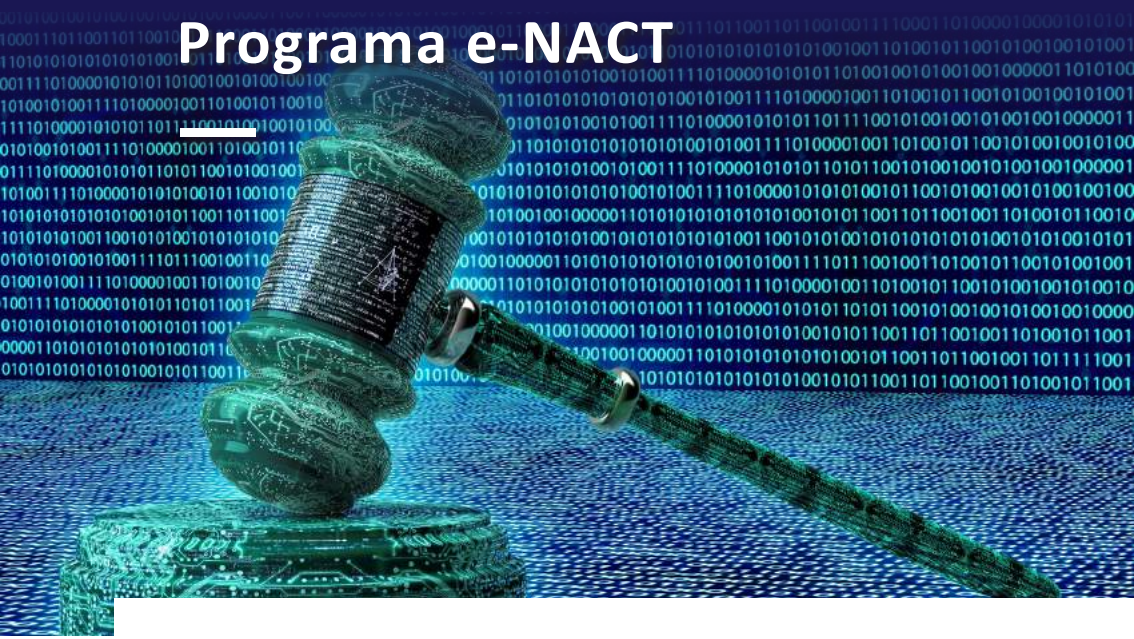
Programa e-NACT



PROTEÇÃO DE DADOS, DIÁLOGO ENTRE TRIBUNAIS E IMPLEMENTAÇÃO DO DIREITO DA UE

Handbook – Guia prático

Financiado pela Comissão Europeia

Programa e-NACT

PROTEÇÃO DE DADOS, DIÁLOGO ENTRE TRIBUNAIS E IMPLEMENTAÇÃO DO DIREITO DA UE

Handbook – Guia prático

e-LEARNING ACTIVE CHARTER TRAINING (e-NACT) 2017-2019

e-NACT (2017-2019) é um programa co-financiado pela Comissão Europeia que tem como principal objetivo a formação de advogados, magistrados do ministério público e juízes da União Europeia sobre a aplicação de ferramentas de diálogo entre tribunais e divulgação de boas práticas na aplicação da Carta dos Direitos Fundamentais da União Europeia.

Os produtos do programa e-NACT incluíram a realização de três workshops para advogados, magistrados do ministério público e juízes, um Handbook- Coletânea de jurisprudência e guia prático por tema, o desenvolvimento da base de dados de jurisprudência nacional ACTIONES e cursos online. Para informação atualizada sobre o projeto podem consultar a página do e-NACT no website do CIDP.

Diretor Nacional do Projeto e-NACT:
Dr. Tiago Fidalgo de Freitas

Coordenadora Nacional do Projecto :
Dr.ª Rita Gião Hanek

Membros do Grupo de Trabalho: Afonso Brás e Sara Azevedo (proteção de dados), Beatriz Esperança (asilo e migração), Marta Carmo e Gonçalo Fabião (liberdade de expressão)

Coordenação do Grupo de Trabalho: Rita Gião Hanek

Tradução e adaptação dos Handbooks - Coletâneas de jurisprudência e guias práticos do programa e-NACT: Rita Gião Hanek

Edição: Rui Bastos Gonçalves

Parceiros:

This handbook was funded by the European Union's Justice Programme (2014-2020). The content of this report represents only the views of the e-NACT consortium and is its sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains

Contribuíram para o conteúdo do Handbook – Coletânea de jurisprudência e guia prático na qualidade de oradores do workshop organizado pelo ICJP/CIDP em parceria com o Instituto Universitário Europeu – 4-5 de Abril de 2019, Faculdade de Direito da Universidade de Lisboa.

Por ordem de trabalhos:

Tiago Fidalgo de Freitas, Diretor do programa e-NACT em Portugal/FDUL-CIDP

Rita Gião Hanek, Coordenadora nacional do programa e-NACT

Domingos Farinho, FDUL-CIDP

Alexander Kargopoulos, Agência dos Direitos Fundamentais (FRA) da União Europeia

Karolina Podstawa, Maastricht University

Pedro Delgado Alves, Deputado à Assembleia da República

Claúdia Monge, FDUL-CIDP/BAS advogados

Luís Salvador Pisco, DECO

Margarida Ferreira, APDPO

Tiago Félix da Costa, MLGTS

Magda Cocco, VdA

Graça Canto Moniz, CEDIS

João Marques, CNPD

Luís Neto Galvão, SRS Advogados

Mário Duarte, Link Consulting

Francisco Paes Marques, FDUL-CIDP

Tabela de conteúdos

Introdução

Sobre os Handbooks - Coletâneas de jurisprudência e guias práticos do programa e-NACT

Os materiais e conteúdos do programa e-NACT – nomeadamente o presente Handbook - Coletânea de jurisprudência e guia prático sobre liberdade de expressão - são traduzidos e adaptados; a versão original encontra-se disponível no website do Instituto Universitário Europeu produzido sob a coordenação da Professora Federica Casarosa no âmbito do programa e-NACT pelo Centro de Cooperação Judiciaria do Instituto Universitário Europeu. Contudo, atendendo à extensão das especificidades nacionais, os Handbooks transnacionais e nacionais podem ser consultados a título complementar.

Os handbooks foram desenvolvidos com o apoio dos grupos de trabalho constituídos por peritos selecionados por cada um dos parceiros do programa.

Este handbook divide-se em quatro secções: Introdução; I. Ferramentas de diálogo entre tribunais; II. Enquadramento jurídico e coletânea de jurisprudência; III. Casos práticos e guia para discussão.

A amostra de jurisprudência nacional selecionada (v. seção III) visa problematizar as seguintes questões:

- Os tribunais nacionais citam a Carta dos Direitos Fundamentais da União Europeia ("Carta")? Se sim, com que objetivo? Ad abundatiam, como auxiliar interpretativo ou mesmo como elemento "catalisador"?
- Que tipo de desafios se colocam à implementação do Direito da União da União Europeia no âmbito dos direitos fundamentais a nível nacional? Na jurisprudência nacional encontram-se os mesmos dilemas que tem sido objeto da jurisprudência do TJEU e do TEDH?
- Que expressões de diálogo entre tribunais encontramos em Portugal? Vertical ou horizontal? Decorre da interpretação conforme ou questão prejudicial? Visam ultrapassar os desafios provocados pelas assimetrias existentes a nível nacional promovendo uma maior coerência e cooperação ou são um exercício de quasi litigação estratégica?
- Entre a jurisprudência selecionada encontramos acórdãos-boas práticas que ultrapassam ou minimizam risco de conflito?

A versão portuguesa dos Hanbooks - Coletâneas de jurisprudência e guias práticos tem por isso como principal objetivo dar a conhecer uma amostra de jurisprudência nacional demonstrativa do tipo de desafios que se colocam à implementação do Direito da União da União Europeia no âmbito dos direitos fundamentais a nível nacional, ao recurso à Carta dos Direitos Fundamentais da União Europeia ("Carta") para lidar com estes mesmos desafios e à divulgação de boas práticas de diálogo entre tribunais.

Para este efeito, a adaptação e tradução dos Hanbooks - Coletâneas de jurisprudência e guias práticos foi informada tanto pela jurisprudência recolhida como pela troca de ideias que teve lugar durante os respetivos workshops temáticos do programa e-NACT. Observa-se por exemplo que as necessidades formativas e a jurisprudência existente nem sempre se conformam aos objetivos estritos do programa. Enquanto nas áreas de liberdade de expressão e asilo e migração se encontram mais exemplos de como o diálogo entre tribunais e o recurso à Carta dos Direitos Fundamentais tem contribuído para a implementação dos direitos fundamentais a nível nacional; na área da proteção de dados as necessidades dos formandos prendem-se atualmente com a familiarização com novos conceitos subjacentes ao RGPD. A adaptação – ainda que respeitando o quadro do programa e-NACT - revela esta ponderação.

Os Hanbooks - Coletâneas de jurisprudência e guias práticos foram desenvolvidos com vista a serem usados como ferramenta de autoaprendizagem. São um convite a explorar a base de dados ACTIONES onde se encontram disponíveis dezenas de acórdãos nacionais de vários Estados Membros da União Europeia sobre os temas proteção de dados, liberdade de expressão e asilo e migração. Adicionalmente incluem casos práticos acompanhados de linhas orientadoras para discussão.

Voltar à Tabela de Conteúdos

Sobre o diálogo entre tribunais (Judicial Interaction Techniques) e divulgação de boas práticas

> "As relações de mútua influência entre o TEDH e os tribunais nacionais tecem-se dentro de um modelo que não reveste natureza processual, seja hierárquica ou normativa. (...) A relação que exista poderá eventualmente ser enquadrada numa categoria de diálogo judicial "semivertical", no sentido em que os tribunais de qualquer dos Estados membros estão também diretamente compreendidos no respeito pelos direitos fundamentais tal como são garantidos pela CEDH, ou seja, com o desenvolvimento e como são interpretados e aplicados pelo TEDH."
>
> Conselheiro Henrique Gaspar

Cfr. A influência da CEDH no diálogo jurisdicional. A perspetiva nacional ou o outro lado do espelho, Intervenção no Colóquio por ocasião da comemoração do 30.º aniversário da vigência da CEDH em Portugal. STJ, 10.11.2008, pp. 7 e 8 e 9. citado no Acórdão do Tribunal da Relação de Évora, Processo n.º 80-16.7GGBJA.E1, de 23.01.2018.

A noção de "diálogo" tem sido amplamente usada pela doutrina para transmitir diferentes significados: um veículo para o "transplante" de ideias entre tribunais; uma forma casual de descrever o estilo de comunicação entre os poderes judicial e político ou, ainda, para descrever um novo paradigma de relações entre tribunais e entre diferentes sujeitos.

O projeto e-NACT entendeu adotar uma abordagem mais neutra, baseada na "interação entre tribunais", i.e., na documentação de episódios de contacto (intencionais ou não) entre tribunais. Estes episódios diferem em intensidade, resultado e tipologia. Em termos gerais, a interação entre tribunais pode ser entendida como um conjunto de técnicas usadas

pelos tribunais e juízes dos Estados membros da União Europeia, com o objetivo de promover a coerência e coordenação (ou, pelo menos, minimizar o risco de conflito) entre diferentes sistemas judiciais e quadros legislativos e de salvaguardar a tradição constitucional europeia e certos bens jurídicos – como os direitos fundamentais – que estão protegidos pelos vários níveis de governo (nacional, internacional e supra nacional). Desta forma, o "diálogo" é um subtipo da "interação entre tribunais", que pode ser vertical ou horizontal, decorrer de interpretação conforme ou questão prejudicial e que visa ultrapassar os desafios provocados pelas assimetrias existentes a nível nacional e os méritos das soluções legislativas adotadas na implementação do direito da UE.

Neste contexto, o programa e-NACT é, por isso, um convite ao diálogo entre tribunais através da divulgação de casos de estudo, sem nunca esquecer a legislação da UE e a Carta dos Direitos Fundamentais.

Ferramentas de diálogo entre tribunais que o programa e-NACT oferece

A escolha de recorrer a técnicas judiciais de interação/diálogo é frequentemente determinada pela existência de um conflito entre o quadro legislativo nacional e as obrigações internacionais. Por exemplo, se o juiz não duvida do significado da norma de direito da união europeia aplicável ao caso concreto, pode considerar se a norma nacional é, ou não, claramente compatível, ou se, sendo, há espaço de manobra para interpretação conforme. Assim, sugere-se que interpretação conforme seja sempre o passo número 1. Se se concluir que a interpretação conforme não providencia uma resposta conclusiva, inequívoca, e indiscutível podem ser consideradas duas outras opções: requerer o apoio do TJUE – passo número 2 – , iniciando o meio contencioso das questões prejudiciais.

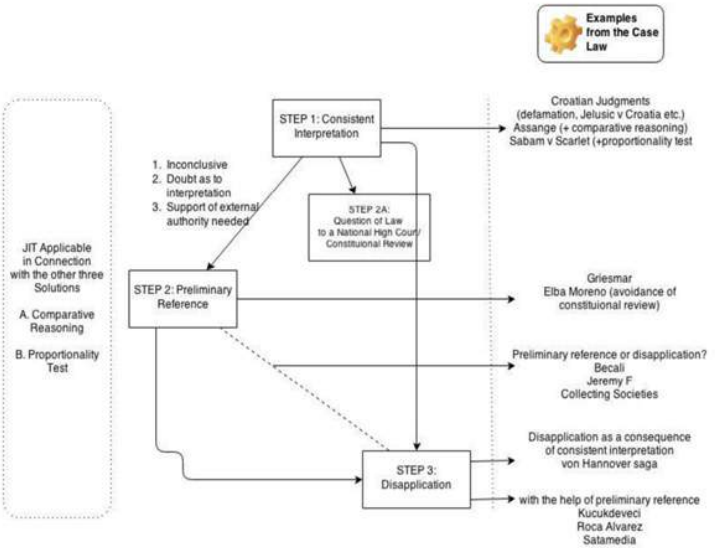
Contudo, se for claro que a norma nacional não é compatível com o Direito da União Europeia, ou se não tem um enquadramento jurídico-constitucional compatível com o TEDH, é necessário desaplicar a norma – passo número 3 – por iniciativa própria, no quadro de jurisprudência existente, nacional ou internacional, ou no seguimento da decisão relativa a uma questão prejudicial.

Voltar à Tabela de Conteúdos

Estes três passos são acompanhados de duas técnicas horizontais: a comparative reasoning e o teste de proporcionalidade, que permitem, explicitamente, recorrer a argumentos de jurisprudência de outros Estados membros da UE.

O gráfico abaixo oferece uma visão geral das ferramentas à disposição de juízes nacionais, indicando o momento em que cada uma das técnicas pode ser aplicada e a forma como os conflitos podem ser ultrapassados.

Quadro sobre Judicial Interaction Techniques (JIT)



Voltar à Tabela de Conteúdos

Enquadramento jurídico

As discussões sobre o enquadramento legal relevante nos ***Handbooks - Coletâneas de jurisprudência e guias práticos do programa* e-NACT** são ditadas pela amostra de jurisprudência. Assim sendo, a análise da moldura legal não é exaustiva, mas antes enquadrado pelos casos de estudo selecionados e pelas disposições relevantes da Carta.

Em Portugal, desde que o Regulamento Geral de Proteção de Dados ("RGPD") começou a ser aplicado- a 25 de maio de 2018 – e até haver legislação nacional de execução do RGPD, a Lei n.º 67/98, de 26 de outubro, continua em vigor em tudo o que não o contrarie aquele Regulamento.

No que respeita aos tratamentos de dados efetuados por autoridades competentes para a deteção, prevenção, investigação e repressão de infrações penais, bem como para a execução de sanções penais, a referida Lei n.º 67/98, de 26 de outubro, mantém-se aplicável na sua totalidade – há, assim, uma certa continuidade no enquadramento legal vigente. Os exemplos de jurisprudência selecionados são um reflexo disso mesmo.

Para efeitos da aplicação dos conceitos subjacentes ao programa E--NACT no âmbito da proteção de dados em Portugal e mais precisamente

para utilização do presente *Handbook* devem ter-se ainda em consideração – entre outras- as seguintes fontes de direito:

- Carta dos Direitos Fundamentais da União Europeia
- Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)
- Regulamento (UE) N.º 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados – GDPR
- Regulamento (UE) N.º 611/2013, de 24 de junho de 2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas
- Regulamento (UE) N.º 604/2013, de 26 de junho de 2013, estabelece critérios de determinação do EM responsável por um pedido de proteção internacional (reformulação)
- Regulamento (UE) N.º 603/2013, de 26 de junho de 2013, cria o sistema «Eurodac» (reformulação)

- Regulamento (CE) N.º 767/2008, de 9 de Julho de 2008, Regulamento VIS, relativo ao Sistema de Informação sobre Vistos
- Diretiva 95/46/CE, de 24 de outubro de 1995, Diretiva de Proteção de Dados Pessoais
- Diretiva 2000/31/CE, de 8 de junho de 2000, Diretiva do Comércio Eletrónico
- Diretiva 2002/58/CE, de 12 de julho de 2002, Diretiva das Comunicações Eletrónicas
- Diretiva 2006/24/CE, de 15 de março de 2006, Relativa à conservação de dados das comunicações eletrónicas e que altera a Diretiva 2002/58/CE **Invalidada pelo Tribunal de Justiça da União Europeia** no caso *Digital Rights Ireland* Casos C-293/12 e C-594/12 ECLI: ECLI:EU:C:2014:238.
- Diretiva (UE) 2016/680, de 27 de abril de 2016, 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
- Diretiva (UE) 2016/681, 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

Voltar à Tabela de Conteúdos

Decisões da Comissão Europeia

Cláusulas contratuais-tipo

- Decisão de 5 de fevereiro de 2010 Relativa às clausulas contratuais-tipo aplicáveis às transferências de dados pessoais para subcontratantes estabelecidos em países terceiros
- Decisão de 27 de dezembro de 2004 Relativa à introdução de um conjunto alternativo de cláusulas contratuais tipo aplicáveis à transferência de dados para países terceiros, alterando a Decisão de 15 de junho de 2001 (Decisão 2001/497/CE)
- Decisão de 15 de junho de 2001 Relativa às cláusulas contratuais-tipo aplicáveis às transferências de dados pessoais para países terceiros

Adequação do nível de proteção de dados

- Decisão de 12 de julho de 2016 (Escudo de Proteção da Privacidade- *Privacy Shield*)
    - Anexos à decisão de execução da Comissão

Outras decisões

- Decisão de 12 de dezembro de 2007, Relativa à proteção de dados no Sistema de Informação do Mercado Interno

- **Decisões do Conselho da União Europeia**

- DECISÃO-QUADRO 2008/977/JAI, Relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria pena

- Acquis de Schengen - Convenção de Aplicação do Acordo de Schengen
- Decisão 2009/917/JAI,de 30 de Novembro de 2009, Relativa à utilização da informática no domínio aduaneiro
- Decisão Eurojust de 16 de dezembro de 2008, Relativa à criação da Eurojust afim de reforçar a luta contra as formas graves de criminalidade
- Decisão 2003/659/JAI, Altera a Decisão 2002/187/JAI
- Decisão do Conselho de 8 de junho de 2004, Estabelece o Sistema de Informação sobre Vistos

Conselho da Europa

- Convenção 108 – Convenção para a proteção das pessoas Relativamente ao tratamento automatizado de dados de carácter pessoa

Voltar à Tabela de Conteúdos

Conceitos base do RGPD

Na sua prática profissional já se deparou com algum caso de proteção de dados em que não fosse claro se estamos ou não perante dados pessoais nos termos do RGPD? E desde a entrada em vigor do RGPD deparou-se com algum caso de aplicação de novos conceitos tais como responsável pelo tratamento ou subcontratante ? Sabe quem é o encarregado de proteção de dados?

Embora a jurisprudência nacional e europeia tenha contribuído para a consagração do regime atual não se observa uma amostra significativa de jurisprudência portuguesa que – por ora -, faça referência à Carta ou ao RGPD.

O RGPD constitui uma das maiores alterações de sempre no que respeita ao modo como deve ser realizado o tratamento de dados de uma pessoa singular por qualquer organismo que proceda ao tratamento de dados de pessoas singulares e que esteja sediado na União Europeia, incluindo fornecedores e outros terceiros a que uma empresa recorra para o tratamento desses dados.

O RGPD constitui uma mudança de paradigma a vários níveis; por um lado porque implica uma devolução do controlo dos dados pessoais aos

seus titulares; e por outro, pelo seu amplo âmbito de aplicação subjetivo e objetivo. O RGPD tem um impacto imediato na área dos serviços, saúde e empresas seguradoras, tendo, contudo, ainda uma enorme repercussão e impacto transversal em departamentos de inúmeras empresas em todo o mundo e em áreas tão dispares do direito como a liberdade de expressão, a segurança, criminalidade ou controlo de fronteiras.

Para além disso, um sem número de inovações ligadas às tecnologias, desde a videovigilância às redes sociais fizeram surgir novos espaços jurídicos que não se reconduzem facilmente às tradicionais esferas que se alargam progressivamente à volta do irredutível núcleo íntimo de privacidade do indivíduo, o que coloca aos tribunais novos desafios em traçar os contornos da privacidade.

Finalmente, o RGPD tem um âmbito de aplicação amplo, aplicando-se a todos os Estados-Membros da União Europeia, bem como ao Reino Unido pós-Brexit, dado que o RGPD, contrariamente às regras de proteção de dados pessoais estabelecidas pela Diretiva 95/46/CE, afeta também quaisquer empresas estabelecidas fora da UE que ofereçam bens ou serviços a pessoas singulares na União, ou que supervisionem o seu comportamento. A título de exemplo, as empresas nos Estados Unidos da América que façam o alojamento de *sites* acessíveis a pessoas singulares na UE serão diretamente afetadas.

Verifica-se por isso – ao contrário de noutras áreas temáticas do programa e-NACT - a necessidade de, em primeiro lugar, oferecer a definição de conceitos base subjacentes ao novo regime jurídico. Alguns destes conceitos já foram abordados pelos tribunais nacionais dos estados membros da união europeia. Toda a jurisprudência abaixo referida encontra-se disponível em versão anotada na base de dados ACTIONES do CJC do Instituto Universitário Europeu.

i. Quem é quem? Alguns conceitos e definições.

- *Dados pessoais: é* qualquer informação identificativa de uma pessoa singular ou a ela respeitante nas mais diversas formas (incluindo aparência física e dados biométricos). Sobre o conflito de normas e interesses jurídicos protegidos (o direito do empregador de monitorar o desempenho profissional e o direito à privacidade); assim como a determinação sobre o que são dados pessoais (correspondência) observe-se por exemplo o acórdão do Tribunal de Pádua, n.º 709/2018, de 24 de Dezembro de 2018.

- *Responsável pelo tratamento ou data controller: é* o responsável pela determinação do fim e dos meios para o tratamento de dados vs. *subcontratante* ou *data processor*: que é quem que trata dos dados em nome do responsável pelo tratamento. Sobre direitos de propriedade industrial e uso de dados pessoais tanto pelo responsável pelo tratamento e pelo subcontratante veja-se por exemplo a anotação ao acórdão do Înalta Curte de Casație și Justiție da Roménia, no. 1059, 16 de Junho de 2017 disponível na base de dados ACTIONES do CJC. Neste caso o tribunal apoiou-se fortemente em decisões do TJUE nomeadamente o caso C-461/10, *Bonnier Auto*, paras 59-60 para decidir sobre o teste de proporcionalidade e nos casos C- 239/08, *Google France SARL* e case C-324/2009, *L'Oreal v. Ebay* na análise dos atos praticados pelo responsável pelo tratamento e o subcontratante.

- *Encarregado de proteção de dados*: nos termos do RGPD, as empresas e quaisquer terceiros responsáveis pelo tratamento de dados pessoais em nome dessas empresas têm de designar um Encarregado da Proteção de Dados ("EPD") se: (i) forem um organismo público; (ii) as atividades principais da empresa ou do terceiro exigirem um controlo de pessoas em grande escala; ou se as atividades principais consistirem em operações de

tratamento em grande escala de categorias especiais de dados pessoais, como dados relacionados com condenações penais e infrações. O EPD tem de ter conhecimentos especializados no domínio do direito da proteção de dados, embora não tenha necessariamente de ser um funcionário, podendo, em vez disso, ser contratado para prestar esse serviço. Os dados do EPD têm de ser comunicados à autoridade de controlo, como a Comissão Nacional de Proteção de Dados (CNPD) em Portugal.

ii. Quem tem de mudar as suas práticas e aplicação territorial.

O regime de aplicação territorial agora consagrado no RGPD resulta de uma evolução cuja principal força motriz é responsabilidade do TJUE:

- *Bodil Lindqvist*, Caso C-101/01 (2003): em que o tribunal considerou que a diretiva não era aplicável à internet como um todo;

- *Digital Rights Ireland*, casos conjuntos C-293/12 e C-594/12 (2014): o caso não era *per se* sobre aplicação territorial, mas o paragráfo 68 indica que a Carta é aplicável mesmo quando os dados são armazenados fora da União Europeia;

- *Google Spain*, Caso 131-12 (2014): determinou que o direito da União Europeia é aplicável quando um estabelecimento na União Europeia está "inextricavelmente ligado" a um estabelecimento fora da União Europeia;

- *Weltimmo,* Caso C-230/14 (2015): sobre jurisdição das autoridades de controlo nacionais;

- *Schrems*, Caso C-362/14 (2015): que afirmou que as transferências de dados devem respeitar os limites da Carta e os direitos fundamentais, Em particular, o tribunal invalidou o *EU-US Safe Harbor scheme* porque não oferecia garantias adequadas ao regime de proteção de dados europeu permitindo o acesso a dados pelas autoridades americanas

- *EU-Canada PNR*, Opinião 1/15 (2017): Avaliou a aplicação das normas da união europeia no Canadá;

- *Google v. CNIL*, Caso C-507/17, Opinião de AG Szpunar (10 Janeiro de 2019): sobre o direito a ser esquecido e ao dever dos motores de busca não associarem resultados a determinadas pesquisas.

Sumariamente, o RGPD pode aplicar-se aos *responsáveis pelo tratamento* e aos *subcontratantes*- empresas, mas também qualquer pessoa singular, organização, autoridade pública, agência ou outro organismo que estejam:

1. Estabelecidos na UE, mesmo que o tratamento de dados tenha lugar fora da União;

2. Estabelecidos fora da UE, mas cujo tratamento de dados se refira a titulares dos dados que se encontrem na eu – esta situação aplica-se oferta de bens ou à oferta de serviços, ainda que estes sejam gratuitos. Fatores determinantes para o respetivo apuramento:

Voltar à Tabela de Conteúdos

- Uso da língua ou moeda de um ou mais Estados membros da UE com a possibilidade de encomendar bens nessa língua;
- Menção explícita a clientes ou utilizadores que se encontrem na UE;
- Intenção de oferecer serviços a titulares de dados pessoais num ou mais Estados membros.

Por outro lado, o mero facto de estar disponível, num sítio *web* da UE, um endereço eletrónico ou outro tipo de contactos do responsável pelo tratamento ou subcontratante, ou, ainda, de um intermediário, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido (e não de um país da UE), não é suficiente para determinar a intenção acima referida.

iii. Consentimento

O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro, que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito. O consentimento não pode ser condição de acesso ao serviço, a não ser que seja inerente à respetiva provisão. O silêncio, as opções pré-validadas ou mesmo a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Por sua vez, sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento a essa operação de tratamen-

to dos dados. Retirar o consentimento que foi prestado deve ser uma operação simples.

Antes de recolher os dados é necessário informar o respetivo *titular* sobre a identidade do *responsável pelo tratamento*, os seus contactos e de como irá utilizar os dados do titular – nomeadamente, se serão partilhados com outros ou se se planeia transferi-los para um país terceiro. Adicionalmente, é ainda necessário informar o titular do tempo que irá durar o respetivo tratamento de dados, os seus direitos de a eles aceder, o direito a ser esquecido ou a terminar o tratamento desses dados, e, ainda, como podem retirar o consentimento ou apresentar uma queixa.

Por fim, torna-se também necessário explicitar se vão ser utilizadas técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

iv. O direito ao apagamento de dados ou o direito a ser esquecido

Se os dados já não são necessários, se foram usados ilegalmente ou, ainda, se o titular exerceu o seu direito de se opor, então esses dados devem ser apagados. Deverá caber ao *responsável pelo tratamento* provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados. O acórdão do Supremo Tribunal Espanhol, ROJ 2836/2016, de 20 de Junho de 2016, disponível na base de dados ACTIONES do CJC esclarece sobre quais devem ser os passos a ser seguidos pelo titular dos dados pessoais para que estes possam ser apagados e quais os critérios; o acórdão do Tribunal Constitucional Espanhol, processo n.º 58/2018, de 4 de Junho

de 2018 refere-se ao direito a ser esquecido como um direito constitucional, apoiando-se explicitamente nos artigos 7.º e 8.º da Carta para esse efeito. Este último recorre ainda à interpretação conforme e cita tanto a jurisprudência do TJUE (caso *Google Spain*) e do TEDH (*Times Newspaper Ltd v United Kingdom*). Adicionalmente o acórdão do Tribunal Constitucional da Roménia processo n.º 424 D/2014 e 478/D/2014, 8 Julho 2014 sobre o teste de proporcionalidade e interferência das autoridades públicas na esfera da vida privada.

v. Direito a opôr-se

Sempre que os dados pessoais forem objeto de tratamento para efeitos de comercialização direta, o titular deverá ter o direito de se opor, em qualquer momento e gratuitamente, a tal tratamento, incluindo a definição de perfis, na medida em que esteja relacionada com a referida comercialização e quer se trate do tratamento inicial quer do tratamento posterior.

vi. Direito a retificação

O titular tem o direito de obter do responsável do tratamento, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo através uma declaração adicional.

vii. Direito de portabilidade dos dados

O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura auto-

mática, e o direito de transmitir esses dados a outro responsável pelo tratamento, sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir dentro de determinados limites. As pessoas singulares têm agora o direito à circulação, cópia ou transferência dos seus dados pessoais de um local para outro ou até mesmo para uma empresa concorrente. Por exemplo, o utilizador de um serviço de música que criou uma lista de reprodução pode levar esta lista consigo, caso decida mudar de fornecedor de serviço. A exigência de tornar os dados verdadeiramente portáteis e fáceis de utilizar por outros irá, muito provavelmente, implicar ajustamentos significativos ao nível das transferências internacionais e, portanto, ao nível dos custos. Sobre o acesso aos dados veja-se a anotação ao acórdão do Tribunal Central Administrativo do Sul, processo n.º 2937/16.6BELSB na base de dados ACTIONES do CJC.

viii. Transferências internacionais

O RGPD confirma a proibição de enviar dados pessoais para um país fora do Espaço Económico Europeu que não garanta proteção *adequada.* Onde não haja decisão de adequação, as transferências apenas podem ser feitas em casos limitados, como quando haja consentimento, sejam utilizadas cláusulas contratuais-tipo publicadas pela Comissão Europeia, ou, no caso de transferências entre empresas, a utilização de Regras Vinculativas Aplicáveis às Empresas. Sobre o impacto que o RGPD pode ter na área da saúde, veja-se, a título de exemplo, a decisão do *European Data Protection Supervisor* sobre a transferência de dados entre o *European Centre for Disease Prevention and Control (ECDC)* para a Organização Mundial de Saúde, de 17 de Janeiro de 2018. Sobre transferências internacionais consulte-se o caso *Schrems*, C-362/14 (2015).

Amostra de jurisprudência nacional

Há uma série de decisões que – embora não citando a Carta explicitamente- merecem destaque por integrarem vários *tipos de interação* em simultâneo, conduzindo a uma verdadeira troca de impressões entre autoridades judiciárias, administrativas e outros sujeitos como associações de consumidores, jornais e polícia de investigação. Estas decisões coincidem tendencialmente com áreas que tem vindo a ser identificadas como aquelas em que a aplicação da moldura legal levanta maiores desafios ao respeito pelos direitos fundamentais pelo seu carácter interdisciplinar. A proteção de dados é um regime transversal que tendencialmente se aplica a todas as áreas do direito. Nas seções seguintes destacamos três casos que visam exemplificar a panóplia de situações – não necessariamente ligadas a serviços- em que o RGDP pode ser posto em causa.

i. Bases de dados, dados biométricos e criminalidade

O acórdão do Tribunal Constitucional n.º 333/2018, processo n.º 195/18, de 27 de junho, sobre a base de dados de perfis de ADN (LBDADN) decidiu *não julgar inconstitucional a norma que determina que a recolha de amostras em condenado por crime doloso com pena concreta*

de prisão igual ou superior a 3 anos, ainda que esta tenha sido substituída, com finalidades de investigação criminal e inserção na base de dados respetiva, é ordenada, mediante despacho do juiz de julgamento, após trânsito em julgado, quando a mesma não foi já realizada, interpretativamente retirada pela decisão do artigo 8.º, n.º 2, da Lei n.º 5/2008, de 12 de fevereiro, na redação dada pela Lei n.º 40/2013, de 25 de junho.

O recorrente tinha alegado que "*No caso concreto dos autos a recolha de ADN ainda se considera mais gravosa, porquanto a recolha das amostras de ADN se destina a construir uma base de dados para fins de investigação criminal e não a instruir um concreto processo, termos em que estamos aqui perante uma gravíssima violação da dignidade humana do arguido, uma vez que as razões que determinam a recolha do ADN são difusas e não fundamentadas, meramente para construir uma base de dados e não por qualquer outra razão atendível, pelo que mais uma vez se reitera estarmos perante uma verdadeira e própria violação da dignidade da pessoa humana, violação essa que ofende o conteúdo mínimo do direito e não se limita ao necessário para acautelar outros direitos*."

O tribunal de primeira instância tinha considerado que "*Como se escreveu no recente acórdão do TRL de 05/05/2015 (tirado no processo n.º 241/11.5JELSB.L1-5 e disponível para consulta em www.dgsi.pt) que subscrevemos e aqui seguimos de perto, da leitura dos n.ºs 1 e 2 do art. 8.º da Lei n.º 5/2008, de 12.2, resulta que a recolha de ADN é automática, não dependendo de qualquer pressuposto, que a Lei não impõe (com exceção da condenação por crime doloso com pena concreta de prisão igual ou superior a 3 anos, ainda que esta tenha sido substituída) e sendo certo que pode ser ordenada logo após a constituição de arguido. A automaticidade da recolha resulta ainda da previsão do n.º 6 daquele artigo 8.º, que prevê a possibilidade de ser dispensada a recolha da amostra,*

mediante despacho judicial, sempre que não tenham decorrido cinco anos desde a primeira recolha e, em qualquer caso, quando a recolha se mostre desnecessária ou inviável. Ora, salvo o devido respeito por opinião contrária, a possibilidade de dispensa é que terá que ser determinada por despacho fundamentado, não a recolha. A intenção do legislador terá sido a de determinar a recolha de ADN como determina a recolha de impressões digitais e, de facto, não se vê como aquela recolha pode restringir direitos fundamentais do arguido entendendo-se, outrossim, que essa determinação não viola qualquer preceito constitucional"

Este acórdão é um exemplo de diálogo vertical e horizontal via interpretação conforme.

Por um lado, oferece um enquadramento jurisprudencial e normativo, citando, inclusivamente, jurisprudência do Tribunal Europeu dos Direitos do Homem, incluindo os seguintes casos: *Van der Velden v. The Netherlands* (caso n.º 29514/05), de 7 Dezembro de 2006; *S. and Marper v. The United Kingdom* (caso n.º 30562/04 e 30566/04), de 4 Dezembro de 2008; *Rotaru v. Romania* (caso n.º 28341/95), de 4 Maio de 2000, *Peruzzo and Martens v. Germany* (caso n.º 7841/08 e 57900/12), 4 junho de 2013; e *Aycaguer v. France* (caso n.º 8806/12), 22 Junho de 2017.

Por sua vez, no que diz respeito à jurisprudência nacional sobre a constitucionalidade de normas que previam a colheita coativa de vestígios biológicos de um arguido para determinação do seu perfil genético, cita designadamente, os Acórdãos n.ºs 155/2007, da 3.ª Secção, e 228/2007, da 2.ª Secção que decidiram no mesmo sentido.

E refere-se, ainda, ao Regulamento Geral de Proteção de Dados (RGPD), adotando uma abordagem de continuidade para esclarecer que «*[a]ntes da recolha da amostra, é assegurado o direito de informação,*

*previsto no n.º 1 do artigo 10.º da Lei da Prote***ção** *de Dados Pessoais, aprovada pela Lei n.º 67/98, de 26 de Outubro, hoje em dia consagrado no artigo 13.º do Regulamento (UE) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (RGPD)*"

Este excerto não dispensa a consulta do texto integral do Acórdão disponível no sítio eletrónico do Tribunal Constitucional.

A versão integral da anotação a este acórdão encontra-se disponível na base de dados de jurisprudência nacional ACTIONES do CJC

ii. Liberdade de expressão, atividade jornalística e proteção de dados

Especificamente sobre os limites da liberdade de expressão no exercício da atividade jornalística e a proteção de dados no âmbito do desenvolvimento da atividade jornalística observe-se o sumário da anota**ção sobre** o Acórdão do Tribunal de *Cassação Terza Sezione Civile*, Ordinanza 26 giugno – 5 novembre 2018 n.º 28084

Em 2009, 27 anos após o incidente, o jornal Unione Sarda republicou um caso de homicídio, mencionando a pessoa condenada pelo nome – neste caso, B., - depois de esta já ter cumprido 12 anos de pena pelo crime cometido. B pediu junto do Tribunal de Cagliari a reparação por danos morais sofridos, assim como pela sua reputação e imagem. A ação foi movida contra o jornal e o jornalista.

O jornal e o jornalista argumentaram que o artigo em questão fazia parte de uma coluna semanal sobre os acontecimentos mais importantes que ocorreram em Cagliari nos últimos 30/40 anos e que a republicação

era de interesse público. Estes argumentos mereceram a concordância do tribunal de Cagliari e do Tribunal de Cassação.

B. recorreu para o Supremo Tribunal com base no direito a ser esquecido. Para além disso, continuou a argumentar que o mérito histórico da republicação de um artigo publicado em 1982 (acompanhado, inclusivamente, de uma foto de B.) é danoso para aquele direito, que tem consagração constitucional.

O direito a ser esquecido foi reconhecido pelo Supremo Tribunal Italiano em 1998, que o descreveu como "o interesse legítimo que cada pessoa tem em não permanecer indeterminadamente exposta a danos causados pela repetida publicação de informação que em tempos foi publicada de forma legítima" (Secção 3, Acórdão n.º 3679, de 09/04/1998). Adotando uma solução de continuidade o Supremo Tribunal decidiu a favor de B tendo considerado que no balanco entre os dois interesses o direito a ser esquecido prevalece especialmente na formulação adotada pelo RGPD.

Mais uma vez, este é um acórdão que aplica o RGPD numa lógica de continuidade explicita e não de rutura; continuidade normativa e continuidade jurisprudencial. O Tribunal recorre à interpretação conforme e diálogo entre tribunais vertical nacional.

Para mais informações sobre o Acórdão do Tribunal de *Cassação Terza Sezione Civile*, Ordinanza 26 giugno – 5 novembre 2018 n.º 28084 consultar base de dados de jurisprudência nacional ACTIONES do CJC.

iii. Redes sociais

Associações de consumidores europeias, incluindo, em Portugal, a DECO Proteste, a Altroconsumo, em Itália, a Test A-chats, na Bélgica e a

OCU, em Espanha, avançaram com uma ação coletiva contra o *Facebook* na sequência do escândalo *Cambridge Analytica*.

A *Cambridge Analytica* é uma empresa especializada em perfis psicológicos. Em 2014, Aleksandr Kogan, investigador da Universidade de Cambridge, propôs um teste de personalidade aos utilizadores do Facebook, através da *app* "Esta é sua vida digital". Para participar no teste, os utilizadores tinham de fazer *login* com os mesmos dados que usavam para entrar no Facebook. Esse teste foi feito por 270 mil pessoas.

Através daquela *app* foram recolhidas as informações destes utilizadores, assim como as dos seus amigos. No total, o investigador teve acesso aos dados de 87 milhões pessoas. , incluindo os relativos à sua localização, lista de amigos, gostos, partilhas, etc.

O investigador partilhou esses dados com a *Cambridge Analytica* que, por sua vez, os utilizou para criar perfis psicológicos e, em particular, para influenciar o comportamento eleitoral dessas pessoas em favor do presidente Donald Trump.

Em 22 de Março de 2018, a DECO Proteste enviou ao *Facebook* um pedido formal de explicações, juntamente com as associações de consumidores acima referidas.

Em 11 de Julho de 2018 o Reino Unido multa o *Facebook*, com o valor máximo estabelecido por lei, por este não respeitar o novo RGPD.

Na mesma data, o ICO, entidade britânica congénere da Comissão Nacional de Proteção de Dados, também multa o Facebook com uma coima de 500 mil libras, por recolha de informações pessoais sem um consentimento suficiente, claro e informado.

O processo judicial começa formalmente em 30 de novembro de 2018. A DECO pede uma indemnização de 200 euros/ano para cada utilizador do Facebook.

Em dezembro de 2018, a organização *Privacy International* publica um estudo relativo a 34 *apps* e revela que 61% delas transferiam dados para o Facebook, independentemente de o utilizador ter conta ou estar ativo na rede social. O Facebook responsabiliza os *developers* que usam a plataforma *Facebook Software Development Kit* – no entanto,essa plataforma estava configurada por defeito para transmitir informação para o *Facebook*.

No final de janeiro de 2019, vem a público a informação de que o Facebook paga até 20 dólares por mês aos utilizadores da *Facebook Research App* - um VPN que transfere dados pessoais e a atividade *online* do smartphone para aquela rede social. O programa é destinado a pessoas entre os 13 e os 35 anos, tendo sidoda *Apple Store* por desrespeitar a política de privacidade do iOS. Porém, continua ativo no sistema operativo Android.

À data em que o *handbook* foi elaborado ainda não existia decisão sobre a ação coletiva. Contudo, este caso é singular – e deve ser observado- na medida em que o diálogo entre associações de consumidores é transfronteiriço e tribunais de diferentes estados membros podem decidir de forma diferente sobre a mesma matéria.

Para mais informações consultar Ações Colectivas no website da DECO Proteste.

Conclusões

A jurisprudência portuguesa recorre pouco a carta dos direitos fundamentais como auxiliar interpretativo recorrendo mais frequentemente a convenção europeia dos direitos do homem.

Ainda assim a jurisprudência nacional acompanha a jurisprudência do TEDH e do TJUE mesmo quando não lhe faz referência explicita, observação que introduz uma nova dimensão ao conceito de diálogo do programa e-NACT que sempre se procura como sendo explicitamente concordante ou discordante.

Independentemente do processo de diálogo, a verdade é que estes tipos de interação conduzem a uma saudável troca de impressões entre autoridades judiciárias: o questionar da doutrina, a atualização de argumentação e práticas executivas ou políticas. Em última análise, contribuem para lidar com dificuldades concretas da aplicação do direito da união europeia a nível nacional naquele que e atualmente um sistema complementar, multinível e multissectorial de proteção de direitos fundamentais.

Voltar à Tabela de Conteúdos

Casos práticos e respetivos guias para discussão (incluindo jurisprudência relevante)

Discussão de casos práticos baseados em jurisprudência portuguesa, jurisprudência nacional de outros EM da UE ou jurisprudência do TEJ ou TEDH.

CASO PRÁTICO 1.

I .

Em 2007, A, diretor de uma empresa, foi acusado de corrupção e as notícias sobre o processo criminal que contra ele corria foram publicadas no «Diário do Dia», um jornal nacional de referência. Na sequência desse processo, A acabou por ser libertado, sendo que nenhum outro artigo relativo aos eventos subsequentes foi publicado naquele jornal.

Em 2017, A descobriu, por acaso, que o arquivo digital do «Diário do Dia» ainda incluía o artigo que sobre ele havia sido publicado, permitindo que qualquer internauta o encontrasse através de uma simples pesquisa

na página *online* do jornal. Adicionalmente, o artigo era ainda o primeiro a aparecer através do motor de busca *Google.pt*, quando a pesquisa era feita pelo primeiro e último nome de A.

Com o objetivo de apagar todas essas referências relativas a esse período da sua vida, e tendo em conta o possível impacto negativo que poderiam ter no seu negócio, A. consultou um advogado.

Nessa sequência, A. apresentou uma providência cautelar perante o Tribunal de Primeira Instância, solicitando a remoção da página do arquivo digital do jornal, argumentando que a informação que lá constava era obsoleta, imprecisa, e, ao mesmo tempo, não podia ser considerada de interesse público, tendo em conta que o processo que havia corrido contra ele tinha terminado com sua absolvição.

Por fim, A. intentou, ainda, uma providência cautelar perante o mesmo tribunal, de modo a bloquear a disponibilidade do *link* nas páginas de resultados do motor de busca.

II.

O Tribunal de Primeira Instância emitiu a providência cautelar em questão, tendo, no entanto, limitado os seus efeitos ao país de origem de A- , Portugal. A *Google* atuou em conformidade com a decisão, embora informando diretamente os webmasters do jornal, bem como o público em geral, da eliminação do artigo através de uma "entrada" online sobre o assunto.

A. apresentou uma queixa contra a Google, argumentando que a entrada que publicou referente à decisão do tribunal anula, na prática, o efeito da providência cautelar.

Caso Prático 1. Guia para discussão

Algumas questões a discutir:

- Identificação do enquadramento legal;
- Direitos fundamentais em causa e respetivo equilíbrio;
- Jurisprudência relevante;
- Argumentos a favor e contra a providência cautelar;
- Em termos de proporcionalidade, que decisão poderia ter sido adotada.

Para a além da legislação vigente (nomeadamente artigos 17.º e 85.º do RGPD), sugere-se a consulta da seguinte jurisprudência:

CJEU Google Spain SL, Google Inc. v Agencia Española de Protección de Datos PRESS RELEASE

TEDH Times Newspapers Ltd v United Kingdom (Nos 1 and 2)

Para 45 "The Court agrees at the outset with the applicant's submissions as to the substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research particularly as they are readily accessible to the public and generally free. The Court therefore considers that, while the primary function of the press in a democracy is to act as a "public watch dog", it has a valuable secondary role in maintaining and making available to the public archives

containing news which has previously been reported. However, the margin of appreciation afforded to the States in striking the balance between the competing rights is likely to be greater where news archives of past events, rather than news reporting of current affairs, are concerned. In particular, the duty of the press to act in accordance with the principles of responsible journalism by ensuring the accuracy of historical, rather than perishable, information published is likely to be more stringent in the absence of any urgency in publishing the material"

TEDH CASE OF EDITORIAL BOARD OF PRAVOYE DELO AND SHTEKEL v. UKRAINE

Para 63. "It is true that the Internet is an information and communication tool particularly distinct from the printed media, in particular as regards the capacity to store and transmit information. The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned."

Disponível na base de dados ACTIONES:

"The *Hamburg Court of Appeal* in a case dated 7 July 2015 addressed the case of an individual seeking an injunctive relief against a publisher of a printed and online newspaper as regards a set of articles reporting

on the investigation proceedings brought against the plaintiff between 2010 and 2011. The claim was dismissed by the Hamburg District court, as deletion or amendment to articles that had initially been lawfully disseminated constituted a serious violation of press freedom. The Court of Appeal then set aside the district court decision and partially allowed the complaint affirming that the breach of the plaintiff personality rights perpetuated by the online availability of the information online and its easy retrievability through search engines was a serious one, and at the same time the public interest in the case was no more existing. Interestingly, the court of appeal affirmed that if according to the Google Spain decision such a right could be claimed against the operators of Internet search engines, then it could be asserted all the more against the authors of the relevant articles.

In Belgium, the Court of Cassation confirmed the decision of the Court of Appeal of Liège which granted the request of an individual to anonymise an article from an online archive on the basis of the right to be forgotten. The decision, dated 29 April 2016, affirmed that the online archive of newspapers can be subject to the application of the right to be forgotten, due to the fact that the online article availability, after several years, may cause disproportionate harm to the applicant vis-à-vis the newspaper's freedom of expression."

CASO PRÁTICO 2.

B. é uma cidadã do Bangladesh que pretende celebrar um contrato de seguro de saúde com a companhia de seguros portuguesa "X". Para este efeito, telefonou para a linha SAÚDE"X"ONLINE.

Ao telefone, a resposta automatizada pediu a B. para, no caso de esta concordar com a gravação da conversa, carregar no 9, , o que B acabou por fazer.. Durante a conversa telefónica com o operador, a companhia de seguros requereu o consentimento de B. para o processamento dos seus dados pessoais e de saúde, com o objetivo de avaliar o pedido que estava a ser feito por B. A título anónimo, foi ainda requerido a B. que identificasse a sua raça e etnia.

O processamento dos dados pela companhia de seguros X incluí o respetivo alojamento numa *cloud* denominada "Y", cuja sede está localizada em Palo Alto, Califórnia, EUA.

No final da fase de escrutínio, foi comunicado a B. que o pedido tinha sido negado com base na sua nacionalidade. Após um pedido de esclarecimento, B foi informada de. que a decisão tinha sido o resultado de um processamento automatizado através de *profiling*.

B. consultou um advogado, com o objetivo de conseguir de X uma reavaliação do seu pedido. Nessa sequência, a reavaliação foi requerida a um funcionário, tendo B ainda solicitado o acesso um conjunto de dados que haviam sido processados.

Contudo, a companhia de seguros X comunicou a B. que esta teria de fazer um novo pedido, na medida em que os dados fornecidos se encontravam- temporariamente "indisponíveis" na *cloud* de Y, não existindo indicação sobre quando voltariam a estar disponíveis.

Como sugerido pelo advogado, B. notificou a CNPD de uma violação de dados pessoais.

Caso Prático 2. Guia para discussão

Algumas questões a discutir:

- Âmbito de aplicação do RGPD (territorial e subjetivo);
- Papel e limites do consentimento no contexto do RGPD;
- Transferências internacionais;
- Conceito de *intervenção humana;*
- Explorar o potencial papel de um OPD no presente caso;
- Explorar o papel da CNPD no presente caso.;
- Avaliar a notificação à CNPD e meios alternativos de tutela.

CASO PRÁTICO 3.

I.

A. chegou a Itália em 2017 com outros refugiados da Síria e foi alojado num campo de refugiados, situado na costa sul daquele país. Pouco tempo depois da sua chegada, o presidente da câmara municipal onde se situava o campo decidiu visitá-lo para verificar as respetivas condições.

Durante a visita, foram tiradas várias fotografias, quer por por um jornalista, quer, também, pelos próprios refugiados, através dos seus telemóveis. De entre os refugiados presentes, A. tirou uma selfie com o presidente da câmara municipal, tendo o jornalista publicado as fotografias dessa visita na versão *online* do jornal para o qual trabalha.

Poucos dias depois da publicação, um político do partido da oposição do presidente da câmara municipal fez um discurso em frente ao campo de refugiados, perante um grupo de simpatizantes do mesmo partido que ali estava presente. Durante o discurso, e para sustentar a mensagem que queria passar, o político mostrou uma cópia do artigo do jornal, com a selfie de A com o presidente da câmara municipal.

O discurso incluiu declarações como: "Estes imigrantes chegam diariamente para roubar, violar e matar! Temos que pôr fim a isto! Nós devemos escorraçá-los para longe do nosso país!"

Face a estas declarações, o Ministério Público iniciou um processo criminal contra o político, por incitação ao ódio.

II.

A foto da selfie foi posteriormente partilhada por internautas, que a editaram de forma a criar um cartaz com o rosto de A, em que se dizia "Procurado" e "Terrorista!" por debaixo do respetivo rosto O cartaz foi então publicado nas redes sociais, motivando comentários de ódio e ameaças contra A.

Posteriormente, A. pediu à rede social para apagar todas as publicações que o visavam, incluindo as imagens e os comentários falsos que haviam sido feitos contra ele. A rede social obedeceu, mas, pouco tempo depois, a imagem volto a aparecer, publicada por internautas anónimos.

A. apresentou uma queixa perante o tribunal local, solicitando uma providência cautelar contra a rede social e obrigando-a excluir definitivamente todo o conteúdo de discurso de ódio que havia sido perpetrado contra A.

Voltar à Tabela de Conteúdos

Caso Prático 2. Guia para discussão

Algumas questões para discutir:

- Identificação da moldura legal aplicável ao caso em apreço;
- Será que as afirmações proferidas por autarcas ou por membros de um partido político estão sujeitas a um controlo mais exigente? Porquê?
- A proximidade do campo de refugiados é um elemento a ter em consideração?
- O discurso pode ser considerado como uma ameaça concreta?
- A que jurisprudência podemos recorrer para apoiar o nosso entendimento?
- É possível impôr uma obrigação de monitorização à rede social?

Para a além da legislação vigente, sugere-se a consulta da seguinte jurisprudência:

TEDH Le Pen v. França, Féret v. Bélgica, Delphi AS v. Estónia, Pihl v. Suécia.

CJEU *Glawischnig-Piesczek v Facebook, C-18/18*, caso pendente, informação disponível na base de dados de jurisprudência nacional ACTIONES do CJC. Em destaque as questões colocadas pelo Supremo Tribunal Austríaco em sede de questão prejudicial:

"O n.º 1 do artigo 15.º da Directiva 2000/31 / CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio

electrónico, no mercado interno (Directiva relativa ao comércio electrónico) impedem o tribunal nacional de fazer uma ordem exigindo que um provedor de hospedagem que não tenha removido prontamente informações ilegais não apenas para remover as informações específicas, mas também outras informações que sejam idênticas na redação?

No que diz respeito à primeira questão, o Artigo 15 (1) exclui tal ordem que exige que o provedor de hospedagem remova essa informação (ou bloqueie o acesso a ela) em todo o mundo ou somente no estado membro relevante?

O Artigo 15 (1) exclui tal ordem que é limitada a remover ou bloquear o acesso à informação ilegal somente do usuário específico que postou o conteúdo e se tal ordem seria aplicável em todo o mundo ou somente no estado membro relevante?

*Se as perguntas anteriores são respondidas em negativo: a mesma resposta se aplica a informa*ções que não são idênticas em termos de palavras, mas semelhantes em significado?

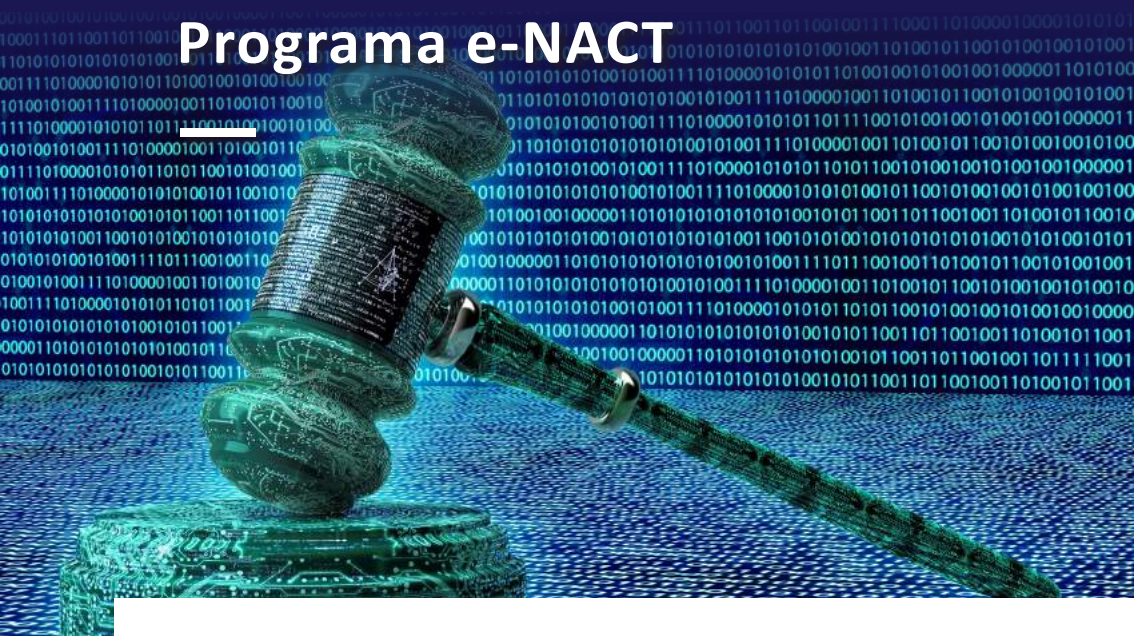
*A mesma resposta se aplica a informações que não são idênticas nas palavras, mas semelhantes em termos de significado, uma vez que o provedor do host tenha conhecimento real das informa*ções?"

Tribunal Alemão Landgericht Würzburg (11 O 2338/16 UVR), 7 de Março 2017 (New York Times)

"*A Syrian refugee whose image showed up in fake news reports linking him to terrorism lost a closely watched case in Germany on Tuesday that sought to prevent Facebook from allowing users to repost the picture. The refugee, Anas Modamani, became a potent symbol of the wave of migrants flooding into Germany, and of the country's immigration poli-*

cy, when he posed for a selfie with Chancellor Angela Merkel in 2015. But the image surfaced in social media posts falsely linking him to terrorist attacks in Brussels and on a Christmas market in Berlin, prompting Mr. *Modamani to seek an injunction against Facebook* in a court in *Würzburg, in the southern German state of Bavaria. In the case on Tuesday, Judge Volkmar Seipel ruled that there were no grounds for an injunction because Facebook had not in any way manipulated the content, which would have made it legally responsible for the distribution. The judge added that a host provider, according to the European Union's electronic commerce laws, could be held responsible for eliminating content from its site only when it was considered technically possible*."

Programa e-NACT



PROTEÇÃO DE DADOS, DIÁLOGO ENTRE TRIBUNAIS E IMPLEMENTAÇÃO DO DIREITO DA UE

Handbook – Guia prático