
CYBERLAW
by CIJIC


**EDIÇÃO N.º V – MARÇO DE 2018**

**REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA**




**CIJIC:** CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

**ISSN 2183-729**

## NOTAS DO EDITOR:

Antes de mais, salientarei uma novidade interna na organização do CIJIC. Desde final de Fevereiro de 2018, depois da assembleia geral, o Centro, passou a estar organizado, sob a Presidência do Professor Doutor Eduardo Vera-Cruz Pinto, coadjuvado por duas Vices, respetivamente, as Professoras Doutoras, Paula Vaz Freire e Raquel Alexandra Brízida Castro, e pelos vogais, Eugénio Alves da Silva e Nuno Teixeira Castro. Mais novidades surgirão em breve.

Feito o ponto de ordem inicial, e abertas as hostilidades, nesta nova edição, sem descurar a proximidade da entrada em vigor, em pleno, 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),* doravante, no acrónimo, RGPD, optamos por trazer a debate algumas tendências de futuro. Obviamente, quase todas com implicações, pungentes, quer ante o instrumento legislativo europeu em foco, quer, e acima de tudo, ante as formas mais tradicionais de relacionamento interpessoal e em sociedade.

Antecipando a tónica, o nosso futuro, já hoje muito intrincado com o digital, dependerá, no seu essencial, da contínua promoção de princípios e valores humanos que, ao longo dos tempos, nos foram acompanhando na evolução enquanto espécie racional. A compreensão, teoricamente mais facilitada até pelo dilúvio informacional

do presente, do conceito, *jus cogens*, de dignidade humana, deveria possibilitar a criação de uma consciência, atrever-nos-íamos a estribar de colectiva, global, do valor individual de cada vida humana em si considerada. Deveria. Porém, pouco disto tem vindo a suceder. As informações e notícias diárias têm vindo a sustentar precisamente um movimento díspar: uma sociedade hedonista mas profundamente egoísta, enamorada por um *surveillance capitalism*[1] reinante, sem espaço para a promoção da fundamentalidade de cada individualidade humana.

O poder inebriante, e sem precedentes na nossa história civilizacional, detido por algumas organizações, denominadas de *tech-giants*, tem rompido as estruturas sociais, políticas, comerciais e, até, tecnológicas. Qual a origem de tão avassalador poder disruptivo destas organizações, destes *tech-giants*?

Em parte, grande, o *graal* destes *tech-giants* deriva de todo o *dilúvio informacional* que percorre a rede. Numa relação de *win-win*, a "*oferta inocente"* de serviços, prosaicamente assimilados como *grátis*, em troca dos nossos dados pessoais, é obnóxia para o indivíduo. Mas profundamente fluída no garante de volumosos acréscimos de capital financeiro, e por conseguinte, de poder, para estas organizações. Bruce SCHNEIER[2], a este propósito, sintetiza de forma lapidar: «*Companies like Facebook and Google offer you free services in exchange for your data. Google's surveillance isn't in the news, but it's startlingly intimate. We never lie to our search engines. Our interests and curiosities, hopes and fears, desires and sexual proclivities, are all collected and saved. Add to that the websites we visit that Google tracks through its advertising network, our Gmail accounts, our movements via Google Maps, and what it can collect from our smartphones. That phone is probably the most intimate surveillance device ever invented. It tracks our location continuously, so it knows where we live, where we work, and where we spend our time. It's the first and last thing we check in a day, so it knows when we wake up and when we go to sleep. We all have one, so it knows who we sleep with. »* Sim, *o smartphone é provavelmente o dispositivo, mais íntimo,* pessoalíssimo mesmo, *de vigilância jamais inventado.* Acompanha-nos permanentemente, 24h/7d, 365d/ano, qual extensão do nosso corpo.

1 https://www.amazon.com/Age-Surveillance-Capitalism-Future-Frontier/dp/1610395697
2 https://www.schneier.com/

E sempre a debitar informação para alguém, transformando-nos no escravo, informacional, do...objecto. Curioso, não?

De facto, disfarçado de *pot-pourri* de intimidade, proximidade e confiança cega, os gigantes tecnológicos têm-nos orientado a um estado de, *quase-completa*, submissão a variadíssimas formas de engenharia social, perfumada por formas competentes e persuasivas de direcção comportamental, categoricamente personalizadas e orientadas para fazermos *algo ao serviço de alguém*; uma verdadeira manipulação individualizada orientada pelo perfil de cada um, de previsão e controlo do nosso comportamento. Fácil de conseguir quando em posse de tão valiosa informação que vamos cedendo, sem limites. Sem conhecimento. Sem oposição. Shoshana ZUBOFF[3], arroja duas questões sufocantes, a cada um de nós, nesta era digital da sociedade informacional: "*Mestre ou escravo*?", "*Casa ou exílio*?". (Conseguiremos responder?)

Os desafios para o futuro da humanidade travam-se. Fugir, ou recear tal, não poderá ser a resposta. Nesta conjuntura crítica, nesta *nova fronteira do poder*, o confronto entre o vasto poder dos gigantes tecnológicos versus os dos governos (enquanto representantes da nossa comunidade colectiva), atira-nos, sem pudor, para um difícil campo de escolhas, civilizacionais diria. O futuro da humanidade tem espaço para a autonomia individual e para os direitos fundamentais? Ou assistiremos impávidos ao desabrochar de novas e sofisticadas formas de desigualdade social? O *el dorado* da era digital possibilitará o fortalecimento dos direitos fundamentais individuais e a sua democratização globalizante? Ou assistiremos impávidos à instrumentalização do indivíduo, segmentado em objecto de informações em meras *strings de bits*, coisificado, servil ao *surveillance capitalism*?

Nesta insolência de questões, e uma vez aqui chegados, foi nossa intenção suscitar a comunidade académica e empresarial a problematizar algumas teorias de resposta. Não assumindo o absolutismo das coisas, o resultado presente é, a nosso ver, profundamente satisfatório. Neste nosso *pot-pourri* que agora publicamos, carreamos *big data*; segurança da informação; regulamento geral de protecção de dados; veículos autónomos e inteligentes; *criptocontratação*; contratos automatizados e contratos

3 http://www.shoshanazuboff.com/

inteligentes; dados pessoais e direitos fundamentais; e, mecanismos de cooperação e coerência no tratamento de dados pessoais.

Agradecidos pelo esforço e pelo trabalho, cumpre-me, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, endereçar um especial reconhecimento a cada um dos autores.

Um sentido e imenso Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

**Boas leituras.**

Lisboa, FDUL, 30 de Março de 2018

Nuno Teixeira Castro


# DOUTRINA


# AS AVALIAÇÕES DE IMPACTO, O ENCARREGADO DE DADOS PESSOAIS E A CERTIFICAÇÃO NO NOVO REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS

**LUÍS PICA** [1]

1 Luís Manuel Pica. Mestre em Direito Tributário e Fiscal pela Escola de Direito da Universidade do Minho; Assistente Convidado do Instituto Politécnico de Beja; Investigador no Lab.- Ubinet do IPBeja. luispica280@gmail.com

## RESUMO

O Regulamento Geral de Proteção de Dados Pessoais, aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, é um diploma que foi negociado durante mais de 4 anos e que se erige como um dos mais importantes na história da União Europeia, tendo em vista modernizar e melhorar a regulamentação anterior (Diretiva 95/46/CE, do Parlamento Europeu e do Conselho), aumentado a segurança jurídica que proporciona a execução imediata, geral e uniforme de um regulamento comunitário. O Regulamento Geral de Proteção de Dados Pessoais surge, aqui, como um instrumento legislativo que procura atualizar as normas jurídicas existentes em matéria de proteção de dados pessoais, mas, também, pretende trazer consigo algumas novidades e inovações que a sua predecessora olvidara ou, simplesmente, não fora atualizada com a evolução da sociedade e das novas tecnologias, bem como inovações a nível procedimental e instrumental. São exemplo destas últimas a ascensão das avaliações de impacto, criadas e desenvolvidas no seio do direito anglo-saxónico, e implementadas expressamente no novo Regulamento Geral de Proteção de Dados Pessoais, ou, ainda, a criação de um novo interveniente procedimental no procedimento do tratamento de dados pessoais, como é o Encarregado de Proteção de Dados Pessoais.



**Palavras-chave:** Proteção de dados; Regulamento Geral Proteção Dados; Avaliação de Impacto; Encarregado Proteção de Dados; Selos e Certificação.

## 1. INTRODUÇÃO

O Regulamento Geral de Proteção de Dados que entrou em vigor no dia 25 de maio de 2016, e que terá plena aplicação legal em todo o território da União Europeia a 25 de maio de 2018, configura-se como um dos monumentos legislativos de maior importância dos tempos hodiernos, substituindo, até então, o que era o diploma que continha as traves mestres em matéria de tutela de dados pessoais das pessoas singulares, como era a Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

Este Regulamento, apesar das novidades e inovações que um diploma destas características e dimensões não deve abdicar, surge num contexto de continuidade e de evolução da sua predecessora, mantendo certa regulamentação já existente nesta matéria, mas inovando e melhorando aspetos que o legislador considerou como necessários para a concretização do seu verdadeiro escopo. De entre estas inovações destaca-se, do ponto de vista formal, a forma jurídica assumida pela nova legislação, isto é, como um regulamento europeu com as derivações daí advenientes, e, do ponto de vista material, a consagração legal das avaliações de impacto ou a ascensão de uma figura que visa o assessoramento das entidades responsáveis pelo tratamento dos dados e a mediação desta com a autoridade competente.

Como se denota, este novo diploma assume aqui importantes conotações que interessa abordar, mas não deixando de lado parte da regulamentação que existia até então e que se mantém neste novo monumento legislativo.

## 2. BREVE RESENHA SOBRE O ENQUADRAMENTO LEGAL

A tutela dos dados pessoais das pessoas singulares assumiu, desde muito cedo, uma das preocupações primordiais da então Comunidade Económica Europeia. Iniciou-se esta tutela através da instituição de diretrizes contidas em normas de direito originário, como a existente nos Tratados, Convenções e Cartas de Direitos Fundamentais, desenvolvendo-se, posteriormente, esta regulamentação através de normas de direito derivado, nomeadamente através da Diretiva 95/46/CE e, mais

recentemente, através do Regulamento (UE) 2016/679.Vejamos, assim, as formas de tutela dos dados pessoais.

## 2.1 - Antecedentes Normativos Europeus

Com o desenvolvimento e a evolução das novas tecnologias o homem viu uma parte da sua privacidade e intimidade, refletida nos dados pessoais, ser tratada de forma automatizada e informatizada. Este tratamento automatizado e a exposição de informação íntima e privada do titular destes dados tornaram possível a ascensão de novos direitos e formas de regulamentação, forçando não só a tutela da intimidade dos sujeitos mas também a busca de garantias que permitissem compatibilizar de forma equitativa a utilização da informática com os vários direitos de que já gozavam estes sujeitos (*v. g.* direito à honra ou o direito ao bom nome)[1]. Foi por isto que nas últimas décadas a proteção dos dados pessoais das pessoas singulares tem vindo a ser alvo de uma constante evolução[2].

Na União Europeia, esta preocupação tem vindo, tendencialmente, a ser marcada pela crescente legislação de normas jurídicas que, na sua génese, tem em vista a tutela destes dados pessoais das pessoas singulares (preocupação imediata), mas também a

1 "*En verdad, el progreso social y el desarrollo tecnológico demandan no sólo protección en la más estricta intimidad del individuo, sino también garantías para asegurar el gobierno de la persona en sus relaciones con terceros"*. Cfr. ANA ISABEL HERRÁN ORTIZ, El Derecho a la protección de datos personales en la sociedad de la información, Cuadernos Desto De Derechos Humanos, N.º26, Universidad de Bilbao, 2002, p.13, disponível em http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf, consultado a última vez em 07/03/2017; LUÍS MANUEL PICA, O direito à autodeterminação informativa dos contribuintes e a proteção dos dados pessoais em matéria tributária, Dissertação Mestrado, Universidade do Minho, Braga, 2016, disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/44452/1/Lu%C3%ADs%20Manuel%20Lopes%20Branco%20Pica.pdf, consultada a última vez em 07/03/2018; JÜRGEN SCHWABE, *Fünfzig Jahre Des Deutschen Bundesverfassungsgerichts Rechtswissenschaft*, Konrad-Adenauer-Stiftung E. V., Berlim, 2005, trad. port. de Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Geraldes Ferreira, *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*, Fundación Konrad-Adenauer, Oficina Uruguay, Montevideo, 2005.

2 "O progresso constante e acelerado no campo das TIC acarreta novas oportunidades para a sociedade, mas também novos desafios de segurança. A combinação de uma cada vez maior dependência destas, com falhas humanas ou danos intencionais, torna a mitigação dos riscos daí derivados muito mais complicada. Se as novas tecnologias comportam, por um lado, um leque alargado de novas oportunidades para o desenvolvimento da sociedade, por outro lado, também implicam novas vulnerabilidades e novas exigências tanto para a segurança das TIC como para toda a sociedade". Cfr. PETR JIRÁSEK, "Non-It Perspetives Of Cyber Security By An It Professional: Challenges And Future Trends", in Cyberlaw by CIJIC, Edição n.º III, fevereiro, 2017, p.20, disponivel em http://www.cijic.org/wp-content/uploads/2017/02/Cyberlaw-by-CIJIC_edicao-n3.pdf, consultado a última vez em 10/03/2018.

uniformização dessas normas em todo o território da União Europeia com vista à concretização do mercado interno (preocupação mediata).

Como primeira manifestação desta tutela encontramos o preceituado no artigo 8.º da Convenção Europeia dos Direitos do Homem, o qual visa, sobretudo, a tutela da vida privada e familiar, e por ingerência, a tutela dos dados pessoais que integram a esfera mais privada e restrita dos cidadãos[3].

Numa aproximação a uma tutela mais rigorosa e expressa, também o artigo 8.º da Carta dos Direitos Fundamentais da União Europeia[4] dispõe no seu n.º1 que "[t]odas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Acresce o n.º2 do preceituado normativo que "[e]sses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei".

Também a regulamentação normativa originária da União vai neste sentido pois o artigo 16.º do Tratado de Funcionamento da União Europeia veio estatuir que "[t]odas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito", criando-se, assim, condições de base à sua tutela. No que toca à regulamentação normativa secundária na União Europeia, foi pioneira a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, criando um instrumento harmonizador com o desiderato de criar mecanismos uniformes de proteção dos dados pessoais das pessoas singulares na União Europeia, bem como instrumentos de circulação desses mesmos dados pessoais, fomentando, assim, a concretização do mercado interno[5].

Estavam assim criadas condições que permitiam uma legislação, entre os Estados-Membros, harmonizada e que criava mecanismos que visavam suprimir os entraves à

3 Sobre esta matéria, Cfr. RITA AMARAL CABRAL, "O Direito à Intimidade da Vida Privada", *in Estudos em Memória do Prof. Doutor Paulo Cunha*, Lisboa, 1989; RABINDRANATH CAPELO DE SOUSA, O Direito Geral de Personalidade, Coimbra Editora, 1995.

4 Sobre a tutela dos dados pessoais na Carta dos Direitos Fundamentais da União Europeia, Cfr. CARLOS RUIZ MIGUEL. "El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Union Europea", *in La Carta de Derechos Fundamentales de la Unión Europea: una perspetiva pluridisciplinar*, Fundación Rei Afonso Henriques, 2003, disponível em http://dialnet.unirioja.es/descarga/articulo/635290.pdf, consultado a última vez em 07/03/2018.

5 Cfr. MANUEL DAVID MASSENO, O novo Regulamento Geral sobre proteção de dados pessoais da União Europeia, 8º Congresso de Direito de Informática e Telecomunicações, setembro 2016, disponível em https://www.academia.edu/31981614/O_novo_Regulamento_Geral_sobre_proteção_de_dados_pessoais_da_União_Europeia?auto=download, consultado a última vez em 12/03/2018.

livre circulação dos dados pessoais, e fomentado a tutela destes no espaço da União Europeia.

### 2.2 - A Lei Proteção de Dados Pessoais - Lei n.º 67/98, de 26 de outubro de 1998

A transposição para o ordenamento jurídico português da já mencionada Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, foi realizada pela Lei n.º 67/98, de 26 de outubro de 1998, a qual aprovou a Lei de Proteção de Dados Pessoais (doravante denominada pelas siglas "LPDP").

A LPDP procurou expressamente a "proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados", tal como se encontra disposto no primeiro artigo da mencionada Lei. Para além disso, a LPDP veio delimitar as formas de recolha, tratamento, transmissão, registo e conservação dos dados pessoais das pessoas singulares, bem como a criação da entidade independente que visa a fiscalização do cumprimento deste normativo legal (nomeadamente a Comissão Nacional de Proteção de Dados).

Quanto aos princípios norteadores em matéria de proteção dos dados pessoais das pessoas singulares, a LPDP erigiu-se como um diploma de base para os vários ramos do direito em que era necessária a utilização, recolha e conservação destes dados, aplicando-se subsidiariamente às várias relações jurídicas constituídas entre sujeitos de direito[6].

Neste sentido, a LPDP veio consagrar um conjunto de diretrizes fundamentais que determinavam o modo como as entidades responsáveis pela recolha e tratamento dos dados pessoais deviam pautar as suas atuações no âmbito deste procedimento:

a) foi assim com o *princípio da licitude* consagrado na alínea a) do n.º1 do artigo 5.º da LPDP, que obrigava as entidades responsáveis pelo tratamento a recolher e tratar

6 Foi assim no âmbito dos contratos de consumo celebrados entre consumidores e prestadores de serviços; também em matéria tributária a Administração Tributária e Aduaneira é pautada por este diploma no que toca à recolha e tratamento dos dados pessoais dos contribuintes; em matéria processual, a transmissão de dados pessoais dos executados, no âmbito da ação executiva, como são os dados de vencimento para penhora de vencimentos, deve ser feita em respeito pelo princípio da proporcionalidade e com vista ao estritamente necessário.

os dados pessoais em respeito pelo princípio da boa-fé obrigando a que a sua recolha seja conseguida de modo legal e dentro dos ditames legais;

b) também o *princípio da finalidade* teve grande importância nesta matéria pois determinava que a recolha dos dados pessoais fosse concretizada para finalidades específicas e expressamente determinadas, encontrando consagração normativa na alínea b) do n.º1 do artigo 5.º da LPDP;

c) outro dos princípios enformadores, e de grande importância em matéria de proteção de dados pessoais, é o *princípio da exatidão e da qualidade* gizado na alínea d) do n.º1 do artigo 5.º da LPDP, conduzindo, principalmente, a que o responsável pelo tratamento dos dados pessoais deve recolher e tratar as informações cujo teor deve ser exato, correto, completo e atualizado, não sendo permitido o seu tratamento quando estes se afigurem como parciais, incompletos ou fracionados e que por conseguinte induzam em erro;

d) por último, os dados pessoais devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

Relativamente aos princípios fundamentais inerentes ao consentimento do titular dos dados pessoais, veio a LPDP ser de enorme importância em matéria de consentimento dado pela titular destes, sendo o seu tratamento consentido[7] para:

a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido;

b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c) Proteção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;

7 Cf. Artigo 6.º da Lei n.º 67/98, de 26 de outubro de 1998.

d) Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.

A LPDP procurou ainda instituir mecanismos de circulação de dados pessoais tanto a nível da União Europeia, sendo o princípio geral o de livre circulação dos dados pessoais entre Estados-Membros da União Europeia[8], como a nível internacional, devendo, nestes casos, ser assegurado um nível de proteção adequado, cabendo à Comissão Nacional de Proteção de Dados a decisão se o País em questão cumpre ou não com os níveis de tutela adequados para ser realizada esta transferência.

Por último, foi criada, com a aprovação da Lei n.º 67/98, de 26 de outubro de 1998, a entidade independente na qual era confiada a tarefa de fiscalização das disposições legais ali aprovadas. A já mencionada Comissão Nacional de Proteção de Dados é a autoridade nacional que tem como principal tarefa controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei[9].

### 2.3 - Regulamento Geral de Proteção de Dados

No dia 25 de janeiro de 2012, a Comissão Europeia apresentou um conjunto de iniciativas de índole legislativa as quais tinham como principal desiderato a reforma do sistema europeu de proteção de dados.

No ato de apresentação da intenção, a Comissária da Justiça e Vice-Presidente da Comissão Europeia, Viviane Reding, realçou a necessidade de reforma[10]. Essa reforma

8 Cf. Artigo 18.º da Lei n.º 67/98, de 26 de outubro de 1998.
9 Cf. Artigo 22º n.º1 da Lei n.º 67/98, de 26 de outubro de 1998.
10 *"Our current data protection rules already contain solid data protection principles. But they were drawn up in 1990 and adopted in 1995, when only 1% of the EU population was using the Internet. In 1995 a 28.8 Kilobytes*

assentava, principalmente, em dois projetos normativos: a) em primeiro, a Comissão apresentara um Projeto de Regulamento do Parlamento Europeu e do Conselho para a proteção dos cidadãos em relação ao tratamento dos dados pessoais e à livre circulação destes; em segundo, a Comissão apresentou um projeto de Diretiva do Parlamento Europeu e do Conselho sobre a proteção dos cidadão em relação ao tratamento dos dados pessoais pelas autoridades competentes com a finalidade de prevenir, investigar, detetar atos criminais ou executar penas, e sobre a livre transferência desses dados.

As iniciativas da Comissão Europeia comportam uma revisão global do sistema europeu de proteção de dados, tanto num âmbito formal como substantivo. Por um lado, o novo normativo europeu será baseado num diferente instrumento legal (o Regulamento Geral sobre a Proteção de Dados em detrimento da Diretiva 95/46/CE) e, por outro lado, resulta evidente que este novo normativo abordará algumas problemáticas até ao momento não satisfatoriamente resolvidas pelas normas vigentes.

Este Regulamento Geral sobre a Proteção de Dados Pessoais na União Europeia (doravante denominado pelas siglas "RGPD"), aprovado pelo 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, a qual foi transposta no ordenamento jurídico português pela já mencionada Lei n.º67/98, de 26 de outubro de 1998, teve origem num largo processo legislativo.

Este novo instrumento jurídico é o resultado de um longo processo que se pode situar, do ponto de vista institucional, no ano de 2010 quando o Conselho Europeu juntamente com a Comissão Europeia avaliaram o funcionamento dos instrumentos aprovados e que se encontravam em vigor na União sobre a tutela dos dados pessoais,

---

*per second modem cost more than 500 euros, Amazon and eBay were still being launched and the founder of Facebook was only 11 years old! It would still be 3 years before the arrival of Google and other household names. But gone are the days of mobile phones the size of bricks and punched card computer programming! Today, just as your computing operating systems and smartphones need regular updates to take new technological developments into account, our data protection rules also needed to be modernised. So we are updating our rules to ensure that they continue to protect individuals in this brave new digital world."* Texto de apresentação de Viviane Reding, Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world, June, 2012, disponível em http://europa.eu/rapid/press-release_SPEECH-12-464_en.htm, consultado a última vez

podendo, em caso de ser necessário, apresentar iniciativas com vista a colmatar as deficiências existentes[11] [12].

Neste sentido, tanto o Parlamento Europeu defendeu a ideia de ser criado um regime geral relativo à proteção dos dados pessoais na União Europeia, bem como a Comissão Europeia defendeu a necessidade de garantir o direito fundamental de proteção dos dados pessoais de forma coerente e em consonância com as políticas existentes na União Europeia[13] [14].

Com isto, no dia 27 de janeiro de 2012, a Comissão Europeia elaborou uma proposta de Regulamento relativo à proteção dos dados pessoais das pessoas físicas e à sua circulação no espaço comunitário.

Por fim, em 4 de maio de 2016 foi publicado no Diário Oficial da União Europeia, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, que visava a proteção das pessoas singulares em matéria de tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE.

Este monumento legislativo entrou em vigor no dia 25 de maio de 2016, sendo que existe um período transitório de 2 anos para a sua total aplicação, tendo os responsáveis pelo tratamento dos dados pessoais o mencionado prazo para se adaptarem às novas regras aprovadas, configurando-se estas normas como diretamente aplicáveis sem necessidade dos Estados-Membros as transporem para a ordem jurídica interna, garantindo-se, assim, uma "total"[15] harmonização legislativa em matéria de tutela dos dados pessoais. Destarte, gozam os responsáveis pelo tratamento dos dados pessoais de

11 Cfr. Programa de Estocolmo, "Uma Europa aberta e segura que sirva e proteja os cidadãos", *in* Jornal Oficial C 115 de 4.5.2010, disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52010XG0504(01), consultado a última vez em 05/03/2018.

12 Cfr. MANUEL DAVID MASSENO, O novo Regulamento Geral sobre proteção de dados pessoais da União Europeia, … *op. cit.*

13 Cfr. Parecer do Comité Económico e Social Europeu sobre a «Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da proteção de dados pessoais na União Europeia», *in COM(2010) 609 final] 2011/C 248/21*, disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52011AE0999&from=ES, consultado a última vez em 05/03/2018.

14 Cfr. Resolução do Parlamento Europeu, de 25 de novembro de 2009, sobre a Comunicação da Comissão – Um espaço de liberdade, de segurança e de justiça ao serviço dos cidadãos – Programa de Estocolmo, P7_TA(2009)0090, disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA2009-0090+0+DOC+XML+V0//PT, consultado a última vez em 05/03/2018.

15 Sublinhamos que a aparência de "total harmonização" não é concretizada na sua completa terminologia pois os Estados-Membros gozam de autonomia para legislar sobre determinadas matérias em que o Regulamento assim o permite.

um período relativamente generoso de *vacatio legis* concedido para que estes possam ir preparando e adaptando as suas organizações aos conteúdos das novas normas e, ao mesmo tempo, permitindo aos Estados a atividade legislativa necessária para adequar o sistema jurídico à plena vigência do Regulamento.

Em suma, podemos afirmar que este Regulamento procura, assim, desenvolver a regulamentação jurídica global europeia existente em matéria de proteção de dados já que, por um lado, esta nova regulamentação irá resultar diretamente e imediatamente aplicável por gozar de natureza de regulamento europeu e, por outro lado, irá proporcionar novos direitos aos cidadãos[16].

## 3. A ESTRATÉGIA PREVENTIVA NO NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: AVALIAÇÃO DE IMPACTO, ENCARREGADO DE PROTEÇÃO DE DADOS, SELOS E CÓDIGOS DE CONDUTA

A era do *Big Data* dificilmente irá encontrar resposta aos riscos que sobrevoam o tratamento dos dados pessoais através (unicamente) de meios repressivos e sancionatórios, ou seja, difícil será admitir que determinado diploma legislativo de tamanha importância tenha como única via de intervenção aquelas situações patológicas da relação jurídica.

Partindo, assim, do pressuposto que o direito melhor tutelado é aquele onde se resolvem, previamente, as vulnerabilidades e se procura tutelar preventivamente os bens jurídicos em questão, o legislador europeu desenhou um conjunto de mecanismos, de natureza preventiva, que tem como desiderato reforçar a tutela dos dados pessoais desde o início do tratamento com vista ao reforço da responsabilização das entidades[17].

16 Cfr. ARTEMI RALLO LOMBARTE, "Hacia un Nuevo Sistema Europeo de Protección de Datos: Las Claves de la Reforma" in UNED. *Revista de Derecho Político* N.º 85, septiembre-diciembre, 2012, pp. 13-56, disponível http://revistas.uned.es/index.php/derechopolitico/article/view/10244/9782, consultado a última vez em 09/03/2018.
17 Cfr. ARTEMI RALLO LOMBARTE, "Hacia un Nuevo Sistema Europeo de Protección de Datos: Las Claves de la Reforma"… *op. cit.*

Em primeiro lugar, o RGPD institui normativamente uma prática preventiva já bastante utilizada nos países de família jurídica Anglo-Saxónica designada como *Privacy Impact Assessment (PIA)*[18], avaliando-se o impacto, em matéria de proteção de dados, sobre o tratamento de determinados tipos de dados pessoais que, pela sua natureza, alcance ou fins, determinem riscos específicos, como poderá ocorrer em situações exemplificativamente previstas no próprio RGPD.

Em segundo lugar, outra das grandes apostas concretizada pelo legislador europeu reside na ascensão de um novo interveniente em matéria de proteção de dados pessoais - já existente em alguns ordenamentos jurídicos como Alemanha ou França -, como é o Encarregado de Proteção de Dados. Este novo interveniente passa a ser obrigatório no organograma de determinada organização, como serão as instituições públicas ou empresas com grande número de trabalhadores. Relevante neste aspeto é o facto de o Encarregado de Proteção de Dados ser uma entidade com competências para se relacionar diretamente com a Comissão Nacional de Proteção de Dados, o público e os interessados, configurando-se como uma entidade que exercerá as suas obrigações de forma independente ao responsável pelo tratamento dos dados pessoais, não podendo receber instruções deste que coloquem em risco a sua isenção. As suas funções assumem-se, assim, em informar e assessorar o responsável pelo tratamento dos dados, instruindo-o sobre as suas obrigações legais e supervisionando as políticas internas de privacidade em respeito pelas garantias de proteção dos dados, desde o desenho à segurança destes, à informação, à notificação de violação, à avaliação de impacto e cooperando com a autoridade de controlo dos dados.

Em terceiro lugar, o legislador europeu manteve o clausulado legal quanto aos códigos de conduta, mas abre outra via de autorregulamentação como são as certificações e os selos com vista a uma exteriorização das competências internas no cumprimento do RGPD.

Vejamos assim com maior precisão de todas estas novas inovações trazidas pelo RGPD em matéria de prevenção na tutela dos dados pessoais das pessoas singulares.

---

18 Cfr. REHAB ALNEMR, ERDAL CAYIRCI, LORENZO DALLA CORTE, ALEXANDR GARAGA, RONALD LEENES, RODNEY MHUNGU, SIANI PEARSON, CHRIS REED, ANDERSON SANTANA DE OLIVEIRA, DIMITRA STEFANATOU, KATERINA TETRIMIDA AND ASMA VRANAKI, "A Data Protection Impact Assessment Methodology for Cloud", in Springer-Verlag Berlin Heidelberg, 2011, disponível em https://pdfs.semanticscholar.org/5b74/2c82769c026f9c487d4d84d46f1ff86ea061.pdf, consultado a última vez em 10/03/2018.

### 3.1 - Avaliação de Impacto sobre a Proteção de Dados

A avaliação de impacto sobre a proteção de dados pessoais é uma das principais medidas normativas aprovadas pelo novo RGPD, encontrando-se este instituto ancorado no artigo 35.º do mencionado diploma legal.

Esta técnica de avaliação de riscos no procedimento de tratamento de dados pessoais não é inovação quanto à sua existência pois esta é bastante conceituada e utilizada nos países anglo-saxónicos, sendo esta a sua origem e daí surgindo a designação de PIA's (*Privacy Impact Assessments).* No entanto a sua regulamentação expressa no plano Europeu configura-se como uma das principais novidades deste diploma.

A avaliação de impacto pode definir como um exercício prévio de análise dos riscos que um determinado sistema de informação, produto ou serviço pode ter sobre algum direito fundamental como é o direito à tutela dos dados pessoais, permitindo afrontar eficazmente os riscos identificados mediante a adoção de medidas necessárias para eliminar ou mitigar estes riscos[19]. Sufragando esta opinião a própria Autoridade de trabalho para proteção de dados da União Europeia afirma que "[u]ma AIPD [Avaliação de impacto] é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos (…) Por outras palavras, uma AIPD é um processo que visa estabelecer e demonstrar conformidade."[20].

Neste sentido dispõe o n.º1 do artigo 35.º do RGPD que "quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede,

19 Cfr. Information Comissioner's Office, *Conducting privacy impact assessments code of practice*, 2014, pp.5 e seguintes, disponível em https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf, consultado a última vez em 05/03/2018.

20 Cfr. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 - Documento WP 248 rev.01, abril, 2017, p.4, disponível em https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf, consultado a última vez em 06/03/2018. (Interpolação nossa).

antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais". Ora, daqui podem-se extrair uma série de ilações que merecem reparo e interessa dissecar.

Em primeiro lugar, e como *supra* referido, o procedimento de avaliação de impacto é um **procedimento prévio** ao início do tratamento dos dados pessoais, ocorrendo assim antes do tratamento destes e com fins de análise ao procedimento principal.

Em segundo lugar, esta avaliação de impacto apenas tem lugar quando for utilizada nova tecnologia e o tratamento dos dados pessoais for suscetível de implicar um **elevado risco**[21] [22] para os direitos fundamentais dos titulares dos dados pessoais, competindo à autoridade de controlo (em Portugal a Comissão Nacional de Proteção de Dados) elaborar uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto[23] [24].

Em terceiro lugar, o tratamento tem de ser suscetível de comportar um elevado risco para os **direitos e liberdades das pessoas singulares,** ou seja, todos os direitos que visem a tutela direta dos dados pessoais e da privacidade do seu titular mas, também, todos os direitos indiretos como serão os direitos de liberdade de circulação, liberdade de expressão ou liberdade de pensamento.

Com esta análise de impacto consegue-se desde logo identificar os possíveis riscos para a proteção dos dados pessoais dos afetados e a valorização da probabilidade de ocorrerem, bem como os danos que causariam se se materializassem. Feita esta

21 Apesar de o RGPD não especificar o que deve ser entendido por "elevado risco", podemos indicar, segundo também vários documentos emitidos pelas autoridades de proteção de dados da União Europeia, como sendo atividades de perigosidade para os direitos dos titulares dos dados pessoais, as seguintes atividades: a) tratamentos que avaliem aspetos pessoais relativos a pessoas físicas, baseados em tratamento automatizado de dados que produzam efeitos jurídicos na esfera jurídica destes, como poderá ser a decisão de obter um crédito bancário baseado unicamente no processamento automático feito por um programa de computador; b) tratamento de dados em setores de natureza vulnerável, como poderá ser o setor laboral; c) tratamento de dados sensíveis como são os dados pessoais que revelem as opiniões políticas e religiosas, o tratamento de dados genéticos, os dados biométricos; a monitorização sistemática em que existem controlos de vigilância; e as transferências internacionais de dados para o espaço externo à União Europeia.

22 Cfr. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) … *op. cit.*, disponível em https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf, consultado a última vez em 06/03/2018.

23 Cf. Artigo 35.º n.º4 do RGPD.

24 No entanto pode a Comissão Nacional de Proteção de Dados identificar negativamente os tipos de operações de tratamento em relação às quais não é obrigatória a elaboração de uma avaliação de impacto, conforme preceitua o n.º5 do artigo 35.º do RGPD.

análise é possível, previamente, determinar as medidas que devem ser implementadas a fim de eliminar ou mitigar os riscos detetados, permitindo adotá-los no tratamento dos dados pessoais a fim de concretizar a tutela dos direitos fundamentais dos titulares destes[25].

Como veremos *infra*, uma das principais novidades que o novo RGPD trouxe face à Diretiva 95/46/CE foi a criação de uma "entidade interna" existente na organização do responsável pelo tratamento dos dados pessoais, o qual tem como tarefa primordial zelar pelo cumprimento das normativas relacionadas com o tratamento destes. Esta "entidade" foi designada pelo legislador como *encarregado da proteção de dados*, passando a entidade de controlo a ter um papel mais residual intervindo, principalmente, nas situações patológicas da relação jurídica constituída entre o responsável pelo tratamento dos dados pessoais e o seu titular.

Uma das principais tarefas do encarregado da proteção de dados é, segundo o conceituado na alínea c) do n.º1 do artigo 39.º do RGPD, o de prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do n.º2 do artigo 35.º. Deste modo, sempre que a entidade responsável pelo tratamento dos dados pessoais possua alguém a exercer as tarefas inerentes à atividade de encarregado da proteção de dados, fica este obrigado a emitir parecer a sobre esta avaliação de impacto.

No entanto, esta avaliação de impacto resulta obrigatória quando o tratamento dos dados pessoais tenha como objeto a avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, devendo este ser baseado no tratamento automatizado, incluindo definição de perfis, tendo como principal objetivo a tomada de decisões que produzam efeitos jurídicos na esfera do titular destes dados pessoais; esta avaliação de impacto configura-se, também, como obrigatória quando haja operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º, e ainda quanto aos dados pessoais relativos a menores; por último é também obrigatório proceder a esta avaliação de impacto nos casos de controlo

25 Neste sentido afirma o considerando 84 do RGPD que "[o]s resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento".

sistemático de zonas acessíveis ao público em grande escala, ou seja, quando seja utilizados meios tecnológicos considerados invasivos da privacidade como serão, a título meramente exemplificativo, vigilância a grande escala, geolocalização, vigilância eletrónica, técnicas genéticas, etc.[26].

Em suma pode-se referir que as entidades obrigadas a realizar este procedimento serão, nomeadamente: as empresas de segurança privada, vigilância e controlo, hospitais e clínicas, escolas, empresas envolvidas no e-commerce, farmácias e comercializadores de energia.

A avaliação de impacto a que se refere o artigo 35.º do RGPD deve conter uma série de elementos, indispensáveis e irrenunciáveis, pois como refere o n.º7 do citado preceito legal deve esta conter, *pelo menos:* uma descrição das operações de tratamento que pretende efetuar e qual a sua finalidade, bem como os interesses do responsável pelo tratamento, se o mesmo não se vislumbrar da finalidade pretendida com o tratamento; deve incluir, também, uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos pretendidos, pois caso os mesmos se configurem como desnecessários e desproporcionais não haverá necessidade deste tratamento ser efetuado da forma descrita e pretendida; uma avaliação sobre os eventuais riscos e ofensas aos direitos fundamentais dos titulares dos dados pessoais em virtude das operações realizadas no tratamento destes; por último é também obrigatório que a avaliação de impacto inclua as medidas reparadoras, preventivas, medidas de segurança e procedimentos que visem assegurar a proteção dos dados pessoais tratados a fim de comprovar a total legitimação entre a operação realizada e o cumprimento das normas presentes no Regulamento Geral.

A avaliação de impacto pode ser considerada como um projeto sobre o procedimento de tratamento dos dados pessoais na medida em que o responsável pelo tratamento dos dados pessoais pode efetuar um estudo prévio sobre estas operações a fim de verificar se os mesmos estão em conformidade com o resultado obtido na avaliação de impacto realizada antes do inicio destas operações[27].

26 Cf. Artigo 35.º n.º3 do RGPD.
27 Cf. Artigo 35.º n.º11 do RGPD.

Daqui podemos encontrar duas situações diversas: ou o resultado da avaliação de impacto é positivo e o tratamento e operações dos dados pessoais não resulta na ofensa de qualquer direito fundamental dos seus titulares; ou, pelo contrário, da avaliação de impacto resulta que as operações a realizar colocam em risco a esfera jurídica do titular destes dados pessoais. Na primeira situação fácil é denotar que, em nada violando o disposto no Regulamento Geral, pode o tratamento ter lugar sem qualquer intervenção de terceiros ou medidas que atenuem ou afastem possíveis riscos aos direitos fundamentais dos titulares dos dados pessoais. Na segunda situação, e havendo já riscos identificados pela avaliação de impacto na ausência de medidas que afastam ou atenuem o risco, deve o responsável pelo tratamento consultar, previamente às operações de tratamento, a entidade de controlo (como referido, em Portugal a Comissão Nacional de Proteção de Dados) devendo comunicar-lhe quem é o responsável pelo tratamento, as finalidades e os meios de tratamento previstos, as medidas e garantias previstas para salvaguardar os direitos e liberdades dos titulares dos dados pessoais, os contactos do encarregado dos dados pessoais (caso este exista na entidade responsável pelo tratamento), o resultado da avaliação de impacto e, ainda, todas as informações que a entidade de controlo venha a solicitar[28].

A *ratio essendi* a esta consulta prévia à autoridade de controlo não é mais que a de salvaguardar os direitos e liberdades dos titulares dos dados pessoais, já que se este tratamento e operações têm subjacentes riscos para estes, não podem estas operações ser realizadas sem uma prévia consulta à autoridade de controlo.

Deste modo é nossa opinião que esta consulta prévia à autoridade de controlo apenas deve ter lugar quando as operações de tratamento resultem num risco para os direitos fundamentais dos titulares dos dados e não existam medidas que afastem ou atenuem este risco, pois caso existam e possam ser implementadas, não será necessária a consulta e intervenção da autoridade de controlo. Neste sentido parece apontar o próprio RGPD quando dispõe que "[s]empre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas,

28 Cf. Artigo 36.º n.º1 e n.º3 do RGPD.

atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais".

Por último, é importante referir a importância deste procedimento para as entidades responsáveis pelo tratamento dos dados pessoais pois, como se encontra expresso na alínea a) do n.º4 do artigo 83.º do RGPD, a não realização da avaliação de impacto - quando devida -, a não conformidade com os requisitos de uma Avaliação de impacto e a realização de forma incorreta de uma avaliação de impacto pode conduzir à imposição de coimas pela autoridade de controlo competente, encontrando-se classificada como uma infração punível com coima até até 10 000 000 EUR ou, no caso de uma empresa, até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

### 3.2 - O Encarregado da Proteção dos Dados (*Data Protection Officer)*

O novo RGPD traz uma alteração substancial no paradigma das relações jurídicas instituídas entre o responsável pelo tratamento dos dados pessoais e a entidade responsável pelo cumprimento da regulamentação legal vigente nesta matéria. Até à aprovação do RGPD pode-se afirmar que o sistema vigente é um sistema de heterorregulação, passando com a aprovação e entrada em vigor do mesmo a ter um sistema de autorregulação onde as entidades responsáveis pelo tratamento são obrigadas a comprovar a utilização do RGPD à entidade que fiscaliza. Passamos, assim, a ter uma entidade fiscalizadora num papel mais passivo e o qual é chamado a intervir nas situações patológicas da relação jurídica.

Mas para haver autorregulação pelas entidades, ou seja, nas quais estas interpretam e adaptam os seus recursos e meios à legislação em vigor, deve existir alguém com competência material para o fazer. Neste desiderato, e sendo uma das grandes inovações trazidas pela publicação e entrada em vigor do novo RGPD, surge a figura do Encarregado da Proteção dos Dados, ou como comummente designado, *Data Protection Officer (DPO).*

A figura do encarregado da proteção dos dados encontra-se ancorada nos artigos 37.º e seguintes do RGPD, como a entidade responsável pela proteção, gestão e tratamento dos dados de uma empresa ou organização, sendo que as suas principais tarefas podem ser, entre outras não previstas no RGPD, as elencadas no n.º1 do artigo 39.º do RGPD, nomeadamente:

a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controlar a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.º;

d) Cooperar com a autoridade de controlo;

e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

A sua principal tarefa consubstancia-se em informar ao responsável pelo tratamento dos dados sobre os aspetos legais e práticos ligados a estas operações, supervisionando que se apliquem as normas jurídicas aprovadas no presente Regulamento, zelando, assim, pelo seu cumprimento. O encarregado da proteção dos dados surge aqui como uma figura de transcendental importância no novo paradigma subjacente à relação entre as autoridades de controlo e as entidades responsáveis pelo tratamento dos dados pessoais, pois, com a entrada em vigor do novo Regulamento, as autoridades de controlo deverão atuar apenas nas situações patológicas da relação

jurídica, devendo as entidades responsáveis pelo tratamento dos dados assegurar o cumprimento estrito do disposto no citado Regulamento, sob pena de incorrerem em pesadas sanções.

Deste modo poderemos identificar como funções do encarregado da proteção dos dados, nomeadamente: assessorar os responsáveis pelo tratamento dos dados pessoais e os trabalhadores destas sobre as obrigações legais que devem cumprir; supervisionar as tarefas que se encontram subjacente ao tratamento dos dados pessoais; avaliar o impacto das ações de risco elevado para os direitos fundamentais dos titulares dos dados pessoais; e, ainda, colaborar com a Comissão Nacional de Proteção de Dados trabalhando como intermediário entre o responsável pelo tratamento dos dados pessoais e a autoridade de controlo[29].

No entanto, a existência do encarregado de proteção dos dados no organograma apenas é obrigatória quando preenchidos alguns requisitos previstos legalmente, os quais não podem aqui ser entendidos como cumulativos. Assim, é obrigatória a designação de um encarregado de proteção de dados quando este tratamento for efetuado por uma autoridade ou organismo público (*v.g.* Autoridade Tributária e Aduaneira; Câmaras Municipais), quando as atividades principais do responsável pelo tratamento subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala[30], ou, então, quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados[31].

Dispõe o n.º4 do artigo 37.º do RGPD que "[e]m casos diferentes dos visados no n.º 1, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designar um encarregado da proteção de dados". Portanto, entidades ou atividades indicadas pelo legislador podem, mediante lei estadual aprovada pelo Estado-

29 Cf. Artigo 39.º do RGPD.
30 Aqui devem apenas ser entendidas as atividades primárias e principais praticadas por estas entidades, pelo que não se incluem as entidades que pratiquem estas atividades a título secundário à sua atividade central.
31 Cf. Artigo 37.º n.º1 do RGPD.

Membro, ser sujeitas à designação de um encarregado de proteção de dados mesmo que não indicadas neste n.º1 do artigo 37.º do RGPD.

Questão que urge ainda analisar é saber quem pode ser designado para encarregado de proteção de dados?

O RGPD não concreta quem é que deve assumir esta posição, no entanto, como se descortina do n.º5 e n.º6 do artigo 37.º do RGPD, o encarregado da proteção de dados é designado e/ou contratado segundo a sua capacidade para exercer as competências fixadas pelo regulamento e, concretamente, pelos seus conhecimentos em matéria de direito e proteção de dados. Para desempenhar esta função, juristas ou pessoas com sólidos conhecimentos sobre o RGPD são de enorme importância para assumirem estes cargos nas empresas e entidades responsáveis por este tratamento, não sendo, pelo momento, necessária qualquer creditação aprovada pela Comissão Nacional de Proteção de Dados para designar determinada pessoa como "competente" para exercer este cargo, pelo que basta a competência da pessoa para exercer esta tarefa.

Este encarregado da proteção de dados surge como uma *figura híbrida* nesta relação jurídica pois, por um lado, surge no organograma da entidade responsável pelo tratamento e, pelo outro, as suas funções assemelham-se como intermediária e um "agente" da Comissão Nacional de Proteção de Dados no cumprimento das normas jurídicas aprovadas no Regulamento. Sufragando esta ideia parece apontar o n.º1 e n.º3 do artigo 38.º do RGPD quando expressamente indica que "[o] responsável pelo tratamento e o subcontratante asseguram que [o encarregado] da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções", acrescentando ainda o ponto 97 das considerações preambulares que "[e]stes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com *independência*".

Pelo exposto, pode-se vislumbrar que o encarregado da proteção dos dados é aqui um sujeito procedimental que goza de certa autonomia face ao responsável pelo tratamento dos dados pessoais, pois não pode aqui ser penalizado pelos atos deste, nem pode ser induzido, conduzido ou influenciado nos atos próprios das suas funções. Fácil

é assim de denotar que a *ratio* desta norma surge na senda que a sua função assume-se como um sujeito que tem como principal desiderato o cumprimento das normas constantes do RGPD, configurando-se como uma ponte de interligação entre a entidade responsável pelo tratamento dos dados e a Comissão Nacional de Proteção de Dados, pelo que a influência por uma destas entidades colocaria em causa esta posição de "intermediário" e por conseguinte o bom cumprimento das normas presentes no Regulamento.

### 3.3 - Códigos de Conduta

Os códigos de conduta constituem uma ferramenta de natureza transversal a todos os ramos do Direito, configurando-se como um instrumento similar ao movimento existente com a codificação que originaram os atuais códigos tipo existentes nos ordenamentos jurídicos.

Em matéria de proteção de dados pessoais, os códigos de conduta surgem no novo regulamento como um instrumento essencial para as organizações responsáveis pelo tratamento destes[32] [33]. Neste sentido, aponta o ponto 98 das considerações preambulares que "[a]s associações ou outras entidades que representem categorias de responsáveis pelo tratamento ou de subcontratantes deverão ser incentivadas a elaborar códigos de conduta, no respeito do presente regulamento, com vista a facilitar a sua aplicação efetiva, tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades específicas das micro, pequenas e médias empresas. Esses códigos de conduta poderão nomeadamente regular as obrigações dos responsáveis pelo tratamento e dos subcontratantes, tendo em conta o risco que poderá

32 A existência de Código de Conduta em matéria de proteção de dados pessoais não é uma novidade pois, a própria Lei n.º67/98 de 26 de outubro, já previa a existência destes códigos conforme preceitua o artigo 32.º do citado diploma legal.

33 Um dos melhores exemplos dos códigos de conduta aprovados e que tem em vista a uniformização das práticas de determinada atividade relacionada com a proteção de dados em consonância com o disposto no RGPD, é o Código de Conduta CISPE (*Cloud Infrastructure Service Providers in Europ*e), aprovado para os Provedores de Serviço de Infraestrutura em Nuvem, e que tem como finalidade uniformizar as normas tendentes a esta atividade. A versão original deste Código de Conduta pode ser consultado na íntegra através de https://cispe.cloud/wp-content/uploads/2017/06/Code-of-Conduct27-January2017-corrected-march20.pdf, consultado a última vez em 05/03/2018.

resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares".

Deste modo, o RGPD reconhece a aprovação de códigos de conduta pois como refere no n.º1 do artigo 40.º do citado diploma, "[o]s Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas". Mas não apenas estas tem legitimidade legal para criar códigos de conduta pois conforme preceitua o n.º2 do citado normativo legal, as associações e outros organismos representativos podem elaborar, modificar ou ampliar um código de conduta com a finalidade de o especificar a e adaptar ao próprio Regulamento.

Neste sentido, o próprio RGPD exemplifica alguns dos parâmetros que os códigos de conduta podem regular, nomeadamente:

*"a) O tratamento equitativo e transparente; b) Os legítimos interesses dos responsáveis pelo tratamento em contextos específicos; c) A recolha de dados pessoais; d) A pseudonimização dos dados pessoais; e) A informação prestada ao público e aos titulares dos dados; f) O exercício dos direitos dos titulares dos dados; g) As informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido; h) As medidas e procedimentos a que se referem os artigos 24.º e 25.º e as medidas destinadas a garantir a segurança do tratamento referidas no artigo 30.º; i) A notificação de violações de dados pessoais às autoridades de controlo e a comunicação dessas violações de dados pessoais aos titulares dos dados; j) A transferência de dados pessoais para países terceiros ou organizações internacionais; ou, k) As ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento e os titulares dos dados em relação ao tratamento, sem prejuízo dos direitos dos titulares dos dados nos termos dos artigos 77.º e 79.º."*

Esta alteração é realizada mediante comunicação à Comissão Nacional de Proteção de Dados, apresentando um projeto de código para que esta o análise e verifique a sua conformidade com o disposto no RGPD.

Após análise desse projeto, a Comissão Nacional de Proteção de Dados emite parecer sobre a conformidade do projeto de código, podendo, aqui, haver duas situações que merecem reparo: caso a atividade de tratamento não esteja relacionada com vários Estados-Membros e o projeto de código esteja em conformidade com as normas presentes no RGPD, o mesmo será publicado e registado para aplicação; em caso da atividade estar ligada a vários Estados-Membros, não pode a Comissão Nacional de Proteção de Dados aprovar e registar o código de conduta de imediato, sem antes de a aprovação ser apresentado o projeto do código, a alteração ou o aditamento, pelo procedimento referido no artigo 63.º, ao Comité, que emite um parecer sobre a conformidade do projeto de código de conduta, ou da alteração ou do aditamento, com o disposto no RGPD, remetendo esse parecer para a Comissão, nos termos do n.º8 do artigo 40.º do RGPD.

A *ratio* subjacente a esta norma que impõe a intervenção das entidades Europeias encontra-se relacionada com a necessidade imperativa de a proteção de dados pessoais das pessoas físicas merecer grande importância e uniformidade na União Europeia, pelo que se determinada atividade é comum a vários Estados-Membros, é necessário, e proveitoso, que seja de aplicar em todos esses Estados-Membros e setores da atividade interligados entre si, com o intuito de quebrar a barreira entre países e fomentar a livre circulação na União Europeia.

Neste sentido parece apontar o n.º9 do artigo 40.º do RGPD, pois o mesmo indica que a Comissão pode, através de atos de execução, decidir que determinado código de conduta, aprovado nos termos *supra* expostos, seja aplicável em todos os Estados-Membros, e por conseguinte aplicado de modo geral na União Europeia.

### 3.4 - Certificação, Selos e Marcas

O procedimento de certificação das operações de tratamento de dados pessoais encontra-se ancorada no novo RGPD, nomeadamente nos artigos 42.º e seguintes deste diploma legal.

A existência de certificações, selos e marcas de procedimentos de tratamento de dados pessoais tem como desiderato demonstrar que determinada operação de

tratamento de dados cumpre com o disposto no RGPD. Como ponto de partida, têm-se em vista que o "Selo Europeu de Proteção de Dados" visa criar confiança entre os interessados, consumidores e titulares dos dados pessoais, dotando-os de maior certeza e rapidez na hora de analisar os produtos e serviços correspondentes.

Neste sentido dispõe o n.º1 do artigo 42.º do RGPD que "[o]s Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento". Pode-se assim afirmar que os selos, marcas e certificação de procedimentos consistem numa forma de atribuição de um "distintivo" que qualifica determinado procedimento, ou operação que envolva o tratamento de dados pessoais, como cumprindo os pressupostos do presente Regulamento em matéria de tutela dos direitos fundamentais dos titulares dos dados pessoais. Configuram-se, assim, como um mecanismo que visa demonstrar o adequado cumprimento do RGPD, por parte dos responsáveis pelo tratamento dos dados pessoais, proporcionando garantias adequadas para as transferências internacionais de dados tendo em conta as características e necessidades específicas dos diferentes setores de tratamento e âmbitos sectoriais.

Sendo como um distintivo que atribuí qualidade à operação em causa, fácil é de denotar que esta atribuição de certificação só pode ser voluntária, podendo o responsável por estas operações, livremente, optar sobre se quer atribuir uma maior publicidade aos consumidores relativamente a estas, ou pelo contrário não a pretende publicitar. Note-se que, como mecanismo que visa exteriorizar a qualidade de determinado tratamento, esta certificação apenas pode ter caráter temporal pois os métodos de tratamento e a tecnologia utilizada evoluem constantemente, pelo que atribuir certificados, marcas e selos vitalícios a procedimentos e operações em que é utilizada tecnologia avançada seria esvaziar o seu conteúdo racional e lógico. Deste modo, estes certificados, marcas e selos apenas são atribuídos por um período máximo de 3 anos, renováveis pelo mesmo prazo caso se verifiquem as condições que deram origem à atribuição da certificação inicial. No entanto, pode esta certificação ser retirada

à entidade responsável pelo tratamento dos dados se os requisitos para a certificação não estiverem ou tiverem deixados de estar reunidos[34].

Para levar a bom porto este procedimento de certificação, o Comité recolhe todos os procedimentos e todos os selos e marcas de proteção de dados aprovados num registo e disponibiliza-os ao público por todos os meios adequados, publicitando-os de modo a comprovar a veracidade dos mesmos e a sua creditação face às entidades que delas disponham[35].

Apesar de a regra em matéria de competência legal para atribuição desta certificação, serem, conforme preceitua o artigo 42.º do RGPD, os Estados-Membros, as autoridades de controlo, o Comité e a Comissão, pode ser atribuído a determinados órgãos a competência para atribuição destes certificados, sempre e quando estas tenham um nível adequado de conhecimento em matéria de proteção de dados.

Esta creditação pode ser realizada pela Comissão Nacional de Proteção de Dados, ou pelo organismo nacional de acreditação, designado nos termos do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, em conformidade com a norma EN-ISO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo, conforme se encontra ancorado no n.º1 do artigo 43.º do RGPD.

Mas para esta acreditação poder ser concretizada, haverá este organismo de certificação de demonstrar, à Comissão Nacional de Proteção de Dados, a sua independência e competência em relação ao objeto da certificação; deverá de comprometer-se a respeitar os critérios de certificação aprovados pela Comissão Nacional de Proteção de Dados; deverá estabelecer procedimentos para emitir, rever e retirar certificações; haverá de estabelecer procedimentos e estruturas para tratar reclamações relativas a infração da certificação; e demonstrar perante a Comissão Nacional de Proteção de Dados que as suas funções e objetivos não dão azo a qualquer conflito de interesses[36]. Esta acreditação do organismo de certificação é realizada por um máximo de cinco anos e pode ser renovado pelas mesmas condições[37], podendo

34 Cf. Artigo 42.º n.º3 e n.º7 do RGPD.
35 Cf. Artigo 42.º n.º8 do RGPD.
36 Cf. Artigo 43.º n.º2 do RGPD.
37 Cf. Artigo 43.º n.º4 *in fine* do RGPD.

também ser revogada se as condições para a acreditação não estiverem ou tiverem deixado de estar reunidas, ou se as medidas tomadas pelo organismo de certificação violarem o presente no RGPD[38].

Sendo concedida, ou revogada determinada certificação, deve o organismo responsável por esta certificação fornecer à Comissão Nacional de Proteção de Dados os motivos que levaram à concessão ou revogação da certificação solicitada.

Com este ato de acreditação a determinados organismos concede-se uma faculdade de "delegação" das competências previstas na alínea n) do n.º1 do artigo 57.º do RGPD, para organismos terceiros que, no âmbito da atividade, estão familiarizados com a matéria de tratamento e proteção de dados pessoais, passando estas a exercer estas competências que, em regra e à partida, estão na esfera jurídica da Comissão Nacional de Proteção de Dados.

38 Cf. Artigo 43.º n.º7 do RGPD.

## 4. CONCLUSÃO

Decorridos mais de 20 anos sobre o primeiro monumento legislativo europeu derivado em matéria de proteção de dados pessoais, o novo RGPD aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, surge como uma oportunidade para o legislador europeu avançar e evoluir no seguimento da evolução das novas tecnologias e dos desafios que estas afrontam para a tutela dos dados privados e íntimos das pessoas singulares.

Com o fim de chegar a este desiderato, o legislador instituiu um conjunto de meios que permitem, de forma mais eficiente e uniforme, a aproximação a este objetivo pretendido. Do ponto de vista formal, através da regulamentação em forma de regulamento europeu, procura-se (e consegue-se) aplicar de forma uniforme e sem necessidade de transposição interna as mesmas normas jurídicas em todos os Estados-Membros da União Europeia, deixando de haver certas disparidades que naturalmente existem quando o diploma existente deriva de uma Diretiva; do ponto de vista material procurou-se instituir novas formas de regulamentação, de natureza preventiva, com vista a responsabilizar os responsáveis pelo tratamento dos dados pessoais e a reforçar a tutela destes dados antes da ocorrência de riscos e violações dos mesmos.

O êxito desta nova estratégia de regulamentação desenhada pelo RGPD irá depender da sua eficácia e, em consequência, credibilidade na garantia efetiva do direito à proteção dos dados pessoais, mas certo é que a União Europeia, com quase duas décadas de experiência nesta matéria, conseguiu com este novo Regulamento complementar os sistema jurídico instituído, criando instrumentos alternativos proactivos que completam o desenho original e que dão melhor resposta ao objeto final pretendido, que mais não é o da tutela dos dados pessoais. Com isto procurou-se combinar instrumentos de regulamentação preventiva e repressiva, com o único objetivo de concretizar o desiderato essencial pretendido.

## REFERÊNCIAS CITADAS


- ALNEMR, REHAB, *et al.*, "*A Data Protection Impact Assessment Methodology for Cloud"*, in Springer-Verlag Berlin Heidelberg, 2011, disponível em https://pdfs.semanticscholar.org/5b74/2c82769c026f9c487d4d84d46f1ff86ea061.pdf;

- CABRAL, RITA AMARAL, "O Direito à Intimidade da Vida Privada", *in Estudos em Memória do Prof. Doutor Paulo Cunha*, Lisboa, 1989;

- HERRÁN ORTIZ, ANA ISABEL, *El Derecho a la protección de datos personales en la sociedad de la información, Cuadernos Desto De Derechos Humanos,* N.º26, Universidad de Bilbao, 2002, disponível em http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf;

- JIRÁSEK, PETR, "*Non-It Perspetives Of Cyber Security By An It Professional: Challenges And Future Trends*", *in Cyberlaw by CIJIC, Edição n.º III*, fevereiro, 2017, Disponível em http://www.cijic.org/wp-content/uploads/2017/02/Cyberlaw-by-CIJIC_edicao-n3.pdf;

- MANUEL DAVID MASSENO, O novo Regulamento Geral sobre proteção de dados pessoais da União Europeia, 8º Congresso de Direito de Informática e Telecomunicações, setembro 2016, disponível em https://www.academia.edu/31981614/O_novo_Regulamento_Geral_sobre_proteção_de_dados_pessoais_da_União_Europeia?auto=download;

- PICA, LUÍS MANUEL, O direito à autodeterminação informativa dos contribuintes e a proteção dos dados pessoais em matéria tributária, Dissertação Mestrado, Universidade do Minho, Braga, 2016, disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/44452/1/Lu%C3%ADs%20Manuel%20Lopes%20Branco%20Pica.pdf;

- RALLO LOMBARTE, ARTEMI, "*Hacia un Nuevo Sistema Europeo de Protección de Datos: Las Claves de la Reforma*" in *UNED. Revista de Derecho Político* N.º 85, septiembre-diciembre, 2012, disponível http://revistas.uned.es/index.php/derechopolitico/article/view/10244/9782;

- RUIZ MIGUEL, CARLOS, "*El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Union Europea*", *in La Carta de Derechos Fundamentales de la Unión Europea: una perspetiva pluridisciplinar,* Fundación Rei Afonso Henriques, 2003, disponível em http://dialnet.unirioja.es/descarga/articulo/635290.pdf;

- SCHWABE, JÜRGEN, *Fünfzig Jahre Des Deutschen Bundesverfassungsgerichts Rechtswissenschaft,* Konrad-Adenauer-Stiftung E. V., Berlim, 2005, trad. port. de Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Geraldes Ferreira, *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão,* Fundación Konrad-Adenauer, Oficina Uruguay, Montevideo, 2005;

- SOUSA, RABINDRANATH CAPELO DE, O Direito Geral de Personalidade, Coimbra Editora, 1995.