo RGPD, a determinação precisa de cada um não deixa de ser determinante.

Naturalmente que no caso das *private blockchain,* aquele que se assume destinatário dos dados enviados pelo titular pode facilmente qualificar-se

---

[33] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 19, disponível em https://papers.ssrn.com (acedido a 08/01/2019).

[34] *Idem*, p. 19.

[35] Art. 4º, n.º 7 do RGPD.

como responsável pelo tratamento[36]. Todavia nas restantes *DLT*, verdadeiramente descentralizados em dezenas ou centenas de *nodes*/computadores, todos podem carregar dados para determinada finalidade e tratar os dados de terceiros. Nesta ordem de ideias, ou concluímos que nenhum deles se pode qualificar como responsável pelo tratamento, já que verdadeiramente inexiste um agir autónomo e independente com propósitos de tratamento, nem tão-pouco se poder dizer que eles ajam com propósitos de tratamento relativamente às informações distribuídas na rede por terceiros; ou então que todos o são porquanto nenhum deles está sujeito a instruções de terceiro no momento em que decidem carregar dados para o *ledger*[37]. Outra alternativa, seria perceber os *nodes* como responsáveis conjuntos pelo tratamento, nos termos do art.º 26.º, n.º 1 do RGPD, mas, para isso, eles teriam que determinar conjuntamente as finalidades e meios comuns de tratamento, o que realmente não acontece[38].

Os *nodes* assumem um papel efetivamente importante no tratamento de dados, já que têm total autonomia para entrar e sair da *blockchain*, escolher que dados querem fornecer etc. Todavia, o poder de decisão quanto aos objetivos do *software* não está nas mãos destes. Com efeito, é o criador de cada *blockchain* que determina o tipo de utilidade para o qual ele será requisitado (realizar registos, promover transações, gestão de propriedade e de ativos financeiros etc.). É neste contexto que surge a possibilidade de onerar os criadores dos vários *DLT's* como responsáveis de tratamento, visto que são efetivamente estes que constroem algoritmos específicos para a subordinação de determinada *blockchain* a finalidades concretas e a propósitos determinados. Mas encontrar no criador do algoritmo o

---

[36] Inclusivamente, como recomendado pelo Parecer da CNIL a respeito (2018), os responsáveis pelo tratamento nas redes de *blockchain* privadas devem ser logo identificados nos respetivos projetos (disponível em: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf (acedido a 15/01/2019)).

[37] Esta parece ser a interpretação do Parecer da CNIL, pág. 2, disponível em https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf (acedido a 15/01/2019): sempre que: "lorsqu'il est une personne physique et que le traitement de données personnelles est en lien avec une activité professionnelle ou commerciale (c'est—à-dire lorsque l'activité n'est pas exclusivement personnelle)".

[38] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 17, disponível em https://papers.ssrn.com (acedido a 20/01/2019).

verdadeiro responsável pelo tratamento nem por isso torna a aplicação do RGPD mais fácil: basta relembrar que o criador da *Bitcoin* (Satoshi Nakamoto) permanece até aos dias de hoje sob anonimato.

Será que os *nodes* estariam então livres de responsabilidade? Se cada pessoa que atua na rede *P2P* constitui um *node* independente; se, como visto acima, cada *node* realiza tratamentos de dados; se os usuários não podem ser qualificados como responsáveis pelo tratamento, mas ainda assim realizam tratamento de dados "em nome" destes; então teremos forçosamente de concluir que cada *node* que se conecta a uma *blockchain* pode ser qualificado como subcontratante. A ser assim, restaria perceber como é que a responsabilidade dada aos subcontratantes pelo RGPD seria aplicável numa rede como esta[39]. E é aqui que ressaltam uma série de perplexidades: (i) o fato de os *nodes* poderem encontrar-se fisicamente nos mais diversos lugares do mundo ou assumirem uma identidade encriptada pode gerar grandes dificuldades na aplicação de sanções[40]; (ii) o fato de os usuários serem apenas utilizadores de um *software* desenvolvido por terceiros, agindo manualmente segundo as instruções registadas pelos criadores daquele num algoritmo *blockchain*; (iii) o fato destes *nodes* armazenarem cópias dos dados do *ledger* nos seus computadores em versões criptografadas ou em *hashing*, que nem podem ser editados; (iv) o fato de o RGPD exigir dos subcontratantes o fornecimento de garantias relativamente à existência de recursos para implementar soluções técnicas de proteção de dados pessoais; soluções estas que lhes são passadas diretamente pelo responsável pelo tratamento via algoritmo e com o qual estes nem sequer podem interagir ou interferir em caso de necessidade para proceder a alterações às medidas já criadas. Em suma, aos olhos de um Regulamento que conceitua o subcontratante como alguém contratado para providenciar soluções técnicas

---

[39] Ramsay, Sebastian. "The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR", *Tese de Mestrado apresentada à Universidade de Estocolmo*, 2018, pág. 48, disponível em http://www.diva-portal.org (acedido a 20/01/2019).

[40] Neste cenário, imensos *nodes* teriam de ser contatados e forçados a cumprir com as disposições do RGDP, o que num cenário normal apenas teria que ser feito perante um único responsável pelo tratamento. No final do dia, poderíamos inclusivamente a uma situação em que o próprio *software blockchain* deixaria de funcionar pela retirada forçada dos *nodes* para poderem cumprir com os direitos de um único titular de dados.

ou processar dados, a qualificação dos *nodes* como subcontratantes perde muito o seu sentido útil.

5.4. Limitação do tratamento

Nos termos do art.º 5.º, n.º1, al. b), do RGPD, os dados recolhidos têm que obedecer a finalidades determinadas, explícitas e legítimas, não podendo extrapolar as finalidades que determinaram a recolha. A compatibilização da *blockchain* com este princípio parece enfrentar também algumas dificuldades visto que na cadeia de blocos os dados armazenados no *ledger* tornam-se irremovíveis por estarem constantemente a ser objeto de subsequentes acréscimos de dados. Já para não falar do fato de que cada *node* armazena cópias de todas as informações que foram lançadas no *DLT*. As soluções apresentadas para o problema do direito ao apagamento e de retificação podem ser trazidas nos mesmos termos para esta situação, por forma a minimizar e limitar os tratamentos sobre os dados coletados; todavia o mesmo *handicap* relativamente aos dados das *public keys* permanecerá por resolver já que estes não podem mesmo ser removidos.

Conclusões

Conforme ficou visto acima, existem vários pontos no Regulamento que precisam ser apreciados com grande cautela quando aplicados à tecnologia *blockchain*. Depois de concluir que os dados importados para a cadeia de blocos têm necessariamente que ser considerados como dados pessoais (ainda que pseudonimizados), a sujeição deste *DLT* ao RGPD torna-se um fato inegável, independentemente de os vários *nodes* existentes na rede poderem ou não ser encontrados em espaço territorial europeu. Se assim é, e porque esta tecnologia implica o armazenamento e uso de dados por todos os seus usuários, a conclusão de que na *blockchain* também se realizam tratamentos de dados não é igualmente difícil de extrair. Chegámos à conclusão que certos conceitos como os de responsável pelo tratamento ou de subcontratante têm sido um dos pontos mais questionados pela doutrina especializada, precisamente por causa da complexidade em perceber (i) quem é que efetivamente desempenha qual papel e (ii) das dificuldades

por detrás do cumprimento do Regulamento a qualquer um deles. Por outro lado, vimos também alguns dos principais direitos consagrados no RGPD encontram-se de alguma forma postos em causa com o sistema *blockchain*; mas que, não obstante os grandes pontos de confronto que ainda têm, começa a ser possível conceber, quer por meios técnicos que modificam o algoritmo ou permitem fugas ao *ledger*, quer por meios legais que atenuam o próprio conceito legal de "eliminação", uma luz ao fundo do túnel possa vir a salvaguardar a compatibilização com o RGPD.

Afinal, por mais fundamental e revolucionária que esta tecnologia possa parecer, ajustes e adequações ao Regulamento terão necessariamente que ser levados em consideração por forma a permitir a sua compatibilização com a política europeia de proteção de dados.

A videovigilância e a compressão da privacidade

Lurdes Dias Alves*

Resumo: Videovigilância e privacidade são conceitos antagónicos mas que se apresentam como um dilema preocupante nesta sociedade do século XXI. Neste texto procuraremos analisar a necessidade de implementação de sistemas de videovigilância em locais públicos, tendo em conta a salvaguarda de direitos fundamentais e a devida adequação dessa instalação e implementação com o Regulamento Geral de Proteção de Dados. Estabelecendo-se o confronto de direitos legalmente protegidos – direito à privacidade *versus* direito à segurança, confronto que merece a devida reflexão. Será a privacidade (tal como a conhecemos) um conceito em vias de extinção ou ainda tem cabimento nesta sociedade cada vez mais pátula? Facilmente concluímos que, nesta sociedade cada vez mais aberta e adepta das novas tecnologias ao dispor, em que a vida privada, e até a vida familiar, é constantemente exposta sem a menor prudência, e até recato, deixou de ter cabimento a noção, e o sentido, da privacidade, tal como a conhecemos.

Palavras Chave: *Videovigilância; privacidade; direitos fundamentais; segurança.*

Abstract: Video surveillance and privacy are antagonistic concepts that present themselves as a worrying dilemma in this 21st century society. In this text we will analyse the need to implement video surveillance systems in public places, considering

---

* Licenciada em Direito pela Universidade Autónoma de Lisboa. Pós-graduada em Direito Comercial e Direito Societário pela Universidade Católica Portuguesa – Escola de Lisboa. Mestre em Direito (especialidade de Ciências Jurídicas) pela Universidade Autónoma de Lisboa. Doutoranda em Direito (especialidade de Ciências Jurídicas) na Universidade Autónoma de Lisboa, onde investiga o tema: "*A proteção de dados pessoais e o sigilo bancário – A derrogação da privacidade*". Investigadora integrada no RATIO LEGIS – Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa. Cocoordenadora de Pós-Graduações em Proteção de Dados Pessoais, Privacidade e Cibersegurança na UE, na Autónoma Academy (Escola de Pós-graduações da Universidade Autónoma de Lisboa).

the safeguarding of fundamental rights and the adequate adaptation of this installation and implementation with the General Regulation of Data Protection. Establishing the confrontation of legally protected rights – the right to privacy versus the right to security, a confrontation that deserves due reflection. Is privacy (as we know it) an endangered concept, or does it still fit in this increasingly patulus society? We easily conclude that in this increasingly open society and adept at the new technologies available, where private life, and even family life, is constantly exposed without the slightest prudence, and even notion, and sense of privacy as we know it.

Keywords: *Video surveillance; privacy; fundamental rights; safety.*

Introdução

É indubitável que vivemos numa sociedade assente na tecnologia – e, por exemplo, basta pensar nas câmaras de videovigilância em grande parte do espaço público e privado; as instituições de crédito e sociedades financeiras sabem onde e como gastamos o nosso dinheiro (mais ainda, sabem como o ganhamos); as grandes superfícies sabem os produtos que consumimos, quais os nossos gostos e tendências, ao ponto de poderem definir um perfil pessoal dos nossos hábitos e rotinas; os «*radares*» e a «*via verde*» sabem por onde nos deslocamos e para onde viajamos; máquinas de «*raio X*» nos aeroportos visualizam os nossos pertences (e até o nosso corpo); a utilização de «*cookies*» permite determinar a nossa utilização e navegação na internet (a tão usualmente designada pegada digital); estas, entre muitas outras situações, mostram a variedade de casos em que, voluntária ou involuntariamente, a nossa privacidade fica mitigada ou até mesmo comprometida.

Nos últimos anos tem-se assistido a um crescimento exponencial do volume de dados gerados por sistemas de informação, em redes sociais, aparelhos móveis, entre outros, ligados em rede e que geram dados, interligados e a uma velocidade não antes imaginável.

O RGPD, apesar de encerrar em si muitos princípios, regras gerais, direitos e obrigações que já constavam da Diretiva N.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 (Diretiva), a verdade é que vem introduzir alterações importantes ao regime anteriormente aplicável.

Uma das alterações introduzidas pelo RGPD é o fim do controlo prévio exercido pela Autoridade Nacional, no caso português, a CNPD. Assim, o tratamento de dados pessoais, onde naturalmente se inclui a videovigilância, deixa de ter a obrigatoriedade de autorização prévia.

Em Portugal e quanto à videovigilância, este facto assume especial relevância, dado que, a Lei de Segurança Privada (Lei 34/2013, de 16 de maio) estabelecia os requisitos a respeitar na instalação e exploração de um sistema de videovigilância. Contudo, sendo que a videovigilância não é um recurso exclusivo da segurança privada, tais requisitos não se impunham se a videovigilância fosse explorada fora do contexto da segurança privada. E é precisamente neste ponto que o controlo prévio exercido pela CNPD era fundamental, permitia que a Comissão estabelecesse as condições de exploração do sistema, especialmente quanto ao prazo máximo de gravação das imagens (geralmente 30 dias), a finalidade (usualmente, a proteção de pessoas e bens), os destinatários dos dados (em regra, apenas órgãos de polícia criminal e autoridades judiciárias, para utilização em processos crime) e o direito de informação (através da afixação em local visível da informação sobre a existência de videovigilância).

Excluindo o RGPD a obrigatoriedade do controlo prévio, nem definindo as regras a cumprir na utilização de videovigilância, existe a necessidade de Portugal, internamente e sem prejuízo da aplicabilidade do Regulamento, criar legislação que regule e fixe os limites da utilização da videovigilância.

Neste contexto, considera-se adequado analisar algumas questões inerentes à utilização da videovigilância, desde logo, enquanto meio de recolha de dados pessoais, a sua utilização à luz do RGPD, a eventual necessidade de avaliação prévia de impacto sobre a proteção de dados e as finalidades, da utilização, previstas em Portugal.

1. A Videovigilância enquanto meio de recolha de dados pessoais

É consensual a definição que a videovigilância se traduz na recolha de imagens por meio eletrónico e que constituem dados pessoais "*informação relativa a uma pessoa singular identificada ou identificável*" (n.º 1 do art. 4.º do RGPD). Logo, as imagens recolhidas por sistema de videovigilância constituem ou, pelo menos, são suscetíveis de constituir dados pessoais,

desde que recolham imagens de pessoas, de objetos ou de equipamentos que permitam, ainda que de forma indireta, a identificação concreta de pessoas.

A este propósito, sempre se dirá que, para que as imagens de videovigilância constituam dados pessoais, não é necessário que integrem imagens explícitas de pessoas, mas tão só imagens que permitam identificar ou localizar pessoas[1]. Sublinha-se que a imagem de pessoas, para além da salvaguarda no contexto da legislação de proteção de dados pessoais, encontra-se legalmente protegida, desde logo, na CRP que, no art. 26.º, n.º 1, ressalva que a todos é reconhecido, entre outros, o direito à imagem e à reserva da intimidade da vida privada. De igual modo, o CC, no art. 79.º, prevê o direito à imagem: "*o retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela...*", bem como o CP que, no art. 199.º, criminaliza as gravações e fotografias ilícitas, prevendo a punição de quem "*fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado*"[2]. Assim, a videovigilância, ao recolher imagens de pessoas, é suscetível de derrogar o direito à imagem e à reserva da vida privada[3].

De facto, existe um conflito de interesses entre o direito à privacidade e o interesse público, ou seja, a promoção e garantia de segurança *versus* o direito à privacidade e o direito à liberdade impõe um exercício

---

[1] Imagens que permitam identificar uma viatura, através da matrícula ou de outra caraterística inequívoca, que permita atribuir a propriedade ou utilização dessa viatura a determinada pessoa, constitui dado pessoal.

[2] Sendo estas as regras, existem, naturalmente, exceções, como a prevista no n.º 2 do art. 79.º do CC, que prevê que "*Não é necessário o consentimento da pessoa retratada quando assim o justifiquem a sua notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didáticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente.*".

[3] A este propósito, o TC, no Acórdão n.º 255/2002, 8 de Julho de 2002, p. 5239, debruçando-se sobre a Lei de Segurança Privada, à data em vigor (Decreto-Lei n.º 231/98 de 22 de julho) e declarando inconstitucional alguns dos seus preceitos, refere que "*Apesar de a lei impor a afixação, em local bem visível nos lugares objecto de vigilância com recurso àqueles meios, de avisos a informar do facto, prescrevendo assim uma espécie de consentimento implícito do cidadão que permanece naqueles locais, a verdade é que tal medida legal constitui também ela uma verdadeira restrição aos direitos à imagem e à reserva da intimidade da vida privada e familiar*", acrescentando, no entanto, que "*O interesse público inerente à actividade de segurança privada, expresso pelo próprio legislador, justificará as restrições em causa*".

permanente, para preservar o bem jurídico e manter o seu equilíbrio. Não foi certamente por mero acaso que, o legislador constitucional não dissociou a liberdade da segurança (art. 27.º CRP), criando normas que se pretendem indissociáveis, não sendo, ainda assim, direitos absolutos, tanto que "*a liberdade de cada um é relativizada pela liberdade de todos*"[4]. A videovigilância, pela proteção e salvaguarda dos direitos fundamentais que possa fazer perigar, tem sido objeto de vastas análises e não raras vezes de reservas quanto à sua utilização.

2. A videovigilância à luz do Regulamento Geral de Proteção de Dados

Começamos por salientar que embora o RGPD seja aplicável a todas as operações de dados em cujas atividades se aplique o direito da União Europeia, não se aplica ao tratamento de dados efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, bem como, também não se aplica quando efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas (art.º 2.º do RGPD).

O tratamento de dados de videovigilância, de modo sintético, pode absorver em si, por um lado, regras genéricas, por serem aplicáveis ao tratamento de todos os dados pessoais e, por outro lado, regras específicas, por serem aplicáveis em exclusivo à videovigilância.

Considerando como regras genéricas, os princípios da licitude, lealdade e transparência (art.º 5.º do RGPD), na origem do tratamento de dados pessoais tem de existir uma fonte de licitude – o consentimento do titular dos dados; execução de um contrato; cumprimento de uma obrigação legal; realização de um interesse legítimo; defesa de interesses vitais (*v.g.* saúde), exercício de funções de interesse público (art.º 6.º do RGPD).

Ainda, deve-se observar os princípios relativos ao tratamento de dados pessoais: o princípio da limitação das finalidades – a recolha e tratamento de dados pessoais deve ter uma finalidade determinada, explícita e legítima,

---

[4] Conforme afirma Dias, Manuel Domingos Antunes. *Liberdade, Cidadania e Segurança*. Coimbra: Almedina, 2001, p. 7.

não podendo posteriormente ser utilizados para outra finalidade que não aquela que previamente esteja identificada; princípio da minimização de dados – os dados a recolher e tratar deverão ser os mínimos e indispensáveis à finalidade a que se destinam, devendo respeitar critérios de proporcionalidade (adequação, necessidade e proporcionalidade em sentido estrito); princípio da exatidão – os dados devem ser exatos e atualizados, devendo ser adotadas medidas tendentes a que os eventuais dados inexatos sejam apagados ou retificados; princípio da limitação da conservação – devem ser definidos prazos limitativos para a conservação dos dados, devendo estes ser preservados apenas durante o prazo em que se mostrem necessários e adequados à finalidade para a qual foram recolhidos; princípio da integridade e confidencialidade – devem ser adotadas medidas de segurança que garantam a proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental; e o princípio da responsabilidade – o responsável pelo tratamento dos dados é responsável pelo cumprimento dos princípios atrás identificados e cabe a este, demonstrar e comprovar esse cumprimento (n.º 2 do art.º 5.º do RGPD).

Quanto a regras específicas a obedecer na exploração de um sistema de videovigilância, partindo do princípio de que estas regras não contrariam o já previsto especialmente na Lei de Segurança Privada, bem como nas autorizações emitidas pela CNPD, ainda que ao abrigo do RGPD, deverão considerar-se: as gravações de imagem obtidas pelos sistemas de videovigilância devem ser conservadas, em registo codificado, pelo prazo de 30 (trinta) dias contados desde a respetiva captação, findo o qual devem ser destruídas[5]; todas as pessoas que tenham acesso às gravações realizadas, em razão das suas funções, devem sobre as mesmas guardar sigilo[6]; nos locais objeto de vigilância com recurso a câmaras de vídeo é obrigatória

[5] Salvo expressa indicação legal em contrário, *v.g.*, o previsto na Lei 51/2006 de 29 de agosto, Lei n.º 54/2012 de 6 de setembro, em que os prazos são de 180 e 90 dias, respetivamente.

[6] Salvo expressa indicação legal em contrário (*v.g.*, o previsto na Lei 51/2006 de 29 de agosto) é proibida a cessão ou cópia das gravações obtidas, só podendo ser utilizadas nos termos da legislação processual penal, com eventual possibilidade da sua utilização para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal.

a afixação, em local bem visível, do sinal identificado da existência de câmaras de vídeo[7]-[8].

3. Avaliação Prévia de Impacto sobre a Proteção de Dados

Embora com o RGPD tenha deixado de existir a figura do controlo prévio, anteriormente exercido pela CNPD, em certa medida, o controlo prévio passará a ser efetuado pelo EPD ou, do inglês, DPO (art.º 39.º do RGPD). Todavia, existe agora a figura da consulta prévia, segundo a qual o responsável pelo tratamento deve dirigir-se à autoridade de controlo antes de proceder a um tratamento de dados pessoais quando se tenha verificado, após uma prévia AIPD (art.º 35.º do RGPD), que se está perante um elevado risco para os direitos e liberdades das pessoas singulares.

Entre as singularidades e particularidades introduzidas pelo RGPD, encontramos a figura do EPD, que, não sendo uma figura nova no quadro da proteção de dados pessoais, individualizou-se assumindo-se como um dos elementos mais determinantes no seio das organizações, para a criação e/ou promoção de uma cultura de proteção de dados pessoais, e uma garantia permanente de *compliance* nesta área tão sensível.

A figura do EPD nas organizações não é nova. A Diretiva não obrigava as organizações a nomear um EPD, mas, ainda assim, a prática da nomeação de

---

[7] Cfr. anexo VIII da Portaria 273/2013, de 20 de agosto, acompanhado da seguinte informação: a) A existência e localização das câmaras de vídeo, *v.g.,* pode colocar-se no local objeto de vigilância uma informação com as seguintes menções «*neste espaço, existem 6 câmaras de videovigilância localizadas nos seguintes espaços: hall (2 câmaras), corredor norte (3 câmaras) e corredor sul (1 câmara)*»". b) A menção «*Para sua proteção, este local é objeto de videovigilância*»; c) A entidade de segurança privada autorizada a operar o sistema, pela menção do nome e alvará ou licença (no caso de a operação ser garantida por entidade de segurança privada); d) A identificação do responsável pelo tratamento dos dados recolhidos perante quem os direitos de acesso e retificação podem ser exercidos.

[8] Contudo, as câmaras, ou outros meios de captação de imagem, não podem incidir sobre: a) Vias públicas ou propriedades limítrofes, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel; b) A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM; c) O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário; d) O acesso e o interior de áreas reservadas aos trabalhadores, designadamente vestiários e instalações sanitárias.

EPD desenvolveu-se em várias organizações dos Estados-Membros ao longo dos anos. Ainda antes da adoção do RGPD, o GT29[9] pugnava pela função do EPD como um pilar da responsabilidade, sendo que, a nomeação de um EPD poderia facilitar a conformidade com o RGPD e, além disso, propiciar uma vantagem competitiva às empresas que nomeassem um EPD[10].

Além de facilitar a conformidade através da implementação de instrumentos de responsabilização (*v.g.*, viabilizando avaliações de impacto sobre a proteção de dados e efetuando ou viabilizando auditorias), os EPD[11] são também intermediários com os *stakeholders* mais relevantes da organização, encimados pela CNPD.

A AIPD, sendo uma das inovações no tratamento de dados pessoais, é indiciadora de preocupação quanto à segurança dos dados e da importância

---

[9] Equipa instituída ao abrigo do artigo 29.º da Diretiva 95/46/CE, foi órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições estiveram descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.) Grupo este que deu lugar após 25 de maio de 2018 com a eficácia plena do RGPD, ao Comité Europeu para a Proteção de Dados.

[10] *Guidelines on Data Protection Officers from WP 29*. [Em linha]. Adotadas em 13 de dezembro de 2016. (Última redação revista e adotada em 5 de abril de 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. p.4. (acedido a 20/05/2018).

[11] A figura do EPD, apesar de não carecer de certificação profissional para o efeito, é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados. A sua existência não é obrigatória para todos os tratamentos de dados, mas apenas para as situações previstas no art.º 37.º do RGPD, destacando-se aquelas em que o tratamento é efetuado por uma entidade pública, nomeadamente pelo Estado, regiões autónomas, autarquias locais, entidades administrativas independentes, institutos públicos, instituições de ensino superior públicas de natureza fundacional, empresas públicas sob forma jurídico pública e associações públicas. É, ainda, necessário designar um EPD quando as operações de tratamento exijam um controlo regular e sistemático dos titulares dos dados em grande escala, ou quando sejam tratados dados em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações, estando estes definidos nos art.º 9.º e 10.º do RGPD, respetivamente. As funções do EPD devem ainda compreender todas as questões relacionadas com a proteção de dados, informando e aconselhando o responsável pelo tratamento ou o subcontratante, controlando o cumprimento das regras e requisitos, nomeadamente o previsto no RGPD, prestando aconselhamento e controlando a realização da avaliação prévia de impacto, bem como cooperando e sendo o ponto de contacto com a autoridade de controlo (art.º 39.º do RGPD).

a esta atribuída. O art.º 32.º do RGPD prevê que "o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, destacando, nomeadamente, as seguintes possíveis medidas: a pseudonimização e a cifragem dos dados pessoais; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento".

No tratamento de dados de videovigilância e considerando que estes são suportados informaticamente, deverá o sistema possuir as habituais medidas de segurança de qualquer sistema informático, que garantam a sua permanente disponibilidade, integridade e confidencialidade. Assim, o acesso a imagens deverá ser precedido de controlos físicos[12] e controlos lógicos[13].

A retirada do sistema de imagens gravadas deverá, para além de restrita a pessoas identificadas segundo critérios de necessidade, obrigar a justificação no próprio sistema. Tratando-se de sistema de videovigilância, cujas imagens apenas possam ser utilizadas para fins processuais penais, uma justificação prática e funcional será, por exemplo, registar no sistema o NUIPC para o qual as imagens serão disponibilizadas.

Ainda no que concerne à segurança dos dados, e não obstante as medidas de segurança que devem ser implementadas[14], sempre que ocorra um incidente de segurança que afete dados pessoais, ou se eventualmente os

---

[12] Controlo do acesso ao espaço físico onde as imagens podem ser visualizadas.

[13] Utilização de login e password individual e personalizado para acesso ao sistema, bem como registo desses mesmos acessos, que permitam conhecer quem acedeu, quando acedeu, ao que acedeu e especialmente que tratamento efetuou.

[14] O RGPD exige que o responsável pelo tratamento aplique todas as medidas técnicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação e para informar rapidamente a autoridade de controlo e os titulares dos dados, deverá ainda, comprovar que a notificação foi enviada sem demora injustificada e importa ter em conta, em especial, a natureza e a gravidade da violação e as respetivas consequências e efeitos adversos para o titular dos dados.

dados forem violados[15] e acedidos por quem não o possa fazer ou utilizados para fim diverso da finalidade prevista, o responsável pelo seu tratamento notifica a autoridade de controlo (Art.º 33.º do RGPD) e, se essa violação for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, essa comunicação é efetuada, também, ao titular dos dados respetivos (Art.º 34.º do RGPD).

Neste contexto, a CNPD não difundiu, ou ainda não difundiu, uma lista de tipos de tratamento de dados cuja avaliação prévia de impacto não é obrigatória, tal como previsto no n.º 5 do art.º 35.º do RGPD. Ainda assim, e considerando que a alínea c) do n.º 3 do art.º 35.º do RGPD prevê a obrigatoriedade de realização desta avaliação em caso de "*controlo sistemático de zonas acessíveis ao público em grande escala*", é defensável que, por defeito, esta avaliação será obrigatória para a videovigilância, particularmente se esta for utilizada em zonas acessíveis ao público em grande escala (*v.g.* uma gare de transportes, um centro comercial ou um arruamento público).

Na senda do que acima foi aqui defendido, a CNPD elaborou e publicitou o Projeto de Regulamento n.º 1/2018[16] relativo à lista de tratamento de dados pessoais sujeitos a AIPD, onde, além do tratamento de dados previstos no n.º 3 do artigo 35.º do RGPD, determina que estão sujeitos a prévia AIPD um elenco de tratamento de dados pessoais. No n.º 6 está prevista a obrigatoriedade de prévia AIPD no tratamento de dados pessoais recolhidos por sistemas de videovigilância.

Ainda que, em algumas situações não seja obrigatória a AIPD, esta pode ser realizada por iniciativa própria e é dispensável para os tratamentos que

---

[15] Em caso de *data breach* o responsável pelo tratamento fica obrigado a assegurar que terá, sempre, «conhecimento» de eventuais violações em tempo útil, para que possa tomar medidas adequadas. O que não se mostra de difícil apuramento e muito menos impossível, até porque, as circunstâncias de uma violação irão ditar as condições exatas em que se pode considerar que um responsável pelo tratamento tem «conhecimento» dessa violação. Casos há em que é relativamente evidente desde o início se tal ocorreu. Todavia, a maior preocupação não deve ser centrada na prova de momento do «conhecimento» da violação de dados, mas sim na ação imediata para investigar o incidente, o que originou a falha ou violação, a fim de determinar se os dados pessoais foram de facto violados e tomar medidas de reparação e notificação.

[16] Anúncio n.º 136/2018 de 12 de julho.

tiverem sido previamente controlados por uma autoridade de controlo[17]. A AIPD será, essencialmente, uma ferramenta de reflexão.

4. Videovigilância – as finalidades previstas em Portugal

Em Portugal, o recurso à implementação de sistemas de videovigilância em locais públicos não existe só enquanto possibilidade, mas mesmo enquanto recurso obrigatório, particularmente no quadro da segurança privada.

Há casos em que, a lei estabelece a obrigatoriedade de implementação de sistema de videovigilância. Impõe a Lei 34/2013, de 16 de maio, que estão obrigados a adotar um sistema de segurança onde, entre outros meios, se inclui videovigilância, desde logo as próprias empresas titulares de alvará para prestação de serviços de segurança privada e as empresas detentoras de licença para serviços de autoproteção, sistemas, a utilizar nas suas próprias instalações operacionais, conforme previsto no art.º 7.º desta Lei e complementarmente na Portaria 273/2013 de 20 de agosto.

Além das empresas de segurança privada, estão, ainda, obrigados a deter sistema de videovigilância as seguintes entidades e estabelecimentos: (i) As instituições de crédito e as sociedades financeiras (alínea b), n.º 1, art.º 8.º da Lei 34/2013 de 16 de maio e art.º 90.º da portaria 273/2013 de 20 de agosto); (ii) Os conjuntos comerciais com área bruta locável igual ou superior a 20.000m2 e as superfícies comerciais com área de venda nacional acumulada de 30.000m2 (alínea b), n.º 2, art.º 8.º da Lei 34/2013 de 16 de maio); (iii) Os estabelecimentos de exibição, compra e venda de metais preciosos e obras de arte, quando o valor seguro for superior a €15.000 (alínea a), n.º 3, art.º 8.º da Lei 34/2013 de 16 de maio e art.º 97.º e 98.º da Portaria 273/2013 de 20 de agosto); (iv) As farmácias e postos de combustível (n.º 4, art.º 8.º da Lei 34/2013 de 16 de maio e art.º 100.º da Portaria 273/2013 de 20 de agosto); (v) Os *Automated Teller Machine* (art.º 10.º da Lei 34/2013 de 16 de maio e art.º 103.º da Portaria 273/2013 de 20

[17] *i.e.*, realizados com base em autorizações emitidas nos termos da Lei n.º 67/98, de 26 de outubro e em condições que não tenham sido alteradas, conforme orientação do GT29 (em conformidade com o art.º 29.º da Diretiva 95/46/CE de 24 de outubro), adotada em 04 de abril de 2017.

de agosto); (vi) Os estabelecimentos de restauração e bebidas com pista de dança e lotação igual ou superior a 100 lugares (art.º 9.º da Lei 34/2013 de 20 de agosto e alínea a), n.º 1, art.º 4.º do D.L. 135/2014 de 08 de setembro); (vii) Os recintos desportivos, onde se realizem espetáculos desportivos de natureza profissional ou não profissional considerados de risco elevado, sejam nacionais ou internacionais (art.º 18.º da Lei n.º 39/2009, de 30 de julho, alterada pela Lei 52/2013 de 25 de julho); (viii) Os operadores de resíduos em cujas instalações se procede ao armazenamento, tratamento ou valorização de metais não preciosos (art.º 2.º da Lei n.º 54/2012 de 06 de setembro).

Uma outra questão, não menos importante, é a videovigilância em táxis, ainda que a sua utilização não seja obrigatória, está legal e expressamente prevista a possibilidade de os táxis disporem de sistema de videovigilância no interior das viaturas e com transmissão das imagens para uma central de receção e arquivo de imagens, devendo esta central estar integrada no conceito de segurança privada; isto é, a sua exploração e gestão apenas pode ser exercida por quem seja detentor de alvará ou licença para a prática da atividade de segurança privada. A instalação e utilização dos sistemas de videovigilância em táxis estão previstas na Lei n.º 33/2007, de 13 de agosto, que, igualmente, impõe que as imagens apenas possam ser utilizadas para promoção da segurança dos motoristas dos táxis e dos utentes, apenas podendo ser mantidas gravadas por estas centrais as imagens que identifiquem situações de risco ou perigo potencial ou iminente e pelo período indispensável à sua comunicação às Forças de Segurança, que nunca pode exceder cinco dias.

Também está prevista a possibilidade de utilização de videovigilância para a deteção de incêndios florestais[18], a vigilância e deteção de incêndios pode ser assegurada, entre outros, "*por rede de videovigilância, que complementa e reforça em todo o território do continente, as funções de deteção fixa de ocorrências de incêndios*", salienta-se, ainda, que, a Rede Nacional de Postos de Vigia (para deteção de incêndios), constituída por postos de vigia públicos e privados e

[18] Encontra-se prevista em dois normativos legais – na Lei 1/2005 de 10 de janeiro, nos art.º 2.º e 15.º, para utilização pelas Forças e Serviços de Segurança; e no D.L. 124/2006 de 28 de junho, alterado pelo D.L. 15/2009, de 14 de janeiro, D.L. 17/2009 de 14 de janeiro, D.L. 114/2011 de 30 de novembro, D.L. 83/2014 de 23 de maio, Lei 76/2017 de 17 de agosto e D.L. 10/2018 de 14 de fevereiro.

"...pode ser complementada por sistema de videovigilância, meios de deteção móveis ou outros meios que venham a revelar –se tecnologicamente adequados..." (art.º 31.º e 32.º do Decreto-Lei n.º 10/2018, de 14 de fevereiro)[19].

A questão mais sensível e que pode comprometer a salvaguarda dos dados pessoais, é a da segurança de pessoas e bens e o seu enquadramento na segurança pública[20], porém encontram-se reguladas (n.º 1, do art.º 2.º da Lei 1/2005, de 10 de janeiro) a identificação e a limitação das finalidades deste tipo de videovigilância, como é o caso da: a) Proteção de edifícios e instalações públicas e respetivos acessos; b) Proteção de instalações com interesse para a defesa e a segurança; c) Proteção da segurança das pessoas e bens, públicos ou privados, e prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência; d) Prevenção e repressão de infrações estradais; e) Prevenção de atos terroristas; f) Proteção florestal e deteção de incêndios florestais.

Para além das finalidades elencadas, de forma muito sumária, importará reputar que: (i) O responsável pelo tratamento dos dados (imagens captadas), é indispensavelmente a força de segurança pública com jurisdição da área de captação ou o serviço de segurança requerente (n.º 2, art.º 2.º da Lei 1/2005, de 10 de janeiro); (ii) A instalação de câmaras fixas está sujeita a autorização do membro do Governo que tutela a força ou serviço de segurança requerente (n.º 1, art.º 3.º da Lei 1/2005, de 10 de janeiro); (iii) A decisão de autorização do Governo é precedida de parecer da CNPD (n.º 2, art.º 3.º da Lei 1/2005, de 10 de janeiro); (iv) Nos locais objeto de vigilância com recurso a câmaras fixas é obrigatória a afixação, bem visível, de informação sobre a existência e a localização das câmaras, a finalidade da

---

[19] Tecnologicamente, a utilização da videovigilância para deteção de incêndios florestais terá a sua génese em projeto desenvolvido pelo INOV, em meados da última década do século XX, com um projeto piloto para o parque nacional da Peneda Gerês. Dadas as dificuldades em vigiar áreas tão extensas, foi desenvolvido o sistema CICLOPE, que se baseia em imagens captadas, com infravermelhos para deteção noturna, integrando e articulando com outros dados recolhidos, nomeadamente dados meteorológicos e dados de qualidade do ar, permitindo uma deteção precoce e fiável de incêndios.

[20] Regulada pela Lei 1/2005, de 10 de janeiro, com as alterações introduzidas pelas Lei n.º 39-A/2005, de 29 de julho, Lei n.º 53-A/2006, de 29 de dezembro e Lei n.º 9/2012, de 23 de fevereiro, regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum.

captação de imagens e sons e a identificação do responsável pelo tratamento dos dados recolhidos, perante quem os direitos de acesso e retificação podem ser exercidos, utiliza-se, para o efeito, o modelo de dístico previsto na portaria 373/2012 de 16 de novembro.

A utilização do recurso de videovigilância para fins de segurança pública será, talvez, a finalidade que mais discussão e polémica tem gerado na sociedade portuguesa[21]. Vejamos a conclusão que chega Catarina Frois[22], que defende que os sistemas de videovigilância em locais públicos de utilização comum falharam redondamente na prevenção e dissuasão criminal, motivo pelo qual este é um tema particularmente sensível e objeto de necessária ponderação.

---

[21] Um dos locais mais conhecidos em Portugal na instalação de videovigilância para segurança pública foi o Bairro Alto, em Lisboa, em exploração desde maio de 2014. A requerimento do Diretor Nacional da Polícia de Segurança Pública, a CNPD deu parecer positivo à utilização deste recurso em determinados arruamentos públicos do Bairro Alto (Parecer n.º 68/2009 da CNPD). Neste parecer, fica bem patente a preocupação da CNPD na ponderação valores ou interesses – por um lado, o da segurança, por outro lado, o direito à imagem e à livre circulação – concluindo que, com a utilização da videovigilância, "*as pessoas não estão impossibilitadas de circular, porém, não o podem fazer de uma forma completamente livre, pois ficam registados todos os seus movimentos, designadamente com quem vão, como vão, entre outros aspetos da sua vida privada*." O parecer positivo da CNPD, ainda que parcial, impõe as seguintes limitações: 1. Período de funcionamento limitado ao período horário entre as 22H00 e as 07H00 (no requerimento, a PSP pretendia utilização permanente 24H/24H); 2. Proibição de recolha e gravação de som; 3. Apenas permite a utilização de câmaras fixas (no total de 27), não permitindo a utilização de câmaras ocultas; 4. Barramento automático de locais privados (portas, janelas, varandas, etc.), através de software denominada "máscara"); 5. Incapacidade técnica de busca inteligente para identificação de pessoas; 6. Colocação de sinalética de aviso da existência do sistema de videovigilância; 7. Obrigatoriedade de divulgação, através da comunicação social, da instalação do referido sistema; 8. Adoção de critérios de segurança lógica de acesso ao sistema; 9. Funcionamento durante um período máximo de 6 meses, prazo após o qual será efetuada reavaliação ao funcionamento do sistema. Mais de quatro anos depois deste parecer, após instalação, o sistema iniciou funcionamento em maio de 2014, mantendo-se em exploração após reavaliação dos fundamentos, particularmente pela CNPD. A entidade responsável pela exploração – Polícia de Segurança Pública – tem, igualmente, efetuado avaliações ao funcionamento e eficiência do sistema.

[22] Frois, Catarina. "Bases de dados pessoais e vigilância em Portugal: análise de um processo em transição", in *A sociedade vigilante: Ensaios sobre identificação, vigilância e privacidade*, Lisboa: ICS Imprensa de Ciências Sociais, 2008, p. 121 e ss.

No contexto da segurança rodoviária identificamos um duplo enquadramento para a utilização de videovigilância[23]. Conforme se perceberá, destacam-se duas principais finalidades e, por conseguinte, dois principais utilizadores da videovigilância: a finalidade de fiscalização, a desenvolver pelas Forças de Segurança; e a finalidade de gestão de tráfego e cobrança de taxas de portagens, a desenvolver pelo gestor da infraestrutura rodoviária nacional.

Na atividade de fiscalização rodoviária das Forças de Segurança (PSP e GNR) tem sido crescente o recurso à tecnologia, incluindo imagem, para deteção e prova de contraordenações, nomeadamente excesso de velocidade onde, à recolha da velocidade, associa-se a imagem da viatura em causa, de modo a fazer prova da viatura em infração. No apoio à atividade das Forças de Segurança, uma das mais recentes inovações é o "*Polícia automático*", que consiste na utilização de câmara de recolha de imagens que, direcionada à matrícula de viaturas e suportada em informação em memória, identifica matrículas de viaturas furtadas ou com outras situações legais pendentes (falta de seguro obrigatório, falta de inspeção periódica obrigatória, etc.).

Na atividade de gestão da infraestrutura rodoviária tem sido igualmente crescente o recurso a videovigilância. Em que poderemos distinguir duas subfinalidades: gestão de tráfego (incluindo ativação de recursos de apoio) e cobrança de portagens. Justifica-se esta distinção porque, em matéria de proteção de dados pessoais, fará toda a diferença.

Sendo que a videovigilância para a finalidade cobrança de portagens é imprescindível a captação de elementos identificativos da viatura (matrícula), pois, de outra forma e nas situações em que a viatura não é utilizadora de sistema de cobrança automática (via verde), seria impossível

---

[23] O previsto no artigo 13.º da Lei n.º 1/2005, de 10 de janeiro e regulamentado pelo Decreto-Lei n.º 207/2005, de 29 de Novembro, para utilização pelas Forças de Segurança, na sua atividade de deteção de infrações rodoviárias e a aplicação das correspondentes normas sancionatórias, bem como de ações de controlo de tráfego e ativação de mecanismo de prevenção e socorro e, ainda, de identificação de viaturas furtadas, com matrículas falsas ou outras situações legais pendentes (sistema polícia automático); e o previsto na Lei n.º 51/2006, de 29 de Agosto, para utilização pela empresa pública Infraestruturas de Portugal (sucedânea da Estradas de Portugal, de acordo com o D.L. 91/2015 de 29 de maio) e concessionários das Estradas, com a finalidade de monitorização do tráfego e consequente promoção de assistência rodoviária, bem como para apoio ao pagamento de taxas de portagens.

imputar o pagamento da portagem. Já para a gestão de tráfego, isto é, para percecionar se existem muitas ou poucas viaturas em circulação, se existe trânsito congestionado ou se existe alguma viatura parada ou mesmo a circular em contramão, não existe necessidade de recolha de elementos identificativos das viaturas. Nesta, como em qualquer outra circunstância, considerando o princípio da minimização dos dados, expresso no art.º 5.º do RGPD, estes deverão ser "*adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados*", motivo pelo qual, para esta finalidade, as imagens recolhidas não deverão permitir identificar pessoas nem dados de viaturas que possibilitem a posterior identificação do seu proprietário. Por conseguinte, e existindo interesse geral no acesso a estas imagens, para que qualquer cidadão possa perceber se determinado troço rodoviário está congestionado e melhor possa identificar o trajeto mais vantajoso, estas imagens poderão ser difundidas e cedidas a operadores de televisão e comunicações (n.º 3, art.º 16.º da Lei 51/2006 de 29 de Agosto).

Porém, a videovigilância, não estando sujeita a consentimento expresso das pessoas, cujos dados pessoais serão tratados, deve respeitar o direito de informação, isto é, em qualquer local onde seja utilizada, deverá ser exposta informação que, de forma clara e acessível, esclareça as pessoas acerca da sua existência, dos locais onde as câmaras estão e quem é o responsável pelo tratamento dos dados, respeitando modelo de sinal informativo.

A finalidade da utilização das imagens de videovigilância deve estar previamente definida, não podendo ser utilizada para além dessa limitação e, só podem ser gravadas por período limitado, normalmente 30 (trinta) dias. Só excecionalmente as imagens podem ser utilizadas para fins que não os processuais penais, isto é, em processos-crime, não podendo ser utilizadas para controlo da atividade laboral de trabalhadores, nestas circunstâncias as câmaras não poderão incidir sobre o interior de áreas reservadas aos trabalhadores ou a clientes e utentes, designadamente vestiários, instalações sanitárias, zonas de espera e provadores de vestuário, dirigidas a zonas de digitação de códigos de caixas multibanco ou terminais de pagamento *Automated Teller Machine*.

Conclusão

A videovigilância é, atualmente, uma tecnologia indispensável no apoio às mais diversas atividades, sendo a sua utilização não só uma possibilidade, mas também uma obrigatoriedade nalgumas circunstâncias (agências bancárias, centros comerciais, ourivesarias, farmácias, postos de combustível, discotecas, recintos desportivos e operadores de resíduos).

Tratando-se de obrigatoriedade ou não, estes sistemas têm, no entanto, de respeitar determinados requisitos, de modo a minimizar o mais possível o impacto da utilização deste recurso nos direitos, liberdades e garantias do cidadão.

O RGPD, aplicável em todos os Estados membros da União Europeia desde o dia 25 de maio de 2018, introduziu várias alterações no tratamento de dados pessoais, entre os quais a videovigilância que, por tratar imagens de pessoas, as mesmas, constituem dados pessoais.

Contudo, a ameaça terrorista após os atentados de 11 de setembro de 2001 nos EUA é mais uma razão para a recolha e troca de dados, desta vez justificadas como medidas de segurança e de prevenção. Porém, esta intrusão, quer das empresas quer das autoridades públicas, ameaça «*desmoronar*» uma das mais importantes conquistas civilizacionais.

Com efeito, o elevado número de recolha, tratamento e troca de dados pessoais que atualmente ocorre, advém da maior disponibilização de informações privadas, cedidas, voluntária ou involuntariamente, pelas próprias pessoas (pelos próprios titulares dos dados pessoais), nomeadamente nas redes sociais.

O avanço tecnológico permitiu também um mais rápido e eficaz desenvolvimento científico. No entanto, apesar destas vantagens, nem sempre a nova ordem digital é acompanhada de medidas protetoras adequadas no plano jurídico, que evitem ou não permitam a proliferação de violações e limitações de direitos, sobretudo de direitos fundamentais e direitos humanos.

Atualmente, em todo o mundo, sobretudo nos países desenvolvidos, os cidadãos não só são perseguidos continuamente no dia-a-dia, como consentem, de livre vontade, na divulgação dos seus próprios dados, com a vigilância e o «*voyeurismo*» da sociedade. Não restem dúvidas: nas últimas décadas assistimos a uma revolução digital que tornou a sociedade numa sociedade de informação.

A tutela da vida privada exige, hoje, mais transparência e controlo no concernente ao tratamento de dados por empresas e autoridades públicas. Ainda assim, teremos de levar em linha de conta os comportamentos das pessoas, que cada vez mais estão menos cientes do seu direito à privacidade, permitindo a divulgação, e divulgando elas mesmo, informações pessoais, sem consciência das reais implicações dos seus atos, em redes totalmente abertas como a internet, nas quais não há controlo nem fiscalização.

O direito à privacidade, como corolário de direitos fundamentais intrínsecos na consciência das sociedades modernas, nem sempre está protegido: os meios tecnológicos disponíveis nos dias de hoje surgiram a uma velocidade que o direito não acompanhou. Assim, e centrando a atenção na União Europeia, tornou-se evidente a necessidade de proceder a uma profunda reforma do direito à proteção de dados pessoais.

Todavia, e um pouco contra a corrente, refira-se que uma hipotética uniformização de direitos fundamentais não deixa de ser preocupante, na medida em que a globalização impõe uma determinada visão do mundo e da vida, sem que os direitos fundamentais possam refletir as autonomias e peculiaridades dos povos, acabando por enfraquecer a diversidade cultural.

Consideramos que é imprescindível sensibilizar os indivíduos para a autoproteção da sua privacidade, os utilizadores das novas tecnologias devem estar cientes dos perigos que estas comportam e, nomeadamente, devem ter consciência de que a divulgação de informações em redes abertas como a *internet* escapa ao seu controlo. Dados uma vez disponibilizados estão para sempre disponíveis. Por isso mesmo, a privacidade, uma vez imiscuída, está imiscuída para sempre. Por tal, as novas tecnologias de informação impõem que o direito à privacidade seja repensado e reconfigurado como um direito ao anonimato.

Ao longo da elaboração deste texto, surge a convicção de que a compressão da privacidade não se verifica somente perante a hegemonia do interesse público (sobretudo por razões de segurança). Nos dias de hoje, tal compressão verifica-se, desde logo, pelos hábitos observados nos últimos anos de milhões de pessoas de partilhar detalhes e acontecimentos (por vezes íntimos) das próprias vidas, criando uma versão pública, *online,* da vida privada – *i.e.*, autocompressão da privacidade individual. A questão que se impõe formular é de saber se perante a revolução digital a que assistimos, será a privacidade (tal como a conhecemos) um conceito em vias de extinção ou ainda tem cabimento nesta sociedade cada vez mais pátula?.

De facto, nesta sociedade cada vez mais aberta, e adepta da era digital, onde se expõe com toda a abertura e transparência a vida privada, e até, a vida familiar, deixou de fazer sentido a privacidade, tal como a conhecemos. Na verdade, assistimos a mudanças de mentalidade e de comportamento social em que o valor da proteção da privacidade deixou de ser um «*bem supremo*», deixando até desvanecer a noção e o valor de que a privacidade é um direito inerentemente humano e um pré-requisito para a manutenção da condição humana com dignidade e respeito.

Os regimes especiais de proteção de dados pessoais: exemplos de poluição legislativa da União Europeia?

Inês Oliveira*

Resumo: O quadro normativo aplicável ao tratamento de dados pessoais é uma teia arquitetada pelo legislador europeu. À aprovação da Diretiva 95/46/CE, desenhada como *lex generalis*, seguiu-se a negociação de uma panóplia de diplomas especiais: para as instituições e órgãos da então Comunidade Europeia; para as autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais; para as operadoras de telecomunicações; e para as transportadoras aéreas. Com a aprovação do Regulamento Geral sobre a Proteção de Dados, todos os diplomas especiais foram (ou estão a ser) revisitados, visando-se, precisamente, o alinhamento com o mesmo. Ora, tal intuito de alinhamento levanta a questão da necessidade de regimes especiais, visto que todos bebem da mesma fonte.

Palavras-chave: *Dados pessoais; Regulamento (UE) 2016/679; Diretiva (UE) 2016/680; Regulamento (UE) 2018/1725.*

Abstract: The normative framework applicable to the processing of personal data is a web designed by the European legislator. The adoption of Directive 95/46/EC, designed

* 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/Ministério da Justiça (2010) e foi bolseira de investigação no ISCTE – IUL, na área da proteção de dados pessoais (2011). Atualmente (desde 2013) é Consultora de Política Legislativa na Direção-Geral da Política de Justiça/Ministério da Justiça, sendo representante de Portugal junto da União Europeia para as questões atinentes à proteção de dados pessoais, incluindo no Comité do Artigo 93.º do Regulamento Geral sobre a Proteção de Dados. Designada Encarregada de Proteção de Dados do Ministério da Justiça pelo Despacho n.º 5643/2018 de Sua Excelência a Ministra da Justiça, datado de 24 de maio de 2018.

as lex generalis, was followed by the negotiation of a number of special diplomas: for the institutions and bodies of the then European Community; to the competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or enforcing criminal sanctions; for telecommunications operators; and for air carriers. With the approval of the General Regulation on Data Protection, all special diplomas have been (or are being) revisited, aiming precisely the alignment with that. Such an aim of alignment raises the question of the need for special regimes, since everyone drinks from the same source.

Keywords: *Personal data; Regulation (EU) 2016/679; Directive (EU) 2016/680; Regulation (EU) 2018/1725.*

1. Enquadramento

A aprovação de um novo regime geral de proteção de dados pessoais – entenda-se, a aprovação do RGPD[1], que modernizou a Diretiva 95/46/CE[2] e que se aplica, como regime regra, aos setores público e privado dos Estados-Membros, espoletou a necessidade de rever os regimes especiais em vigor. Vejamos.

Por um lado, imprimiu a necessidade de revisitar as normas especiais aplicáveis ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, tendo o legislador europeu aprovado, para esses efeitos, a Diretiva (UE) 2016/680[3].

Por outro lado, a utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave passou a ser disciplinada

---

[1] Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[2] Directiva 95/46/CE, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[3] Diretiva (UE) 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

pela Diretiva (UE) 2016/681[4], que cria obrigações especiais para as transportadoras aéreas.

O setor das comunicações eletrónicas, regulado pela Diretiva 2002/58/CE[5], também mereceu revisão por parte do legislador europeu, constando a proposta legislativa da Comunicação COM(2017) 10 final[6].

Por fim, as normas aplicáveis aos organismos da União Europeia também foram alvo de revisão. Recorde-se que o tratamento de dados pessoais pelas instituições e órgãos da União encontrou abrigo no Regulamento (CE) n.º 45/2001[7], 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 então plasmado na citada Diretiva de 1995. Enquanto o processo legislativo que culminou na aprovação do Regulamento (CE) n.º 45/2001 foi instruído pela Diretiva 95/46/CE, a revisão do referido Regulamento de 2001 – gizada na Comunicação COM(2017) 8 final[8] e materializada pelo Regulamento (UE) 2018/1725[9] – teve como principal objetivo o alinhamento com o RGPD.

Ora, aludido o regime geral – o RGPD – e apontados os regimes especiais, cumpre questionar esta multiplicidade de diplomas aplicáveis.

---

[4] Diretiva (UE) 2016/681, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

[5] Diretiva 2002/58/CE, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.

[6] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE.

[7] Regulamento (CE) n.º 45/2001, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

[8] Proposta de Regulamento do Parlamento e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.

[9] Regulamento (UE) 2018/1725, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.

Neste artigo iremos elencar as diferenças entre o RGPD e a Diretiva (UE) 2016/680, por um lado, e, por outro, as dissemelhanças entre o RGPD e o Regulamento (UE) 2018/1725, na tentativa de dar resposta à questão de saber se são curiais regimes especiais no que toca à temática da proteção de dados pessoais.

2. O RGPD e a Diretiva (UE) 2016/680: a duplicidade de regimes justifica-se?

A duplicidade de regimes criada pela aprovação do RGPD e da Diretiva (UE) 2016/680 remonta à legislação transata – importa recordar que a Diretiva 95/46/CE, aplicável ao mercado interno, era complementada pela Decisão-Quadro 2008/977/JAI[10], que visou, então, disciplinar o tratamento de dados no âmbito da cooperação policial e judiciária em matéria penal.

Relativamente à relação entre o RGPD e a Diretiva (UE) 2016/680, traga-se à colação o entendimento de DE HERT e PAPAKONSTANTINOU, que acentuaram que a dualidade de regimes foi e está construída sobre uma distinção ilusória entre dados para fins comerciais e dados relativos à segurança[11]. 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 extremamente difícil, se não mesmo impossível, de delimitar, insistindo-se em

---

[10] Decisão-Quadro 2008/977/JAI, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal.

[11] De Hert, Paul; Papakonstantinou, Vagelis, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", in *Computer Law & Security Review* 28, 2012, p. 132: "This distinction, that is maintained in the reform, has proven over the years to be schematic and artificial. Today, datasets that are created by private data controllers for their own purposes may be accessed at some future point by law enforcement agencies. The opposite is not inconceivable too. Case law provides very little assistance to this end. The distinction in scope between the two instruments is therefore extremely difficult, if not impossible, to make. By insisting on two separate instruments for each type of processing, the Commission risks to prolong ambiguity in the field each time law enforcement agencies and the private sector interact.".

dois instrumentos separados e arriscando-se a prolongar a ambiguidade existente.

Na verdade, a aprovação de um diploma específico para o tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais redunda em três diferenças. Com efeito, a Diretiva (UE) 2016/680, em comparação com o RGPD, acolhe as seguintes particularidades:

i) em primeiro lugar, é obrigatória a distinção entre categorias de titulares de dados, designadamente entre suspeitos, arguidos, condenados, vítimas, testemunhas e outros terceiros. A par disso, obrigatória é também a distinção entre diferentes tipos de dados pessoais: dados baseados em factos devem ser claramente separados de dados baseados em apreciações pessoais. Ora, este regime, plasmado nos art. 6.º e 7.º da Diretiva (UE) 2016/680, não tem paralelo no RGPD.
ii) em segundo lugar, e no que concerne aos sistemas de tratamento automatizado, é obrigatória a conservação de registos cronológicos das operações. Sublinhe-se que tanto a consulta como a divulgação de dados devem gerar registos que permitam determinar o motivo, a data e a hora dessas operações e, se possível, a identificação da pessoa que consulta ou divulga e a identidade dos destinatários desses dados (art. 25.º da Diretiva (UE) 2016/680). Note-se que esta obrigação também não tem paralelo no RGPD.
iii) em terceiro e último lugar, note-se que às autoridades de controlo nacionais não são atribuídos poderes sancionatórios (art. 47.º da Diretiva (UE) 2016/680), ao contrário do que sucede no âmbito do RGPD, que confere, designadamente, o poder de impor coimas (alínea i) do n.º 2 do art. 58.º).

A estas três diferenças somam-se várias singularidades – e não verdadeiras diferenças da Diretiva (UE) 2016/680, quando comparada com o RGPD. Vejamos.

Por um lado, o preceito definitório consagra a noção de autoridade competente (art. 3.º da Diretiva (UE) 2016/680 vs. art. 4.º do RGPD); por outro, o único fundamento legitimador do tratamento de dados pessoais é a lei, não sendo admissível outra base jurídica para justificar o tratamento,

como o consentimento do titular ou um contrato (art. 8.º da Diretiva (UE) 2016/680 vs. art. 6.º do RGPD).

Por seu turno, a Diretiva (UE) 2016/680, além de suprimir alguns dos direitos dos titulares dos dados conferidos pelo RGPD, densifica as limitações a esses direitos – entenda-se aos direitos de informação, acesso, retificação, apagamento e limitação do tratamento (art. 13.º a 16.º da Diretiva (UE) 2016/680) – quando estão em causa, mormente, inquéritos, investigações ou outros procedimentos ou quando relevem valores como a segurança pública, a segurança nacional ou direitos e liberdades de terceiros (n.º 3 do art. 13.º, art. 15.º e n.º 4 do art. 16.º da Diretiva (UE) 2016/680 vs. art. 23.º do RGPD). Em bom rigor, tais limitações não são, pois, uma particularidade, uma vez que também são expressamente admitidas no RGPD.

Por outro lado, e se é certo que a Diretiva (UE) 2016/680 suprime alguns dos direitos enumerados pelo RGPD, facto é que prevê a eventualidade de os direitos poderem ser exercidos através da autoridade de controlo (art. 17.º da Diretiva (UE) 2016/680).

Já no que concerne à disciplina das transferências internacionais de dados pessoais para países terceiros ou organizações internacionais, a Diretiva (UE) 2016/680 prevê expressamente as condições a preencher para a sua efetivação, dado o especial âmbito de aplicação material (art. 35.º da Diretiva (UE) 2016/680).

Importa sublinhar que, na nossa opinião, tais singularidades não consubstanciam verdadeiras diferenças, uma vez que, ainda na linha do RGPD, apenas conformam a sua aplicação ao âmbito da Diretiva (UE) 2016/680; ou seja, ao tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais.

Abstraindo-nos destas singularidades, corolários do pensamento do legislador do RGPD, as três diferenças a que aludimos espoletam a questão da necessidade de um instrumento especial, autónomo, diferente do RGPD. Inclinamo-nos a responder negativamente, na senda de DE HERT e PAPAKONSTANTINOU, vislumbrando-se variadas vantagens na condensação, num único diploma, das regras a aplicar no que toca à proteção de dados pessoais.

Na verdade, no nosso entendimento, repetir normas – *ipsis verbis*, não só nos preceitos definitórios, mas também no articulado atinente

aos princípios basilares – em diplomas diferentes não se mostra curial, mormente numa análise sob o prisma legístico; teria sido avisado, ao invés, criar capítulos, num mesmo diploma, para preceituar as especialidades que se mostrassem efetivamente necessárias. Aliás, esta solução facilitaria a aplicação por parte dos operadores, que, como salientado anteriormente, se deparam com dificuldades acrescidas face aos âmbitos de aplicação difíceis de delimitar na prática do dia-a-dia.

Só para dar um exemplo, veja-se o caso das polícias, que aplicam o RGPD ao tratamento de dados administrativos (dados dos trabalhadores, dados das pessoas que entram nos edifícios, dados no âmbito da contratação, etc.), tendo de aplicar, em paralelo, a lei de transposição da Diretiva (UE) 2016/680 ao tratamento de dados realizado no âmbito das investigações de crimes.

3. O tratamento de dados efetuado pelos organismos da União Europeia

O tratamento de dados efetuado pelos organismos da União Europeia mereceu regulação especial – veja-se o Regulamento (UE) 2018/1725, especial, sublinhe-se, relativamente ao regime geral plasmado no RGPD. O legislador europeu entendeu dar continuidade a esta especialidade, já que, anteriormente, a Diretiva 95/46/CE não tinha aplicação quando estava em causa o tratamento de dados pela própria União. Comparando o Regulamento (UE) 2018/1725 com o anteriormente aplicável Regulamento (CE) n.º 45/2001, que aquele revogou, são muitas as continuidades.

Principiemos com o âmbito de aplicação: também agora, como anteriormente, existem normas especialíssimas, aplicáveis ao tratamento de dados efetuado pela Europol e pela Procuradoria Europeia, bem como pelas missões no âmbito da política comum de segurança e defesa, que faz parte integrante da política externa e de segurança comum (art. 2.º do Regulamento (UE) 2018/1725).

Os princípios basilares – da finalidade, da minimização, da conservação limitada e da proibição de tratamento de dados sensíveis – também se mantêm inalterados, tal como a disciplina das transmissões dentro da União (art. 4.º e 9.º do Regulamento (UE) 2018/1725).

Por outro lado, os direitos concedidos aos titulares dos dados são os tradicionais: referimo-nos aos direitos de informação, acesso, retificação,

bloqueio, apagamento, oposição e não sujeição a decisões automatizadas (art. 15.º e ss do Regulamento (UE) 2018/1725). As vias de recurso à disposição dos cidadãos configuram outra continuidade: a par do direito de queixa junto da Autoridade Europeia para a Proteção de Dados, as pessoas têm direito a intentar uma ação judicial junto do Tribunal de Justiça da União Europeia (TJ), podendo, nessa sede, exercer o seu direito de indemnização (art. 63.º e ss do Regulamento (UE) 2018/1725).

As obrigações também espelham o regime anterior, continuando a ser exigidas as medidas técnicas, organizativas e de segurança necessárias, assim como a designação de um encarregado de proteção de dados (art. 26.º e ss do Regulamento (UE) 2018/1725). A supervisão continua a ser competência da Autoridade Europeia para a Proteção de Dados, sendo essencial a cooperação desta autoridade com as autoridades de controlo nacionais criadas ao abrigo do RGPD (art. 53.º e ss do Regulamento (UE) 2018/1725).

Vejamos agora as novidades introduzidas pelo Regulamento (UE) 2018/1725. Em primeiro lugar, ao rol dos princípios são agora expressamente aditados valores como a transparência, a integridade, a confidencialidade e a responsabilidade. A par disso, o arquivamento, para fins de interesse público, é, agora, expressamente, um tratamento posterior compatível com a recolha inicial dos dados (art. 4.º do Regulamento (UE) 2018/1725).

As regras atinentes ao consentimento encontram-se densificadas, reforçando-se a proteção conferida aos titulares dos dados, não apenas porque é consagrada a possibilidade de retirada, a todo o tempo, do consentimento anteriormente dado, mas também porque é exigida a autorização dos pais nos casos em que o titular é menor de 13 anos (art. 7.º e 8.º do Regulamento (UE) 2018/1725).

Como já referimos, os direitos dos titulares dos dados configuram uma continuidade. No entanto, ao mesmo passo, podemos vislumbrar um reforço da proteção do cidadão, que vê ampliado o seu direito à informação, devendo esta ser clara e simples. A par disso, é agora determinado o prazo de um mês para resposta aos pedidos dos titulares, pedidos esses que devem ser, por regra, submetidos gratuitamente (art. 14.º do Regulamento (UE) 2018/1725).

Ainda no que concerne aos direitos, destaque-se o direito à obtenção de uma cópia dos dados tratados, o alargamento do âmbito de aplicação

do direito ao apagamento, a introdução do direito à portabilidade dos dados e a possibilidade de representação nos recursos (art. 17.º, 19.º, 22.º e 67.º do Regulamento (UE) 2018/1725). Por outro lado, e mau grado para a proteção dos cidadãos, assistimos ao alargamento das situações em que pode haver decisões individuais automatizadas e das situações-tipo em que são legítimas restrições aos direitos (art. 24.º e 25.º do Regulamento (UE) 2018/1725).

A disciplina atinente às obrigações do responsável pelo tratamento – entenda-se, dos organismos da União – introduz, também, algumas novidades: passa a ser obrigatório demonstrar o cumprimento das obrigações, isto é, documentar os tratamentos de dados efetuados (art. 26.º do Regulamento (UE) 2018/1725); é imposta a proteção de dados desde a conceção e por defeito (art. 27.º do Regulamento (UE) 2018/1725), assim como o registo das atividades de tratamento (art. 31.º); é obrigatória a notificação de violações de dados à Autoridade Europeia para a Proteção de Dados (art. 34.º do Regulamento (UE) 2018/1725) e, em certos casos, a comunicação dessa violação ao próprio titular (art. 35.º do Regulamento (UE) 2018/1725); e obrigatória passa a ser também a avaliação de impacto e, em determinados casos, a autorização prévia da Autoridade Europeia para a Proteção de Dados (art. 39.º e 40.º do Regulamento (UE) 2018/1725).

Por fim, importa destacar a introdução do regime das coimas, a aplicar pela AEPD (art. 66.º do Regulamento (UE) 2018/1725), bem como de um capítulo especialmente aplicável ao tratamento de dados operacionais no exercício de atividades compreendidas no âmbito da cooperação policial e judiciária em matéria penal, que acolhe regras gerais com a ressalva de que podem ser derrogadas por normas específicas (art. 70.º e ss do Regulamento (UE) 2018/1725) – capítulo, aliás, cujo aditamento não se alcança, uma vez que copia as normas previstas nos artigos anteriores.

Ora, excecionando este capítulo especialmente aplicável ao tratamento de dados operacionais, dúvidas não restam de que todas as restantes novidades visam o alinhamento com o RGPD, sendo, pois, um decalque do regime geral a que já fizemos referência. Esta constatação leva-nos, novamente, a questionar a aprovação de um diploma diverso, especial para os organismos da União. Na verdade, se são tantos os pontos de contacto entre o Regulamento (UE) 2018/1725 e o RGPD, qual a razão que presidiu à opção do legislador europeu de não fazer aplicar o RGPD também ao setor público da própria União, já que o fez aplicar ao setor público dos

Estados membros? Inclinamo-nos para uma razão histórica: no regime anteriormente vigente, existia igualmente uma duplicidade de diplomas aplicáveis.

4. O RGPD e o Regulamento (UE) 2018/1725: diferenças a assinalar

Antes de nos focarmos nas diferenças entre os regimes, cumpre assinar as singularidades, que, não consubstanciando verdadeiras – e próprias – diferenciações, são antes especificações necessárias à luz do âmbito de aplicação do Regulamento (UE) 2018/1725 – recorde-se, o tratamento de dados efetuado pelas instituições e organismos da União Europeia (art. 1.º do Regulamento (UE) 2018/1725).

Em primeiro lugar, no que concerne à licitude do tratamento, os interesses legítimos do responsável pelo tratamento ou de terceiros não integram o elenco dos fundamentos legitimadores, ao contrário do que sucede ao abrigo do RGPD, que enumera tais interesses como base legítima para o tratamento de dados (art. 5.º do Regulamento (UE) 2018/1725 vs. art. 6.º do RGPD). Esta singularidade compreende-se à luz dos Tratados, mormente à luz do art. 5.º do Tratado da União Europeia[12], que consagra o princípio da atribuição, nos termos do qual a União atua unicamente dentro dos limites das competências que os Estados membros lhe tenham atribuído nos Tratados para alcançar os objetivos por estes fixados.

De difícil compreensão mostra-se o art. 25.º do Regulamento (UE) 2018/1725, que acolhe outra das singularidades que cumpre assinalar. Vejamos. O Regulamento (UE) 2018/1725, na linha do RGPD, sublinhe-se, prevê limitações aos direitos dos titulares dos dados – o Regulamento (UE) 2018/1725 fá-lo no art. 25.º e o RGPD no art. 23.º. No entanto, enquanto o RGPD obriga a que tal limitação, que é, em bom rigor, uma restrição ao direito fundamental à proteção de dados, conste de medida legislativa, o Regulamento (UE) 2018/1725 admite – *rectius*, permite – que tal restrição seja aprovada, não só por atos jurídicos adotados com base nos Tratados – o equivalente a medidas legislativas – mas também por fontes infralegislativas internas, isto é, por exemplo, por um regulamento interno de um organismo.

---

[12] Tratado da União Europeia (versão consolidada).

Ora, tal particularidade, apesar de poder ter explicação no quadro da orgânica própria da União, parece ser de difícil aceitação à luz do n.º 1 do art. 52.º da CDFUE. Na verdade, nos termos deste artigo, qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Sublinhe-se, por lei, e não por meras normas infralegislativas. Apesar desta não ser a sede para analisar a questão em apreço, não poderíamos deixar de a sinalizar, não só como singularidade, mas também como ponto controverso à luz da lei fundamental da União.

Como outra singularidade, aluda-se ao preceituado atinente à confidencialidade das comunicações eletrónicas nas redes das instituições e organismos da União (arts. 36.º e ss do Regulamento (UE) 2018/1725). Note-se que, no mercado interno, a confidencialidade das comunicações eletrónicas é regulada pela Diretiva 2002/58/CE, a que já fizemos alusão, instrumento legislativo especial e que complementa o RGPD.

Por fim, saliente-se o dever de informar a Autoridade Europeia para a Proteção de Dados, aquando da elaboração de medidas administrativas e regras internas, e de consultar essa autoridade e o Comité Europeu para a Proteção de Dados, aquando da elaboração de atos legislativos (art. 41.º e 42.º do Regulamento (UE) 2018/1725 vs. alínea c) do n.º 1 do art. 57.º do RGPD).

Vistas as singularidades do Regulamento (UE) 2018/1725, vejamos as diferenças face ao RGPD. A primeira, sem lugar paralelo no RGPD, é acolhida no art. 9.º do Regulamento (UE) 2018/1725, que prevê as transmissões de dados pessoais a destinatários estabelecidos na União diferentes das instituições e organismos da União, estabelecendo as condições para essa transferência especial de dados. São elas: o destinatário demonstrar que os dados são necessários ao desempenho de funções de interesse público ou inerentes ao exercício da autoridade pública de que o destinatário se encontra investido ou que é necessário transmitir os dados para um fim específico no interesse público e o responsável pelo tratamento, quando houver motivos para pressupor que os interesses legítimos do titular dos dados possam vir a ser prejudicados, estabelecer que a transmissão dos dados pessoais para esse fim específico é proporcionada, depois de comprovadamente ponderar os diferentes interesses em jogo.

Segunda diferença: a entidade com poderes de fiscalização é a Autoridade Europeia para a Proteção de Dados (art. 53.º e ss do Regulamento (UE)

2018/1725). Note-se que a Autoridade Europeia para a Proteção de Dados é nomeada pelo Parlamento Europeu e pelo Conselho por um período de 5 (cinco) anos e cuja independência, atribuições e poderes são semelhantes às autoridades de controlo nacionais previstas no RGPD (art. 51.º e ss do RGPD). De sublinhar a cooperação e a supervisão coordenada entre Autoridade Europeia para a Proteção de Dados e as autoridades de controlo nacionais (art. 61.º e 62.º do Regulamento (UE) 2018/1725).

Por fim, e como já referimos, o Regulamento (UE) 2018/1725 acolhe, no seu corpo, um capítulo aplicável especialmente ao tratamento de dados pessoais operacionais no exercício de atividades abrangidas pela cooperação policial e judiciária em matéria penal (art. 70.º e ss).

Ora, será que estas três diferenças são bastantes para legitimar um diploma especial face ao RGPD? Não nos parece. Aliás, é muito questionável o capítulo a que acabámos de fazer alusão, mormente sobre o prisma legístico, dada a repetição de normas aí contidas. Mais: como veremos de seguida, o Regulamento (UE) 2018/1725 é complementado por outros instrumentos legislativos, especialmente aplicáveis.

5. O Regulamento (UE) 2018/1725 e os regimes especialíssimos

Como assinalámos anteriormente, o Regulamento (UE) 2018/1725 não se aplica ao tratamento de dados efetuado pela Europol e pela Procuradoria Europeia, assim como ao tratamento efetuado pelas missões no âmbito da política comum de segurança e defesa, que faz parte integrante da política externa e de segurança comum (art. 2.º). Ora, este âmbito de aplicação cria, pois, regimes especialíssimos.

Com efeito, a especialidade do Regulamento (UE) 2018/1725 face ao RGPD não cria, em bom rigor, uma dualidade de normas aplicáveis. Na verdade, dentro do regime especial aplicável à estrutura orgânica da União Europeia encontramos regimes especialíssimos, pelo que estamos perante uma multiplicidade de regimes a aplicar. Confuso? Nós também.

Com efeito, o tratamento de dados operacionais realizado pelas agências com competências penais – referimo-nos à Europol, à Eurojust e à Procuradoria Europeia – é regulado em diplomas próprios.

Uma leitura atenta do que já deixámos 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). Aos dados administrativos é aplicável a disciplina do Regulamento (UE) 2018/1725. Por seu turno, aos dados operacionais são aplicáveis as normas gizadas na legislação especialmente aplicável, a par do capítulo inserto no Regulamento (UE) 2018/1725 que se dedica a essas matérias (art. 70.º e ss). Uma especialidade dentro da especialidade, se assim se preferir.

Ora, a Europol – Agência da União Europeia para a Cooperação Policial – encontra regulação no Regulamento (UE) 2016/794[13], que acolhe normas especificamente aplicáveis aos dados operacionais tratados por esta agência.

Por outro lado, a Agência Europeia para a Cooperação Judiciária Penal – Eurojust, que foi criada pela Decisão do Conselho 2002/187/JAI[14], revista pela Comunicação COM(2013) 535 final[15], também aplica um regime especial quando trata dados operacionais[16].

Por seu turno, o Regulamento (UE) 2017/1939[17], que institui a Procuradoria Europeia, também prevê preceitos especiais para o tratamento de dados operacionais.

Na nossa opinião, esta multiplicidade de regimes aplicáveis à estrutura orgânica da União Europeia espelha a complexidade que o legislador europeu vem criando desde 1995, depois de aprovar a Diretiva 95/46/CE e, sucessivamente, regimes especiais – para as polícias, procuradorias e tribunais, por um lado, e para setores privados como as comunicações eletrónicas ou o transporte aéreo, por outro.

---

[13] Regulamento (UE) 2016/794, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho.

[14] Decisão do Conselho, de 28 de Fevereiro de 2002, relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade.

[15] Proposta de Regulamento do Parlamento Europeu e do Conselho que cria a Agência Europeia para a Cooperação Judiciária Penal (Eurojust).

[16] Regulamento (UE) 2018/1727, que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust) e que substitui e revoga a Decisão 2002/187/JAI do Conselho.

[17] Regulamento (UE) 2017/1939, que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia.

6. Diferenças entre o Regulamento (UE) 2018/1725 e o Regulamento Europol

O Regulamento (UE) 2018/1725 é, ao mesmo tempo, uma lei especial – face ao RGPD – e a lei geral aplicável às instituições e organismos da União, uma vez que, no que concerne à estrutura orgânica da União, aplicam-se regimes especiais quando está em causa o tratamento de dados operacionais efetuado pela Europol, pela Eurojust e pela Procuradoria Europeia.

Comparámos já o RGPD com a Diretiva (UE) 2016/680, por um lado, e, por outro, com o Regulamento (UE) 2018/1725. Façamos agora o mesmo exercício comparativo entre o Regulamento (UE) 2018/1725 e o Regulamento (UE) 2016/794, que regula a Europol.

Antes de mais, cumpre destacar as similitudes. E são muitas: referimo-nos aos regimes atinentes aos princípios, às categorias de dados e de titulares, à segurança do tratamento, aos direitos dos titulares e aos recursos, bem como ao preceituado sobre a proteção de dados desde a conceção, a violação de dados, a consulta prévia, o registo e a supervisão.

Vejamos agora as particularidades do Regulamento (UE) 2016/794. A primeira reside, como não podia deixar de ser, nas finalidades do tratamento. Com efeito, e uma vez que estamos perante a agência que prossegue o objetivo de apoiar a cooperação entre as autoridades policiais da União, as finalidades do tratamento são, pois, correlações deste objetivo (art. 18.º do Regulamento (UE) 2016/794).

Em segundo lugar, o normativo aplicável à transferência e intercâmbio de dados pessoais facilita, efetivamente, a troca de dados (art. 24.º a 27.º do Regulamento (UE) 2016/794). Tal regime facilitador aplicável à troca de dados é equilibrado com a previsão de uma rigorosa disciplina de avaliação da fiabilidade e exatidão dos dados (art. 29.º do Regulamento (UE) 2016/794), que se afigura a terceira especificidade. Em quarto e último lugar, destaque-se a atribuição de competências ao Conselho de Cooperação (art. 45.º do Regulamento (UE) 2016/794).

Ora, o regime especialmente gizado no Regulamento (UE) 2016/794 concretiza-se em quatro especificidades. As diferenças elencadas justificaram a criação da complexidade legislativa criada por regimes que se sobrepõem? Vai bem o legislador europeu a arquitetar esta multiplicidade

de regimes? 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.

Considerações finais

A disciplina jurídica aplicável ao tratamento de dados pessoais é uma teia arquitetada pelo legislador europeu. À aprovação da Diretiva 95/46/CE, desenhada como *lex generalis*, seguiu-se a negociação de uma panóplia de diplomas especialmente aplicáveis: às instituições e órgãos da então Comunidade Europeia; às autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais; às operadoras de telecomunicações; às transportadoras aéreas, para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

Com a aprovação do RGPD, e consequente revogação da Diretiva 95/46/CE, todos os diplomas especialmente aplicáveis foram (ou estão a ser) revisitados, visando-se, precisamente, o alinhamento com o RGPD. Ora, tal intuito de alinhamento levanta a questão da necessidade de regimes especiais, visto que todos bebem da mesma fonte. Acresce que, como deixámos dito, as particularidades não são vincadas ao ponto de serem necessários outros regimes, autónomos, separados. Mais: a multiplicidade de regimes aplicáveis resulta numa complexidade tal que o cidadão acaba por ficar desprotegido, quando o desígnio do legislador europeu era precisamente a proteção.

Neste artigo questionámos a aprovação de uma panóplia de regimes especiais face, primeiro, à Diretiva 95/46/CE e, agora, ao RGPD, visto que em todos se decalca o normativo da *lex generalis*. De facto, a leitura desta teia legislativa permite-nos concluir que são muitas as similitudes e poucas as especificidades que consubstanciam verdadeiras diferenças. Mais: esta complexidade de regimes esta construída em alicerces falaciosos, uma vez que a distinção entre setores público e privado é ilusória e artificial. Tudo isto, somado ao âmbito de aplicação difícil de delimitar, parece resultar na desproteção – efetiva – do cidadão.

Não nos restam dúvidas de que estamos perante diplomas legais que provocam um efeito negativo no sistema jurídico, causando como principal dano a desproteção do cidadão. Por isso mesmo, podemos afirmar que os regimes aplicáveis ao tratamento de dados pessoais são um exemplo de poluição legislativa da União Europeia.

Birds flying high: A Diretiva (UE) 2016/681 e a proposta de Lei 137/XIII da Presidência do Conselho de Ministros

Ricardo Rodrigues de Oliveira*

Resumo: Este texto dá a conhecer o desenvolvimento da Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. Em seguida, analisa-se a proposta de Lei do Conselho de Ministros para transposição deste texto para o ordenamento jurídico português, pois que o conhecimento desta legislação junto do público é ainda assaz incipiente. Contribui-se assim para refletir sobre as opções legislativas europeias e nacionais e sobre o seu impacto nos direitos e liberdades dos cidadãos.

Palavras-chave: *Diretiva (UE) 2016/681; PNR; aviação civil; dados pessoais*

Abstract: This text makes known the development of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Then, it analyses the proposed legislation of the Council of Ministers for the transposition of this text into the Portuguese legal order, as the knowledge of this legislation by the public is still considerably incipient. This is thus a contribution to reflect on the European and national legislative choices and their impact on the rights and freedoms of citizens.

Keywords: *Directive (EU) 2016/681; PNR; civil aviation; personal data*

* Doutorando no Instituto Universitário Europeu (EUI), Investigador do Centro de Investigação em Direito Público da Faculdade de Direito da Universidade de Lisboa (FDUL) e Investigador da Jurisnova da Faculdade de Direito da Universidade Nova de Lisboa (FDUNL).

Introdução

Os meios de transporte de massas têm sido um alvo preferencial nos ataques terroristas em solo europeu. A aviação civil é disso exemplo cimeiro, sendo que são de realçar como mais recentes o plano falhado de um cidadão britânico de detonar explosivos de plástico escondidos nos seus sapatos num avião de Paris para Miami, a 22 de dezembro de 2001, o atentado abortado, de 9 de agosto de 2006, que pretendia detonar explosivos líquidos em vários voos transatlânticos entre o Reino Unido e os EUA e a tentativa de ataque a bordo de uma ligação entre Amesterdão e Detroit com explosivos de plástico escondidos na roupa interior de um passageiro nigeriano, a 25 de dezembro de 2009. Tendo sido planeados pela al-Qaeda, nenhum destes ataques se consumou.

Apesar da redução de ataques terroristas na Europa, boa parte destas atividades tem uma natureza transnacional e os agentes criminosos utilizam frequentemente a aviação civil para se deslocarem. Isto tem levado a um constante incremento na legislação e políticas de segurança nesta área. O mais recente exemplo disso na UE é a legislação em apreço neste artigo, a Diretiva (UE) 2016/681[1]. O seu objetivo é a recolha e tratamento de registos de identificação dos passageiros (PNR na sigla em língua inglesa) de voos extra-UE[2] "para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave" (art. 1º).

Os dados PNR consistem em informações pessoais não verificadas disponibilizadas pelos clientes de serviços de transporte aéreo aquando dos processos de reserva e aquisição de voos. Os registos dos potenciais passageiros são recolhidos pelas companhias de aviação nos seus sistemas informáticos de reserva e controlo de partidas[3] e são por elas utilizados para fins comerciais, nomeadamente marketing e gestão de passageiros frequentes. Alguns exemplos destas informações são as datas e itinerários das viagens,

---

[1] Diretiva (UE) 2016/681, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

[2] Muito embora esteja prevista a extensão da sua aplicação a voos intra-UE nas legislações nacionais de transposição, nos termos do art. 2º.

[3] Normalmente através de plataformas eletrónicas especializadas em reservas em massa, como o sistema Amadeus, disponível em https://www.amadeus.net/home. (acedido a 26/06/2018).

informações de contato, meios de pagamento e dados relativos às bagagens. Estes dados são mais completos que as informações antecipadas de passageiros (*Advance Passenger Information*)[4], o conjunto de informações biométricas presentes na zona de leitura ótica dos passaportes e que se restringem, com algumas variações, ao nome, data e local de nascimento, sexo, número de identificação pessoal, altura e nacionalidade. Estes são verificados aquando do desembarque de voos provenientes de fora da União para controlo fronteiriço e combate à migração ilegal, sendo o sistema *Advance Passenger Information* uma espécie de 'antecessor' do PNR. Não obstante, a potencialidade de monitorização e o escopo de controlo[5] deste sistema vão muito além do *Advance Passenger Information*, desde logo porque os "dados PNR são utilizados principalmente como uma ferramenta em matéria de informações criminais em vez de uma ferramenta de verificação da identidade"[6].

A escolha deste tema deve-se à insuficiência de estudos sobre o PNR na literatura jurídica portuguesa[7], especialmente relativos à Diretiva (UE) 2016/681 — a maioria dos trabalhos debruça-se sobre os acordos celebrados entre países terceiros e a União. Este texto está dividido em duas seções substantivas. A primeira dá a conhecer a Diretiva PNR, elucidando, em especial, sobre o seu contexto e o caminho percorrido pelas instituições europeias em termos legislativos e institucionais até à sua aprovação. Não há espaço para se fazer uma análise aturada dos diversos aspetos deste percurso ou sequer da Diretiva, preferindo-se antes um breve exame de alguns pontos essenciais que se ligam com a parte seguinte. O segundo trecho analisa a proposta nacional para transposição daquela legislação, realçando os pontos em que o texto português vai para além do europeu, e recorre aos pareceres requeridos pela AR a diversas entidades para

---

[4] Reguladas pela Diretiva 2004/82/CE, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras.

[5] Por exemplo, pelo tipo de crimes, voos afetados, a utilização dos dados para outros fins ser a exceção e não a regra ou ainda pelo período de retenção das informações API ser apenas de 24 horas.

[6] Comunicação da Comissão sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros (COM(2010) 492 final, 21.9.2010), p. 4.

[7] Como apontou Oliveira, Emellin. "O *Passanger Name Record* e a proteção de dados pessoais: Uma análise sobre a transferência da informação dos passageiros aos Estados", *Anuário de Proteção de Dados*, 2018, p. 147-167.

apresentar algumas das críticas que podem ser assacadas a esta legislação no contexto do ordenamento jurídico português.

1. A Diretiva (UE) 2016/681

Com os ataques de 11 de setembro de 2001, os EUA decidiram renovar a sua legislação relativa à segurança no transporte aéreo, entrando, a par com outros países, numa espécie de "deriva securitária"[8]. Nos termos da seção 122.49b do *Code of Federal Regulations* e do art. 44909º do *U.S. Code*, as companhias de aviação que operem voos com proveniência estrangeira que partam, aterrem ou passem pelos EUA devem transferir para a *Customs and Border Protection* do *Department of Homeland Security* os dados PNR dos passageiros transportados. As informações devem ser recolhidas a partir dos sistemas de reserva e transmitidas antes da partida dos aviões. Estes dados são processados pelos agentes da *Customs and Border Protection* para determinar que passageiros precisam de ser sujeitos a medidas adicionais de inspeção e controlo ou detidos no âmbito de uma investigação criminal.

1.1. Pressões externas

Perante a nova regulação norte-americana, a UE viu-se confrontada com uma situação complexa. Por um lado, a Diretiva 95/46/CE[9] não previa esta transmissão de informações nem os acordos relativos ao nível de proteção adequado para transferências de dados pessoais entre a UE e os EUA[10] criavam a base legal necessária para esta nova realidade. Por outro, as companhias aéreas preferiam violar as normas europeias em matéria de privacidade e partilha de dados pessoais a perderem direitos de aterragem e trânsito nos aeroportos norte-americanos.

Logo em junho de 2002, a Comissão avisou as autoridades dos EUA do conflito entre as novas exigências legislativas e o quadro legal

---

[8] Urbano de Sousa, Constança. "Segurança *versus* privacidade: Breves notas a propósito do acordo UE-EUA sobre a transmissão de dados PNR (*Passenger Name Record*)", *Themis*, ano XII, número 22/23, 2012, p. 51-65. Este texto é ainda útil pela maior densidade na análise cronológica dos acordos entre a UE e os EUA, em particular o de 2012, que se mencionará adiante.

[9] Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[10] Decorrentes dos arts. 25º ss. desta Diretiva.

europeu[11] mas a situação arrastou-se algum tempo[12], até a Comissão encetar negociações para o estabelecimento de acordos internacionais que enquadrassem e acolhessem as obrigações das operadoras aéreas no panorama jurídico da União. Apesar do número crescente de países a recorrer a estes dados e a pedir a sua transmissão a companhias a atuar no espaço europeu[13], a UE estabeleceu, até agora, acordos PNR com apenas 3 países terceiros: os EUA[14], o Canadá[15] e a Austrália[16].

---

[11] De apontar ainda o Regulamento (CEE) 2299/89, relativo a um código de conduta para os sistemas informatizados de reserva, entretanto revogado pelo Regulamento (CE) 80/2009.

[12] Com significativa preocupação por parte das companhias aéreas visto que os EUA não abdicaram de impor penalidades àquelas que não cumprissem os requisitos de transmissão das informações a partir de 5 de março de 2003.

[13] A 14 de julho de 2015, o chefe dos serviços administrativos fiscais do México, Aristoteles Nuñez, e o comissário europeu para as migrações, negócios internos e cidadania, Dimitris Avramopoulos, reuniram-se para lançar as negociações de um acordo PNR EU-México, resultando a reunião no *Joint statement: Beginning of negotiations between Mexico and the European Union on PNR data transmission* (STATEMENT/15/5374). Também a Nova Zelândia e a Coreia do Sul estão já a utilizar dados PNR e outros países têm vindo a adotar normas ou a testar a utilização deste sistema, como a África do Sul, a Arábia Saudita, o Japão e Singapura.

[14] Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento (Acordo PNR 2007) (JO L 204/18, 4.8.2007), entretanto substituído pelo Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna dos Estados Unidos (JO L 215, 11.8.2012).

[15] Acordo entre a Comunidade Europeia e o Governo do Canadá sobre o tratamento dos dados relativos às informações antecipadas sobre os passageiros e aos registos de identificação dos passageiros (JO L 82/14, 21.3.2006). A revisão deste acordo em 2014 levou, porém, à sua suspensão pois que, no seguimento de um pedido de aprovação do texto pelo Conselho da União Europeia ao Parlamento Europeu, este pediu ao Tribunal de Justiça que se pronunciasse sobre a compatibilidade do acordo com o Direito da UE, nomeadamente com as normas relativas ao respeito pela vida privada e à proteção dos dados pessoais, e o Tribunal acabou por declarar que o acordo não podia ser concluído como estava por ser incompatível com direitos fundamentais reconhecidos na CDFUE, segundo o Parecer 1/15, 26 de julho de 2017 (2017/C 309/03, JO C 146, 4.5.2015).

[16] Acordo entre a UE e a Austrália sobre o tratamento de dados originários da União Europeia contidos nos Registos de Identificação dos Passageiros (PNR) e a transferência desses dados pelas transportadoras aéreas para os serviços aduaneiros da Austrália (JO L 213/47,

Em 2003, foi apresentada uma comunicação da Comissão dirigida ao Conselho e ao Parlamento que definiu as bases para a atuação futura da UE relativamente aos dados PNR e, em particular, ao desenvolvimento das negociações com os EUA[17]. Um dos principais objetivos era (e mantém-se) a uniformização dos acordos e das políticas no âmbito da ação externa da UE através de critérios que "constituirão a base de negociações futuras sobre acordos PNR com países terceiros"[18].

1.2. Harmonização do espaço comum

A criação de legislação para o mercado interno foi, porém, mais lenta que a celebração dos acordos internacionais. As iniciativas legislativas foram sendo justificadas com a pretensão de regular a utilização dos dados PNR entre os Estados-Membros, apesar do diminuto número de países a legislar internamente sobre esta matéria antes de 2016[19]. A primeira proposta

---

8.8.2008), entretanto substituído pelo Acordo entre a UE e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Serviço Aduaneiro e de Proteção das Fronteiras australiano (JO L 186, 14.7.2012).

[17] Comunicação da Comissão ao Conselho e ao Parlamento Europeu 'Transferência de dados contidos nos registos de identificação dos passageiros aéreos (PNR – *Passenger Name Records*): uma abordagem global da UE' (COM(2003) 826 final, 16.12.2003). Esta foi posteriormente desenvolvida pela Comunicação da Comissão sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros (COM(2010) 492 final, 21.9.2010).

[18] Comunicação (COM(2010) 492 final, 21.9.2010), p. 3. Nas conclusões (p. 12), é inclusivamente referido que "a UE deve examinar a possibilidade de substituir, a médio prazo, os acordos bilaterais por um acordo multilateral entre todos os países que utilizam dados PNR".

[19] Só o Reino Unido é que, até então, tinha um sistema completo de PNR em funcionamento, sendo que a Bélgica, Dinamarca, França, Holanda e Suécia estavam a adotar legislação na área ou mesmo a testar a sua implementação. Não obstante, segundo a proposta de Diretiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave {SEC(2011) 132 final}{SEC(2011) 133 final} (COM(2011) 32 final, 2011/0023 (COD), 2.2.2011), p. 4, um dos receios que esteve na base da aprovação de legislação a nível europeu foi o facto de que, à medida que se verificasse um efeito de contágio legislativo entre os diversos países quanto a esta matéria, se chegasse ao ponto de coexistirem até "27 sistemas significativamente diferentes, daí resultando níveis

surgiu em 2007[20] mas, não tendo sido adotada pelo Conselho até então, tornou-se desadequada com a entrada em vigor do Tratado de Lisboa[21].

Em 2010, na seção intitulada 'Uma Europa que protege' do Programa de Estocolmo[22], o Conselho exortava a Comissão a "propor a adoção de uma medida da União, que [garantisse] um elevado nível de proteção de dados, no domínio do PNR[,] no intuito de prevenir, detetar, investigar e reprimir infrações terroristas e formas graves de criminalidade com base numa avaliação de impacto". Ainda nesse ano, a Comissão fez uma Comunicação sobre os pontos essenciais que deveriam orientar a política da União quanto a esse tipo de dados[23] e o Parlamento aprovou uma resolução[24] sobre esta abordagem global e, especificamente, sobre o papel dos acordos internacionais no combate ao terrorismo e outras formas de criminalidade transnacional[25]. Ambos os documentos referem os recuos sentidos na evolução desta legislação e acolhem a ideia de desenvolvimentos legislativos futuros[26].

---

desiguais de proteção de dados pessoais na UE, lacunas de segurança, aumento dos custos e insegurança jurídica para as transportadoras aéreas e os passageiros".

[20] Proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name record* – PNR) para efeitos de aplicação da lei {SEC(2007) 1422} {SEC(2007) 1453} (COM(2007) 654 final, 2007/0237 (CNS), 6.11.2007).

[21] Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de dezembro de 2007 (JO C 306, 17.12.2007).

[22] Programa de Estocolmo – Uma Europa aberta e segura que sirva e proteja os cidadãos, p. 19.

[23] Comunicação (COM(2010) 492 final, 21.9.2010).

[24] Vinda na esteira da Resolução do Parlamento Europeu, de 20 de novembro de 2008, sobre uma proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* – PNR) para efeitos de aplicação da lei (P6_TA(2008)0561).

[25] Resolução do Parlamento Europeu, de 11 de novembro de 2010, sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros, e sobre as recomendações da Comissão e do Conselho tendo em vista autorizar a abertura de negociações entre a União Europeia e a Austrália, o Canadá e os Estados Unidos da América (2012/C 74 E/02) no âmbito da Estratégia externa da UE relativamente aos dados dos registos de identificação dos passageiros (PNR) (P7_TA(2010)0397) (JO C 74E, 13.3.2012).

[26] Comunicação (COM(2010) 492 final, 21.9.2010), p. 5, e, indiretamente pelo acolhimento favorável daquela Comunicação, Resolução (P7_TA(2010)0397) (JO C 74E, 13.3.2012), p. 10.

No seguimento desta Comunicação, surgiu em 2011 uma proposta de Diretiva[27] informada pelas anteriores resoluções do Parlamento Europeu e por alguns pareceres de entidades de supervisão[28]. Foi, porém, rejeitada a 24 de Abril de 2013 na votação da Comissão de Liberdades Civis do Parlamento Europeu[29] por dúvidas quanto à proporcionalidade do esquema de coleção, uso e retenção dos dados dos passageiros — especialmente pela irrelevância da sua condição de inocência ou suspeição — e ao respeito pelos seus direitos fundamentais, nomeadamente à proteção de dados.

A 30 de agosto de 2014, o Conselho Europeu apelou ao Parlamento e ao Conselho de Ministros que finalizassem o trabalho iniciado na proposta PNR. A 11 de novembro, a Comissão de Liberdades Civis do Parlamento Europeu voltou a discutir o assunto mas somente em 2015, com os dois atentados terroristas em Paris, é que se verificaram desenvolvimentos substanciais. No seguimento do ataque de janeiro, o Parlamento Europeu aprovou uma resolução sobre medidas de combate ao terrorismo em que incluía a Diretiva PNR como um dos seus compromissos legislativos a concretizar até ao final do ano. Nessa resolução igualmente instava a Comissão a tirar conclusões do acórdão do TJ sobre a Diretiva de conservação de dados[30] e a convidar peritos para "contribuírem com as suas opiniões e os seus princípios [...] relativamente à necessidade e à proporcionalidade do

---

[27] Proposta de Diretiva (COM(2011) 32 final, 2011/0023 (COD), 2.2.2011).

[28] Parecer da Autoridade Europeia para a Proteção de Dados sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* – PNR) para efeitos de aplicação da lei (JO C 110, 1.5.2008), Parecer conjunto dos GT29 (145, 5.12.2007) e do Grupo de Trabalho em matéria de Polícia e de Justiça (01/07, 18.12.2007) sobre a proposta de Decisão-Quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* – PNR) para efeitos de aplicação da lei, apresentada pela Comissão em 6 de novembro de 2007 (02422/07/PT) e Opinião de 2008 da Agência dos Direitos Fundamentais da União Europeia sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* – PNR) para efeitos de aplicação da lei.

[29] Apesar da forte militância em prol da sua aprovação pelo *rapporteur* dessa Comissão, o eurodeputado britânico Timothy Kirkhope.

[30] Acórdão do TJ, C-301/06, *Irlanda/ Parlamento Europeu e Conselho*, ECLI:EU:C:2009:68, sobre a Diretiva 2006/24/CE, 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, e que altera a Diretiva 2002/58/CE.

PNR", bem como incentivava o Conselho a desenvolver a legislação sobre proteção de dados[31] para que o processo legislativo pudesse correr em simultâneo com o da Diretiva PNR[32].

Esta posição seria reiterada em julho, na Agenda Europeia para a Segurança, em que o Parlamento reconheceu "o apelo urgente da Comissão para concluir os trabalhos sobre a adoção da Diretiva PNR da UE" e comprometeu-se a fazê-lo até ao final do ano, incitando a própria Comissão a manter o seu suporte ao processo, nomeadamente "fornecendo elementos adicionais relevantes para a necessidade e proporcionalidade"[33]. Pouco tempo após o segundo atentado em Paris, em novembro, o Parlamento aprovou outra resolução em que sublinhava, no âmbito do "reforço do intercâmbio de informações sobre a radicalização terrorista na Europa", o seu compromisso em elaborar a Diretiva PNR até ao final do ano. A demora em aprovar esta legislação prendeu-se sobretudo com as razões que levaram à sua rejeição pela Comissão de Liberdades Civis do Parlamento Europeu em 2013, como a necessidade de "garantir que essa diretiva [seria] conforme com os direitos fundamentais e livre de quaisquer práticas discriminatórias

---

[31] O chamado pacote de proteção de dados que estava a ser preparado para renovar (reformar, na nomenclatura institucional europeia) a legislação em matéria de dados pessoais e sua proteção através da substituição da Diretiva 95/46/CE já estava a ser planeado há algum tempo e a Diretiva PNR é que o veio acompanhar, acelerada, de certo modo, pelos ataques terroristas em Bruxelas, a 22 de março de 2016. Toda esta legislação foi aprovada em maio desse ano e dela constam o Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (RGPD), a Diretiva (UE) 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho e a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) 45/2001 e a Decisão 1247/2002/CE (COM/2017/08 final – 2017/02 (COD)).

[32] Resolução do Parlamento Europeu, de 11 de fevereiro de 2015, sobre medidas de combate ao terrorismo (P8_TA(2015)0032) (2015/2530(RSP)), parágrafo 13.

[33] Resolução do Parlamento Europeu, de 9 de julho de 2015, sobre a Agenda Europeia para a Segurança (P8_TA(2015)0269) (2015/2697(RSP)), parágrafo 27.

com base na estigmatização ideológica, religiosa ou étnica, e [que respeitaria] plenamente os direitos de proteção de dados dos cidadãos da UE"[34].

Apesar de toda esta aparente emergência, a Diretiva PNR só foi aprovada em abril de 2016, no seguimento dos atentados terroristas de março em Bruxelas. O texto foi aprovado com 461 votos a favor, 179 contra e 9 abstenções, tendo entrado em vigor a 24 de maio. O processo de aprovação foi bastante rápido em comparação a todo o historial anterior. Apesar de ter seguido o processo legislativo ordinário e de terem havido discussões junto do Conselho logo a 18 de novembro e a 15 de dezembro de 2015, a primeira leitura e emissão de uma opinião pelo Parlamento Europeu deram-se a 14 de abril de 2016, sendo o texto aprovado com alterações. Será novamente discutido em Conselho a 15 e a 18 de abril, sendo aprovado, de novo em primeira leitura, a 21, e assinado pelos presidentes do Parlamento Europeu e do Conselho em simultâneo aos textos de proteção de dados a 27 desse mês.

1.3. A transposição

Dois anos volvidos, a 25 de maio de 2018, cessou o prazo de transposição da Diretiva (UE) 2016/681. Ao contrário do pacote de proteção de dados, esta legislação imiscui de forma considerável nos dados pessoais mas não o faz com o objetivo principal de reforçar a sua proteção. Como já foi referido, o PNR não pretende ser um instrumento de controlo de identidades mas é, assumidamente, um instrumento de retenção de informações no âmbito da agenda europeia de política criminal. Foi desenhado para que as autoridades recolham e processem informações dos cidadãos europeus no âmbito de contra-terrorismo e combate à criminalidade grave, utilizando a

---

[34] Resolução do Parlamento Europeu, de 25 de novembro de 2015, sobre a prevenção da radicalização e do recrutamento de cidadãos europeus por organizações terroristas (P8_TA(2015)0410) (2015/2063(INI)), parágrafo 42. É relevante replicar as considerações subsequentes do Parlamento Europeu em que este dizia "que a diretiva PNR da UE será apenas uma medida de luta contra o terrorismo e que é necessária uma estratégia holística e abrangente no domínio do combate ao terrorismo e à criminalidade organizada, que envolva a política externa, a política social, a política da educação e os órgãos policiais e judiciários, de forma a prevenir o recrutamento de cidadãos europeus por organizações terroristas".

aviação civil meramente como ferramenta para obtenção desses dados em massa (comumente designados em língua inglesa por *big data*).

A 21 de fevereiro de 2018 teve lugar uma conferência sobre o futuro do PNR promovida pela presidência búlgara do Conselho da União Europeia que contou com a presença de diversos governantes, altos representantes e profissionais de 24 Estados-Membros, bem como da Austrália, EUA e Suíça e agentes das instituições e agências europeias, nomeadamente o Coordenador da Luta Antiterrorista, Gilles de Kerchove, o Secretário-Geral do Conselho da União Europeia, Jeppe Tranholm-Mikkelsen, o Supervisor Europeu de Proteção de Dados, Giovanni Buttarelli, e membros da Comissão, Agência dos Direitos Fundamentais da União Europeia, Europol, eu-Lisa e FRONTEX. Nela abordaram-se temas como a qualidade, fiabilidade, troca, proteção e uso efetivo dos dados PNR, os desafios extraordinários e potenciais soluções no que concerne a implementação da Diretiva, nomeadamente tendo em conta o trabalho desenvolvido pelo Grupo de Trabalho Informal sobre o PNR, o *state of play* dos diversos Estados-Membros, as relações com países terceiros e o papel da Europol no tratamento das informações, bem como as melhores práticas no uso deste sistema no combate ao terrorismo e criminalidade grave[35].

Alguns dias depois, a 26 de fevereiro, o Conselho da União Europeia emitiu uma nota referindo que a implementação é regularmente discutida no Grupo de Trabalho Informal sobre o PNR, presidido pela Alemanha à altura, e em diversas reuniões organizadas pela Comissão[36]. Deu-se conta igualmente do progresso alcançado nos meses anteriores, resultado da confiança mútua sentida entre Estados-Membros nestas reuniões e da assistência P2P através da troca aberta de experiências e lições aprendidas, bem como da assistência financeira e legal prestada pela Comissão diariamente

---

[35] *Note from the Presidency of the Council of the European Union to the Working Party on Information Exchange and Data Protection (DAPIX) on the Conference on the future of PNR data – effective use and challenges (Sofia, 21 february 2018)* (6104/18, 23.2.2018). Outras iniciativas foram tendo lugar ao longo dos anos, nomeadamente sob a alçada do DAPIX, mas este texto apenas se debruça sobre os acontecimentos mais recentes e relevantes até à data da sua escrita.

[36] *Note from the Presidency of the Council of the European Union to the Permanent Representatives Committee/Council on the Directive (EU) 2016/681 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime – Implementation of the PNR Directive / Exchange of views* (6017/18, 26.2.2018).

em cooperações bilaterais. Na seção de *exchange of views*, a instituição sublinhou a importância deste instrumento na resposta ao terrorismo e à criminalidade grave e convidou os ministros competentes a trocarem ideias sobre o estado de implementação da legislação, nomeadamente refletindo sobre questões como saber se todos os mecanismos possíveis estariam a ser postos em prática para assegurar uma adoção rápida das legislações nacionais de transposição, quais seriam os principais desafios ainda a abordar e que tipo de apoio esperariam de outros Estados-Membros ou da Comissão para facilitar a implementação tempestiva.

Apesar destes esforços, a transposição da Diretiva tem-se arrastado. Logo em novembro de 2016, a Comissão emitiu um plano de implementação com seis marcos que os países deveriam atingir em alturas bem definidas para a transporem[37]. Igualmente foram sendo incluídas as matérias PNR nos sucessivos relatórios sobre a segurança na União e o último destes à data da escrita do presente artigo dava conta de que, até 7 de junho de 2018[38], somente catorze Estados-Membros[39] haviam comunicado à Comissão terem adotado as medidas necessárias para transpor a Diretiva[40]. Nove destes países produziram legislação através dos parlamentos nacionais e, daqueles que ainda não tinham apresentado medidas de transposição, cinco já tinham, pelo menos, textos em vigor que permitiam às autoridades recolher informações PNR. Vinte e quatro

---

[37] De acordo com o *Commission staff working document 'Implementation Plan for Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime'* (SWD(2016) 426 final, 28.11.2016), estes são: i) produzir legislação que implemente a Diretiva; ii) estabelecer as UIPs; iii) desenvolver soluções técnicas para o tratamento dos dados PNR; iv) obter recursos humanos para as UIPs; v) envolver as autoridades competentes; e vi) assegurar a conetividade das transportadoras aéreas. As UIPs são as entidades que devem recolher os dados PNR providenciados pelas transportadoras aéreas e proceder ao seu tratamento, nos termos do art. 6º da Diretiva (UE) 2016/681.

[38] Data da primeira reunião entre a Comissão e os Estados-Membros após 25 de maio de 2018 para debater a aplicação da Diretiva.

[39] Sendo que a Dinamarca preferiu utilizar da sua prerrogativa de *opt out* quanto a este documento.

[40] Alemanha, Bélgica, Croácia, Eslováquia, Estónia, Hungria, Irlanda, Itália, Letónia, Lituânia, Luxemburgo, Malta, Polónia e Reino Unido. As medidas nacionais de transposição que vão sendo comunicadas à Comissão ficam disponíveis em https://eur-lex.europa.eu/legal- content/EN/NIM/?uri=CELEX:32016L0681 (acedido a 25/07/2018).

Estados-Membros já possuíam os meios técnicos exigidos para processar os dados, enquanto que os outros três estariam a finalizar a implementação de soluções técnicas. Finalmente, doze países encontravam-se numa fase avançada de estabelecer conetividade com as companhias de aviação e em onze havia, pelo menos, uma transportadora a transmitir informações em tempo real às UIPs.

A Comissão considerou assim que, na globalidade, foram feitos avanços importantes no sentido da aplicação da Diretiva mas que ainda há lacunas relevantes a tratar e que, "dada a importância crucial deste instrumento para a resposta comum da UE ao terrorismo e à criminalidade grave, a Comissão recorrerá a todas as medidas ao seu dispor para garantir a aplicação do direito da União, incluindo procedimentos por infração, se for caso disso [pois que] a não transposição constitui um entrave à eficácia global do mecanismo (...), diminui a segurança jurídica para as transportadoras aéreas (...) e prejudica a proteção efetiva dos dados pessoais em toda a UE"[41]. Nesse sentido, a 19 de julho de 2018, a Comissão enviou cartas de notificação a catorze países[42] por não terem comunicado a adoção tempestiva de legislação que transpusesse plenamente a Diretiva. Estes tiveram até meados de setembro para responder, sob pena de aplicação de sanções.

Até junho de 2018, o Grupo de Trabalho Informal sobre o PNR reuniu-se quatro vezes, sendo que no último encontro, a 5 e 6 desse mês em Haia, a Austrália apresentou o seu esquema de implementação PNR[43] para permitir um termo de comparação com as práticas de autoridades extra-europeias e para mostrar propostas de solução a problemas operacionais específicos[44].

---

[41] Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu e ao Conselho 'Décimo quinto relatório sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz' (COM(2018) 470 final, 13.6.2018), p. 12.

[42] Áustria, Bulgária, Chipre, Eslovénia, Espanha, Estónia, Finlândia, França, Grécia, Luxemburgo, Países Baixos, Portugal, República Checa e Roménia.

[43] Na reunião de abril tinha sido o Canadá a fazê-lo.

[44] *Note from the General Secretariat of the Council to the Working Party on Information Exchange and Data Protection (DAPIX) on the Update on the Informal Working Group on PNR* (10139/18, 21.6.2018).

1.4. Alguns contras à Diretiva no ordenamento jurídico europeu

Parece, especialmente à luz de algumas críticas que podem ser tecidas ao texto atual e que já vinham das redações e discussões anteriores, que a aprovação da Diretiva PNR não deveu a sua entrada na ordem jurídica da União somente à oportunidade surgida com o pacote de proteção de dados aprovado pela mesma altura. Esta é uma legislação fruto do ambiente de terror que grassava, de certa maneira, na Europa em 2015 e 2016. Apesar do nível de violência em solo europeu não ser comparável a regiões em conflito ou com relevante presença de agentes e organizações terroristas, a intensidade das transmissões destes fenómenos na Europa pelos meios de comunicação social, os sentimentos de proximidade e vizinhança e, talvez, a estranheza causada pelo terrorismo no Ocidente, *inter alia*, têm condicionado fortemente as políticas nacionais e europeias no seu combate. É até razoável afirmar que, em circunstâncias distintas, esta legislação diretamente tão intrusiva da intimidade dos cidadãos não passaria no crivo da proporcionalidade e da necessidade nas discussões legislativas das instituições europeias. Aliás, a reprovação de 2013 é espelho disso mesmo.

Esta é uma legislação que dá um passo considerável na monitorização dos movimentos dos cidadãos europeus, possivelmente lesando as liberdades de circulação de maneira contrária ao Direito da União supra-legal[45]. Um mecanismo que permite a transmissão dos dados pessoais dos passageiros de transporte aéreo (por agora) de voos extra-UE (por agora) por parte de UIPs para autoridades competentes nos diversos Estados-Membros em todos os voos para que se proceda a uma "avaliação dos passageiros antes da sua chegada prevista (...) ou da sua partida prevista (...), a fim de identificar as pessoas que, pelo facto de poderem estar implicadas numa infração terrorista ou numa forma de criminalidade grave, devem ser sujeitas a um controlo mais minucioso"[46] ou, caso a caso, através de "pedidos devidamente fundamentados, baseados em motivos suficientes (...) para fornecer e tratar dados PNR, em casos específicos, para efeitos de prevenção, deteção, investigação e repressão de infrações terroristas ou da criminalidade

---

[45] E, ao contrário do que defende Oliveira, Emellin, *op. cit.*, não parece que esteja em causa somente a mitigação do princípio de presunção de inocência mas a sua total desconsideração.

[46] Alínea a) do n.º 2 do art. 6º da Diretiva (UE) 2016/681.

grave"[47] fora do âmbito restrito de uma investigação judiciária autorizada ou mandatada por um tribunal ou órgão judicial independente, não parece ser totalmente conducente com as "medidas adequadas" de controlo que assegurem a "livre circulação de pessoas" previstas nos termos do n.º 2 do art. 3º do Tratado de Lisboa[48] nem com o direito de "qualquer cidadão da União (...) de circular e permanecer livremente no território dos Estados-Membros" expresso no n.º 1 do art. 45º da CDFUE.

Para além destes "pedidos devidamente fundamentados, baseados em motivos suficientes", poderem redundar em solicitações pró-forma das entidades nacionais — que poderão nem sequer ser OPCs — justificadas em razões de natureza investigatória que não são passíveis de controlo e verificação *ex ante* pelas UIPs, pelas autoridades nacionais responsáveis pela proteção de dados ou por um tribunal, esta legislação apresenta ainda um risco potencial de contágio. O medo que infetou a sua génese já levou alguns Estados-Membros a aprovar legislação PNR para outros meios de transporte[49] e alguns países já notificaram a Comissão quanto a quererem incluir os voos intra-UE nas suas legislações internas[50]. A juntar aos riscos

---

[47] Alínea b) do n.º 2 do art. 6º da Diretiva (UE) 2016/681.

[48] Em que se lê, de forma completa, que "[a] União proporciona aos seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas, em que seja assegurada a livre circulação de pessoas, em conjugação com medidas adequadas em matéria de controlos na fronteira externa, de asilo e imigração, bem como de prevenção da criminalidade e combate a este fenómeno".

[49] Veja-se, a título de exemplo, a *Loi du 25 Décembre 2016 relative au traitement des données des passagers* (2016-12-25/43, 25.1.2017), especialmente os seus arts. 4º e 54º quanto aos meios de transporte incluídos no esquema PNR belga.

[50] Aliás, muito embora o Parlamento Europeu se tenha oposto à inclusão de voos intra-EU, no Conselho da União Europeia de 18 de Abril de 2016 os Estados-membros ignoraram aquela oposição e não só declararam que iriam utilizar a abertura permitida pelo art. 2º da proposta de Diretiva quanto à possibilidade de inclusão daquelas ligações nas legislações nacionais como ainda demonstraram querer acrescentar dados PNR provenientes também de transportadores não aéreos, isto é, entidades que fornecem serviços relacionados com viagens, incluindo a reserva de voos, como agências de viagens e operadores turísticos (*'I/A' item note from the General Secretariat of the Council to the Permanent Representatives Committee/Council on the Draft Directive of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (first reading) – Adoption of the legislative act (LA + S) = Statement* (7829/16 ADD 1, 18.4.2016)). Até ao dia 1 de Junho de 2018, estes eram a Alemanha, Bélgica, Bulgária, Croácia, Eslováquia,

para a proteção das informações pessoais que representam aqueles pedidos sem 'fiscalização', a verdade é que o sistema PNR não pode ser, em boa verdade, imposto em todos os meios de transporte pelo que a eficiência e eficácia deste sistema, de um ponto de vista global, estarão sempre comprometidas. Basta pensar nas inúmeras ligações ferroviárias locais ou regionais que não requerem qualquer informação pessoal dos passageiros para pensar em uma, de muitas, formas dos terroristas ou criminosos escaparem totalmente a este sistema. E mesmo que se impusesse esta medida a esses outros meios, seria (praticamente) impossível processar os dados de todos os utentes em tempo útil[51]. De facto, será que colocar um manto de suspeição sobre todos os passageiros é a forma mais adequada de combater o terrorismo e a criminalidade grave? Serão realmente úteis os dados de milhares de não suspeitos para as potenciais investigações criminais que se preveem, especialmente quando o sentido de oportunidade e a celeridade são, por vezes, essenciais ao sucesso investigatório? As razões por detrás deste meio de obtenção de dados estão truncadas pelo *fumus* de que há uma vontade de monitorização dos cidadãos por detrás de tudo isto. Aliás, nem sequer há relatórios públicos de proporcionalidade que demonstrem a adequação de se impôr um sistema PNR em certos meios de transporte, quanto mais na aviação civil (o meio de transporte já mais controlado e, quiçá, seguro que existe na atualidade, deste ponto de vista), através do balanço entre a intrusão nos dados pessoais e os efeitos, de facto, produzidos em termos de combate à criminalidade.

A proteção dos meios utilizados na aviação, nomeadamente os espaços aeroportuários e as aeronaves, não é o objetivo específico desta legislação, ao contrário de outras normas relacionadas[52]. A Diretiva não se restringe ao combate aos crimes praticáveis no e contra o *airside* (espaço restrito) dos

---

Hungria, Itália, Letónia, Lituânia, Malta, Polónia, Reino Unido e Suécia. A Comunicação (COM(2018) 470 final, 13.6.2018), p. 12, refere que são 19 e não 13 países a terem decidido aplicar a Diretiva a voos intra-UE mas, como não os nomeia, não é possível confirmar quais serão os restantes 6 Estados-membros.

[51] Worth, Jon, *Why Belgium's plan for PNR for rail and buses/coaches must be stopped*, Jon Worth Euroblog, disponível em https://jonworth.eu/why-belgiums-plan-for-pnr-for-rail-and-busescoaches-must-be-stopped/ (acedido a 25/07/2018).

[52] Como as relativas ao controlo de passageiros nos termos do Regulamento (CE) 300/2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil, que revoga o Regulamento (CE) 2320/2002 (JO L 97, 9.4.2008), e a sua atualização pelo

aeroportos e contra os aviões mas a diversos tipos de criminalidade grave e terrorismo. Ou seja, a ligação à aviação civil é meramente instrumental, sendo esta um meio relativamente inócuo de obter grandes quantidades de dados pessoais. Inócuo no sentido de que as rotinas de segurança que se desenvolveram ao longo dos anos em torno do transporte aéreo, pela sua natureza crescentemente intrusiva, 'entorpeceram' a sensibilidade tanto de viajantes como de políticos na balança entre a privacidade individual e o bem de interesse público que é a segurança. Donde, os dados PNR serão provavelmente encarados pela opinião pública, de forma incorreta, como um mal necessário que deve ser acolhido sem relevante oposição ou consternação, como se de mais um controlo se tratasse.

2. A proposta nacional e a Diretiva

A AR chegou a pronunciar-se sobre a proposta de Diretiva (COM(2011) 32 final, 2011/0023 (COD), 2.2.2011), a primeira resenha PNR a nível da União[53]. A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, a pedido da Comissão de Assuntos Europeus, apreciou o seu respeito pelo princípio da subsidiariedade e considerou que este não era violado por aquela proposta visto que os seus objetivos não poderiam ser realizados individualmente de forma suficiente pelos Estados-Membros mas somente a nível coletivo. Assim sendo, uma Diretiva seria, no entender da Comissão de Assuntos Constitucionais, Direitos, Liberdades e

---

Regulamento (CE) 272/2009, que complementa as normas de base comuns para a proteção da aviação civil definidas no anexo ao Regulamento (CE) 300/2008.

[53] Também já tinha emitido a Resolução 71/2009 sobre a Proposta de Decisão Quadro COM (2007) 654 final SEC (2007) 1422 e 1453, relativa à utilização dos dados do registo de identificação de passageiros (*passenger name record* — PNR) para efeitos de aplicação da lei para fins de combate ao terrorismo e à criminalidade organizada de 23.7.2009 (série I, número 157, 14.8.2009), em que recomendava ao Governo referir às instituições europeias que essa Proposta não mostrava cabalmente a importância de um sistema PNR uniforme nem o estabelecia, visto que apenas impunha a criação de um mecanismo nacional por parte dos Estados-Membros. Daqui talvez se possa extrair já uma vontade bastante antecipada da AR de ver aplicado um sistema PNR em todo o espaço da União, vontade essa que se mantém até hoje, embora quiçá com pouca discussão parlamentar sobre todas as suas implicações, nomeadamente ao nível da (des)proporcionalidade da intrusão na privacidade dos cidadãos.

Garantias, o instrumento mais adequado para aproximar as diferentes legislações nacionais e atingir os objetivos da proposta. Um aspeto interessante a referir é que, tanto em 2011 como na proposta legislativa de 2018, a inclusão de voos intra-UE ao esquema PNR nacional foi sempre a opção preferencial de Portugal, suscitando até "algumas preocupações" que certos Estados-Membros apenas pretendessem aplicar este sistema a voos extra-UE. Mesmo com este elemento adicional, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias considerou que vinte e sete sistemas PNR diferentes criariam "lacunas de segurança, aumento dos custos e insegurança jurídica para as transportadoras aéreas e os passageiros" e que, por tudo isso, a proposta de Diretiva não violava o princípio da subsidiariedade[54].

No dia 6 de junho de 2018, deu entrada na AR a proposta de Lei 137/XIII do Conselho de Ministros que regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, transpondo a Diretiva (UE) 2016/681[55]. Foi admitida no dia seguinte, tendo seguido imediatamente para a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias. O texto desta proposta — apresentado pelo Governo à AR com prioridade e urgência visto o seu atraso face ao prazo de transposição — é muito semelhante ao da Diretiva, reforçando o argumento de que as Diretivas são de tal modo

---

[54] Relatório da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias de 16.3.2011 (série II-A, número 125, 14.4.2011), pp. 102 ss.

[55] Curioso verificar, porém, que esta não parece ser a primeira vez que um esquema PNR é introduzido no ordenamento jurídico nacional pois que a Portaria 603/2015 de 21.7.2015 (série II, número 151, 5.8.2015) veio autorizar a Polícia Judiciária a realizar uma despesa tendo em vista a compra de um sistema PNR, cujo procedimento de contratação foi classificado como confidencial. Os custos diluíram-se pelos anos 2015 e 2016 (101 191,97€ no primeiro e 910 727,68€ no segundo ano), tendo sido financiados por fundos europeus disponibilizados pelo Programa de Prevenção e Luta contra o Crime da União Europeia em cerca de 90%, mas nada mais é referido no documento sobre o propósito e funcionamento deste esquema, nem o público afectado. Com início em janeiro de 2014, o que coloca esta contratação fora dos períodos mais críticos de atividade terrorista na Europa, a própria organização policial apenas adianta que esta é uma "ferramenta de investigação de entradas e saídas de pessoas por via aérea, com capacidades analíticas e preditivas que [permitem] agilizar a identificação e resposta ao crime organizado". Disponível em https://www.policiajudiciaria.pt/piu-pt/ (acedido a 3/08/2018).

cada vez mais minuciosas que os textos nacionais de transposição pouco mais são que cópias ligeiramente emendadas das fontes europeias[56].

A proposta nacional especifica que a UIP mencionada na Diretiva será, em Portugal, o Gabinete de Informações de Passageiros, que atua junto do Ponto Único de Contato para a Cooperação Policial Internacional e cujo coordenador será nomeado pelas tutelas da administração interna e justiça de entre agentes dos órgãos de polícia criminal. Também se referem a composição e estrutura do Gabinete, bem como as técnicas de tratamento de dados e a designação e formação dos futuros trabalhadores, remetendo-se para documentos legais complementares (art. 3º). Não parece que haverá assim, por ora, uma UIP comum a Portugal e outro Estado-Membro.

Um segundo desenvolvimento diz respeito às sanções previstas nestes diplomas. No art. 14º da Diretiva 2016/681 refere-se que os Estados-Membros definem as sanções a aplicar perante a violação das normas presentes nas leis nacionais, bem como as medidas adequadas para forçar a sua aplicação, com especial enfoque nas penas (nomeadamente pecuniárias) que podem recair sobre as transportadoras caso não transmitam os dados de forma correta. Já a proposta de Lei 137/XIII concretiza aquele enunciado criando, primeiro, um dever de sigilo profissional (art. 18º) sobre todos aqueles que tratem os dados recolhidos ou que deles tenham conhecimento, sob pena de prisão nos termos do art. 383º do CP[57]. No art. 19º definem-se pesadas sanções para as companhias de aviação, nomeadamente sujeitando-as a coimas entre 20 000€ e 100 000€, por viagem, caso transfiram as informações dos passageiros "de forma incorreta, incompleta, falsificada ou após o prazo" (n.º 1) e a sanções de 10 000€ a 50 000€ se não enviarem os dados *Advance Passenger Information* conforme o n.º 5 do art. 4º ou se o fizerem em formatos e seguindo protocolos não reconhecidos nos termos do art. 17º (n.º 2). A negligência é punível (n.º 3) e as coimas, cuja aplicação é da responsabilidade da CNPD (n.º 4), revertem a favor desta

---

[56] Já o anexo I às conclusões da Presidência do Conselho Europeu 'Declaração Laeken sobre o futuro da União' (DOC/01/18, 14-15.12.2001), p. 5, referia que as Diretivas têm evoluído gradualmente no sentido de uma maior minúcia legislativa. Introduzindo alguns dos problemas de classificação dos atos da UE, veja-se Hartley, Trevor, *The foundations of European Union Law*, 8.ª ed., Oxford University Press, 2014, p. 108 ss.

[57] Decreto-Lei 48/95, de 15 de março, sucessivamente alterado e republicado por último pela Lei 16/2018, de 27 de março.

e do Estado (n. 5º). É ainda feita uma remissão para outro diploma (ainda a ajustar no final do procedimento legislativo) para tratar das violações às normas respeitantes à proteção de dados, às quais se aplicará um regime contraordenacional.

Não há mais diferenças relevantes a assinalar entre a Diretiva e a proposta de Lei, salvo, no anexo II, a abertura de escopo do crime de exploração sexual na listagem de infrações a investigar para efeitos desta legislação[58] e alguns ajustes de terminologia penal. Diversas entidades emitiram pareceres sobre esta proposta, sendo que aí foram levantadas questões relevantes quanto à sua adequação ao sistema jurídico português. Na próxima seção serão aflorados alguns dos pontos mencionados nestes pareceres, com especial incidência naqueles que parecem criticar a proposta com maior veemência ou exigir uma revisão das suas normas[59].

2.1. A CNPD

A CNPD já se havia pronunciado sobre esta matéria em pareceres relativos ao funcionamento da UIP nacional e às tecnologias envolvidas no tratamento de dados destinados ao Ministério da Justiça[60]. Reproduziu neste último parecer algumas das suas conclusões anteriores, reforçando parte das críticas prévias e elaborando novas em face do potencial efeito negativo desta nova legislação nos direitos dos cidadãos.

O primeiro comentário negativo de relevo prende-se com a não identificação das autoridades com competência para aceder aos dados. De facto, no n.º 1 do art. 7º referem-se apenas as "entidades policiais e aduaneiras e as autoridades judiciárias" autorizadas a tratar com crimes graves e terrorismo quando elas deveriam ser enumeradas explicitamente,

---

[58] Por oposição a "exploração sexual de crianças" presente no n.º 3 do anexo II da Diretiva.

[59] À altura da escrita do presente texto, ainda não estavam disponíveis os pareceres da Ordem dos Advogados e do Conselho Superior do Ministério Público. O parecer e nota técnica anexa da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias começam precisamente por criticar o Governo por não ter feito acompanhar a proposta de todos os contributos e pareceres resultantes das consultas e audições obrigatórias que terá levado a cabo.

[60] Parecer 61/2017, processo 18564/2017, e Parecer 62/2017, processo 18572/2017. Relevante é também o Parecer 39/2011, processo 3303/11, relativo à proposta de Diretiva (COM(2011) 32 final, 2011/0023 (COD), 2.2.2011).

em prol dos princípios da transparência e da certeza jurídica. Tem razão a CNPD ao referir que a "formulação genérica do articulado é inibidora de um escrutínio rigoroso quanto à transposição correta da Diretiva" mas, por outro lado, também só avança com a Polícia Judiciária como exemplo de entidade competente. Parece que outras poderiam caber aqui, nomeadamente a Polícia de Segurança Pública, a GNR e o Serviço de Estrangeiros e Fronteiras, já que há criminalidade grave incluída no anexo II da proposta de Lei que não consta da lista de crimes sob competência reservada de investigação da Polícia Judiciária, nos termos do art. 7º da Lei de organização e investigação criminal[61]. Isso mesmo reconhece a CNPD ao mencionar que não todos mas somente a "grande maioria" dos crimes elencados na Diretiva estão sob a sua competência reservada[62].

Seguidamente, aponta para a falta de base legal flagrante na proposta de Lei no que respeita ao Gabinete de Informações de Passageiros e ao Ponto Único de Contacto para a Cooperação Policial Internacional. Segundo o n.º 1 do art. 4º da Diretiva, os Estados-Membros devem criar uma autoridade ou designar uma seção de uma autoridade já existente que tenha competência para prevenir, detetar, investigar ou reprimir infrações terroristas e crimes graves. Ora, um gabinete "não é, em si, uma autoridade nem é competente na aceção da Diretiva"[63], mesmo estando sob a alçada do Ponto Único de Contacto para a Cooperação Policial Internacional, porque este também não o é. Nos termos do n.º 1 do art. 23º-A da Lei de segurança interna[64], o Ponto Único de Contacto para a Cooperação Policial Internacional é um centro operacional que coordena a cooperação policial, não uma autoridade. O seu Gabinete de Gestão, segundo o n.º 4, é, de facto, constituído por elementos de OPCs que o coordenam mas serem estes elementos provenientes de autoridades competentes não torna o Ponto Único de Contacto para a Cooperação Policial Internacional uma autoridade ou entidade competente em si para o combate à criminalidade grave e ao terrorismo, faltando a devida base legal.

---

[61] Lei 49/2008, de 27 de agosto, sucessivamente alterada e republicada por último pela Lei 57/2015, de 23 de junho.

[62] Parecer 31/2018, processo 9827/2018, p. 2v.-3.

[63] Parecer 31/2018, processo 9827/2018, p. 3v.

[64] Lei 53/2008, de 29 de agosto, sucessivamente alterada e republicada por último pelo Decreto-lei 49/2017, de 24 de maio.

Surge ainda um potencial *spilling effect* que, embora importante, talvez tenha contornos diferentes dos mencionados no parecer da CNPD. É referido que os dados transmitidos às autoridades estrangeiras devem ser reencaminhados em cópia para o Ponto Único de Contacto para a Cooperação Policial Internacional. No entanto, nos termos do n.º 3 do art. 8º da proposta de Lei, não se diz que as informações transmitidas devem ser dadas a conhecer ao centro operacional mas parece antes que somente tem de ser dada a conhecer a própria transmissão. Ou seja, o Ponto Único de Contacto para a Cooperação Policial Internacional tem de saber que houve uma receção de dados por parte do Gabinete de Informações de Passageiros no âmbito da sua atividade de gestão da cooperação policial mas não parece derivar obrigatoriamente da norma que os dados transmitidos lhe tenham de ser fornecidos em cópia, como afirma a CNPD. Até porque, no número anterior, se diz que o Gabinete de Informações de Passageiros pode transmitir autonomamente ("por sua iniciativa") dados que tenha armazenado para entidades de outros Estados-Membros. Donde, talvez não haja lugar ao derrame, nestas situações concretas, de mais dados do que já sucede na atividade normal de tratamento de dados PNR.

Não obstante, a falta de clareza do texto permite a interpretação que acabou por levar a cabo a CNPD. Mais, convém frisar que a quantidade de dados a tratar será maciça e não há referências na proposta à capacidade ou aos meios técnicos de tratamento das informações, especificamente no que concerne a configuração das bases de dados ou os graus de acesso[65]. Se, na prática, se verificar que há uma duplicação do tratamento dos dados pessoais através da remissão de cópias para o Ponto Único de Contacto para a Cooperação Policial Internacional então não só haverá um problema de potencial falta de legitimidade (que já ocorre, de qualquer modo) como este requisito adicional ao processo a implementar gorá boa parte das expetativas de combate à criminalidade do legislador europeu.

O ponto seguinte parece ser de especial preocupação, muito embora a sua formulação se desvie do problema principal. Nos termos da alínea a) do n.º 1 do art. 6º, as informações PNR devem ser comparadas com "bases de dados das forças e serviços de segurança". Ora, para a CNPD o problema é a falta de menção explícita destas bases de dados porque o

[65] Parecer 31/2018, processo 9827/2018, p. 5.

fim descrito pode não corresponder às finalidades impressas na legislação europeia e, assim, poderiam consultar-se bases não idóneas. Não parece, porém, que faça sentido limitar as bases de dados a que deve ter acesso o Gabinete de Informações de Passageiros porque, se por um lado, os fins pelos quais o deve fazer estão mencionados expressamente na proposta e estes alinham-se tanto com o restante texto como com a Diretiva PNR, por outro, é conveniente ter aqui alguma margem de liberdade administrativa para produzir resultados significativos e úteis. Estar a nomear as bases de dados que são relevantes para alcançar os fins desta legislação poderia torná-la desatualizada de cada vez que surgisse uma nova, se renovasse ou se extinguisse uma determinada base. E raramente se saberá de antemão onde estarão as entradas que poderão fazer *match* com as informações introduzidas na busca do sistema.

Sendo que os fins estão limitados, o que importa é, na verdade, não restringir as bases de dados a consultar num momento histórico concreto mas sim garantir que quaisquer *hits* que surjam para além do catálogo de fins específicos sejam descartados ou que sejam aproveitados depois de criada a base legal que permita ir além destes escopos (e dos crimes enumerados no anexo) e que assim possam surgir investigações criminais dentro dos limites da legalidade. Ou seja, que os conhecimentos que sejam fortuitamente obtidos nestas comparações de dados e que não sejam relevantes nos termos desta legislação sejam tratados de forma juridicamente isenta e, de preferência, com base legal expressa[66].

A derradeira crítica da CNPD encerra, quase por acidente, um dos aspetos mais controversos deste tipo de bases de dados. É da competência da CNPD a aplicação de coimas às transportadoras aéreas que violem as suas obrigações de transferência de dados, segundo o n.º 4 do art. 19º da proposta de Lei. No seu parecer, porém, dá a entender que tal não cabe nas suas atribuições, bem como considerou que, sendo "uma autoridade de garantia dos direitos fundamentais, (...) afigura-se absurda a imputação de uma competência sancionatória por desrespeito de uma obrigação que consiste em transmitir a terceiros dados pessoais de todos os passageiros, recolhidos inicialmente com uma finalidade bem distinta". Apesar do foco

[66] À semelhança da admissibilidade dos meios de prova no âmbito de escutas telefónicas presente no n.º 7 do art. 187º do Código do Processo Penal, Decreto-lei 78/87, de 17 de fevereiro, sucessivamente alterado e republicado por último pela Lei 1/2018, de 29 de janeiro.

principal de atenção da CNPD ser (ou parecer ser) a falta de atribuições na legislação que rege a sua atividade, o que escreve em seguida é o que bem poderia ser a sua crítica substantiva fundamental a esta proposta mas que não o é, quiçá, por se tratar de legislação de origem europeia e, assim sendo, por não ter esta referência grande cabimento como crítica *per se*. Escreve a CNPD que essa competência ainda mais aburda é "por se inserir num quadro legislativo de evidente violação do princípio da proporcionalidade e de intrusão excessiva na privacidade das pessoas"[67]. Este sim é um ponto que merecia ser explorado por parte desta entidade neste parecer em face da falta de tradição nacional de recolha e tratamento de *big data* dos cidadãos nacionais e que, infelizmente, parece surgir quase por acaso.

2.2. O Conselho Superior da Magistratura e a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias

O parecer do CSM[68] é bastante mais sucinto e a sua apreciação resume-se à enumeração de alguns pontos que os magistrados consideraram mais relevantes, embora sem os explorarem aprofundadamente nem tecendo críticas como a CNPD.

São de mencionar, somente, dois aspetos. Primeiro, que a ontologia jurídica usada no catálogo de crimes anexo à proposta de Lei, como mencionado anteriormente, precisa de ser ajustada de forma plena à nomenclatura da ordem jurídica interna, até para facilitar a aplicação das normas pelos tribunais. Por outro lado, o CSM não encontra, ao contrário da CNPD, quaisquer incompatibilidades entre a Diretiva e a proposta no que respeita à criação e funcionamento do Gabinete de Informações de Passageiros e do Ponto Único de Contacto para a Cooperação Policial Internacional, concluindo, no geral, que a proposta é compatível com os termos da Diretiva. Parece ser a posição da CNPD mais avisada e o parecer dos magistrados menos aturado do que poderia ter sido.

O parecer da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias é igualmente omisso quanto a uma análise substantiva,

---

[67] Parecer 31/2018, processo 9827/2018, p. 5v.

[68] 2018/GAVPM/5633, 2.7.2018.

ficando antes por referências formais, nomeadamente que ver com a comumente designada Lei formulário[69]. É acompanhado de uma ficha técnica bastante detalhada sobre a evolução e o contexto legislativos da proposta de Lei, tanto a nível nacional como europeu, e, à parte a crítica já mencionada feita à falta de junção dos pareceres e resultados das consultas obrigatórias que o Governo deverá ter levado a cabo, a Comissão apenas sublinhou a má técnica legislativa de vários artigos da proposta[70] remeterem para diplomas ainda em apreciação pela AR. Embora reconheça não ser algo inédito, a verdade é que isto torna "difícil assegurar que haverá aprovação (e atempada) destas leis [de remissão], se serão ambas promulgadas e se poderão sair publicadas subsequentemente, de modo a que estas referências possam ser coordenadas aquando da publicação e, assim, fazer sentido"[71].

Conclusão

Apesar das críticas presentes nos diferentes pareceres, e muitas outras que lhe podem (e devem) ser assacadas[72], no dia 6 de julho de 2018, a proposta foi aprovada na generalidade em apenas 25 minutos[73], tendo em seguida descido à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, comissão competente para a discutir na especialidade. Foi apresentada pela Secretária de Estado Adjunta e da Administração Interna, Isabel Oneto, e debatida em reunião plenária, por arrastamento da agenda do Governo, em simultâneo com as propostas de Lei 125/XIII/3.a, sobre as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações

---

[69] Lei 74/98, de 11 de novembro, sucessivamente alterada e republicada por último pela Lei 43/2014, de 11 de julho.

[70] Arts. 10º, 12º, 14º, 16º e 20º.

[71] Nota técnica anexa ao Parecer de 4.7.2018, p. 6.

[72] A título de exemplo, veja-se Carpanelli, Elena, e Lazzerini, Nicole. "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR conundrum after Opinion 1/15 of the CJEU", in *Air & Space Law*, v. 42, n. 4 e 5, 2017, p. 377-402.

[73] Marcelino, Valentina, "Governo quer todas as polícias com acesso às informações de quem viaja de avião", *Diário de Notícias*. Disponível em https://www.dn.pt/edicao-do-dia/07-jul-2018/interior/governo-quer-todas-as-policias-com-acesso-as-informacoes-de-quem-viaja-de-aviao-9561024.html?target=conteudo_fechado, (acedido a 3/08/2018).

penais ou de execução de sanções penais e que transpõe a Diretiva (UE) 2016/680, e 126/XIII/3.a, que altera o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial. Por fim, foi aprovada com os votos do Partido Socialista e do Partido Social Democrata, tendo votado contra o Bloco de Esquerda, Os Verdes e o Partido Comunista Português e tendo-se abstido o Partido do Centro Democrático e Social-Partido Popular e o Pessoas-Animais-Natureza.

Da discussão parlamentar é relevante, porém, extrair alguns comentários que apontam precisamente para a natureza algo insidiosa do esquema PNR. Começou o deputado José Manuel Pureza, do Bloco de Esquerda, a ridicularizar a transformação de dados antes puramente comerciais em chaves essenciais para a "investigação de crimes de terrorismo e de alta criminalidade". Ademais, criticou que se introduza na ordem legal portuguesa uma medida que se intromete abusivamente "em todas as nossas vidas e o [faça] de uma forma totalmente desproporcionada, violando assim, grosseiramente, os princípios elementares do Estado de direito", e, em seguida, questionou a manutenção na posse de entidades administrativas de dados pertencentes a pessoas não tidas como suspeitas, a omissão expressa das autoridades competentes do texto da proposta e a transmissão dos dados da Polícia Judiciária para o sistema de segurança interna[74].

No final do debate, o deputado do Partido Comunista Português António Filipe realçou outros aspetos importantes, nomeadamente a "policialização das companhias aéreas [e o facto destas passarem] a recolher um conjunto de dados relativos a todos os passageiros, dados esses que migram imediatamente para um gabinete de controlo que, imagine-se, está sob a égide do secretário geral do Sistema de Segurança Interna, não havendo, aqui, sequer, autoridades judiciárias envolvidas"[75]. De facto, a falta de um mandato judicial ou instrumento semelhante no esquema PNR é uma das características mais criticáveis do regime. Por isso, quando Isabel Oneto apresenta a medida referindo que, na "sequência de ações de prevenção criminal que tenham de ser desenvolvidas, terá de ser feita a comunicação às autoridades judiciárias, nomeadamente ao Ministério Público ou a um

---

[74] Debate parlamentar de 6.7.2018 (série I, XIII legislatura, sessão legislativa 3, número 104), pp. 39-40.

[75] *Idem*, p. 43.

juiz, sendo que as competentes investigações serão desencadeadas pelo DCIAP"[76], isto não corresponde nem às exigências normativas presentes na proposta de Lei nem na Diretiva — estas comunicações não estão previstas, pelo que é procedente a crítica do deputado comunista. E tal adensa-se visto que, como continua, "[d]epois, há, ainda, a possibilidade de esses dados migrarem para países terceiros sem que haja a possibilidade de controlar qual será o seu alcance". Não estaremos, então, perante uma verdadeira "paranoia securitária que nada justifica, que é desproporcional e que só pode ter a nossa oposição"[77]?

Como mencionado, outras críticas substantivas podiam ser feitas ao regime que está prestes a entrar em vigor em Portugal[78]. O debate parlamentar parcialmente aqui transcrito elucida sobre algumas delas. Já os pareceres analisados podiam ter avançado mais nesse sentido mas, por outro lado, talvez não fossem o local indicado para críticas mais profundas visto a proposta de Lei não ser uma inovação nacional mas somente a transposição de indicações europeias bastante restritivas; o impulso legiferante está alhures, pelo que as críticas de fundo deveriam ser dirigidas ao legislador europeu e não tanto às instâncias nacionais. É quase como se a transposição nacional já estivesse para lá do ponto de não retorno, preferindo os parlamentos nacionais a sua aceitação em detrimento das sanções aplicáveis pela não transposição de forma correta e tempestiva.

Embora não seja algo novo, este é um dos perigos principais desta nova medida de política criminal: paira sobre si uma aura de insuspeição e aparenta de tal modo ser essencial no cumprimento dos objetivos de combate ao terrorismo e à criminalidade grave que vai sendo aceite nas diversas instâncias até fazer parte do sistema jurídico. Só que, em bom rigor, estamos perante uma legislação altamente intrusiva da privacidade e intimidade dos cidadãos da UE que fará mover informações entre as esferas pública e privada mais depressa que os meios de comunicação social ou o sistema financeiro[79] e que vem parcialmente oculta sob a sombra de um pacote bastante protetor dos dados pessoais das pessoas. Mas deste bastante se

---

[76] *Idem*, p. 39.

[77] *Idem*, pp. 43-44.

[78] A título de exemplo, veja-se Urbano de Sousa, Constança, *op. cit.*

[79] De Goede, Marieke. "The chain of security", in *Review of International Studies*, v. 44, 2017, p. 24-42. Vejam-se, igualmente, Amoore, Louise. *The politics of possibility*, Duke

fala e do PNR pouco se sabe. Parece uma atitude esquizofrénica e muito perigosa, tanto da parte da classe política como dos próprios meios de comunicação social. Só que nem todos os meios justificam os fins[80].

A proposta deveria ter sido revista em sede de especialidade para acomodar muitas das recensões que as entidades e alguma doutrina mais avisada vão fazendo, nomeadamente quanto a aspetos pouco debatidos, como a inclusão de voos intra-UE. No entanto, já no final do processo de revisão do presente texto, a proposta foi aprovada ignorando as críticas anteriores e tornou-se na Lei 21/2019, de 25 de fevereiro[81]. Este tipo de legislação é inédito em Portugal, mesmo à sombra da União, e a sua aceitação pouco criteriosa pode não produzir os resultados esperados junto do público e em termos de eficiência e eficácia das investigações criminais. Aliás, a pergunta principal que talvez um dia venha a ser colocada perante os tribunais será a de saber se a intrusão nas informações pessoais dos passageiros pelo sistema PNR justifica e é verdadeiramente proporcional face aos resultados que os OPCs obterão. No nosso entender, não.

University Press, 2013 e Bellanova, Rocco, e Duez, Denis. "A different view on the making of EU security", in *European Foreign Affairs Review*, n. 17, 2012, p. 109-214.

[80] Muito embora haja autores que consideram que a Diretiva PNR está apta para respeitar o nível de protecção de dados pessoais na UE, mesmo que a sua legalidade seja contestada junto do TJ. Veja-se, a título de exemplo, Lowe, David. "The European Union's Passenger Name Record data Directive 2016/681: Is it fit for purpose?", in *International Criminal Law Review*, n. 16, 2016, p. 856-884.

[81] De forma completa, Lei 21/2019, de 25 de fevereiro, que regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, transpondo a Diretiva (UE) 2016/681 e procede à terceira alteração à Lei 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna.

A nova lei das secretas: A imperatividade constitucional como dilema às novas ameaças num contexto global de defesa e segurança

Sérgio Sousa Lopes Freire de Azevedo*

Resumo: 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 política. 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 da 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 Tribunal Constitucional. 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. Mas os dilemas constitucionais não se esgotam na supressão e no aprofundamento das inconstitucionalidades decretadas continuando a constituir-se como barreira à resposta necessária às neoameças da sociedade global de risco.

***Palavras-Chave**: Segurança; Direitos individuais; Tribunal Constitucional.*

Abstract: Intelligence accompanied the history of the founding of Portugal. From the affirmation of our nationality to the present day, passing through a black period of political persecution. Global threats require intelligence services to respond to the vulnerabilities brought about by globalization by endowing the State with the benefit that the principiis obsta cannot only translate into internal and external security, but

* Deputado à Assembleia da República (AR) na XII e XIII legislatura. Advogado-estagiário. Doutorando em Direito e Segurança na Faculdade de Direito da Universidade Nova de Lisboa (FDUNL).

also in the protection of strategic sectors of the State which also guarantee survival of the democratic rule of law. The access to metadata by intelligence services finds legal tranquility in their required authorization and control by judicial authority. This requirement suppresses the unconstitutionality previously decreed by the Constitutional Court. They are just another mechanism of anticipation. An anticipated judicial and civilian oversight by the supervisory board, but are also new supports for cooperation between services and security forces in response to growing non-traditional threats to national and collective security. But the Constitutional dilemmas are not exhausted by the suppression and deepening of the unconstitutionalities decreed by the Constitutional Court, continuing to constitute a barrier to the necessary response to the neo-threats of the global risk society.

Keywords: *Security; Individual rights; Constitutional Court.*

1. Contextualização contemporânea dos Serviços de Informações da República Portuguesa

Socorrendo-nos das palavras de Rui Pereira "o primeiro ensinamento a retirar da experiência da polícia política é a inconveniência de uma confusão entre as actividades de produção de informações, manutenção da ordem pública, investigação criminal e direcção do processo penal. O que torna a polícia política um instrumento perigoso é a confusão de todas estas competências. A par, claro está, da possibilidade de perseguir delitos políticos – delitos que não se confundem com crimes contra o Estado (...), resultando antes da denegação de direitos cívicos como os de expressão, reunião, manifestação ou associação"[1].

Ao nível da segurança do Estado, este foi o maior desafio que o regime constitucional democrático enfrentou desde o seu estabelecimento. A implementação de um serviço de informações inconfundível com a ação persecutória e opressora da polícia política, capaz de produzir infomação de segurança incolidível com os direitos, liberdades e garantias constitucionalmente estabelecidos. Aliás, a este respeito, não é por mero acaso que o texto constitucional democrático de 1976, na sua versão original, reflete

[1] Pereira, Rui. "A Segurança na Constituição", in *Estudos de Direito e Segurança*, v. II, 1ª ed., Lisboa: Almedina, 2015, p. 415–416.

sobretudo uma sistematização das correntes ideológicas e políticas que emanam do período revolucionário seguinte à queda do regime autoritário e fascizante do Estado Novo e que se afirma, até à primeira revisão constitucional de 1982, como cânones intransponíveis quer da percepção social da época como da própria letra fundamental.

Um exemplo paradigmático desta aceção é aquilo a que Gomes Canotilho apelida de "momento maquievélico constitucional"[2], com a introdução de uma norma de recorte constitucional atípico que estabelecia, no art.º 309.º do seu texto originário, a incriminação retroativa e o julgamento dos agentes da PIDE/DGS pelas "atividades terroristas das mencionadas organizações que fizeram do crime institucionalizado a sua razão de ser (...)" já anteriormente estabelecida pela Lei n.º 8/75, de 25 de julho de 1975.

Porém, que não se pense que do ponto de vista estratégico-militar Portugal tivesse ficado sem qualquer serviço de informações de defesa, não fosse, alías, o movimento revolucionário um movimento liderado por militares constituindo-se num Conselho da Revolução[3], constitucionalmente consagrado como órgão de soberania, como garante do regular funcionamento das instituições democráticas, como garante do cumprimento da Constituição, como órgão político e legislativo em matéria militar e como garante da legitimidade revolucionária[4], apenas extinto na democratização plena do regime com a revisão constitucional de 1982.

Após a Revolução de 25 de Abril de 1974, os serviços de informações militares ficaram a cargo da Segunda Divisão do Estado-Maior-General das Forças Armadas assegurando, assim, a produção de informações militares de exclusivo interesse da segurança externa do país. Contudo, após as conturbações políticas de 11 de março de 1975, acabaria por ser extinta dando lugar ao Serviço Diretor e Coordenador da Informação, por força do Decreto-Lei n.º 250/75, de 23 de maio, de dependência direta do Conselho da Revolução e que viria, mais tarde em 1977, a dar origem à Divisão de Informações.

---

[2] Gomes Canotilho, J. J. *Direito Constitucional e Teoria da Constituição*. 7ª ed., Coimbra: Almedina, 2003, p. 205-206.

[3] *Vide* Lei n.º 5/75, de 14 de março, que extingue a Junta de Salvação Nacional e o Conselho de Estado e institui o Conselho da Revolução.

[4] *Vide* os art.º 142.º a 149.º do texto originário da Constituição de 1976.

Não obstante, a criação de um serviço de informações de carácter não militar e produtor de segurança do Estado, e dos cidadãos em particular, era assunto indesejável fruto das ainda muito recentes experiências com a atuação da PIDE/DGS. Como nos refere Marques Ferreira "faltava ainda a maturidade para conceber as informações ao serviço de uma noção de segurança nacional que antecipasse a avaliação da ameaça a partir de um quadro por elas subscrito" [5].

E de facto assim foi e nunca nenhum impulso foi devidamente concretizado fruto de uma realidade, à época, toldada pela desconfiança e oposição de um país impreparado e receoso dos tempos assombrosos da PIDE/DGS. Conforme Jorge Bacelar Gouveia: "Havia um trauma a vencer, um trauma psicológico, trauma histórico e trauma político: a necessidade de criar serviços de informações do Estado, mas tal nunca podendo significar qualquer regresso ao passado, protagonizado que foi pela actividade de informações levada a cabo por duas instituições que tinham ficado com as cicatrizes do horror do regime do Estado Novo" [6].

Apenas volvidos dez anos da revolução de abril é que a "maturidade" do regime permitiu que o legislador pudesse fazer aprovar a Lei Quadro n.º 30/84, de 5 de setembro, estabelecendo a criação do SIRP quebrando, desta forma, o vazio no domínio de um serviço de informações que contemplasse três vertentes essenciais: estratégicas, de defesa e de segurança. Chegaria, assim, o reconhecimento de que a produção de informações era central no domínio da segurança interna e externa e que o seu desenvolvimento não só ocorre a montante da investigação criminal e da direção do processo penal, embora existam serviços que, nalguns casos, o possam desempenhar – não foi essa a nossa opção, como é crucial no preencimento de lacunas que põem em causa a vivência em segurança da comunidade.

Foi exatamente isso que provaram os acontecimentos à época. Quer as manifestações, com a consequente dificuldade de previsão de ação e desmantelamento, das "Forças Populares 25 de Abril" e do grupo de extrema-direita "Rede Bombista do Norte" e de alguns episódios relevantes oriundos da atuação de redes terroristas estrangeiras a atuar em Portugal,

---

[5] Marques Ferreira, Arménio. "O Sistema de Informações da República Portuguesa", in *Estudos de Direito e Segurança*, v. I, 2ª ed, Lisboa: Edições Almedina, 2015, p. 77.

[6] Bacelar Gouveia, Jorge. "Os Serviços de Informações de Portugal: Organização e Fiscalização", in *Revista de Direito e Segurança*, ano I, n. 1, Lisboa, 2013, p. 67–68.

como são o atentado contra a Missão diplomática de Israel em Lisboa, em 1979, o assassinato de um diplomata turco em Lisboa, em 1982, reinvidicado pelo Exército Revolucionário Arménio ou, em 1983, o assassinato em Montechoro do dirigente da OLP, Issam Sartawi, que participava numa reunião da Internacional Socialista, reivindicado pela organização terrorista líbia FATAH – Conselho revolucionário, também conhecida pela adoção do nome do seu fundador, Abu Nidal.[7]

Surgia, deste modo, o SIRP, contemplando três serviços de informações distintos: o SIED, o SIS e o SIM[8].

Independentemente das vicissitudes que o SIRP sofreu até aos dias de hoje[9], mas que não são objeto de tratamento neste artigo, mantém, de uma maneira geral, a sua missão e os seus objetivos fundacionais[10]. Em todo o caso, notou-se uma evidente preocupação do legislador na atribuição expressa de uma norma dedicada ao princípio da exclusividade que imbui os órgãos do SIRP à prossecução estrita dos objetivos previstos na lei proibindo-os de prosseguir outros que não esses[11].

A ratio da norma é evidente. Mediante a experiência passada o legislador viu-se compelido a deixar de forma expressa e inequívoca os limites da atuação dos Serviços[12] clarificando a proibição de desempenharem funções policiais ou de direção do processo penal, "toda a instrução, deve

---

[7] *Vide* Diário da AR n.º 88 série I, de 24 de março de 1984, p. 3825 e ss., Marques Ferreira, Arménio. "O Sistema de Informações (...)", *op. cit.*, p.78 e Reis, Sónia; Botelho da Silva, Manuel. "O Sistema de Informações da República Portuguesa", in *Revista da Ordem dos Advogados*, Ano 67, Lisboa, 2007, p. 1258.

[8] Extinto por força do Decreto-Lei n.º 254/95, de 30 de setembro, e na sequencia da aprovação da Lei n.º 4/95, de 21 de fevereiro, com as suas competências integradas no SIED, à época e com a alteração SIEDM, e anteriormente por força da Lei n.º 48/93, de 26 de fevereiro com a criação da Divisão de Informações Militares (DIMIL), hoje CISMIL, separando por completo as informações de segurança militar das restantes.

[9] Cinco alterações ao diploma original.

[10] Sobre a criação e desenvolvimento do SIRP *vide* a explanação completa e detalhada de Bacelar Gouveia, Jorge. "Os Serviços de Informações (...)", *op. cit.*, p. 63–85, Marques Ferreira, Arménio. "O Sistema de Informações (...)", *ob. cit.*, p. 67–94 e Cardoso, Vizela. "As informações em Portugal (...)", *op. cit.*, p. 489–514.

[11] Art.º 6.º do texto originário da Lei n.º 30/84, de 5 de setembro – Lei Quadro do Sistema de Informações da República Portuguesa.

[12] Fá-lo até triplamente, art.º 3.º e 4.º do texto originário da Lei n.º 30/84, de 5 de setembro – Lei Quadro do Sistema de Informações da República Portuguesa.

ser, portanto, produzida no seio do processo penal, ao abrigo das normas garantísticas deste, não podendo ser utilizada prova colhida na actividade de informações. A actividade de informações visa, fundamentalmente, iluminar as políticas públicas de segurança – legislativas ou administrativas – com um conhecimento rigoroso da realidade que possibilite a sua formulação óptima, mas não se destina diretamente à investigação processual penal ou à manutenção da ordem pública".[13]

2. O alcance do *principiis obsta* na recolha das informações e o seu alcance em tempos de risco global

Ulrich Beck, identificando o terrorismo e as alterações climáticas como as principais ameaças da sociedade de risco global, aponta que "a possibilidade de externalização do perigo desencadeou um ressurgimento da guerra enquanto guerra rápida e limitada. O critério de sucesso reside, entre outros aspetos, na dissimulação da elevada vulnerabilidade das sociedades civis ocidentais(...) portanto os ataques terroristas têm de se colocar de tal forma que a economia, a política e a vida social sejam atingidas no cerne da paz sentida".[14]

Ou seja, a importância e a missão da produção de informações já não é apenas um capricho das sociedades não liberais, mas antes uma necessidade tangente não apenas à segurança interna e externa dos Estados, realizada evidentemente fora da latitude da investigação criminal e da atividade de polícia, como se constitui como um pilar nos objetivos estratégicos dos Estados muito além do mero sentido estrito de segurança, da proteção do cidadão e do zelo pelas suas liberdades individuais que, numa perspetiva somatória, constituem os pilares do Estado de Direito.

Quer isto dizer que a atividade de recolha de informações, numa sociedade cada vez mais complexificada pelas relações económicas transmitentes, não raras vezes de interesses difusos fruto das ligações que lhes emergem nos mais diversos patamares da vida social e política,

---

[13] Reis, Sónia; Botelho da Silva, Manuel. "O Sistema de Informações da República Portuguesa", in *Revista da Ordem dos Advogados,* ano 67, Lisboa, 2007, p. 1277.

[14] Beck, Ulrich. *Sociedade de risco mundial em busca da segurança perdida*. 1ª. ed., Lisboa: Edições 70, 2015, p. 287.

são um factor decisivo de ponderação dos Estados em matéria económica, tecnológica, energética ou ambiental. Como nos lembra Marques Ferreira "as informações que aqui importa considerar, como objeto, não são meras notícias mais ou menos contextualizadas. São antes elementos de conhecimento sistematizados em quadros interpretativos, através de critérios que sobrepõem a estrutura de sentido à relação causal. São produzidas através de um método próprio e preservadas da atenção e conhecimento de terceiros. O seu destino é o de integrarem os trabalhos preparatórios das disposições e determinações dos decisores políticos"[15].

Por conseguinte, nos tempos de hoje a dimensão do *principiis obsta*, ou seja, de impedir no início, constitui a dimensão primacial da produção de informações. Uma dimensão que transcende a percepção histórica e tradicional da finalidade das informações, mas que a reforça e completa atribuindo-lhe condições de relevo não apenas de otimização das condições necessárias a uma governação atinente aos interesses estratégicos nacionais, mas também, cumprindo o seu papel fundador de salvaguarda da segurança.

Ora, o desafio de um sociedade integrada, global e moderna como a nossa, de resto, constitutiva de um Estado de direito em permanente construção e realização, mas paradoxalmente dotado de uma crescente vulnerabilidade fruto da diversificação de poderes, é saber responder dentro do quadro constitucional, isto é, numa profunda valoração pelas nossas liberdades individuais, à necessidade de criação de um conjunto de políticas integradas de prevenção dos novos fenómenos de criminalidade transnacional organizada, às ameaças enunciadas por Beck e a todas aquelas que quotidianamente surgem por força da intensa e permanente globalização e que colocam a segurança do Estado num caleidoscópio confuso e dinâmico. Mas, sobretudo, sem cairmos no risco da indeterminação da ação que mais não faz do que agravar a insegurança, ou pior, o seu sentimento.

Quer isto, então, dizer que deve existir, em todo o caso, um desligamento entre a produção de informações e a investigação criminal? De maneira nenhuma. A produção de informações em Portugal, não sendo confundível com investigação criminal, e já o vimos que não é por

---

[15] Marques Ferreira, Arménio. "O Sistema de Informações (...)", *op. cit.*, p. 69.

força da Constituição[16] e da lei, constitui a antecâmera da investigação criminal, a fase que a antepõe, está "para a investigação criminal como os crimes de perigo para os crimes de dano – constituem uma antecipação da tutela que é proporcionada pela intervenção formal do direito penal" [17].

É portanto neste patamar diacrónico, na sua relação com as restantes forças de segurança a quem compete a investigação criminal[18], que se conjuga a sua atuação. Aos serviços de informação importa a recolha de informação que permita aferir uma certa potencialidade de atividades ilícitas, "perante a ordem jurídica portuguesa, os serviços de informações jamais assumem a natureza de polícia de investigação criminal, embora possam produzir informações com interesse para o cumprimento das missões das Forças e demais serviços de Segurança, no domínio da prevenção e até da investigação criminal"[19]. Subsumem-se, assim, as potencialidades ilícitas típicas que resultam do terrorismo, da criminalidade internacional organizada e todas outras, diria atípicas, que decorrem quer dos interesses estratégicos do Estado no exterior, quer da penetração que organizações terceiras pretendem assumir em áreas estratégicas do Estado e que se podem consubstanciar em áreas tão diversas como as questões ambientais, de inovação tecnológica, a economia, a saúde ou outra qualquer área exposta às dinâmicas das relações de globalidade.

Mas esta diacronia não confina a atividade de recolha de informações apenas à esfera dos serviços de informação. As forças de segurança podem elas também ser produtoras de informações. O que as distingue é a sua essência. Enquanto que os serviços de informação no processo de recolha de informação fazem-no não partindo de uma realidade ou atividade pré-existente, com exceção de raríssimos casos, mas sim como fundamento de juízo de critério para a realidade, que poderá desencandear

---

[16] N.º 1 do art.º 219.º da CRP de onde se extrai o princípio da legalidade da ação penal onde se convoca, com evidência, a política de direção criminal, ou seja, as prioridades sobre a investigação criminal, a direção da ação penal e a execução de penas e medidas de segurança.

[17] Pereira, Rui. "Informações e Investigação Criminal", in *I Colóquio de Segurança Interna – ISCPSI*. Lisboa, 2005, p. 157.

[18] Lei n.º 49/2008, de 27 de agosto, que regula a Organização e Investigação Criminal.

[19] Clemente, Pedro. "A polícia de informações em Portugal", in *Volume Comemorativo 20 anos ISCPSI*, Lisboa: Edições Almedina, 2005, p. 374.

em investigação criminal, as forças de segurança recolhem-na partindo de uma investigação existente, ou seja como uma diligência instrumental para o desenvolvimento de elementos probatórios que podem, ou não, desencadear o desenvolvimento da ação penal.

Quanto mais não seja, porque a própria atividade dos serviços de informação está reduzida a um quadro predicativo juridicamente limitado, até por força do nosso texto fundamental[20] e que em caso algum pode pôr em causa direitos, liberdade e garantias dos cidadãos.

3. A lei das "secretas" e a posição do Tribunal Constitucional: dois momentos distintos

Torna-se inquestionável hoje afirmar que a segurança é contemporânea do constitucionalismo. Desde o texto fundamental de 1822, com a trilogia liberdade-segurança-propriedade, ao texto constitucional atual que a segurança surge como expressão inequívoca dos direitos e deveres individuais dos cidadãos tornando-a numa assunção jusfundamental incontroversa. Mas é sem margem para dúvidas na Constituição de 1976, em rigor na sua quarta e quinta revisão, que ela se aprofunda e manifesta na sua plenitude no ordenamento jurídico português passando a atuar como direito, liberdade e garantia no mesmo plano que as mais diversas liberdades constitucionalmente estabelecidas. Mais, é aqui que ela assume condição de tutela para o exercício de outros direitos fundamentais, mas é também aqui, neste contexto constitucional, que emerge a relação de interdependência entre o conceito de segurança e o conceito de liberdade. Fazendo-nos pressentir que um não existe sem o outro, mas que ao mesmo tempo e em diversas situações podem produzir mutuamente relações antinómicas[21].

---

[20] *Vide* anotação n.º VII ao art.º 272.º da CRP de Gomes Canotilho, J. J., Moreira, Vital. *Constituição da República Portuguesa Anotada*, v. II, 4ª ed, Coimbra: Coimbra Editora, 2014, p. 860-861.

[21] Azevedo, Sérgio. "A Segurança como Direito, Liberdade e Garantia: uma perspetiva histórico-constitucional", in *Revista de Direito e Segurança*, ano V, nº 10, Lisboa, 2017, p. 197-224.

3.1. O Decreto n.º 426/XII da AR e a posição do TC

Em sede de fiscalização preventiva da constitucionalidade, o TC apreciou[22] o diploma que aprovou o Regime Jurídico do Sistema de Informações da República Portuguesa[23], em concreto o disposto no número 2 do artigo 78.º que estabelecia que "os oficiais do SIS e do SIED podem, para efeitos do disposto na alínea c) do n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados ou proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado"[24], declarando a sua inconstitucionalidade por considerar que a norma em apreço consubstanciava uma ingerência na vida privada dos cidadãos, "pondo em causa direitos fundamentais das pessoas envolvidas no ato comunicacional"[25] violando desta forma o preceito constitucional estabelecido pelo artigo 34.º da Constituição da República Portuguesa[26].

Pode considerar-se que, de facto, o legislador não soube acautelar da melhor forma a densificação da norma que estabelecia o acesso aos dados causando uma evidente desconformidade com o preceito constitucional previsto no art.º 34.º n.º 4 da CRP.

Ainda que com nuances[27] gerou-se, em sede de fiscalização, um alargado consenso jurídico nas manifestações do voto dos conselheiros do TC (12 votos a favor e um conta) demonstrando a inconstitucionalidade do art.º 78.º n.º 2 em três aspetos essenciais:

---

[22] Acórdão do TC n.º 403/2015, Proc. n.º 773/15, de 27 de agosto de 2015.

[23] Decreto n.º 426/XII da AR, de 31 de julho de 2015 – Regime Jurídico do Sistema de Informações da República Portuguesa.

[24] N.º 2 do art.º 78.º do Decreto n.º 426/XII da AR, de 31 de julho de 2015 – Regime Jurídico do Sistema de Informações da República Portuguesa.

[25] Ponto 12 do Acórdão do TC n.º 403/2015, 27 de agosto de 2015.

[26] "O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis."

[27] *Vide* declarações de voto anexas ao Acórdão doTC n.º 403/2015, 27 de agosto de 2015.

1. O carácter meramente administrativo da Comissão de Controlo Prévio, apesar da sua composição constituir-se por três magistrados do Supremo Tribunal de Justiça, atribuindo-lhe uma ausência de soberania jurídico-normativa na organização judicial;
2. A proibição de ingerência de autoridade pública, salvo nos casos previstos na lei em matéria de processo penal, nas comunicações e, por conseguinte, na proteção que os dados em causa assumem[28];
3. A impossibilidade de intervenção dos serviços de informações em matéria de investigação criminal[29].

Ora, com exceção do insuficiente grau de precisão normativa, quer relacionado com os fundamentos de acesso a dados[30] quer com as atribuições e constituição da Comissão de Controlo Prévio, o entendimento do TC não nos merece acolhimento ontológico porquanto, como refere Maria Lúcia Amaral, "a existência de Serviços de Informações da República – cujos fundamentos constitucionais o Tribunal pura e simplesmente não aborda – numa ordem, como a nossa, de Estado de Direito democrático, justifica-se pela necessidade de salvaguardar bens jurídicos, coletivos e individuais, que ocupam na axiologia constitucional um lugar não menor que os bens tutelados por normas penais incriminadoras"[31].

Quer isto inevitavelmente dizer que, apesar da inequívoca proibição dos serviços de informação praticarem atos de competência exclusiva dos

---

[28] Ponto 15 do Acórdão do TC n.º 403/2015, 27 de agosto de 2015 , "(...) Na verdade, o acesso aos dados de tráfego pode constituir uma ingerência gravosa na vida privada das pessoas já que se pode aceder a informações relativas a todas as chamadas efetuadas, incluindo as chamadas para as linhas de serviço de emergência/SOS/similares, ao número de chamadas, aos números de telefone chamados, à hora de início e duração de cada chamada e às respetivas unidades de contagem.".

[29] Idem ponto 19 "Por conseguinte, os serviços de informação não possuem quaisquer atribuições policiais ou de investigação criminal, ou seja não se destinam a garantir o respeito e cumprimento das leis gerais (v.g. defesa da ordem pública), nem apurar da autoria da prática de crimes, estando-lhe legalmente vedada tais atividades (...)".

[30] N.º 2 do art.º 78.º conjugado com a al. c) do n.º2 do art.º 4.º do Decreto 426/XII da AR nomeadamente a expressão indeterminada "alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido".

[31] *Vide* declaração de voto da Juíza Conselheira Maria Lúcia Amaral anexa ao Acórdão do TC n.º 403/2015, 27 de agosto de 2015 .

órgãos de polícia criminal e das autoridades judiciárias ou atos lesivos dos mais diversos direitos, liberdades e garantias, apesar da distinção absoluta entre produção de informações e investigação criminal[32]; na verdade, a prevenção primária e a segurança do Estado assumem uma incontornável relevância na sociedade de risco global, sobretudo desde a mutação conceptual e operativa do conceito de segurança provocada pelo evento do 11 de setembro, que levou à reavaliação e adaptação de meios de defesa quanto a perigos que emanam da complexa criminalidade transnacional organizada e dos atentados contra os fundamentos do Estado.

Isso faz das informações um instrumento da investigação criminal. São, se quisermos, a manifestação do *principiis obsta,* ou seja, a fase prévia da investigação criminal. O desejável impedimento inicial de crimes que atentem contra o estado de direito consubstanciando-se numa antecipação da tutela proliferada pelo direito penal.

3.2. O Decreto n.º 147/XII da AR

O pedido de fiscalização do diploma que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do SIS e do SIED redunda no lamentável equívoco e na indesejável contradição de confundir recolha de informações com investigação criminal, direção do processo penal e manutenção da ordem e tranquilidade pública.

O acesso a metadados pelos Serviços de Informações, na sua nova formulação normativa[33], encontra tranquilidade jurídica na sua exigível

---

[32] No entanto, ainda que sejam coisas distintas, seria igualmente um equívoco se negligenciássemos a existência da sua relação.

[33] Art.º 1.º do Decreto n.º 147/XIII da AR de 19 de julho de 2017, que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário) ,"A presente lei regula o procedimento especial de acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP) relacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo, o qual é sujeito a acompanhamento do Ministério Público e controlo judicial".

autorização e controlo por autoridade judicial. Este requisito vem suprimir a inconstitucionalidade anteriormente decretada pelo TC.

Aliás, a experiência internacional que, inexplicavelmente, não se manifestou na inspiração legislativa do Decreto n.º 426/XII da AR e que acabou por ser declarado inconstitucional, ajuda-nos a compreender esta nova redação e o inevitável reposicionamento do legislador português. Ainda que com vicissitudes quanto às competências dos diversos Serviços de Informação, é-nos possível encontrar semelhanças no que respeita ao acesso a comunicações em países com ordenamentos jurídicos tão distintos como a Alemanha, o Reino Unido ou a Espanha[34].

Assim, é em moldes mais garantísticos, e de certa forma correspondentes às exigências maioritárias do TC, que o Decreto n.º 147/XIII da AR densifica não apenas determinados conceitos-base indispensáveis e com suficiente grau de precisão quanto aos objetivos a atingir (art.º 2.º), atribui fundamento concreto para o exercício de restrições de direitos, liberdades e garantias (art.º 12.º) com a sua recondução a ilícitos muito específicos tipificados no ordenamento jurídico-penal (art.º 3.º e 4.º), reveste com cunho garantístico prévio e póstumo a necessidade imperiosa de controlo judicial (art.º 5.º, 10.º 12.º n.º 2 e n.º 3) por uma formação das secções criminais do Supremo Tribunal de Justiça e com conhecimento do Procurador-Geral da República[35], deixando a esse Tribunal a apreciação dos requisitos de necessidade, adequação e proporcionalidade, e um certo poder de direção/intervenção à atividade de recolha de informações afastando por completo o indeterminismo da expressão "controlo prévio" assumida pelo diploma anterior.

São, se quisermos, apenas o reforço dos mecanismos de antecipação que cabem na missão dos serviços de informações. 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

---

[34] Barradas, João Pires. "O Decreto n.º 147/XII como demonstração de maturidade democrática", in *Revista de Direito e Segurança*, ano V, nº 10, Lisboa, 2017, p.78-80.

[35] O que nos parece acertado existir "apenas" um "acompanhamento" do Ministério Público e nunca uma validação, ainda que facultativa, evitando-se assim o trágico equívoco entre recolha de informações e investigação criminal, uma vez que, por disposição constitucional e de lei, recolha de informações não é recolha de prova e ação preventiva não é direção processual penal. Para tal existe a imposição subsumida no art.º 13.º do Decreto n.º 147/XIII.

em resposta às crescentes ameaças não tradicionais à segurança nacional e coletiva.

Ainda assim, é nossa opinião que subsiste um dilema tendencialmente inultrapassável, a não ser por via de uma imponderável revisão Constitucional ou por via, absolutamente indesejável de resto, da equiparação dos Serviços de Informações a Órgãos de Polícia Criminal assumindo, deste modo, poderes de investigação criminal, manutenção da paz e da ordem pública e coadjuvação na direção do processo penal.

E o dilema é, evidentemente, a previsível, mas indesejada, declaração de inconstitucionalidade novamente por força da violação do art.º 34.º da CRP[36]. Claro que aqui somos forçados a acompanhar a interpretação de Jorge Miranda e Rui de Medeiros, porquanto a inviolabilidade de princípio deve entender-se limitada "(...) pela própria Constituição no seu todo, em especial pelo equilíbrio entre os diferentes direitos fundamentais, máxime o direito à vida ou à integridade física. Constata-se, desta forma, que o recorte do conceito de inviolabilidade utilizado no artigo 34.º deve ser aferido à luz de uma leitura sistemática da Constituição, e não através de uma leitura atomística do referido preceito"[37] e deste modo assumir que o TC deverá dar espaço de respiração à sua interpretação constitucional. Mas essa não tem sido a sua tradição.

A rigidez na interpretação restritiva de limitações ao exercício de direitos fundamentais, de resto como prática clássica do Direito Constitucional, conducente quer à identificação clara e objetiva da violação de determinado direito fundamental, quer na garantia de que essa ingerência, ou violação, é necessária e justificável muito provavelmente vingará.

Numa perspetiva de proporcionalidade quer do ponto de vista do objetivo que ela pretende alcançar, da sua eficácia e necessidade face à existência de medidas menos intrusivas que alcancem esse fim, quer na justificação de que ela se reveste na menor desvantagem possível para a posição jusfundamental decorrente do direito[38].

---

[36] Tomando como referência a tradição interpretativa do TC em relação ao art.º 34.º da CRP.

[37] Miranda, Jorge; Medeiros, Rui. *Constituição Portuguesa Anotada*, Tomo I, Coimbra: Coimbra Editora, 2005, p. 757-758.

[38] *Vide* Declaração de Voto vencido do Juiz-Conselheiro José António Teles Pereira acerca do Acórdão do TC n.º 403/2015, 27 de Agosto de 2015.

Até mesmo muito provavelmente até quando em confronto ou em colisão de direitos. Afinal valerá tanto, e da mesma forma, a inviolabilidade de correspondência em confronto com a inviolabilidade da vida, da integridade física ou da segurança do Estado?

Uma síntese conclusiva

O quadro presente no que respeita à produção de informações e ao alcance da sua importância na segurança interna e externa do Estado e no suporte estratégico que lhe está subjacente atravessou, com algumas adaptações, dois grandes momentos da abordagem mundial da *intelligence* e das virtudes que o seu produto pode representar na construção de uma sociedade global e das relações que daí advém entre Estados. Referimo-nos a um primeiro período condizente com o fim da "guerra fria" e, a um segundo, que decorre do atentado de 11 de setembro de 2001 que alterou conceitos e dimensões de insegurança para os quais o mundo não estava preparado para enfrentar.

Quando Michael Herman refere que "as informações de segurança podem ter alvos domésticos e estrangeiros, mas, numa lógica de alteridade, face a uma ameaça ao Estado, os alvos domésticos devem ser encarados como alvos estrangeiros. Informação não é autoconhecimento. É sobre 'eles' e não 'nós'" [39] está precisamente a valorar a importância que o *principiis obsta*, o impedir no início, representa para as sociedades contemporâneas onde preside o primado do Estado de direito e o irrenunciável respeito pelas mais diversas liberdades individuais, onde a perspetiva de segurança interna e segurança externa se tende a confundir obrigando a respostas integradoras e intensas que não só promoverão uma articulação e partilha de conhecimentos com outros Estados, como tenderão a confundir-se as atribuições que hoje caracterizam o SIS e o SIED.

Assim, obriga-se a que, com a distância que o tempo já nos concedeu e com a memória dos condicionalismos históricos passados, as ameaças da sociedade de risco global devam ser encaradas numa perspetiva integrada e multidisciplinar que envolva o Estado e a sociedade civil, esta última

---

[39] Herman, Michael. *Intelligence power in peace and war,* 3rd. ed., Cambridge: Cambridge University Press, 1999, p. 34.

importantíssima na fiscalização da ação pública, assim como com uma cooperação internacional integrada que responda eficazmente às manifestações de insegurança contemporâneas que põem em causa o Estado de direito, a legalidade democrática e as nossas liberdades individuais.

Atente-se às palavras de Maria Lúcia Amaral, "uma Constituição não é nunca, apenas, um instrumento de limitação do poder. É também ao mesmo tempo unidade política, construída pelo texto e reconstruída quotidianamente por quem o interpreta. Em sociedades e mundividências plurais, a unidade política constrói-se e reconstrói-se através da interpretação e concretização das normas relativas a direitos fundamentais; mas essa actividade de integração quotidiana saldar-se-á em nada se o sistema se não dotar de espaço de respiração"[40].

Significa, portanto, que há um caminho árduo, mas necessário, a percorrer para um encontro de harmonização plena entre o nosso texto fundamental e a necessária resposta à constante mudança do espaço internacional e comunitário[41], com o confronto a um conjunto de neo-ameaças que extravasam as nossas fronteiras nacionais. Elas incluem o terror totalitário-jihadista contra o Ocidente, as conquistas do Islamic State of Iraq and Syria/Estado Islâmico da Síria e do Levante/Estado Islâmico pelo terror no Oriente Médio e África ou os ciberataques em infraestruturas críticas. E outras, não menos relevantes preocupações que incluem a instabilidade causada pelos conflitos regionais e os chamados "Estados fracassados", uma intensíssima crise migratória de refugiados no Mediterrâneo, os perigos decorrentes do crime organizado (armas, drogas e tráfico de seres humanos) bem como as suas ligações com o terrorismo internacional. Estes perigos não ameaçam apenas um único país na União Europeia ou na Europa, mas todos os que a constituem.

A compreensão da segurança implica uma tripla conceção inseparável. A de direito fundamental individual, a de garantia para o exercício de

---

[40] Amaral, Maria Lúcia. "Justiça constitucional, protecção dos direitos fundamentais e segurança jurídica ou que modelo de justiça constitucional melhor protege os direitos fundamentais?", in *Anuário Português de Direito Constitucional*, v. II/2002. 1ª ed. Coimbra: Coimbra Editora, 2004, p. 22.

[41] Veja-se, por exemplo, o aprofundamento da Política Comum de Segurança e Defesa da UE (PCSD) emanada da recente implementação da "EU Global Strategy" com a criação do Fundo Europeu de Defesa (FED) e a Cooperação Estruturada Permanente (PESCO).

outros direitos e liberdades individuais e, não menos importante, o de dever primacial do Estado. Porém nada disto se consubstancia, e se determina, na nossa esfera individual e coletiva sem forças e serviços de segurança que desempenhem um papel crucial na prevenção de um quadro dinâmico e alargado de ameaças, capazes, e não menos importante, capacitados a superar certos constrangimentos graves face a essas neoameaças nacionais e internacionais que exigem um evidente reforço da sua capacitação operacional que só assim poderá responder eficaz e eficientemente perante as crescentes exigências de segurança e a defesa dos interesses nacionais, assim como à prossecução da sua missão numa inquestionável dimensão ética profundamente respeitadora dos mais diversos direitos, liberdade e garantias dos cidadãos.

O Estado está em permanente mutação e dele se requer que responda àquilo que a sociedade, cumpre. Não quer isto dizer que a mudança reside na sua conceção e organização jurídico-formal, mas sim na forma como deve encarar o cumprimento da mais antiga das suas liberdades constitucionais: a segurança. Conforme Jorge Bacelar Gouveia: "A chegada do século XXI e de um novo milénio fez acentuar um conjunto de problemas (...) a globalização derrubaria fronteiras em todos os domínios, não se excluindo a circulação de pessoas e a migração, para além do facto directa ser feita à escala global, não já dentro de espaços economicamente protegidos"[42].

Por conseguinte, os constantes desafios que se vão colocando aos Estados põem em causa a sua natureza e utilidade. Questionam-nas quanto à forma como foram desenhados, num contexto muito próprio decorrente da II Guerra Mundial, e quanto às prestações que produzem, e deverão produzir, considerando os fortíssimos fatores de mudança decorrentes do contexto da globalização e do multiculturalismo que lhe é inerente.

Todas estas mudanças são inquestionáveis e colocaram em crise a eficácia do Estado social, havendo já quem afirme que nos encontramos num Estado pós-Social considerando a complexidade e multiplicidade de fenómenos e preocupações emergentes, quer sejam elas no plano ambiental, tecnológico ou humano a verdade é que aludem a uma nova configuração dos poderes públicos, da forma como eles se relacionam entre si, com os cidadãos e com ou seus homólogos estrangeiros.

---

[42] Bacelar Gouveia, Jorge. *Manual de Direito Constitucional*, v. I, 2ª ed., Coimbra: Almedina, 2007, p. 224-225.

A globalização traz aos Estados o desafio de proteção de novos direitos fundamentais, de novas liberdades a que a segurança, como seu braço armado, não pode deixar de acompanhar. A sociedade complexificou-se, "é complexa pelo aspeto que nos oferece (heterogeneidade, dissensão, caos, desordem, diferença, ambivalência, fragmentação), pela sensação que produz (intransparência, incerteza, insegurança) e pelo que se pode ou não fazer com ela (ingovernabilidade, inacessibilidade)"[43].

Isso remonta-nos às dimensões objetivas e subjetivas de segurança e à sua interligação na perceção das vulnerabilidades de segurança e as capacidades de resposta existentes cuja vivificação do mundo e da globalidade influi nos Estados e, por maioria de razão, nas forças e os serviços de segurança.

[43] *Vide* Valente Dias, Hélder. "Metamorfoses da Polícia: (...)", *ob. cit.*, p. 107.

Índice Geral

O Anuário do Direito da Proteção de Dados Pessoais é uma revista jurídica de livre acesso, disponível em linha no sítio http://protecaodedadosue.cedis.fd.unl.pt/, que pretende divulgar estudos doutrinários sobre o direito à proteção de dados pessoais. O Anuário é editado pelo Observatório para a Proteção de Dados Pessoais, grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da Faculdade de Direito da Universidade Nova de Lisboa. Aberto a qualquer interessado, o Observatório integra atualmente oito investigadores (dois doutorados) oriundos de faculdades de direito (professores e doutorandos), de empresas e do setor público.

Os nove artigos publicados na edição de 2019 do Anuário resultam de uma chamada lançada em setembro de 2018 no sítio da internet do Observatório para a Proteção de Dados Pessoais. Os textos foram depois selecionados e revistos pelos coordenadores do Anuário.

Jurisnova
Associação da Faculdade de Direito da Universidade Nova de Lisboa

SRS ADVOGADOS

FUTURA