ANDRÉ SOARES GUERREIRO

AS REGRAS VINCULATIVAS PARA EMPRESAS (*BINDING CORPORATE RULES*) NO NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: O RECONHECIMENTO DA CO-REGULAÇÃO E DO "PRINCÍPIO DA RESPONSABILIDADE" COMO MEIO PARA PASSAR DA TEORIA À PRÁTICA NA PROTEÇÃO DE DADOS PESSOAIS

Dissertação com vista à obtenção do grau de Mestre em Direito Internacional e Europeu

Orientador:

Doutor Francisco Pereira Coutinho, Professor da Faculdade de Direito da Universidade Nova

Junho de 2018

ANDRÉ SOARES GUERREIRO

AS REGRAS VINCULATIVAS PARA EMPRESAS (*BINDING CORPORATE RULES*) NO NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: O RECONHECIMENTO DA CO-REGULAÇÃO E DO "PRINCÍPIO DA RESPONSABILIDADE" COMO MEIO PARA PASSAR DA TEORIA À PRÁTICA NA PROTEÇÃO DE DADOS PESSOAIS

Dissertação com vista à obtenção do grau de Mestre em Direito Internacional e Europeu

Orientador:

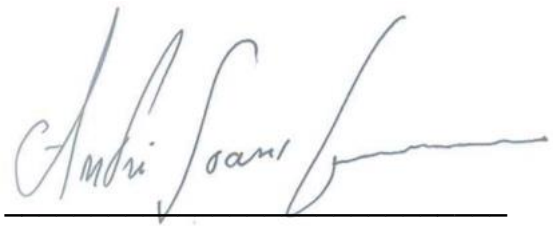
Doutor Francisco Pereira Coutinho, Professor da Faculdade de Direito da Universidade Nova

Junho de 2018

Declaração Antiplágio

Declaro por minha honra que o trabalho que apresento é original e que todas as citações estão corretamente identificadas. Mais declaro que tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 12 de junho de 2018



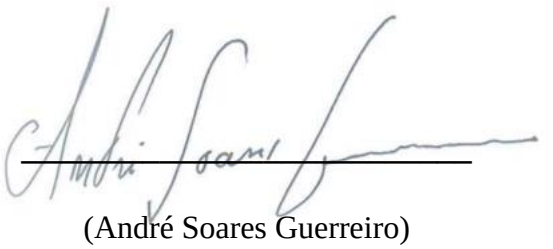
(André Soares Guerreiro)

Declaração de Conformidade do Número de Caracteres

Declaro que o corpo da tese, incluindo espaços e notas de rodapé, contém um total de 199.743 caracteres.

Mais declaro que o Resumo é composto por 2.291 caracteres e o *Abstract* 2.048 caracteres, ambos incluindo espaços.

Lisboa, 12 de junho de 2018



(André Soares Guerreiro)

Agradecimentos

Resultante do facto do elenco de agradecimentos ser algo extenso – como um filme *major* que inclui nos créditos o empregado do café que me desejou boa sorte #2 *as himself* – vejo-me obrigado a ceder à cliché fórmula do "eles sabem quem são". Prefiro, porém, disfarçar tal fórmula com o véu, conceptualmente adequado, da proteção dos dados pessoais dos visados.

Especialmente, e qual parede de museu com o nome dos mecenas, queria aqui cimentar o nome dos seguintes patronos académicos, emocionais e vivenciais.

Primeiro, queria agradecer ao Professor Doutor Francisco Pereira Coutinho, cuja orientação e ajuda na preparação desta tese foram instrumentais para a dissipação de vários pontos de interrogação que esta tese suscitava.

Ao Tiago, Tomé e Marta, por todo a paciência e incentivo simbolicamente representados em neo-imagética digital bicep: espero poder repor todos os cafés perdidos soon enough.

Aos amigos do Mestrado, por toda a ajuda e coexistência em tempos relativamente difíceis, e por todo o incentivo – ainda que por vezes traduzido em mensagens de "COMO VAI A TESE???" (Olá Mariana. Obrigado!).

À Joana, o alicerce emocional que tornou possível todo este malabarismo de afazeres e responsabilidades dos últimos meses. Que o futuro seja menos *scoop di woop* e afins. Um **obrigado** em bold para ti, apenas.

Por fim, aos meus pais, Joaquim e Sofia. Não há linguagem que conheça, nem mecanismo enfático que permita exprimir a minha gratidão.

Modos de Citar e Outros Esclarecimentos

1. O modo de citar empregado na presente dissertação observa o disposto nas Normas Portuguesas n.ºs 405-1 e 405-4, homologadas pelo Instituto Português de Qualidade.

2. As monografias, artigos e partes de livro são citadas com referência ao autor, título e página. A partir da segunda citação refere-se apenas o apelido do autor, a indicação da nota onde primeiramente se faz referência ao autor, e a página.

3. Quando as obras ou artigos tenham sido consultadas na Internet e estejam disponíveis em *site* de acesso público, os seguintes elementos constam da citação: autor, título da obra/artigo, hiperligação e data de consulta.

4. Quando a obra, artigo ou documento seja originário de uma pessoa coletiva, o nome desta substitui o do autor, nos termos acima definidos.

5. Utilizou-se o itálico para destacar palavras e expressões de língua estrangeira, latinismos e como elemento estilístico para enfatizar determinadas instâncias de *liberdade poética.*

6. As transcrições de textos em língua estrangeira encontram-se traduzidas para português. A tradução é da responsabilidade do autor da presente dissertação.

7. Relativamente às publicações do Grupo de Trabalho do Artigo 29º, algumas destas estão disponíveis em português e outras apenas em inglês. Quando o documento original referenciado está em inglês, optou-se por manter o nome do órgão nesta língua, na citação, de forma a poder demonstrar essa diferença.

8. A presente dissertação encontra-se escrita segundo as regras do novo Acordo Ortográfico.

Lista de Abreviaturas e Siglas

al.	Alínea
APEC	Cooperação Económica Asia-Pacifico
art.	Artigo
arts.	Artigos
CNPD	Comissão Nacional de Proteção de Dados
Convenção 108	Convenção Para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal
Diretiva	Directiva 95/46/CE, de 24 de outubro de 1995
EUA	Estados Unidos da América
n.º	Número
OCDE	Organização para a Cooperação e Desenvolvimento Económico
p.	Página
pp.	Páginas
Regulamento	Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679 de 27 de abril de 2016)
TFUE	Tratado sobre o Funcionamento da União Europeia
UE	União Europeia

Resumo

As constantes e imprevisíveis mutações no ambiente tecnológico comportam, não obstante os potenciais benefícios, um elenco progressivamente mais extenso de perigos para o cidadão. Acresce, a esta realidade, o facto de os dados pessoais dos cidadãos constituírem na realidade contemporânea uma "moeda de troca" *de facto* do ambiente digital, tendo as empresas evoluído de forma a fazer dos dados pessoais dos titulares o epicentro dos seus modelos de negócio.

A Diretiva 95/46/CE, por diversas razões apontadas no presente estudo, dificilmente poderia ser ainda considerado o instrumento normativo adequado para responder aos desafios acima enunciados. A desadequação funcional da Diretiva revelava-se particularmente no domínio das transferências internacionais de dados pessoais: a prevista proibição de transferências de dados para um país terceiro que não assegurasse um nível de proteção "adequado", sem a consagração expressa de mecanismos alternativos apropriados, põe em risco os princípios e os objetivos de proteção dos dados pessoais do cidadão ínsito à existência da Diretiva.

É neste contexto que surge o novo Regulamento de Proteção de Dados, cuja aplicação se iniciou no dia 25 de maio de 2018, constituindo um dos objetivos latentes deste instrumento a redução da clivagem observada entre a realidade normativa e a proteção de dados no terreno.

Uma das relevantes inovações legislativas do Regulamento, relativamente a transferências massivas e sistemáticas de dados pessoais para países terceiros, é a consagração das regras vinculativas aplicáveis às empresas. A existência de tais regras, mediante aprovação da autoridade de controlo competente, permite a transferências de dados pessoais entre as empresas de um grupo empresarial.

Na presente dissertação procura-se perceber de que forma é que as regras vinculativas aplicáveis às empresas poderão ser consideradas um mecanismo que garante a material proteção dos dados pessoais dos respetivos titulares, materializando os objetivos últimos da legislação vigente em matéria de proteção de dados. Neste sentido, atenta-se às características deste mecanismo que o definem como um esforço co-regulatório, bem como constituindo um fator relevante para o cumprimento do "princípio da responsabilidade" previsto no Regulamento.

Palavras-chave: Proteção de Dados Pessoais; Regras Vinculativas Aplicáveis às Empresas, Fluxos Internacionais de Dados Pessoais; Regulamento Geral de Proteção de Dados; Princípio da Responsabilidade; União Europeia.

Abstract

The constant and unpredictable changes in the technological landscape have determined that the list of potential dangers pertaining to the use of personal data of the data subject is ever-increasing. Furthermore, the personal data of citizens constitutes a *de facto* currency in the digital environment, with the companies shaping their business models with personal data as its core.

The Directive 95/46/CE, for various reasons outlined in this thesis, can no longer be considered the appropriate normative instrument to meet the challenges emerging in the data protection field. The functional inadequacy of the Directive was particularly apparent in the international data transfers field: the prohibition of data transfers to a third country without an "adequate" level of protection, and without establishing appropriate alternative mechanisms, jeopardizes the principles and aims underlying the existence of the Directive.

It is in this background that the new General Data Protection Regulation came into effect as of 25 May 2018, being one of its latent aims is the reduction of the chasm between normative reality and data protection on the field. One of the relevant legislative innovations of the GDPR regarding massive and systematic transfers of personal data to third countries is the legal recognition of the binding corporate rules. The existence of such rules, subject to approval by the competent control authority, allow the transfer of personal data between the undertakings of a corporate group.

In this thesis it is sought to understand why and how the binding corporate rules can be considered a mechanism that guarantees the material protection of the personal data of the data subjects, materializing the relevant purposes of the current legislation on the data protection field. In this sense, it is studied the atributtes of this mechanism that qualifies it as a co-regulatory effort, as well as a relevant factor for compliance with the "accountability principle" established in the Regulation.

Keywords: Data Protection; Binding Corporate Rules; International Data Transfers; General Data Protection Regulation; Accountability Principle; European Union.

1. Introdução

Os dados pessoais desempenham um papel extremamente relevante na configuração contemporânea do mundo globalizado: os avanços tecnológicos sustentam possibilidades infinitas de utilização e manipulação dos dados pessoais dos cidadãos que seriam impensáveis num passado recente, o que se traduziu num aumento exponencial do seu valor no ambiente digital.

O fenómeno da *Big Data*, intrinsecamente conexo à possibilidade de descobrir correlações e padrões de comportamento dos indivíduos, articulado com o fenómeno da *Internet das Coisas* - o conceito de que praticamente todos os objetos que o cidadão utiliza no seu quotidiano estão conectados à Internet e que funcionam numa rede simbiótica - demonstra a inescapável e contínua produção de dados pessoais gerada pela simples existência de um indivíduo.

Apesar dos potenciais benefícios, tais circunstâncias comportam um potencial de abuso sério, podendo traduzir-se na existência de fraudes, cibercrime e usurpação da identidade. Todavia, o potencial distópico do uso de dados pessoais do cidadão não se prende apenas com essas formas, essencialmente mais clássicas, de crime: a manipulação do aparente livre-arbítrio do cidadão é um perigo absolutamente real e infinitamente mais difícil de determinar e, consequentemente, controlar.

Com efeito, os perigos que advém das novas estruturas comerciais são fundamentalmente difusos, mais das vezes não tendo sequer o utilizador conhecimento de qualquer descriminação que teve lugar, e de que forma, e até que extensão, é que os seus dados pessoais foram o motor primário dessa decisão. A ausência do elemento físico resulta na incompreensão, por parte do cidadão, dos perigos em que a sua existência digital se desdobra. Como refere Kang, os "indivíduos hoje em dia estão extensamente desinformados quanto ao uso dos seus dados pessoais no ciberespaço"[1].

Atendendo ao exposto *statu quo*, é absolutamente essencial que o direito intervenha e regule as referidas matérias, de maneira a mitigar os potenciais efeitos nefastos das mudanças globais atuais, e procure reduzir as assimetrias de informação existentes entre as empresas e o cidadão. Um ator internacional particularmente relevante e ativo na matéria é a União

[1] Cit. por RUBINSTEIN, Ira S. - Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, p. 339.

Europeia: fatores históricos e o operacional ideário de proteção dos direitos fundamentais dos seus cidadãos e residentes como princípio enformador da sua atuação legiferante e coerciva, ditaram a existência do novo Regulamento de Proteção de Dados Pessoais[2], que revoga e substitui a Diretiva 95/46/CE.

Apesar de todos os esforços e dos aspetos positivos em que a Diretiva se traduziu, a verdade é que esta demonstrou que não basta existirem normas fortemente prescritivas para que a legislação europeia possa ter reflexo na prática: a atual clivagem entre a proteção de dados teoricamente fixada e a observação destas pelas empresas e organizações é bastante reveladora. São necessárias soluções pragmáticas que procurem o envolvimento das empresas e entidades com os meios e fins regulatórios, na demanda de soluções que se traduzam na efetiva e material proteção dos direitos dos cidadãos.

A presente dissertação tem por objeto, nesses termos, indagar sobre se as regras vinculativas aplicáveis às empresas poderão constituir um mecanismo adequado para prosseguir esses objetivos. Particularmente, procura-se compreender a evolução do conceito e de que forma é que o novo Regulamento o prevê; procura-se, igualmente, perceber de que forma é que as regras vinculativas aplicáveis às empresas poderão representar um esforço co-regulatório e que de forma é que estas estão ligadas ao princípio da responsabilidade postulado no Regulamento.

Tais preocupações modelam de forma notária a estrutura da presente dissertação. Por nos encontrarmos, à data, a viver os "entretantos", uma espécie de *terra de ninguém* legal e temporal em matéria de proteção de dados – entre o fim da vida útil da Diretiva e o início da aplicação do novo Regulamento – existem ainda muitas "áreas cinzentas" quanto aos reais efeitos das novas normas.

Tal estado embrionário de aplicação do Regulamento não obsta, de forma manifesta, aos fins da presente dissertação, na medida em que releva sobretudo perceber, no plano teórico, que materiais efeitos e finalidades prossegue este elemento legislativo. Assim, é necessário compreender a evolução quer do instituto, em termos de previsão legal e legitimidade funcional, bem como dos mecanismos de aprovação que lhe estavam subjacentes – na medida

[2] 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.

em que toda essa experiência necessariamente moldou e conduziu à atual formulação. Dessa forma, a Diretiva ainda é um instrumento relevantíssimo para o estudo por ora encetado.

O facto de o Regulamento finalmente consagrar taxativamente as regras vinculativas aplicáveis às empresas não significa, porém, de que a sua forma deverá ser final, carecendo de reformulação, como se demonstrará. Resta saber se a evolução do conceito terá de sofrer alteração da sua letra ou se bastará uma mudança na tónica interpretativa.

Explicite-se, por ora, a estrutura da presente dissertação. O capítulo 1 constitui a presente Introdução; o Capítulo 2 introduz a matéria de uma forma mais lata, descrevendo os antecedentes históricos da Diretiva que determinaram a sua introdução, bem como da descrição sumária de algumas características deste importante marco histórico na disciplina de proteção de dados, à escala global.

O Capítulo 3 elenca as mudanças de circunstâncias que ditaram a necessidade de reforma e adoção de um instrumento legislativo mais adequado para fazer face aos desafios presentes e futuros em matéria de proteção de dados. Procede-se também à identificação das mais relevantes – para os fins do presente estudo – alterações promovidas pelo novo Regulamento, procurando-se demonstrar, essencialmente, dois vetores de pensamento: primeiro, que o Regulamento não constitui uma quebra abrupta com o diploma legal anterior, como tem sido aventado; segundo, que as novidades trazidas pelo Regulamento procuram uma maior tradução prática das intenções legislativas tradicionais e a material proteção dos direitos fundamentais e liberdades dos cidadãos.

O Capítulo 4 procura enquadrar e desenvolver, primeiro em sede da Diretiva, e depois no âmbito das alterações promovidas pelo Regulamento, a matéria dos fluxos internacionais de dados. Na medida em que as disposições nesse âmbito não afastam a necessidade de aplicação dos princípios base quanto ao tratamento dos dados, visando-se tão só o efetivo cumprimento destes, mesmo quando os dados pessoais sejam alvo de transferência para fora da União Europeia, justifica-se a contraposição do regime fixado pela Diretiva, para melhor compreensão das anunciadas mudanças nesta parte específica do Regulamento. Considerou-se também relevante debruçar sobre a possibilidade de existência de um segundo caso Schrems (tendo o Acórdão Schrems I determinado a invalidade do "porto seguro" existente relativamente às transferências entre a União Europeia e os Estados Unidos) e da presente discussão quanto à invalidade das Cláusulas Contratuais-tipo. Afigurou-se necessária tal referência, atendendo aos potenciais efeitos sérios nos fundamentos legais para as

transferências internacionais de dados e o seu impacto provável nas regras vinculativas aplicáveis às empresas.

O Capítulo 5 tem como objeto direto as regras vinculativas aplicáveis às empresas. No ponto 5.1. faz-se uma súmula da noção e história deste mecanismo que permite, dentro de um grupo empresarial, a transferência legítima de dados para uma empresa estabelecida fora da União Europeia. Descreve-se o anterior sistema de aprovação das regras vinculativas aplicáveis às empresas, demonstrando as suas falhas, explicando-se assim as prováveis razões para a limitada exploração deste, apesar das significativas valências.

No ponto 5.2. apresentam-se os requisitos gerais que necessariamente deverão constar das regras vinculativas aplicáveis às empresas. Pela sua relevância e maior número de ónus a observar, optou-se por fazer referência exclusiva aos requisitos que deverão constar das regras vinculativas aplicáveis às empresas para responsáveis pelo tratamento. Tal decisão de expor os requisitos surge do facto de o Grupo de Trabalho do Artigo 29 (grupo independente que é composto, essencialmente, por membros das autoridades de controlo dos vários Estados-Membros – portanto, as entidades que irão, na prática, autorizar as regras vinculativas aplicáveis às empresas) ter já publicado documentos de trabalho que densificam os requisitos presentes no Regulamento, sendo tal articulação necessária para a compreensão efetiva do escopo de composição das regras vinculativas aplicáveis às empresas.

No ponto 5.3. procura-se caracterizar as regras vinculativas aplicáveis às empresas como exemplificativas de um fenómeno de co-regulação. Atenta-se, neste âmbito, ao enquadramento da co-regulação na moldura legal europeia e aos benefícios que a introdução deste tipo de mecanismos poderá representar na prática, por oposição à legislação prescritiva clássica, neste específico campo do direito.

O ponto 5.4. da presente dissertação tem por finalidade a demonstração das regras vinculativas aplicáveis às empresas como corolário do princípio da responsabilidade ("*accountability")* positivado no novo Regulamento. Para esse efeito, examina-se o regime fixado em termos de responsabilidade, e o que é este significa, relativamente às obrigações que deverão ser observadas pelas entidades envolvidas no tratamento de dados, e de que forma é que este se articula com as regras vinculativas aplicáveis às empresas.

No ponto 5.5. procura-se perceber de que forma é que as regras vinculativas aplicáveis às empresas poderão contribuir para um padrão global de proteção de dados, bem como se sugerindo potenciais vias evolutivas do conceito.

O Capítulo 6 encerra a presente dissertação, apresentando-se as conclusões do estudo prosseguido.

2. A Diretiva 95/46/CE: os Antecedentes da Proteção de Dados Pessoais no Direito da União Europeia

Na sequência do período de reestruturação e cicatrização identitária e institucional que surgiu no pós-2ª Guerra Mundial, começou a aflorar no consciente coletivo do legislador europeu a necessidade de consagrar na lei um "direito à vida privada".

Atendendo ao facto de muitas das tragédias e atrocidades observadas na Segunda Guerra Mundial terem advindo da existência de amplas bases de dados com dados pessoais de um igualmente relevante número de pessoas, instrumentais para a discriminação de minorias e mecanismo essencial do genocídio, tornou-se manifesta a necessidade de existência de mecanismos legais que procurassem impedir a intrusão de governos e elementos do poder na esfera privada dos cidadãos[3].

Michael Kirby, juiz australiano que liderou o grupo de trabalho encarregado de produzir as Diretrizes da Organização para a Cooperação e Desenvolvimento Económico para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais[4] (doravante, Diretrizes da OCDE), descreve os contundentes argumentos de um elemento do público numa conferência promovida pelo referido grupo de especialistas, dirigindo-se ao então presidente da República Francesa, Valéry Giscard d'Estaing:

"*Sr. Presidente, porque sobreviveram tantos refugiados em França durante a Guerra? Porque sobreviveram tão poucos combatentes da resistência e Judeus na Holanda?", disse ele. "Assim aconteceu porque, na década de 1930, o governo holandês, com a eficiência característica, tinha concebido um cartão de identidade com uma barra de metal instalada através da fotografia. Este era então o mais recente em tecnologia segura. Na França, tínhamos uma simples fotografia, colada em cartão. Era facilmente imitado. Nessa diferença, penderam as vidas de milhares de boas pessoas. Na França, sobreviveram. Na Holanda pereceram. A*

[3] RAND REPORT – Review of the European Data Protection Directive, p. 6.

[4] OECD – Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980) Disponível em:<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> [consultado em 26/04/2018].

eficiência não é tudo. Uma sociedade livre defende outros valores. O controlo pessoal sobre dados é um desses valores"[5].

Os argumentos acima aduzidos demonstram bem o *statu quo* do pós-guerra, e da prevalência da necessidade de um certo protecionismo do cidadão individual contra a possibilidade da ingerência governamental. Tal mentalidade acabou por permear o texto de vários instrumentos legislativos, internacionais e europeus, da época: tanto a Declaração Universal dos Direitos Humanos[6] de 1948, a Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais de 1950[7], como o Pacto Internacional dos Direitos Civis e Políticos[8] de 1966, taxativamente reconhecem nos seus respetivos textos o direito a não ser objeto de qualquer intrusão arbitrária e ilegal na sua vida privada.

Enquanto estes instrumentos tinham por objeto (face à *ratio* inerente à sua origem) limitar a potencial ingerência de autoridades públicas, os desenvolvimentos tecnológicos, nomeadamente o cada vez mais avultado uso de tecnologias de informação observado na década de 70, permitiram o acesso cada vez mais fácil a empresas e outras entidades do sector privado a dados pessoais de clientes e funcionários, acoplado de fundados receios quanto ao seu potencial abuso.

Tais preocupações quanto ao potencial uso indevido (irrelevante, para o efeito, se por negligência ou atuação dolosa) por parte de entidades do sector privado de dados pessoais dos cidadãos, articuladas com a necessidade de densificar o escopo regulatório dos instrumentos internacionais referidos – a mera referência a "proteção da vida privada" não sendo já suficiente para garantir um nível de proteção adequado, constituindo uma mera declaração de intenções sem observação prática – funcionaram como catalisador para uma nova vaga legislativa quanto

[5] KIRBY, Michael – The history, achievement and future of the 1980 OECD guidelines on privacy, p. 9.
[6] Declaração Universal dos Direitos Humanos promulgada pelas Nações Unidas em 10 de dezembro de 1948 na Resolução 217. Disponível em: http://www.un.org/en/universal-declaration-human-rights/ [consultado em 26(04/2018].
[7] Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 4 de novembro de 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf [Consultado a 26/04/2018].
[8] Pacto Internacional dos Direitos Civis e Políticos de 16 de dezembro de 1966, ratificação e adesão pela resolução 2200-A da Assembleia Geral das Nações Unidas. Disponível em www.nanowrimo.org/en/forums/europe-portugal/threads/61945 [Consultado a 26/04/2018].

ao respeito da vida privada, materializada na limitação das operações de tratamento automatizados de dados pessoais – a génese da proteção de dados pessoais[9].

Dessa nova vaga, para além de várias leis nacionais[10] e das Diretrizes da OCDE – sendo que a primária razão de existência destas diretrizes era a regulação dos fluxos transnacionais de dados pessoais, ainda que de uma perspetiva económica e não de direitos humanos e liberdades fundamentais– emergiu em 1981 a Convenção Para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, comummente designada por Convenção 108[11], promulgada pelo Conselho de Europa, tendo atualmente 51 países signatários[12].

A Convenção 108 constitui um marco histórico relevante no domínio da proteção de dados, por ser o primeiro instrumento internacional vinculativo destinado a garantir a proteção dos "dados de carácter pessoal" de todas as pessoas singulares que se encontrem no território das partes signatárias, independentemente da nacionalidade e residência, de forma a prover pelo respeito pelos seus direitos e liberdades fundamentais, em especial o direito à vida privada (art. 1º).

A Convenção define "dados de carácter pessoal" como qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação (art. 2º, al. a)).

A Convenção 108 procura, essencialmente, conciliar a proteção que se deve garantir aos cidadãos, nos termos acima aduzidos, e a livre circulação dos fluxos de informação[13] (onde, necessariamente, se integram os dados pessoais). Esta aplica-se tanto ao setor privado quanto ao público (art. 3º, n.º 1).

De forma a alcançar um equilíbrio funcional entre tais imperativos, a Convenção prescreve um número de princípios base que deverão necessariamente constar das legislações nacionais dos respetivos Estados-parte (art. 4º).

[9] Nesta altura a proteção de dados ainda não era configurada, portanto, como um direito autónomo, mas como uma derivação do direito à privacidade e reserva da vida privada adaptada à emergente industrialização tecnológica.

[10] Países como o Reino Unido, Suécia, Alemanha e França adotaram legislação que refletia uma embrionária preocupação relativamente a questões de proteção de dados.

[11] Disponível em https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm [Consultado em 27/04/2018].

[12] GREENLEAF, Graham - Data protection Convention 108 accession eligibility: 80 Parties now possible, p. 1.

[13] *Cfr.* Preâmbulo Convenção 108.

Vários princípios fundamentais que viriam a fazer parte da Diretiva 95/46/CE tiveram a sua génese neste instrumento: o princípio da legitimidade do tratamento, a restrição de tratamento de dados pessoais que não sejam compatíveis com as finalidades para os quais foram recolhidos, o direito de acesso e retificação por parte dos titulares dos dados, entre outros. Também a possível limitação de fluxos transnacionais de dados para países terceiros (no caso, Estados não contratantes) foi conceptualizada pela primeira vez neste instrumento.

Apesar de a Convenção ter sido instrumental na forma como trouxe para a superfície política e legislativa dos Estados signatários preocupações quanto à proteção dos dados pessoais dos cidadãos e ter delineado princípios e uma estrutura legal que ainda hoje sustêm a legislação vigente nesta matéria, determinadas circunstâncias obstaram ao seu completo sucesso.

Cumpre referir que esta Convenção carecia de efeito direto nas ordens jurídicas estaduais, não criando diretamente direitos para as pessoas singulares, nem poderia ser judicialmente invocada contra entidades privadas; cabia aos Estados implementar na esfera legal interna as disposições nela consagradas.

No fundo, o seu sucesso e material proteção dos direitos das pessoas singulares encontrava-se diretamente conexo à implementação prática que lhe devia ser dada pelos Estados signatários. Ora, alguns Estados-Membros implementaram a Convenção de forma tardia, e outros impuseram, inclusivamente, restrições aos fluxos de dados, mesmo entre Estados-Membros[14].

Tal implementação inconsistente da Convenção pelos Estados-Membros signatários naturalmente feriu de insucesso os objetivos deste instrumento, na medida em que o seu sucesso essencialmente dependia da concertação de esforços e dos impulsos regulatórios entre os seus membros; tal fragmentação obstava, de forma manifesta, ao desenvolvimento do mercado interno do qual os tratamentos de dados pessoais iriam ser pedra basilar[15].

Foi a necessidade de harmonizar os regimes de proteção de dados praticados na União Europeia, face ao esperado incremento significativo de fluxos de dados pessoais entre os Estados-Membros resultante do estabelecimento e funcionamento do mercado interno

[14] HUSTINX, Peter - EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, p. 128.
[15] *Ibidem*, p. 9.

(considerando 3,5 e 7 da Diretiva) que enformou a emergência de adoção da Diretiva 95/46/CE[16].

Esta Diretiva tem, do ponto de vista regulatório, uma natureza mista/híbrida que se manifesta em variados quadrantes. Primeiro, nela coexistem normas de direito público e de direito privado; segundo, tal heterogeneidade é também visível em relação aos objetivos da Diretiva. Tal como a Convenção 108, a Diretiva, por um lado, serve uma função económica ao promover o livre fluxo de dados e, por outro, serve propósitos sociais e éticos, ao prover pela proteção dos direitos fundamentais do cidadão.

O âmbito de aplicação da Diretiva é bastante amplo na medida em que se aplica ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados (art. 3º).

Quanto aos princípios nela consignados, a Diretiva recupera os princípios-base já presentes na Convenção 108, mas surgem *ex novo* seis princípios que legitimam o tratamento de dados, a saber: o consentimento inequívoco do titular dos dados; ser necessário para a execução do contrato do qual o titular dos dados é parte ou diligências pré-contratuais; ser necessário para cumprimento de obrigação legal; ser necessário para a proteção dos interesses vitais do titular dos dados; ser necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública; ou o tratamento ser necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa (art. 7º).

Impõe-se também fazer uma breve referência[17] à proibição de transferências de dados para países terceiros (i.e., que não sejam Estados-Membros ou membros do Espaço Económico Europeu) que não tenham um "nível de proteção adequado" (considerando 57 e art. 25º).

Embora tal princípio esteja sujeito às derrogações previstas no art. 26º, foi diversas vezes documentado o efeito que este teve à escala mundial, sendo argumentado que este constitui uma das principais razões pela qual o sistema europeu tanto influenciou outras jurisdições. Vários países terceiros na procura de uma decisão de adequação, de forma a terem

[16] Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[17] Breve porque tal matéria será objeto de capítulo autónomo no presente estudo (*cfr.* Capítulo 4.)

mais fácil acesso ao relevante mercado europeu, replicaram as regras europeias da forma mais extensa possível.

Lynskey avança, porém, que "*a proliferação global de regimes como o da União Europeia é defensavelmente, portanto, mais um ato de pragmatismo do que um apoio implícito do regime da União Europeia*"[18].

Lynskey define também esta situação como "s*upremacia por defeito, em vez de supremacia por conceção*"[19], na medida em que tal hegemonia *de facto* constituiu um desenvolvimento orgânico, não necessariamente prosseguido pelas regras europeias de proteção de dados. Apesar de acusações de protecionismo e paternalismo regulatório[20], a verdade é que o efeito extraterritorial da Diretiva decorria necessariamente da necessidade de proteger os cidadãos e a concreta realidade dos dados pessoais destes serem comummente objeto de fluxo internacional.

Apesar de todos os benefícios e relevância da Diretiva, inclusive a nível do panorama global na área de proteção de dados, várias circunstâncias – desde circunstancialismos contemporâneos a problemas estruturais – determinaram a desadequação *funcional* da Diretiva durante a sua vida útil.

A necessidade de reforma e o Regulamento que daí resultou é objeto de estudo no próximo capítulo.

[18] LYNSKEY, Orla – The Foundations of EU Data Protection Law, p. 43.
[19] *Ibidem*.
[20] BERGKAMP, Lucas - The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy, p. 37.

3. A necessidade de reforma e o Novo Regulamento de Proteção de Dados Pessoais

3.1. Considerações gerais

Embora um elemento fulcral na decisão de implementar a Diretiva tivesse sido o incremento esperado do volume de fluxo de dados por motivos do mercado interno, nada fazia prever as profundas transformações no tecido societário promovidas pela globalização, com os dados pessoais como matéria prima das novas estruturas de funcionamento das relações comerciais e pessoais estabelecidas no mundo contemporâneo. O crescimento exponencial e atual escala das operações de tratamento é, como referido, estritamente proporcional às consequências nefastas do seu abuso.

Face à hodierna proliferação dos riscos que o indevido uso de dados pessoais poderá representar, é cada vez mais difícil apreciar positivamente o *trade-off* existente entre a proteção dos direitos fundamentais dos cidadãos e o objetivo de não influir significativamente no mercado (de forma a que não prejudique a inovação e o desenvolvimento económico).

Aliado ainda ao facto de grande parte dos danos que possam ser consequência das operações de tratamento de dados pessoais serem, na sua maioria, intangíveis e inquantificáveis, necessário se torna que o direito da União acompanhe e esteja preparado para responder a estes desafios. Dúvidas surgiram se a Diretiva ainda seria o instrumento legislativo adequado para garantir os direitos nela consignados.

Vários fatores indicavam para que a Diretiva não seria flexível o suficiente para tender aos desafios enunciados, principalmente no contexto cada vez mais internacional das questões.

Releva lembrar que na altura da entrada em vigor da Diretiva, o *Google* ainda não existia e apenas 1% da população mundial tinha acesso à Internet[21].

Acresce ao quadro factual acima apresentado a falta de transparência e controlo sentida pelos cidadãos no ambiente digital, em que os titulares dos dados desconhecem que dados estão a sacrificar pelo seu acesso a bens e serviços apresentados como "gratuitos". Os próprios

[21] LYNSKEY, Orla – cit. 18, p. 4.

desenvolvimentos tecnológicos, como a computação na nuvem[22], não permitem ao titular dos dados saber exatamente onde se encontram os seus dados e quem teve acesso aos mesmos.

As próprias estruturas das empresas e o funcionamento destas, nomeadamente a nível das cadeias contratuais, sofreram profundas alterações. As organizações estão incrementalmente mais complexas, desenvolvendo relações comerciais igualmente intrincadas, não sendo claro como se distribui equilíbrio de poder nas estruturas verticais e de subcontratação das empresas.

A globalização dos serviços e o motor funcional da competição resultando num mais variado leque de opções estratégicas na procura de maximização de lucro, permite que os dados pessoais sejam movidos para onde sejam mais eficientes para a organização em causa, não resultando absolutamente claro onde esta se encontra e que lei é aplicável.

Foi na tentativa de modernizar e tornar mais efetivo o regime de proteção dos cidadãos europeus quanto ao tratamento dos seus dados pessoais que foi introduzido o Regulamento 2016/679, aplicável a partir de 25 de maio de 2018 (doravante, Regulamento).

A escolha do instrumento do Regulamento por oposição a uma nova e revista diretiva, como inicialmente discutido, reveste uma importância determinante face aos demonstrados desafios.

Apesar de, como demonstrado previamente, um dos motivos subjacentes à adoção da Diretiva ter sido a inoperante fragmentação observada a nível da transposição dos Estados-signatários da Convenção 108 - que frustrava o pleno funcionamento do idealizado mercado interno europeu - a verdade é que este problema não foi verdadeiramente solucionado, particularmente quando considerada a nova realidade globalizada em que a proteção de dados se insere. Atendendo ao facto de a implementação da Diretiva por parte dos Estados-Membros ter sido relativamente diversificada, pelo espaço de manobra concedido por esta, empresas a atuar à escala europeia tinham que corresponder a um complexo mosaico de leis e de cumprir requisitos diferentes dos Estados-Membros – o que provocou que, na prática, tais requisitos e disposições legais fossem totalmente ignoradas.

[22] Tecnologia que permite que os dados não estejam armazenados fisicamente numa dada localização, encontrando-se disseminados por várias localizações na rede, sem localização estável dentro dos seus serviços.

Ainda hoje é possível perceber que, para as empresas nacionais, é muitas vezes o ato de notificação do tratamento à autoridade de controlo que é visto como a principal obrigação em matéria de proteção de dados, e não o respetivo tratamento, o real objeto de previsão[23].

O problema de aplicação de diferentes leis encontra-se, na sua maior parte, resolvido, através da escolha do mecanismo legal de um regulamento. Tratando-se de um regulamento, não carecendo de implementação a nível nacional[24], o que acaba por facilitar o *compliance* das empresas e organizações, promovendo a harmonização pretendida. Os efeitos dessa articulação e da aplicação do mesmo regime poderão também repercutir-se na esfera dos cidadãos, devido à maior segurança jurídica existente.

O simples facto de o Regulamento, pela sua natureza regulatória, prescrever um regime unificado de proteção de dados pessoais é, por si, um fator já extremamente relevante, como referido. Pretende-se, assim, sintonizar o regime jurídico com a realidade prática do objeto de previsão legal.

Encontra-se fora do escopo do presente estudo a cabal identificação de todas as alterações provocadas pelo Regulamento no panorama de proteção de dados a nível europeu; porém, serão abordadas as mais significativas transformações operadas no âmbito do objeto de estudo prosseguido no presente trabalho.

3.2. O novo Regulamento: inovação e continuidade

Desde logo, importa referirmo-nos ao âmbito material e territorial do Regulamento. Como já decorria do regime fixado na anterior Diretiva, o Regulamento tem uma faceta tecnologicamente neutra, i.e., tanto se aplica ao tratamento de dados pessoais por meios automatizados (uma base de dados, por exemplo) tal como a qualquer outro meio, ainda que não automatizado, de organizar dados pessoais (considerando 15 e art. 2º, n.º 1) – tal como, por hipótese, a *dossiers* organizados de informação sobre clientes.

[23] Entendimento perfilhado por vários autores, como Hustinx (cit. 14, p. 130), e que tive hipótese de confirmar através da minha experiência como advogado estagiário.

[24] Sem prejuízo das disposições do Regulamento relativas a situações específicas de tratamento, como o tratamento de dados pessoais no contexto laboral ou quanto às obrigações de sigilo, que possibilitam a densificação normativa nacional (*cfr.* arts. 85º a 91º).

A principal novidade, neste âmbito, prende-se com o alargar do âmbito territorial no campo da proteção de dados. Enquanto a ora revogada Diretiva requeria um elemento físico de conexão à União Europeia – quer seja na presença de estabelecimento ou de meios de tratamento nesta – o Regulamento introduz a vinculação de qualquer empresa, em qualquer parte do mundo, às regras e princípios europeus de proteção de dados, desde que esta ofereça bens ou serviços a residentes na União ou monitorizem o comportamento de residentes na União Europeia, desde que o comportamento tenha lugar na União (art. 3º, n.º 1 al. b)).

Assim sendo, as transferências de dados por empresas não sediadas na Europa para empresas europeias, ou empresas estabelecidas fora da União que processem dados pessoais de europeus estarão sujeitas aos mecanismos previstos no Regulamento. Procura-se, assim, a adaptação da legislação vigente em matéria de proteção de dados à realidade vivida na Internet e no ciberespaço, como se uma pulseira eletrónica dos dados se tratasse. Embora tal aplicação extraterritorial seja criticada em várias instâncias[25] , a verdade é que o legislador europeu não poderia permitir qualquer fuga à lei, pelo simples facto do responsável pelo tratamento/subcontratante[26] se encontrar estabelecido fora da Europa – tal obstaria à procura de uma efetiva proteção do cidadão europeu.

Outros académicos argumentam, porém, que esta é uma disposição realista e que não há razões para duvidar do efeito positivo na alteração do *statu quo* quanto à proteção de dados nos países terceiros, à semelhança da Diretiva[27].

Um dos argumentos para este potencial efeito positivo é, como por ocasião da Diretiva, um argumento pragmático decorrente do poder de mercado da União:

"*O poder combinado de mercado de 500 milhões de consumidores no mercado europeu ajudará também a assegurar o cumprimento"*[28].

Lynskey, ao contrário do que acontecia na Diretiva em que dizia que a influência desta refletia uma "supremacia por defeito", quanto à positivação do âmbito territorial do Regulamento por ora demonstrado, sugere que constitui um exemplo de "supremacia por conceção"[29].

[25] BERGKAMP - cit. 20, p.43.
[26] Definição destas duas figuras constante da página 29 da presente dissertação.
[27] HUSTINX - cit. 14, p. 153.
[28] HUSTINX - cit. 14, p. 158.
[29] LYNSKEY - cit. 18, p. 43.

O Grupo de Trabalho do Artigo 29[30], na sua opinião "O Futuro da Privacidade"[31], quanto à necessidade de um novo enquadramento jurídico, refere que "*os princípios existentes de proteção de dados precisam de ser apoiados e complementados com medidas que executem estes princípios de forma mais eficaz (e para assegurar uma mais eficaz proteção dos dados pessoais dos cidadãos)*"[32].

E é isto precisamente o que acontece em sede do novo Regulamento: os princípios clássicos de proteção de dados mantêm-se intactos, sendo adicionalmente legitimados; tais princípios são, simplesmente, alvo de esclarecimento quanto a algumas particularidades casuísticas da aplicação.

O Grupo de Trabalho reitera que:

"*A mensagem central é a de que os princípios fundamentais da proteção de dados são ainda válidos apesar destes importantes desafios. O nível de proteção de dados na União Europeia pode beneficiar de uma melhor aplicação dos princípios existentes de proteção de dados praticados"*[33].

Isto não significa, porém, que é despiciente a alteração legislativa feita. No fundo, e tal encontra-se refletido no texto do Regulamento, os princípios e disposições gerais da Diretiva mantêm a sua atualidade; simplesmente os mecanismos que esta prescrevia não demonstraram assegurar a observação na prática dessas realidades teóricas, não tendo criado uma cultura de cumprimento *de facto* e material proteção dos direitos fundamentais dos cidadãos. Novos mecanismos foram contemplados, antigos princípios tiveram a hipótese de ser esclarecidos, e novas estratégias legislativas foram delineadas para procurar a aplicação efetiva destes princípios.

Quanto aos princípios, como já foi dito, o Regulamento mantém a previsão de uns, esclarecendo os requisitos de outros. Por exemplo, sob a égide do novo Regulamento, o consentimento é mais difícil de obter, sendo que o consentimento tem, necessariamente, de ser

[30] O Grupo de Trabalho do Artigo 29 é um grupo de trabalho independente, com caráter consultivo, composto pelas autoridades de proteção de dados dos Estados-Membros, por um representante das autoridades criadas para os organismos comunitários e por um representante da Comissão Europeia. O seu nome deriva do artigo da Diretiva que legitimou à sua criação.

[31] ARTICLE 29 DATA PROTECTION WORKING PARTY – WP168 The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.

[32] *Idem, ibidem*, para. 15.

[33] *Idem, ibidem*, para. 8.

prestado através de um ato positivo, inequívoco e informado. O consentimento tácito, prestado através de silêncio ou omissão – nomeadamente as opções pré-validadas – deixa de ter qualquer validade (considerando 32).

A Diretiva procura também resolver as assimetrias de informação e de poder nas relações comerciais existentes em matéria de proteção de dados, dispondo que, caso se verifique um manifesto desequilíbrio entre o titular e o responsável pelo tratamento dos dados, o consentimento presume-se que não foi prestado de livre vontade (considerando 43).

Um claro exemplo do mencionado desequilíbrio é, por hipótese, se um contrato vincular o titular dos dados a permitir o tratamento de dados que não são estritamente necessários para a execução desse contrato (art. 7º, n.º 4). Atendendo a tal facto, o tratamento posterior desses dados seria ilícito.

De forma análoga, também a Diretiva descreve o consentimento como tendo que constituir uma demonstração de vontade informada, apesar de não elucidar de que forma é que se operacionaliza esse conceito; o mesmo não acontece no Regulamento. Em sede deste diploma, os responsáveis pelo tratamento deverão formular uma declaração de consentimento inteligível e de fácil acesso, em linguagem simples e clara (considerando 42).

O titular dos dados deverá ser também informado do direito que lhe assiste de, a qualquer momento e sem qualquer tipo de entrave e/ou repercussão negativa, poder retirar o consentimento previamente dado (art. 7º, n.º 3). A retirada do consentimento não afeta a licitude do tratamento feito antes desse ato unilateral do titular dos dados.

Fixa também o Regulamento que quando o consentimento for dado no contexto de uma declaração escrita que envolva outros assuntos, o pedido de consentimento do titular de dados deverá ser apresentado de uma forma que claramente o distinga desses outros assuntos, sob pena do consentimento prestado nestes termos não ser vinculativo (art. 7, n.º 2). Daqui que se infere que, a título de exemplo, o pedido de consentimento não deverá constar do corpo de uma lista de termos e condições, sem estar devidamente assinalado de forma clara, simples e inteligível.

Releva também o facto de ser sobre as empresas que impende o ónus de prova quanto ao consentimento, devendo estas poder demonstrar que ao tratamento de dados empreendido está subjacente o consentimento válido do respetivo titular dos dados (art. 7, n.º 1), nos termos já descritos.

Tais esclarecimentos quanto ao conceito e aplicação do mecanismo do consentimento como fundamento legal de determinadas operações de tratamento, como já se aflorou, são excelentes exemplos da tentativa implicitamente enunciada no Regulamento de reduzir as assimetrias de informação existentes entre o titular de dados e do responsável pelo tratamento.

O objetivo de redução de assimetrias, de forma a corrigir as deficiências na distribuição de recursos num dado sistema de mercado é, por excelência, um objetivo de regulação de cariz económico: como já dito no presente estudo, um dos elementos que integra o *adn* da regulação da proteção de dados.

A redução de assimetrias entre o titular de dados e do responsável pelo tratamento também é um objetivo prosseguido na outorga de direitos aos titulares dos dados.

Os direitos dos titulares dos dados existentes na revogada Diretiva, foram todos confirmados em sede do novo Regulamento, e ao mesmo tempo estendidos e reforçados[34].

Um exemplo disso, e indicador de uma reveladora modificação da tónica da responsabilidade no Regulamento, encontra-se consubstanciada no direito de oposição ao tratamento. No novo Regulamento não é já o titular dos dados – ao contrário do que acontecia na Diretiva – que tem de demonstrar o interesse legítimo que justifique a sua oposição, mas é o responsável pelo tratamento quem tem de demonstrar o interesse fundado na operação de tratamento em causa (considerando 69).

O legislador europeu assegura assim a efetiva proteção dos cidadãos mesmo quando (e é, muitas vezes, infelizmente, o caso) a literacia em termos de privacidade no ambiente digital dos titulares dos dados é extremamente limitada; mesmo quando os titulares dos dados, no decurso do seu quotidiano, não exerçam qualquer medida de proteção dos seus dados pessoais.

Foi já argumentado que, no novo Regulamento "*a ênfase está claramente a mudar dos direitos da pessoa em causa para os deveres dos responsáveis pelo tratamento.*"[35]. Também tem sido reiterado que "*o foco está claramente a mudar para a questão «o que deverão fazer os responsáveis pelo tratamento», da questão de saber «quais os direitos do titular dos dados»*"[36].

[34] HUSTINX - cit. 14, p. 128.
[35] KISS, Attila e SZOKE, Gergely – Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation, p. 312.
[36] *Idem, ibidem*, p. 328.

Demonstrou-se assim, que apesar do pânico generalizado no mundo empresarial na antecipação do novo Regulamento, que se deve concordar com o postulado por Peter Hustinx[37] quando afirma que "*apesar de toda a inovação – há muita continuidade*"[38].

Resta-nos observar mais instâncias de novidade, fazendo uma breve referência a algumas das novas características.

Embora, como referido, o Regulamento tenha reforçado a legitimidade de vários princípios e principais mecanismos constantes da Diretiva, existem novidades neste âmbito: como o princípio da transparência, o princípio da minimização de dados e a consagração da segurança do tratamento dos dados como princípio, na tentativa de integrar os esforços tecnológicos na procura de uma solução holística para uma mais efetiva proteção dos dados pessoais das pessoas singulares.

Face ao ónus que recai sobre os responsáveis pelo tratamento quanto à demonstração e envio ao respetivo titular dos dados da informação quanto aos dados que detêm sobre este, surge consequentemente a necessidade do tratamento se pautar pelo princípio da transparência (articuladamente, os considerandos 39, 58 e 60 e arts. 5º, n.º 1 al. a) e 12º, n.º 1).

A aplicação, na prática, deste princípio significa que as informações a serem transmitidas ao titular dos dados deverão ser de fácil acesso e em linguagem simples e clara. Significa também que, nos mesmos termos, os responsáveis pelo tratamento deverão alertar os titulares dos dados para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e os meios de que tem ao seu dispor para exercer e salvaguardar os seus direitos.

Os responsáveis pelo tratamento deverão também respeitar o princípio de minimização do tratamento de dados, determinando o Regulamento que o tratamento de dados deverá cingir-se ao mínimo indispensável à prossecução da finalidade invocada para o específico tratamento de dados. Assim sendo, os responsáveis pelo tratamento não deverão recolher dados que não sejam fundamentais às finalidades e objetivos previamente traçados para o tratamento de dados pessoais efetuado.

Uma última novidade neste âmbito é a consagração da segurança do tratamento dos dados que, embora constituísse um mecanismo já presente na Diretiva, é por ora consagrado

[37] Anterior European Data Protection Supervisor.
[38] HUSTINX - cit. 14, p. 144.

como princípio (art. 5º, n.º 1 al. f)), decorrente da importância nuclear que assume. Em sede deste princípio, os responsáveis pelo tratamento deverão implementar medidas técnicas e organizativas eficazes e adequadas à proteção dos dados contra acessos não autorizados, perda ou destruição destes.

Os já referidos avanços tecnológicos verificados desde a vigência da Diretiva, nomeadamente, o uso global da Internet que acabou por representar o uso de nuvens de dados, a democratização das operações de tratamento de dados permitindo o acesso a empresas a dados pessoais com custos reduzidos, tornaram efetivamente complicado perceber e alocar responsabilidades dentro das múltiplas e interconectadas relações comerciais (*supply chain*).

A Diretiva não estava preparada para os desenvolvimentos nas relações comerciais subjacentes aos fluxos de dados pessoais: tal facto é perfeitamente exemplificado através da previsão de responsabilidade única do responsável pelo tratamento.

O responsável pelo tratamento (definições que primeiro constaram da Diretiva e que foram posteriormente mantidas no Regulamento) é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais (art. 4º, n.º 7); o subcontratante é uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trata os dados pessoais por conta do responsável pelo tratamento destes (art. 4º, n.º 8).

Na Diretiva apenas o responsável pelo tratamento estava adstrito a toda e qualquer responsabilidade pelos danos sofridos pelo titular dos dados (art. 23º) no âmbito do tratamento de dados pessoais. Embora o responsável pelo tratamento pudesse ilidir tal presunção, demonstrando que determinado dano ou prejuízo não lhe pode ser imputado (art. 23º, n.º 2), a verdade é que não existia qualquer disposição que permitisse ao titular dos dados responsabilizar diretamente o subcontratante (art. 23º, n.º1 *a contrario*), pondo – por exemplo – uma ação em tribunal contra este. O subcontratante apenas incorria em responsabilidade contratual, tendo o responsável pelo tratamento direito de regresso sobre este.

Ora, essa ausência de responsabilidade direta não é adequada no atual panorama empresarial, como refere Purtova:

"[O] *sistema atual, que assenta na responsabilização dos responsáveis pelo tratamento, não motiva os intervenientes que não podem ser classificados inequivocamente como responsáveis pelo tratamento a agir no sentido de assegurar um nível adequado de proteção de dados"*[39].

O Rand Report também identifica as definições das entidades relacionadas com o tratamento de dados pessoais como "*simplista e estático"*[40], constituindo uma das mais relevantes falhas da Diretiva, mais dizendo que "*a relação entre o subcontratante e o responsável pelo tratamento prevista na Diretiva não cobre adequadamente todas as entidades envolvidas no tratamento de dados pessoais numa moderna economia em rede"*[41].

Para fazer face à desadequação formal e funcional dos conceitos e da correspondente responsabilidade passível de ser assacada, o Regulamento prescreve a possibilidade de existir mais que um responsável pelo tratamento em relação a determinadas operações de tratamento e que poderão responder conjuntamente por qualquer dos danos que daí resultem.

Caso haja responsáveis conjuntos pelo tratamento, deverão estes definir por acordo, de forma transparente, as responsabilidades que cabem a cada um relativamente ao cumprimento das obrigações decorrentes do Regulamento, principalmente quanto ao exercício dos direitos do titular dos dados e aos deveres de prestar as informações aquando da obtenção dos dados pessoais dos titulares (art. 26º, n.º 1). O essencial deste acordo deverá ser disponibilizado ao titular dos dados (art. 26º, n.º 2).

Independentemente do teor e conteúdo do acordo estabelecido entre os responsáveis conjuntos pelo tratamento, o titular dos dados poderá exercer os direitos que o Regulamento prevê em relação a qualquer um dos responsáveis pelo tratamento (art. 26º, n.º 3), nomeadamente em matérias indemnizatórias. Assim, os titulares dos dados poderão obter de um responsável pelo tratamento indemnização integral dos danos causados pelo tratamento em causa, sem prejuízo da existência de um direito de regresso desse responsável pelo tratamento em relação a outro responsável pelo tratamento que conjuntamente tenha participado no tratamento de dados ou de qualquer subcontratante (considerando 146).

O Regulamento prescreve também várias obrigações diretamente aplicáveis ao subcontratante, como o dever de cooperar com a autoridade de controlo (considerando 82), o

[39] PURTOVA, Nadezhda – Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence, p. 47.
[40] RAND REPORT - cit. 3 p. 36
[41] *Ibidem.*

dever de manter documentação demonstrativa dos registos de atividades de tratamento sob a sua responsabilidade (considerando 82), entre outros.

3.3. A abordagem baseada no risco como elemento essencial do Regulamento

A desadequação da Diretiva exacerbada pelas transformações societárias e tecnológicas verificadas nos últimos anos advém, no entendimento dos especialistas do Rand Report, não na prescrição dos princípios *per se*, mas na falta de uma adequada previsão da necessidade de verificação de determinados mecanismos e da sua proporcionalidade – e, sobretudo, na ausência de uma abordagem baseada no risco. Como se pode ler no relatório acima referido:

"*De um modo geral, essas fraquezas* [da Diretiva] *parecem ser indicativas de um quadro regulatório que se concentra não só nos princípios da proteção de dados (como a legitimidade, a transparência, a restrição de utilização para certos fins, etc.) e nos resultados procurados, mas também nos processos e mecanismos utilizados para implementar esses princípios (obter o consentimento da pessoa em causa, redação de políticas, apresentação de notificações, etc.), sem considerar adequadamente se o resultado desejado é promovido por esses processos e mecanismos ou se esses requisitos resultam num resultado proporcional ao encargo que representam."*[42]

Os especialistas do Rand Report concluem que tal configuração da proteção de dados "*corre o risco de criar uma cultura organizacional que se concentra em cumprir formalidades para criar conformidade que apenas funciona no papel (através de caixas de seleção, políticas, notificações, contratos, (...), em vez de promover melhores práticas de proteção eficazes"*[43].

Reitere-se que é necessária uma maior proteção de dados na prática, com efeitos reais na efetiva e material proteção do cidadão. Para atingir esse objetivo e face à inevitabilidade de vários dos riscos dos tratamentos de dados, é necessário um certo pragmatismo regulatório, que poderá ser atingido através de uma abordagem baseada no risco, como já é feito em muitos campos do direito[44].

[42] *Ibidem.*
[43] *Ibidem.*
[44] Por exemplo, na regulação de questões ambientais. Diga-se também, que a gestão e avaliação de riscos são um clássico elemento da governação de empresas, nomeadamente em sociedades de gestão financeira.

Esta abordagem baseada no risco é instrumental para a criação de uma cultura de proteção de dados pessoais adequada em face dos riscos que apresenta, e não apenas estruturas formalistas de conformidade sem real compromisso.

Ora, como diz Peter Hustinx:

"*É essencial que as disposições gerais nas atuais e futuras molduras sejam inerentemente escalonáveis. Especificações inapropriadas podem exigir exceções inapropriadas. Esta busca pelo equilíbrio certo está agora a ter lugar sob o termo "abordagem baseada no risco"*[45].

Esta abordagem baseada no risco obriga a um escalonamento dos riscos apresentados por cada operação de tratamento, baseada no risco casuisticamente definido destas; por exemplo, se estamos perante dados que integram as categorias especiais de dados.

Sendo que estes riscos terão de ser necessariamente considerados e avaliados pelas entidades envolvidas no tratamento, cimenta-se uma material cultura de proteção de dados numa dada organização, na medida em que decisões conscientes e pensadas têm de ser tomadas quanto à alocação de recursos para as áreas mais sensíveis dos tratamentos de dados pessoais por uma dada entidade. Ora, para que uma decisão quanto à distribuição de recursos possa ser tomada, é necessário um completo e abrangente diagnóstico das áreas e categorias de dados que mais carecem de proteção face aos riscos evidenciados. Promove-se, dessa forma, um autoconhecimento das empresas e organizações em matéria de proteção de dados, por oposição ao genérico e mecânico satisfazer dos requisitos burocráticos que se encontravam prescritos aquando da vigência da Diretiva.

O Regulamento adota esta abordagem à proteção de dados com base no risco de forma clara em várias normas. Um exemplo disso, entre outros[46], é a prescrição da necessidade de fazer avaliações de impacto 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*" (art. 35º, n.º 1).

Apesar disto, importa tomar em consideração que o risco é inerente a cada operação de tratamento, e que os direitos dos cidadãos deverão ser respeitados independentemente de

[45] HUSTINX - cit. 14, p. 151

[46] Como a proteção de dados desde a conceção, a segurança dos dados pessoais que se integrem nas categorias especiais de dados pessoais, entre outros.

qualquer consideração relativamente ao risco[47]. Exemplificativo desta postura, é o Regulamento ser bastante prescritivo em operações que não estão intrinsecamente ligadas a um risco específico. Veja-se, por exemplo, quando o Regulamento prescreve que "*o responsável pelo tratamento deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido"*(Considerando 59).

Como se disse, o instituir de uma abordagem à proteção de dados baseada no risco deve-se, primariamente, a razões de eficiência, devido à possibilidade de prioritizar – na teoria – o investimento de recursos escassos (seja económicos ou humanos) na real e efetiva proteção dos cidadãos e consequente cumprimento das obrigações legais existentes nesta matéria.

Outra forma em que a abordagem e gestão de risco está presente no Regulamento está consubstanciada na eliminação, por motivos de eficiência e de respeito por uma ideia de proporcionalidade e diminuição de encargos administrativos desnecessários, dos mecanismos *ex ante* em que se traduziam os poderes de supervisão das autoridades de controlo[48]. Por exemplo, a necessidade de notificação prévia às autoridades de controlo das operações de tratamento deixa de existir[49], passando o poder de supervisão das autoridades de controlo a ser exercido *a posteriori*, através de um princípio que está estritamente conexo à gestão de risco: o princípio da responsabilidade ("*accountability*").

Não só as entidades que processam dados pessoais estão adstritas à abordagem á proteção de dados baseada em programas de gestão de risco: também os escassos recursos quanto ao poder de supervisão das autoridades de controlo deverão ser feitos nesta base, atuando com um plano estratégico.

Esta abordagem não está isenta de riscos (passe a aparente redundância conceptual): o facto de não existir uma taxinomia abrangente relativamente aos potenciais perigos e riscos para os direitos e liberdades dos cidadãos emanantes das operações de tratamento de dados pessoais, obsta a que possa haver uma efetiva gestão destes – como se pode ler num editorial escrito por Kuner, Cate, *et al.*:

[47] HUSTINX - cit. 14, p. 153.

[48] As autoridades de controlo são entidades administrativas independentes com poderes de autoridade, em matéria de proteção de dados. Em Portugal, a autoridade de controlo é a Comissão Nacional de Dados (CNPD).

[49] Pelo menos genericamente; o Regulamento prevê a possibilidade de consulta prévia às autoridades de controlo quando uma avaliação de impacto indicar que determinada operação de tratamento de dados pode resultar num elevado risco para os titulares dos dados – *cfr.* art. 36º do Regulamento.

"*(...) uma das omissões mais óbvias até à data é uma compreensão clara dos danos ou impactos negativos que a gestão de riscos pretende identificar e mitigar na área de proteção de dados. (...) Esta é uma falha grave porque fazer com que a gestão de riscos funcione de forma eficaz e consistente exige que haja uma amplamente divulgada classificação de repercussões - positivas e negativas - em indivíduos, nas organizações e na sociedade em geral"*[50].

Outra razão que motivou a reforma da legislação vigente em matéria de proteção de dados foram as alterações legislativas a nível da estrutura legal da própria União Europeia: a proteção de dados foi reconhecida como um direito autónomo (já não uma simples extensão da reserva da vida privada) na Carta dos Direitos Fundamentais da União Europeia[51] e o Tratado de Lisboa inclui nos tratados uma nova base jurídica, o art. 16º do Tratado de Funcionamento da União Europeia (TFUE).

Estas inovações normativas demonstram perfeitamente como a proteção de dados é vista como uma preocupação global da União como direito autónomo e objeto de consagração enquanto fim em si mesmo, e não já como algo instrumental para a concretização do mercado interno.

[50] KUNER, Christopher, CATE, Fred *et al* – Editorial: Risk Management in Data Protection em *International Data Privacy Law*, Volume 5, Issue 2 Disponível em https://doi.org/10.1093/idpl/ipv005.
[51] *Cfr.* Art. 8º da Carta dos Direitos Fundamentais da União Europeia.

4. Os Fluxos Internacionais de Dados e o Direito à Proteção de Dados Pessoais na União Europeia

4.1. Na Diretiva 95/46/CE

Quanto aos fluxos internacionais de dados, e para além da Diretiva impossibilitar que os Estados-Membros restrinjam as transferências de dados entre eles (art. 1º, n.º 2), estabelecia como princípio máximo a proibição de transferências de dados para um país terceiro, salvo a hipótese de o "*país terceiro em questão assegurar um nível de proteção adequado"* (25º, n.º 1).

Antes de mais, releva expor que o conceito de tratamento de dados é bastante amplo e abrange a mera transferência[52], quer na Diretiva quer no novo Regulamento (art. 4º, n.º 2).

O n.º 2 do artigo 25º da Diretiva contém as características que deverão estar subjacentes à determinação de um "nível de proteção adequado": tal enunciada adequação será apreciada em função de "*todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final , as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa , bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país"*.

Caso algum país seja considerado apresentar um "nível de proteção adequado", as regras da União Europeia quanto aos fluxos internacionais de dados pessoais não se aplicam, tendo este de se pautar exclusivamente pelas normais disposições da Diretiva, como se de uma transferência entre Estados-Membros se tratasse.

[52] «*Tratamento de dados pessoais» («tratamento»), qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição*" - *cfr.* art. 2º b) da Diretiva.

É à Comissão a quem cabe o papel de tomar as decisões de adequação, considerando todos os fatores acima descritos, constantes na lei. Na prática, só um número muito limitado de países adquiriu tal decisão de adequação[53].

Vários países procuraram obter uma decisão de adequação no pressuposto de que constituiria uma espécie de *carte blanche* para um maior fluxo de dados para os países em causa, e que tal se traduziria num maior volume de atividade económica[54] - daí a relativa osmose verificada em países terceiros por motivos de pragmatismo económico que deu origem à ideia de "supremacia por defeito" da Diretiva e do corresponde sistema europeu de proteção de dados, como já abordado em capítulo anterior.

Kuner, de forma a ilustrar tais efeitos, refere o exemplo de um estudo feito numa província do Canadá em que foi decretada legislação a restringir o fluxo de dados transnacionais:

"(...) um estudo sobre o impacto da legislação regional canadiana quanto à restrinção do fluxo de dados transfronteiriços afirma que isso causou" menos serviços disponíveis para os órgãos públicos canadianos e para os residentes, aumento da burocracia e redução significativa da eficiência, custos financeiros mais elevados, risco de danos tangíveis à saúde e segurança, e falta de concorrência para os organismos públicos "e do setor de serviços em expansão do Canadá".[55]

Vários benefícios são identificados quanto à livre possibilidade de transferir dados pessoais internacionalmente, particularmente de carácter económico e societário. Tem sido apontado, por exemplo, que certos direitos fundamentais só podem ser, em muitos casos, completamente exercidos além-fronteiras, como a liberdade de expressão, que muitas vezes envolve, na sua exteriorização, o tratamento de dados pessoais[56].

Os cidadãos incorporaram já nas suas vidas o uso e acesso a vários serviços *online* que necessariamente envolvem transferências de dados para além das fronteiras físicas do seu país de origem ou residência.

Também os governos (e, teoricamente, os cidadãos) têm um vasto interesse na possibilidade de livremente transferir e ser recipiente de dados pessoais, para efeitos de

[53] Andorra, Argentina, Ilhas Faroé, Guernsey, Ilha de Man, Israel, Jersey, Nova Zelândia, Suíça e Uruguai.
[54] KUNER, Christopher – Transborder Data Flows and Data Privacy Law, p. 106.
[55] *Ibidem*.
[56] *Idem, ibidem*, p. 102.

cooperação internacional, em áreas como a supervisão financeira, aplicação da lei, entre outros[57].

Porém, como característica praticamente inalienável deste campo do direito como um campo/contracampo jurídico, aos benefícios elencados correspondem riscos que coexistem de forma aparente.

Particularmente relevante é a existência de um *status quo* de espionagem ao cidadão, como demonstrado pelas renovações de Edward Snowden[58], sendo que atualmente vivemos numa época de *Dataveillance* na definição de Roger Clarke: o sistemático uso de sistemas de agregação e tratamento de dados pessoais para fins de investigação e monitorização de ações ou comunicações de uma ou mais pessoas[59].

As transferências de dados pessoais para países terceiros poderão também afetar os cidadãos na medida em que podem dificultar o exercício dos seus direitos e de promover ações judiciais nesse sentido, atendendo à dificuldade de exercer, noutras jurisdições, os direitos que lhes assistem.

Vários autores, incluindo Kuner, apontam as severas fragilidades do sistema de adequação, dizendo que é um sistema "*moroso, caro, lento e passa a mensagem errada aos países terceiros*"[60]. Acresce o facto de ser um sistema que tem implicações políticas sérias: não só pelas tensões políticas emergentes do paternalismo da União Europeia no processo de decidir se a estrutura jurídica de um determinado país é, ou não, "adequada" em matéria de proteção de dados; mas também por, segundo Kuner, pressões políticas e comerciais ditarem uma "adequação" que não se verifica na prática, como no caso da Argentina[61]. Dúvidas semelhantes têm sido levantadas relativamente à provável e eminente decisão de adequação quanto ao Japão[62].

---

[57] *Ibidem.*

[58] Famoso ex-administrador de sistema da CIA e funcionário da NSA que primeiro denunciou as práticas de monitorização e espionagem a escalas massivas efetuadas pelas referidas agências de informação americanas aos cidadãos.

[59] Este conceito desdobra-se em vigilância pessoal e vigilância massiva, sendo que no primeiro caso caracteriza-se por a investigação ter por objeto uma pessoa identificada; o segundo elemento do conceito refere-se à vigilância de grupos de pessoas, normalmente para identificar um perfil de indivíduos que são de um determinado grau de interesse para a organização que promove a vigilância em causa - *cfr.* Roger Clarke - Information and Dataveillance disponível em http://www.rogerclarke.com/DV/CACM88.html [consultado em 28/07/2018].

[60] KUNER, Christopher – Developing an Adequate Legal Framework for International Data Transfers, p. 263.

[61] *Idem, ibidem*, p. 265.

[62] Quanto a esta questão *cfr.*, de forma geral: GREENLEAF, Graham – Questioning "Adequacy" (Pt I) – Japan.

Embora este sistema tenha como *ratio* de existência o desejo de manter um elevado nível de proteção de dados independentemente de onde esta se encontre e, de forma conexa, evitar a fuga à aplicação das regras que prescreve (impedindo assim que um responsável pelo tratamento transfira as suas obrigações para um subcontratante estabelecido fora da União, num país com baixo nível de proteção, por exemplo) não é considerado um princípio fundamental da proteção de dados[63]. Tal conclusão é sustentada pelo facto de, nas suas decisões de adequação, a Comissão Europeia não requerer que os países terceiros proíbam, eles próprios, as transferências de dados para países terceiros com leis de proteção de dados passíveis de ser consideradas como "não adequadas"[64]. Veja-se, a esse título, o caso do Canadá[65].

Kuner propõe, em face da manifesta desadequação do sistema de adequação, substituir este sistema por um baseado no principio da responsabilidade, na medida em que o exportador dos dados continue responsável por cada dano ou prejuízo resultante do mau uso feito dos dados pessoais em questão[66].

A Diretiva, no seu artigo 26º, prevê derrogações ao princípio geral acima enunciado, contendo uma lista taxativa dos fundamentos legais que permitem que se proceda a transferências de dados para países terceiros sem um nível de proteção adequado, tendo o legislador europeu considerado justificadas por serem compatíveis com a proteção dos direitos fundamentais das pessoas e a livre circulação do fluxo internacional da informação[67].

Tais derrogações são as seguintes: o consentimento inequívoco do titular dos dados; a transferência em causa ser necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento (ou diligências pré-contratuais a pedido do titular dos dados); a transferência ser necessária à execução ou celebração de um contrato ,celebrado ou a celebrar, entre o responsável pelo tratamento e um terceiro; a transferência ser necessária ou legalmente exigida para a proteção de um interesse público importante, ou para a declaração, o exercício ou defesa de um direito num processo judicial; a transferência ser necessária para proteger os interesses vitais do titular dos dados; ou a transferência ser realizada a partir de um registo

[63] KUNER, Christopher - cit. 60, p. 266.
[64] *Idem, ibidem*, p. 267.
[65] Canadian Personal Information Protection and Electronic Documents Act, S.C 2000, c. 5.
[66] KUNER, Christopher - cit. 60, p. 269.
[67] ARTICLE 29 WORKING PARTY - Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, p. 9.

público que, nos termos da lei, se destine à informação do público e se encontre aberto à consulta do público em geral, ou por qualquer pessoa que possa provar um interesse legítimo (art. 26, n.º 1).

Estas derrogações têm de ser, segundo o Grupo de Trabalho do Artigo 29, interpretadas de forma restritiva[68]. Desta forma, o Grupo de Trabalho recomenda que as transferências de dados pessoais quando sejam feitas de forma repetida, em massa ou estruturais, sejam efetuadas dentro de um quadro normativo específico (cláusulas contratuais-tipo e regras vinculativas aplicáveis às empresas [*binding corporate rules*])[69].

O referido quadro normativo específico encontra-se - algo abstratamente - previsto no nº 2 do Art 26º. Estipula esta norma que, sem prejuízo das derrogações previstas, e desde que o responsável pelo tratamento apresente garantias suficientes de proteção da vida privada e dos direitos e liberdades fundamentais dos titulares dos dados, determinadas transferências de dados pessoais para países terceiros poderão ser permitidas. Mais refere o artigo que tais garantias podem resultar, designadamente, de cláusulas contratuais.

Para além das regras vinculativas aplicáveis às empresas[70], para transferências repetidas - em massa ou estruturais - existem dois tipos de estruturas de cláusulas que podem ser usadas pelas entidades envolvidas no tratamento de dados pessoais com entidades estabelecidas em países terceiros: as cláusulas *ad hoc* (art. 26º, n.º 2), cláusulas personalizadas pelas partes envolvidas para os operações de tratamento específicas, tendo estas de ser aprovadas pelas autoridades de controlo nacionais; e as cláusulas contratuais-tipo.

4.1.1. As Cláusulas Contratuais-Tipo

As cláusulas contratuais-tipo constituem, como referido, um dos mecanismos previstos na Diretiva (art. 26º, n.º 4) que permite a transferência de dados pessoais, a partir de qualquer Estado-Membro, para um país terceiro que não tenha obtido uma decisão de adequação.

[68] ARTICLE 29 WORKING PARTY, cit. 67, p. 7.
[69] ARTICLE 29 WORKING PARTY, cit. 67, p. 9.
[70] As regras vinculativas aplicáveis às empresas são objeto de um estudo mais aprofundado no capítulo 5.

Obviamente, tais cláusulas reportam-se exclusivamente à fixação de deveres e obrigações na área da proteção de dados, podendo ser incluídas outras cláusulas correlacionadas com a relação comercial regida pelo contrato entre as partes, desde que não contradigam as cláusulas contratuais-tipo[71].

Estas cláusulas contratuais-tipo, pela sua natureza, não carecem de autorização das autoridades de controlo competentes, embora seja a estas que caiba a supervisão da sua observação na prática, bem como se estas estão em conformidade com a lei nacional[72].

A Comissão emitiu três decisões em que prevê três conjuntos de cláusulas contratuais-tipo, dois para responsáveis pelo tratamento[73] e um para subcontratantes[74].

As cláusulas contratuais-tipo têm como objetivo "compensar" a ausência de um nível adequado de proteção no país de destino dos dados pessoais objeto da previsão, pelo que deverão vincular as entidades envolvidas no tratamento dos dados pessoais a determinadas obrigações específicas. Neste âmbito, as cláusulas em causa têm que prever garantias adicionais aos titulares de dados, decorrendo do facto de a transferência estar a ser feita para um país terceiro sem proteção adequada e, portanto, adstrito à observação de determinadas normas de proteção de dados com carácter coercivo[75].

---

[71] *Cfr.* Considerando 5 da Decisão Da Comissão de 15 de Junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Diretiva 95/46/CE.

[72] *Idem, ibidem* – Considerando 15.

[73] Decisão Da Comissão de 15 de Junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Diretiva 95/46/CE disponível em https://www.cnpd.pt/bin/legis/internacional/DecCom15-6-01-CCT.pdf; e Decisão Da Comissão de 27 de Dezembro de 2004 que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros.
Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32004D0915&from=PT [consultado a 28/04/2018].

[74] Decisão Da Comissão de 5 de Fevereiro de 2010 relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010D0087&from=PT [todos consultados a 28/04/2018].

[75] GRUPO DE TRABALHO DO ARTIGO 29 – WP9 Documento de Trabalho: Observações preliminares relativas ao uso de cláusulas contratuais no contexto da transferência de dados pessoais para países terceiros, p. 3.

O titular dos dados tem o direito de acionar e de obter indemnização do exportador de dados, do importador de dados ou de ambos[76], por quaisquer danos resultantes dos atos incompatíveis com os deveres resultantes das cláusulas contratuais-tipo[77].

O exportador e o importador de dados só não serão responsáveis se conseguirem demonstrar que, nos termos acima referidos, o dano ou prejuízo não lhes pode ser imputado[78].

4.2 No Regulamento

As disposições relativamente às transferências de dados foram sujeitas a alterações e a esclarecimentos. O Regulamento introduz um princípio geral de transferências de dados (art. 44º) que fixa que "*qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se (...) as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante*".

Tal disposição resulta no facto de, ao contrário do que prescrevia a Diretiva, as regras quanto às transferências terem também de ser observadas pelos subcontratantes.

Apesar das críticas, o Regulamento mantém o regime de adequação ("regime baseado no território"[79]) primeiramente definido pela Diretiva 95/46/CE: as transferências, sem prejuízo da existência de mecanismos que podem ser usados na ausência de uma decisão de adequação, só poderão ser feitas se o país de destino tiver sido considerado pela Comissão Europeia como dispondo de um "nível de proteção adequado" (art. 45º).

A desadequação/inflexibilidade desta norma é algo mitigada pelo facto de a decisão de adequação passar a incluir não só países, mas também territórios destes ou um ou mais sectores

[76] *Cfr.* Considerando 20 Decisão da Comissão - cit. 75;" *(...) embora o direito de regresso entre responsáveis, não constituindo uma exigência para garantir um nível adequado de protecção aos titulares dos dados, pudesse não ter lugar, está incluído nas cláusulas contratuais-tipo para efeitos de esclarecimento e para evitar a necessidade de as partes negociarem caso a caso cláusulas de indemnização*".
[77] *Idem, ibidem* – considerando 19.
[78] *Ibidem.*
[79] MOEREL, Lokke – Binding Corporate Rules: Corporate Self-Regulation of Global Transfers, p. 26.

específicos (art. 45º, n.º 1). Os fatores determinantes que a Comissão Europeia deverá observar aquando da decisão de adequação de dado país também foram atualizados, conforme o referido na decisão do Tribunal de Justiça da União Europeia, no âmbito do Acórdão Schrems[80].

Neste julgamento o Tribunal de Justiça defendeu que a expressão «nível de proteção adequado» deve ser entendida no sentido de que se exige que esse país terceiro assegure efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União[81]. Decorre da interpretação desse argumento que a proteção dada num dado país terceiro não terá que emular o regime europeu; o que releva é que haja um essencialmente equivalente nível de proteção, sejam quais forem os concretos mecanismos instituídos.

Assim, os fatores essenciais subjacentes ao processo decisório quanto à adequação de um determinado território deixaram de reportar-se às circunstâncias que rodeiam a transferência ou o conjunto de transferências de dados (art. 25º, n.º 2 da Diretiva) para passar a relevar mais especificamente o primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, incluindo (de forma relevante, atendendo à jurisprudência do Tribunal de Justiça no Acórdão Schrems I) o acesso das autoridades públicas a dados pessoais e a existência de mecanismos judiciais que assegurem o efetivo ressarcimento e reparação hipotética dos danos sofridos pelos cidadãos (art. 45º, n.º2 al. a) do Regulamento).

Importante, também face à decisão constante do Acórdão Schrems I, é o papel relevante da existência de uma (ou mais) autoridade de controlo independente no país terceiro, responsável por assegurar a e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir os titulares de dados, bem como da capacidade destas de colaborar com as autoridades de controlo dos Estados-Membros.

4.2.1. Derrogações

[80] Acórdão Maximillian Schrems v. Data Protection Commisioner, relativo ao Processo C-362/14 (doravante, Acordão Schrems I)

[81] *Cfr*. para. 73 Schrems I.

O Regulamento permite um maior número do que tem sido denominado de soluções "*organizational based*"[82] quanto a transferências de dados transnacionais, desde que estes instrumentos prevejam garantias adequadas, nomeadamente no que se reporta à possibilidade dos cidadãos puderem exercer os direitos que lhes assistem e que estejam asseguradas o acesso a medidas jurídicas corretivas eficazes (art. 46º, n.º 1). Os instrumentos jurídicos em causa incluem as cláusulas contratuais-tipo (art. 46º, n.º 2 al. d)); as cláusulas contratuais *ad hoc* (art. 46, n.º 3 al. a)); códigos de conduta (desde que acompanhados de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas (art. 46º, n.º 2 al. e)); e procedimentos de certificação (art. 46º, n.º 2 al. f)). Muito relevante, para os fins do presente estudo, é o reconhecimento da validade das regras vinculativas aplicáveis às empresas (art. 46, n.º 2 al. b)), prescrevendo uma série de requisitos a serem observados (art. 47º).

Cumpre também atentar ao disposto nos arts. 45º, n.º 9 e 46º, n.º 5 do Regulamento e ao conteúdo do considerando 171, que confirmam que as decisões da Comissão Europeia (decisões de adequação e as autorizações de cláusulas contratuais-tipo e que as decisões das autoridades de controlo nacionais) feitas sob a égide das disposições da Diretiva mantêm a sua vigência e validade, até que sejam alteradas, substituídas ou revogadas, caso se justifique.

As derrogações já determinadas em sede da Diretiva não sofreram alterações, excetuando na esfera do consentimento, nos termos já enunciados.

4.2.2. Schrems II e a potencial invalidade das Cláusulas Contratuais-Tipo

Em 25 de junho de 2013, Maximilian Schrems, cidadão austríaco, apresentou formalmente uma queixa dirigida à autoridade de controlo irlandesa (*Data Protection Commissioner*) , tendo em vista a proibição de transferências de dados pessoais por parte da

[82] MOEREL – cit. 79, p. 26.

Facebook Ireland (sendo que os dados pessoais dos utilizadores do Facebook residentes no território da União são, no todo ou em parte, transferidos para servidores pertencentes à Facebook Inc., situados em território dos Estados Unidos, onde são objeto de tratamento) para os Estados Unidos.

Desde 2000, que as empresas europeias podiam transferir dados pessoais para os Estados Unidos da América ao abrigo do "porto seguro"[83] (*safe harbour*), mediante adesão a determinados princípios expostos neste regime-quadro. Cerca de 4000 empresas estariam certificadas no âmbito deste acordo[84].

Tal queixa teve como motivo as revelações feitas por Edward Snowden sobre a ingerência de várias agências governamentais americanas de serviços de informação, especialmente a National Security Agency (doravante, NSA) na esfera privada dos cidadãos, e sobre o facto de o Facebook estar a, voluntariamente, submeter dados pessoais dos seus utilizadores a esta agência, no âmbito do programa "PRISM"[85].

A queixa foi, porém, arquivada pela autoridade de controlo irlandesa por aparente falta de fundamento, considerando que não existiam provas de que a referida agência americana tivesse especificamente acedido aos dados pessoais do interessado[86].

Schrems interpôs recurso desta decisão para o Supremo Tribunal de Justiça Irlandês, tendo este órgão declarado que o acesso massivo e indiscriminado a dados pessoais de cidadãos europeus era contrário ao princípio da proporcionalidade e aos valores fundamentais protegidos pela Constituição Irlandesa[87] bem como do direito da União na matéria[88].

O Supremo Tribunal de Justiça Irlandês observou que, muito embora tal não tenha sido expressa e formalmente contestado por Schrems, este no fundo questiona a legalidade do

[83] Estabelecido pela Decisão 2000/520 que determina que o nível adequado de proteção de dados pessoais necessário pode ser conseguido entre a União Europeia e os Estados Unidos da América, desde que as organizações deem cumprimento aos princípios do "porto seguro" relativos à proteção de dados pessoais transferidos de um Estado-Membro para os EUA (*cfr.* Considerando 5 da Decisão).

[84] MOEREL, Lokke - The implications of the Schrems judgment of the European Court for data transfers to the U.S., p. 2.

[85] *Cfr.* Reclamação de Max Schrems disponível em http://www.europe-v-facebook.org/prism/facebook.pdf [consultado em 27/04/2018].

[86] *Cfr.* para. 29 Acórdão Schrems I.

[87] *Cfr.* para. 33 e 34 do Acordão Schrems I.

[88] Veja-se que a questão da proporcionalidade e a sua observação na prática foi também o fator que ditou a invalidade da Diretiva 2006/24/CE, Digital Rights Ireland (*cfr.* Acórdão do Tribunal de Justiça de 8 de abril de 2014, relativo aos processos apensos C-293/12 e C-594/12).

regime do "porto seguro" existente relativamente à transferência de dados pessoais provenientes de residentes dos Estados-Membros da União Europeia para os Estados Unidos da América[89]. O Supremo Tribunal de Justiça irlandês decidiu, nessas condições, suspender a instância e reenviar as seguintes questões prejudiciais ao Tribunal de Justiça: se o Comissário para a Proteção de Dados irlandês está vinculado em termos absolutos à decisão de adequação exarada pela Comissão Europeia relativamente, *in casu*¸ aos Estados Unidos da América, contida na Decisão 2000/520; se, em alternativa, pode/deve o referido tribunal fazer a sua própria investigação sobre a matéria, em face dos desenvolvimentos recentes que tiveram lugar após a supramencionada decisão de adequação da Comissão[90].

Em Acórdão proferido pelo Tribunal de Justiça da União Europeia, após análise das questões prejudiciais apresentadas pelo Supremo Tribunal de Justiça Irlandês, este lembrou que só o Tribunal de Justiça é competente para declarar a invalidade de um ato da União Europeia[91], não podendo as autoridades de controlo dos Estados-Membros rejeitar dar cumprimento à decisão de adequação da Comissão, dado o seu caráter obrigatório[92].

Todavia, esse facto não pode impedir os titulares de dados pessoais que possam ter sido objeto de transferência para país terceiro de exercer o seu direito de reclamação perante a específica operação de tratamento em causa[93].

O Acórdão do Tribunal de Justiça teve assim como efeito, para além do reforço do poder de fiscalização das autoridades de controlo dos Estados-Membros, a invalidade da Decisão 2000/520 que institui o "porto seguro" entre a União Europeia e os Estados Unidos da América. Tal decisão adveio do facto, já exposto no Acórdão Digital Rights Ireland, que uma regulamentação que permita às autoridades públicas aceder de modo generalizado e indiscriminado ao conteúdo das comunicações eletrónicas de cidadãos deve ser considerada como lesiva do direito fundamental ao respeito da vida privada[94] e do facto de o particular afetado não poder recorrer a qualquer via de direito que lhe permita exercer os direitos que a normativa europeia em proteção de dados pessoais prevê. Assim, o artigo 1º da referida Decisão é inválido, na medida em que este estipula que a observação destes princípios assegura um

[89] *Cfr*. para. 35 Acórdão Schrems I.
[90] *Cfr*. para. 36 Acórdão Schrems I.
[91] *Cfr*. para. 61 Acórdão Schrems I.
[92] *Cfr*. para. 51 Acórdão Schrems I.
[93] *Cfr*. para. 53 Acórdão Schrems I.
[94] *Cfr*. para. 94 Acórdão Schrems I.

nível considerado "adequado" de proteção dos dados pessoais transferidos no âmbito desta Decisão.

Também na medida em que o artigo 3º da Decisão 2000/520 excluía a possibilidade de as autoridades de controlo tomarem medidas destinadas a assegurar o respeito do artigo 25º da Diretiva quanto às transferências internacionais de dados seria também inválido[95], pelo facto de a Comissão estar a ultrapassar a sua competência.

Face às considerações acima expostas, e atendendo ao facto de os artigos 1º e 3º terem sido considerados inválidos pelo Tribunal de Justiça e estando estes intrinsecamente conexos aos restantes artigos da Decisão, toda a Decisão foi considerada inválida[96].

4.2.3. Um novo Acórdão Schrems II?

Após a determinação do Tribunal de Justiça da ilegalidade das transferências de dados pessoais entre a União Europeia e os Estados Unidos da América efetuadas no âmbito do "porto seguro" definido nos termos referidos no ponto anterior, a autoridade de controlo irlandesa decidiu formalmente investigar a queixa de Schrems, tendo este sido convidado a reformular a sua queixa (para. 27 da Decisão Schrems II[97]) – já que não fazia sentido o foco existente na decisão quanto ao "porto seguro", entretanto invalidado.

Schrems, na sua queixa reformulada, mantêm essencialmente os mesmos pontos de discussão: a validade das transferências dos seus dados pessoais entre Facebook Irlanda e Facebook Inc. (servidores localizados nos Estados Unidos) e o seu tratamento subsequente[98]. Este explica também que a vigilância e monitorização *en masse* feita nos Estados Unidos constituem um ponto secundário na avaliação da legalidade dessa transferência internacional de dados.

[95] *Cfr*. para. 104 Acórdão Schrems I.
[96] *Cfr*. para. 105 e 105 Acórdão Schrems I.
[97] Decisão do Tribunal Superior Comercial da Irlanda de 3 de outubro de 2017 (Caroline Costello), *The Data Protection Comissioner v. Facebook Ireland Limited, Maximillian Schrems* [2016 No. 4809 P.].
[98] *Cfr*. para. 30 Decisão Schrems II.

De forma a poder reformular a sua queixa, os advogados de Schrems entraram em contacto com o Facebook, pedindo que esta entidade identificasse as bases legais de que faz uso para transferir os dados pessoais do Reclamante para os Estados Unidos da América[99].

O Facebook não indicou todas as bases legais pedidas. Referiu, porém, a existência de uma solução contratual entre o Facebook Irlanda e o Facebook Inc. que faz uso da decisão 2010/87/UE, relativamente a uma das opções de cláusulas contratuais-tipo[100]. Neste sentido, o Facebook argumenta que estão previstas as garantias adequadas nos termos do artigo 26, n.º 2 da Diretiva relativamente ao respeito da proteção da privacidade e pelos direitos fundamentais e liberdades dos residentes da União Europeia subscritores do Facebook[101].

Através das investigações feitas, a autoridade de controlo irlandesa chegou à conclusão de que parecem existir dúvidas razoavelmente fundamentadas para a ausência de efetivo solução de recurso legal para os residentes da União Europeia na lei americana e que as cláusulas contratuais-tipo consigam efetivamente remediar tal circunstância[102].

Nessa medida, a autoridade de controlo irlandesa considerou, face ao já decidido em sede do Acórdão Schrems I, que a investigação não poderia concluir-se sem uma decisão quanto à validade ou invalidade das cláusulas contratuais-tipo pelo Tribunal de Justiça da União Europeia[103].

Com a intenção de obter o reenvio dessas questões prejudiciais para o Tribunal de Justiça da União Europeia, a autoridade de controlo irlandesa intentou, em 2016, uma ação perante o Tribunal Superior de Comércio da Irlanda. A decisão de reenvio foi proferida a 3 de outubro de 2017 pela juíza Caroline Costello (a Decisão Schrems II referida nesta secção).

A juíza do caso desconsiderou os argumentos do Facebook, no sentido de o direito da União na matéria não se aplicar a operações de tratamento de dados pessoais para fins relacionados com a segurança nacional, independentemente de o tratamento ter lugar na União Europeia ou em países terceiros, como os Estados Unidos da América[104]. A juíza referiu que tal argumento era inconsistente com a decisão Schrems I, em que essa matéria de jurisdição nunca foi levantada por qualquer das partes[105]. Tal argumento também seria inconsistente com

[99] *Cfr.* para. 31 Decisão Schrems II.
[100] *Ibidem.*
[101] *Cfr.* para. 35 Decisão Schrems II.
[102] *Cfr.* para. 40 Decisão Schrems II.
[103] *Cfr.* para. 42 Decisão Schrems II.
[104] *Cfr.* para. 51 e 52 Decisão Schrems II.
[105] *Cfr.* para. 61 (2) Decisão Schrems II.

as visões do Grupo de Trabalho do Artigo 29[106] e da Comissão Europeia e dos Estados Unidos da América, na medida em que estas partes adotaram o Escudo de Proteção da Privacidade UE-EUA[107] precisamente para superar a ingerência das agências governamentais americanas de segurança nacional na esfera dos dados pessoais dos cidadãos europeus[108].

Relativamente ao Escudo de Proteção da Privacidade UE-EUA, o Tribunal considerou que a existência deste não preclude a necessidade de julgar a questão em causa, na medida em que o Facebook está a fazer uso das cláusulas contratuais-tipo como base legal para as transferências *sub judice* e não com base no Escudo de Proteção da Privacidade UE-EUA[109].

A juíza do caso considerou, após extensa análise das leis americanas e europeias relevantes, que existem vários obstáculos ao recurso judicial por parte de residentes europeus em relação ao tratamento dos seus dados pessoais efetuado por agências de inteligência americanas[110]. Não existe, por exemplo, a possibilidade de um residente na União obter o devido acesso, retificação ou apagamento dos seus dados pessoais, e administrativo ou judicial ressarcimento ou compensação[111], apesar das aparentes inúmeras possíveis causas de ação[112].

A juíza do caso concluiu que apesar das transferências feitas ao abrigo do artigo 26º (que constitui uma derrogação do artigo 25º) não serem feitas com base na adequação relativamente ao nível de proteção do país para os quais os dados pessoais são transferidos, esses dados ainda assim carecem de um elevado nível de proteção[113].

Referiu ainda que as autoridades de controlo europeias têm a obrigação de garantir que os dados pessoais recebem esse elevado nível de proteção e estão, na normativa europeia, previstos poderes para suspender ou proibir transferências de dados se as leis desse país terceiro limitam ou impedem a existência desse elevado nível de proteção[114].

Na medida em que existam sérios obstáculos à observação na prática dos elementos de proteção garantidos pela União nas leis dos Estados Unidos da América, defende a magistrada

[106] *Cfr.* para. 61 (3) Decisão Schrems II.
[107] Regime-quadro que permite a transferência de dados pessoais da UE para uma empresa sediada nos Estados Unidos, desde que estejam verificados os pressupostos nele consignados; substitui o anterior *Safe Harbour*.
[108] *Cfr.* para. 61 (5) Decisão Schrems II.
[109] *Cfr.* para. 66 Decisão Schrems II.
[110] *Cfr.* para. 226 Decisão Schrems II.
[111] *Cfr.* para. 227, 2º parte Decisão Schrems II.
[112] *Cfr.* para. 232 Decisão Schrems II.
[113] *Cfr.* para. 153 Decisão Schrems II.
[114] *Ibidem.*

que as Cláusulas Contratuais-tipo não compensam tais deficiências regulatórias[115]. *In casu*, essas soluções contratuais privadas não vinculam o poder de autoridade dos Estados Unidos da América nem as suas agências.

A questão relevante quanto às Cláusulas Contratuais-tipo, no entendimento da juíza do caso, é a de saber se o poder discricionário que as autoridades de controlo detêm de suspender ou proibir transferências de dados para países terceiros é suficiente para considerar que tais Cláusulas não deverão estar feridas de invalidade[116]. Nesse sentido, a magistrada considera apropriado e necessário o reenvio das questões para o Tribunal de Justiça da União Europeia[117].

Algo curioso é o facto de Schrems ter objetado ao reenvio da questão sobre a invalidade das Cláusulas Contratuais-tipo: expõe que não estava a questionar a validade destas Cláusulas *tout court*, mas a concreta conformidade da atuação do Facebook com as disposições constantes das Cláusulas Contratuais-tipo a que se tinham vinculado[118]. A autoridade de controlo irlandesa argumenta que, como autoridade independente, não se encontra vinculada ao conteúdo da queixa apresentada por Schrems[119], e que, ao contrário deste, não acredita que a existência do artigo 4º das decisões das Cláusulas Contratuais-tipo sejam suficientes para assegurar a sua validade[120], necessitando da decisão do Tribunal de Justiça para poder concluir a investigação que iniciou[121].

Face às dúvidas acima aduzidas, a juíza que presidiu ao caso decidiu reenviar a questão da validade das Cláusulas Contratuais-tipo ao Tribunal de Justiça da União Europeia. Esta determinou também que formulação concreta destas questões só seria final após audição das partes.

A 11 de abril de 2018, o Tribunal Superior de Comércio irlandês definiu 11 questões[122] relacionadas com a validade das Cláusulas Contratuais-tipo a serem decididas pelo Tribunal de Justiça da União Europeia a título prejudicial, conforme o disposto no art. 267º do TFUE. Embora o Facebook tenha tentado recorrer da decisão de reenvio, a juíza irlandesa Caroline Costello pronunciou-se no sentido de considerar tal tentativa como uma manobra dilatória da

[115] *Cfr.* para. 154 Decisão Schrems II.
[116] *Cfr.* para. 321 Decisão Schrems II.
[117] *Ibidem, a contrario.*
[118] *Cfr.* para. 322 Decisão Schrems II.
[119] *Cfr.* para. 328 Decisão Schrems II.
[120] *Cfr.* para. 329 Decisão Schrems II.
[121] *Cfr.* para. 328 Decisão Schrems II.
[122] *Cfr.* Pedido de Decisão Prejudicial do Tribunal Superior de Comércio da Irlanda. Disponível em http://www.europe-v-facebook.org/sh2/ref.pdf [Consultado a 10/06/2018]

entidade em causa, ordenando o reenvio imediato das questões formuladas ao Tribunal de Justiça da União Europeia[123].

Ora, a posição da autoridade de controlo irlandesa e do Tribunal acima expostas parecem sofrer de certos erros estruturais na fundamentação, na medida em que não se pode considerar unicamente o facto de os Estados Unidos da América não disporem de um nível de proteção adequado, na medida em que as Cláusulas Contratuais-tipo constituem, precisamente, uma derrogação ao sistema de adequação. Cumpre assim analisar se, atendendo às circunstâncias específicas do caso, as transferências de dados visadas por estas Cláusulas têm um efeito adverso substancial na esfera de vida dos indivíduos[124], o que não é o mesmo que avaliar a adequação do país em causa, nos termos do artigo 25º da Diretiva.

Diga-se também, que, embora não estando diretamente aqui em discussão, reflexamente também as regras vinculativas aplicáveis às empresas poderiam ser objeto de invalidade, na mesma lógica aduzida quanto às Cláusulas Contratuais-tipo.

Como diz Lokke Moerel:

"*Qualquer outra interpretação levaria ao presente sistema de derrogações relativamente a transferências de dados para países não-adequados sob a Diretiva não ter qualquer tipo de função"*[125].

Parece, assim, duvidoso que o Tribunal de Justiça invalide totalmente as atuais decisões relativas às Cláusulas Contratuais-tipo[126]: mas caso o Tribunal de Justiça escolha focar-se exclusivamente nos casos mais gravosos (por exemplo, a já referida possibilidade de uma agência de inteligência americana requerer acesso injustificado a dados pessoais de cidadãos europeus), a decisão poderá bem ser outra.

[123] LOMAS, Natasha "Facebook denied a stay to Schrems II privacy referral" *Tech Crunch.* Disponível em https://techcrunch.com/2018/05/02/facebook-denied-a-stay-to-schrems-ii-privacy-referral/ [Consultado a 10/06/2018].
[124] MOEREL – cit. 79, p. 14.
[125] *Idem, ibidem*, p. 15.
[126] *Idem, ibidem* - p. 16.

5. As Regras Vinculativas Aplicáveis às Empresas (*Binding Corporate Rules*)

5.1. Considerações gerais

5.1.1. A adequação e necessidade das regras vinculativas aplicáveis a empresas

Os desenvolvimentos tecnológicos e a exploração do poder económico dos dados pessoais pelas empresas e a correspondente adaptação e mutação das estruturas funcionais das empresas no mundo contemporâneo decorrente das potencialidades oferecidas nesse âmbito, determinou que o volume de dados pessoais que uma multinacional gere e lida no seu dia-a-dia – sejam dados pessoais de clientes, fornecedores, parceiros comerciais, funcionários – é colossal e deixa de ser relevante apenas para a empresa em causa.

Devido à globalização das atividades das multinacionais, da centralização de vários serviços nucleares da multinacional e mesmo da organização de várias multinacionais em áreas territoriais (agrupando vários países e, consequentemente, várias jurisdições como, por exemplo, América do Norte) tais dados pessoais são de importância nuclear para todo o grupo de empresas.

Acresce o facto de relativamente a certas tecnologias recentes, como a computação na nuvem, nem se perceber exatamente onde é que os dados pessoais estão, na medida em que o ciberespaço é uma falácia conceptual, podendo os dados pessoais estar a ser utilizados em vários servidores, em qualquer parte do mundo, simultaneamente. Dessa forma, seria preferível que existisse um mecanismo que tornasse irrelevante a multitude de leis aplicáveis que a atividade de uma multinacional necessariamente espoleta.

Para uma empresa de relativa dimensão, que esteja em relação de grupo com outras empresas, e estando uma ou mais destas estabelecidas fora da União Europeia, não é nem exequível nem viável entrar numa rede de contratos com cláusulas contratuais-tipo infindável. Reitere-se que também não é lícito usar alguma das derrogações ao princípio geral, no sentido em que as transferências de dados pessoais feitas por estas empresas no decorrer da sua atividade não constituem transferências ocasionais. Sendo transferências efetuadas de forma

continuada e sistémica, requerem-se que estejam abrangidas por um quadro normativo específico: os mecanismos jurídicos presentes no art. 46º, n.º 2 do Regulamento.

Em vez de celebrar um número infindável de contratos com as cláusulas contratuais-tipo entre todas as empresas do grupo, faz muito mais sentido que exista um código de conduta interno[127] que vincule todas as empresas do grupo, impondo regras estritas relativamente às operações de tratamento de dados pessoais[128]: é esse o papel das regras vinculativas aplicáveis às empresas.

Materialmente, tal código de conduta teria o mesmo efeito que os infinitos contratos e cláusulas contratuais-tipo; aliás, teria o valor acrescentado de ser uma condensação de toda a política do grupo num só documento, o que permitiria aos titulares dos dados (sejam trabalhadores das empresas em causa ou clientes) uma maior segurança jurídica e cognoscibilidade quanto aos princípios e mecanismos instituídos relativamente ao tratamento dos seus dados por determinada entidade.

Este mecanismo foi reconhecido no novo Regulamento como assegurando garantias adequadas (46º, n.º 2 al. b)), por, nomeadamente, pretender conferir expressamente aos titulares dos dados direitos relativamente ao tratamento dos seus dados pessoais, sendo condição *sine qua non* da sua aprovação (art. 47º, n.º 1 al. b)).

Como se demonstrará, esta é uma forma de co-regulação, na medida em que é permitido aos grupos de empresas determinar as concretas medidas e termos da sua conformidade com as regras vigentes em matéria de proteção de dados, de acordo com a realidade prática das suas necessidades e operações de tratamento prosseguidas. A co-regulação está, assim, estritamente ligada à abordagem baseada no risco prevista – ainda que implicitamente – no Regulamento, e ao princípio da responsabilidade (art. 5º, n.º 2).

Neste sentido, as regras vinculativas aplicáveis às empresas geram um "porto seguro" para um dado grupo de empresas, em que os fluxos de dados pessoais intra-grupo podem ocorrer livremente, sem adicionada burocracia.

[127] Embora constitua um código de conduta, por consubstanciar um normativo interno que deve necessariamente ditar a atuação de todos os seus membros, convém não confundir com a terminologia adotada tanto na Diretiva como no Regulamento, onde "código de conduta" representa o conjunto de regras definidas por um determinado setor de atividade, sendo vinculativo para as empresas que – voluntariamente – aderirem a tal documento.
[128] MOEREL – cit. 79, p. 1.

Face à desadequação do instituto da decisão de adequação – mesmo a versão atualizada presente no Regulamento – e sendo que a maior parte dos parceiros económicos da União Europeia (Brasil, China, Índia, *etc*) não são, nos termos da normativa europeia relativa à proteção de dados, países com um "nível de proteção adequado" (como referido, atendendo ao parco número de países reconhecidamente "adequados" pela Comissão, tal derrogação tem efeitos muito limitados para multinacionais que operam à escala mundial) torna-se necessária a existência de alternativas pragmáticas, especialmente as regras vinculativas aplicáveis às empresas. Caso contrário, estimula-se o incumprimento das referidas disposições[129].

5.1.2. As regras vinculativas aplicáveis às empresas durante a vigência da Diretiva: criação, pressupostos e procedimentos de aprovação

O problema quanto ao potencial incumprimento era ainda mais pronunciado aquando da vigência da Diretiva, antes da existência do mecanismo das regras vinculativas aplicáveis às empresas: antes da harmonização prevista pelo Regulamento, os grupos de empresas tinham que assegurar a conformidade com as leis de vários países da União Europeia, com requisitos muito diferentes os quais, por vezes, chocavam entre si. Esses conflitos de lei aplicável tornavam impossível o completo e total cumprimento consistente das multinacionais[130].

Em vez de procurar uma impossível conformidade total com a lei em cada país onde se estabeleciam, as multinacionais preferiram uma abordagem "top-down"[131] ,em que a empresa-mãe dá instruções às restantes empresas do grupo, implementando políticas de governação de privacidade à escala mundial – o que constituía uma forma de auto-regulamentação.

As autoridades de controlo foram tremendamente pressionadas para reconhecer a validade e legitimidade de tais políticas como instrumento de garantias adequadas de proteção de dados pessoais objeto de tratamento e transferência internacionais, onde quer que estejam localizadas, recaindo no âmbito de previsão do art. 26, n.º 2, da Diretiva.

[129] RAND REPORT – cit. 3, p. 43.
[130] MOEREL – cit. 79, p. 8.
[131] *Idem, ibidem*, p. 91.

Tal reconhecimento deste instrumento pelo Grupo de Trabalho do Artigo 29º acabou por ser postulado em janeiro de 2003, através do documento de trabalho WP74[132], sendo neste documento que foram aduzidas as primeiras ideias do que deveriam ser as características e requisitos obrigatórios a constar das regras vinculativas aplicáveis às empresas.

Estas regras reportavam-se unicamente às obrigações do responsável pelo tratamento[133]. Tal circunstância afigura-se óbvia, na medida em que a Diretiva apenas prescrevia obrigações para esta figura (art. 6º, n.º 2), devendo qualquer subcontratante seguir exclusivamente as instruções deste (art. 16º).

Necessário se torna clarificar, porém, uma situação: estas regras vinculativas aplicáveis às empresas, embora exclusivamente para responsáveis pelo tratamento, continuam a aplicar-se quando, por hipótese, certa empresa do grupo preenche o papel de subcontratante, por estar a proceder ao tratamento de dados em nome de uma outra empresa do grupo[134].

Na medida em que essa empresa se qualifica, quanto a essa específica operação de tratamento, como um responsável pelo tratamento, as regras vinculativas aplicáveis às empresas aplicam-se. Assim já não seria se uma empresa do grupo estivesse a funcionar como uma subcontratante para uma empresa terceira não pertencente ao grupo de empresas da multinacional[135] ou procedesse ao tratamento de dados pessoais em nome dos seus clientes – tais operações de tratamento estariam fora do âmbito de proteção e das reconhecidas garantias adequadas asseguradas pelas regras vinculativas aplicáveis às empresas do grupo[136].

Importante referir, antes de mais, que pelo facto de estas regras vinculativas aplicáveis às empresas não estarem taxativamente previstas na Diretiva, a Comissão Europeia não tinha qualquer poder para proceder à sua aceitação, recaindo tal poder decisório nas autoridades de controlo dos Estados-Membros.

---

[132] ARTICLE 29 WORKING PARTY - Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers.

[133] *Idem, ibidem*, p. 7.

[134] Um exemplo seria se uma multinacional fizesse uso de um sistema centralizado, como um centro de processamento de dados – incluindo necessariamente dados pessoais – dos seus funcionários de todas as empresas do grupo. Na medida em que essa empresa do grupo recolhe e agrupa (o que recai na definição de "tratamento" no âmbito da legislação de proteção de dados) tais dados pessoais está a agir como subcontratante, porque procede a operações de tratamento em nome de todas as empresas do grupo que integra.

[135] MOEREL – cit. 79, p. 106.

[136] Pelo que seria necessário introduzir outro mecanismo, como as cláusulas contratuais-tipo.

Como é possível depreender do seu nome, o caráter vinculativo destas regras é um elemento essencial: só garantindo a oponibilidade das regras se poderá considerar que as regras vinculativas aplicáveis às empresas preveem garantias adequadas[137], nos termos do artigo 26º, n.º 2 da Diretiva. As regras deverão ser quer internamente vinculativas, devendo vincular todas as empresas do grupo (incluindo os seus funcionários; art. 47º, n.º 1 al. a)[138]) bem como produzir efeitos externamente, na medida em que conferem direitos aos cidadãos – o que se compreende, na medida em que estas regras vinculativas aplicáveis às empresas funcionam como uma ficção operante da realidade europeia em matéria de proteção de dados independentemente da real localização das empresas e, consequentemente, dos dados pessoais objeto de tratamento.

Quanto ao carácter vinculativo a nível interno das regras, o Grupo de Trabalho do Artigo 29 considera que não é suficiente que sejam teoricamente vinculativas, terão de ser demonstradamente vinculativas na prática[139]. Significa isto que devem existir mecanismos internos que assegurem que as empresas do grupo e os funcionários que as integram se sintam obrigados a cumprir as regras definidas nesse âmbito. Mecanismos sugeridos pelo Grupo de Trabalho do Artigo 29 incluem a existência de sanções disciplinares em caso de incumprimento das regras, ações de formação para os funcionários e prestadores de serviço, etc.[140]

Quanto ao carácter vinculativo externo, deverão as regras vinculativas aplicáveis às empresas prever cláusulas de terceiros beneficiários para os titulares de dados[141]. Estas regras teriam, nomeadamente, de prever a possibilidade de os titulares dos dados poderem apresentar uma queixa quer na autoridade de controlo competente quer no tribunal competente. Tal requisito é cumulativo, e de extrema importância para o Grupo de Trabalho do Grupo 29, atendendo ao facto de a queixa para a autoridade de controlo não dever constituir uma última instância, na medida em que os titulares dos dados poderão não concordar com a decisão desta, sendo necessário existir uma instância de recurso, especialmente pelo facto dos poderes desta

[137] ARTICLE 29 WORKING PARTY – cit. 99, p. 8.

[138] As opiniões do Grupo de Trabalho do Artigo 29 (*cfr*. WP256, p. 6) referem que tal vinculação com os funcionários poderá ser feita através de uma cláusula nos respetivos contratos de trabalho. Na minha experiência profissional, como advogado estagiário, já tive acesso a vários contratos de trabalhadores de grandes empresas que continham cláusulas que genericamente obrigam estes a observar o disposto nos códigos de conduta e políticas sobre variadas matérias vigentes; não parece ser necessário proceder à atualização tais contratos para que estejam em conformidade com a disposição por ora em análise.

[139] ARTICLE 29 WORKING PARTY – cit. 99, p. 10

[140] *Ibidem.*

[141] *Idem*, p. 11.

a nível de coerção serem limitados. Acresce o facto de que, sob a égide da Diretiva, nenhuma autoridade de controlo ter a legitimidade para garantir indemnizações a particulares, tarefa da competência exclusiva dos tribunais.

Daqui se retira um dos óbvios benefícios das regras vinculativas aplicáveis às empresas: cidadãos de países com legislação em matéria de proteção de dados menos protetoras dos cidadãos poderão beneficiar, quanto àquela empresa e grupo em que se insere, de toda a miríade de direitos previstos pela legislação europeia nessa matéria. Tal circunstância poderá servir como catalisador de uma mudança significativa em termos de mentalidade e consciencialização para as questões da privacidade e dos dados pessoais à escala mundial.

Cumpre, aliás, recordar que as regras quanto aos fluxos transfronteiriços de dados para países terceiros não desobrigam as entidades envolvidas no tratamento de cumprir os restantes princípios constantes do diploma legal respetivo; constituem uma adicional camada regulatória que pretende, precisamente, evitar a fuga ao cumprimento dessas normas.

Um dos requisitos então enunciados era precisamente que a empresa-mãe do grupo[142] deveria aceitar responsabilidade em nome de todas as empresas do grupo, inclusive relativamente ao pagamento de qualquer indemnização, por qualquer dano ou prejuízo que decorra da violação das regras vinculativas aplicáveis às empresas[143].

Querendo, o que sempre dependerá da estratégia interna do grupo, pode a empresa-mãe ou a empresa delegada ter direito de regresso relativamente aos custos e prejuízos que sofreu resultantes da violação das regras vinculativas aplicáveis às empresas por uma empresa do grupo[144].

O Grupo de Trabalho do Artigo 29 admite a hipótese, porém, face a diferentes estruturas empresariais, de não ser uma específica empresa do grupo a arcar com todas as responsabilidades. Neste caso, o grupo em causa terá de demonstrar que não pode nomear uma

[142] Se esta estivesse estabelecida na União Europeia; caso contrário, a empresa-mãe deveria delegar numa empresa do grupo com sede na União Europeia para tomar esse papel - *cfr*. ARTICLE 29 WORKING PARTY – cit. 99, p. 11.
[143] ARTICLE 29 WORKING PARTY - cit. 99, p. 18.
[144] *Idem, ibidem*, p. 19.

única empresa, e terá de propor outros mecanismos de responsabilidade que a ela melhor se adequem[145].

Releva referir que a responsabilidade definida nestes termos só se estende na medida em que se tratem de dados pessoais que estejam abrangidos pela proteção consignada nos diplomas legais referidos[146], ainda que as regras vinculativas aplicáveis às empresas de um dado grupo de empresas abranjam outros dados pessoais. Tal incumprimento do código de conduta relativo a transferência de dados pessoais[147] poderá, não obstante, resultar em responsabilidade noutros termos[148].

O Grupo de Trabalho do Artigo 29 não prescreve a forma de vincular internamente as regras vinculativas aplicáveis às empresas, cabendo ao grupo em causa demonstrar que cumpriu este requisito, quer seja através de um acordo em que todas as empresas do grupo são outorgantes, ou por contrato individual (ainda que idêntico) celebrado pela empresa-mãe com cada uma das empresas do grupo[149].

5.1.2.1. Os procedimentos de aprovação das regras vinculativas aplicáveis às empresas pelas autoridades de controlo europeias

Só em 2005 (tendo tal demora sido alvo de críticas por vários interessados[150]), o Grupo de Trabalho do Artigo 29 definiu um regime-quadro para um Procedimento de Cooperação

[145] ARTICLE 29 WORKING PARTY – Working Document on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules, p. 3.
[146] *Idem, ibidem*, p. 19.
[147] Imagine-se, por exemplo, que determinado grupo de empresas incluiu nas suas *binding corporate rules* toda a sua política de tratamento de dados, e o incumprimento reportava-se a um funcionário proveniente da África do Sul a trabalhar numa filial na Argentina; existindo um incumprimento relativo a este efabulado titular dos dados esse facto não despoleta a aplicação das sanções previstas no direito europeu.
[148] Tem sido referido que vários fundamentos de incumprimento podem ser alegadas quanto ao incumprimento de códigos de conduta disponíveis ao público (como seria o caso das regras vinculativas aplicáveis às empresas relativamente aos dados pessoais dos clientes) na legislação europeia, podendo o incumprimento do código de conduta constituir: violação da lei por publicidade enganosa; prática comercial injusta; e violação dos princípios de conformidade dos bens com o disposto no contrato. Porém, tais bases legais não garantem, necessariamente, qualquer indemnização ou qualquer recurso para o terceiro beneficiário. (*cfr*. MOEREL - cit. 83, p. 134).
[149] ARTICLE 29 WORKING PARTY – cit. 99, p. 3.
[150] RAND REPORT – cit. 3, p. 35.

entre as autoridades de controlo dos Estados-Membros para efeitos de aprovação de regras vinculativas aplicáveis às empresas [151].

Este regime segue a "abordagem de rede" que decorre do Art. 28º, n.º 6 da Diretiva, que prescreve que cada autoridade de controlo pode ser solicitada a exercer os seus poderes por uma outra autoridade de controlo de outro Estado-Membro. Esta norma refere também que as autoridades de controlo deverão cooperar entre si na medida do necessário ao desempenho das suas funções (*in casu*, aprovação das regras vinculativas aplicáveis às empresas no Estado-Membro respetivo e verificação da sua correta aplicação prática), em especial através do intercâmbio de quaisquer informações que sejam reputadas como úteis.

Através deste procedimento, as regras vinculativas aplicáveis às empresas eram submetidas à aprovação de uma designada autoridade de controlo competente (sendo sobre o grupo de empresas que recai o ónus de escolher a autoridade de controlo e explicar os motivos subjacentes a tal escolha[152]), devendo remeter a esta as "informações apropriadas"[153] para o efeito, nomeadamente, a natureza e estrutura geral das operações de tratamento a ter lugar na União Europeia/Espaço Económico Europeu, localização e natureza das afiliadas na União Europeia, o número de funcionários ou titulares dos dados envolvidos, os meios e finalidades das operações de tratamento, entre outras informações.

Depois de receber estas informações, a autoridade de controlo considerada competente pelo grupo de empresas requerente teria de reencaminhá-las para as outras autoridades de controlo relevantes, com a indicação se concorda, ou não, em estarem verificados os requisitos para ser a principal autoridade neste âmbito[154]. As outras autoridades de controlo teriam então duas semanas (sendo prorrogável por igual período, a pedido destas) para se pronunciar quanto à competência da autoridade de controlo primeiramente designada, devendo fundamentar a sua decisão.

[151] ARTICLE 29 WORKING PARTY - Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules".
[152] As autoridades de controlo reservam-se ao direito de decidir uma autoridade de controlo competente diferente (*cfr*. para. 2.2, *idem, ibidem*).
[153] *Idem, ibidem*, p. 3.
[154] *Ibidem.*

Depois deste período de consulta prévio, as autoridades de controlo deveriam chegar a uma conclusão quanto à autoridade de controlo com principal autoridade no caso em concreto[155].

Depois de definida qual a autoridade de controlo com principal autoridade, teriam inicio as negociações com o grupo requerente, tendentes à conclusão de um "projeto consolidado" de regras vinculativas aplicáveis às empresas, sendo tal projeto distribuído pelas autoridades de controlo relevantes para comentários. O prazo, também este apenas meramente indicativo[156], fixar-se-ia em um mês.

Após o período de comentários, retomar-se-iam as negociações entre a autoridade de controlo com autoridade principal e o grupo requerente, se necessário[157]. Se a referida autoridade de controlo considerasse que o grupo estava em posição de integrar satisfatoriamente as recomendações que lhes foram endereçadas, convidaria este a apresentar um "projeto final", que seria remetido – outra vez – para as autoridades de controlo relevantes para se pronunciarem quanto à adequação das garantias apresentadas quanto ao tratamento de dados pessoais, confirmando a sua adequação.

Não restam dúvidas que constituía um processo extremamente intrincado e complexo, cujos prazos poderiam estender-se em demasia, podendo tal processo de aprovação traduzir-se na incerteza jurídica quanto à legalidade dos fluxos transfronteiriços durante a sua duração. O potencial dano económico de tal demora para o grupo requerente não é passível de ser quantificado. Acresce ainda o facto de cada autoridade de controlo nacional poder obrigar a alterações específicas, agravando consideravelmente o que já era um processo custoso e moroso[158].

Outro ónus que recaía sobre o grupo requerente que adicionalmente complexificava o quadro de referência acima apresentado é o facto de quer o "projeto consolidado" quer o "projeto final" das regras vinculativas aplicáveis às empresas a serem apresentados às

[155] *Ibidem.*

[156] "Em circunstâncias normais, o período para comentários no projeto consolidado não deverá exceder o prazo de um mês" (sublinhado nosso) - *cfr*. *Ibidem.*

[157] *Ibidem.*

[158] MESAIKOU, Evangelia – Examining the Binding Corporate Rules as the most promising solutions for the cross border data transfers of multinational companies under the EU Data Protection Directive – A Comparative study with the Cross Border Privacy Rules developed in the APEC, p. 4.

autoridades de controlo relevantes teriam de ser apresentados em inglês e na língua oficial de todos os Estados-Membros onde estivessem estabelecidas.

Na tentativa de ultrapassar, de certa forma, os excessivos ónus e demora associados ao mecanismo de cooperação descrito *supra*, vários Estados-Membros aderiram ao "Procedimento de Reconhecimento Mútuo"[159]. Este procedimento integrou dezanove autoridades de controlo dos Estados-Membros e tinha como objetivo tornar mais rápido o processo de aprovação de regras vinculativas aplicáveis às empresas acima delineado.

Essencialmente, o Procedimento de Reconhecimento Mútuo, como o nome indica, previa que as autoridades de controlo deveriam reconhecer e aceitar a decisão quanto à adequação das garantias prestadas pelas regras vinculativas aplicáveis às empresas tomada pela autoridade de controlo com autoridade principal (neste procedimento coadjuvada por duas autoridades de controlo onde o grupo de empresas aplicante tivesse uma "forte presença").

Depois do processo (mais expedito que o Procedimento de Cooperação anteriormente apresentado) estar finalizado, aquando da decisão final de aprovação das regras vinculativas aplicáveis às empresas pela autoridade de controlo com autoridade principal, tal decisão seria automaticamente replicada e reconhecida nos restantes membros do Procedimento de Reconhecimento Mútuo, não carecendo da aprovação expressa destas.

Relativamente às autoridades de controlo dos Estados-Membros que não tomaram parte do referido Procedimento de Reconhecimento Mútuo (e na medida que a aprovação destas é necessária por alguma empresa do grupo requerente estar estabelecido nesses países) a autoridade de controlo com autoridade principal que aprovou as regras vinculativas aplicáveis às empresas deveria iniciar o Procedimento de Cooperação com as autoridades de controlo casuisticamente relevantes que ainda não se pronunciaram, nos termos já expostos *supra*.

Porém, nem todas as autoridades de controlo aderiram ao mecanismo de cooperação acima descrito, nem reconheceram a validade e legitimidade das regras vinculativas aplicáveis às empresas. Outras decidiram impor requisitos adicionais aos previstos pelo Grupo de Trabalho do Artigo 29[160].

A este propósito, cumpre lembrar que ainda que o Grupo de Trabalho do Artigo 29 seja considerado um regulador *de facto* em matéria de proteção de dados, pelo facto de as suas

[159] ARTICLE 29 WORKING PARTY - Press Release (de 2 de outubro de 2008).
[160]MOEREL – cit. 79, p. 109.

recomendações e opiniões serem efetivamente observadas na prática (o que não é alheio à circunstância de este grupo de trabalho ser efetivamente composto por membros das autoridades de controlo cuja atividade procura regular), este grupo de trabalho apenas desempenha um papel consultivo. Dessa forma, as autoridades de controlo nacionais não estão vinculadas à produção normativa do Grupo de Trabalho, podendo decidir o seu próprio caminho.

Veja-se, por exemplo, o caso de Portugal. A Comissão Nacional de Proteção de Dados (doravante, CNPD), como autoridade de controlo portuguesa recusou-se a integrar o Procedimento de Reconhecimento Mútuo sob o fundamento de que as regras vinculativas aplicáveis às empresas são "*declarações unilaterais que não são válidas para transferências internacionais de dados*"[161].

Não obstante, a CNPD publicou em 2015 uma deliberação em que reconhece e aceita a validade de Acordos Intragrupo. Ora, esta entidade define este tipo de acordo como sendo "um *contrato multilateral entre várias empresas do mesmo grupo empresarial, nos termos do qual as partes se vinculam a cumprir um conjunto de normas de garantia dos direitos de proteção dos dados pessoais e da privacidade dos titulares dos dados"*[162], mesmo que tal grupo empresarial abranja empresas localizadas em países terceiros.

Tais acordos parecem, assim, enformados pela mesma lógica que as regras vinculativas aplicáveis às empresas: a diferença essencial sendo obviamente a natureza contratual destes acordos. Aliás, a CNPD embora não refira expressamente as regras vinculativas aplicáveis às empresas na deliberação em análise, fez a seguinte implícita ressalva:

---

[161] "(…) *na página 59 do seu Relatório de Atividades para 2003/2004, a CNPD descreve a participação do seu representante nas discussões do Grupo do Artigo 29 sobre as regras vinculativas aplicáveis às empresas, referindo-se aos mesmos como "declarações unilaterais auto-vinculativas". O relatório continua dizendo que, embora os representantes da CNPD tenham participado no debate, recusaram-se a tomar uma posição oficial nas discussões devido ao facto de "declarações deste tipo não poderem constituir uma fonte de obrigação na legislação portuguesa". A sua decisão baseou-se no facto de não existir uma disposição legal ou outra autoridade reconhecida pela lei portuguesa (ou da UE) que possa conferir às regras vinculativas aplicáveis às empresas qualquer efeito juridicamente vinculativo "* (*cfr.* TRAÇA, João e EMBRY, Bernardo – The Portuguese Regulatory Regime for Binding Corporate Rules, p. 207).
Será interessante perceber qual será a resposta da CNPD ao expresso reconhecimento deste mecanismo no Regulamento, face à argumentação usada.

[162] CNPD - Deliberação n.º 1770/2015 relativa ao procedimento de análise dos Acordos Intragrupo (IGA) para transferências de dados para fora da UE, p. 2.

"*Não nos referimos aqui a declarações unilaterais autovinculativas por parte das empresas, mas sim a contratos"*[163].

Decorrente das características apresentadas dos processos anunciados de aprovação das regras vinculativas aplicáveis às empresas, é fácil compreender que possa ser um fator dissuasor das empresas que queiram proceder à adoção destas regras. O sistema apresentava claros problemas, o que justificava a baixa adesão ao mesmo.

Outro problema consistia na maior parte das aplicações de regras vinculativas aplicáveis às empresas estarem concentradas num reduzido número de autoridades de controlo[164].

5.1.3. As regras vinculativas aplicáveis às empresas no Regulamento

O início da aplicação, a 25 de maio de 2018, do Regulamento 2016/679 irá alterar significativamente o *statu quo* quanto à legitimidade e relevância das regras vinculativas aplicáveis às empresas no âmbito da proteção de dados pessoais. O Regulamento especificamente prevê as regras vinculativas aplicáveis às empresas como um mecanismo apropriado para demonstração de garantias adequadas (artigo 46º), promovendo várias alterações ao supramencionado regime-quadro delineado aquando da vigência da Diretiva.

Como referido anteriormente, a escolha do Regulamento como instrumento tem várias vantagens, incluindo do ponto de vista da harmonização jurídica entre os Estados-Membros, o que se pode traduzir num mais expedito processo de aprovação das regras vinculativas aplicáveis às empresas: sendo direitamente aplicável nas esferas jurídicas dos Estados-Membros, estas regras deixam de carecer de autorização nacional. Tal não significa que certas

[163] *Ibidem.*
[164] MOEREL – cit. 79, p. 114.

normas a observar não sejam endógenas de um determinado país, constituindo obrigações legais que deverão ser observadas conjuntamente com as previstas no Regulamento[165].

Outra novidade que decorre necessariamente das alterações legislativas efetuadas sob a égide do Regulamento, prende-se com a consagração[166] das regras vinculativas aplicáveis às empresas destinadas a subcontratantes: o que se afigura natural, na medida em que o rol de deveres e real responsabilidade desta figura no âmbito do Regulamento foram densificadas (art. 44º).

As regras vinculativas aplicáveis às empresas aquando do seu tratamento de dados enquanto subcontratantes visam facilitar e promover o tratamento de dados pessoais feitos por uma entidade subcontratante, em nome e sob as instruções documentadas de um responsável pelo tratamento estabelecido na União Europeia, e que são tratados ulteriormente a nível do grupo de empresas desse subcontratante inicial.

As regras vinculativas aplicáveis às empresas dos subcontratantes deverão ser anexadas ao contrato de prestação de serviços celebrado com o responsável pelo tratamento[167], de forma a demonstrar o compromisso dos subcontratantes com as regras estabelecidas nesse documento e que poderão responder pela violação das mesmas[168]. Caso considere existir uma violação dessas regras, o responsável pelo tratamento tem direito a interpor ação judicial, e a deduzir o conexo pedido de indemnização, contra qualquer empresa do grupo do subcontratante[169].

As regras vinculativas aplicáveis às empresas destinadas aos subcontratantes devem estabelecer expressamente que estes se comprometem a fornecer aos responsáveis pelo tratamento as informações necessárias e relevantes para o cumprimento das suas obrigações para com os titulares dos dados.

Estas regras deverão respeitar as mesmas regras quanto ao carácter vinculativo – interno e externo – tal como definido quanto às regras vinculativas aplicáveis às empresas dos responsáveis pelo tratamento.

---

[165] Pense-se por exemplo na obrigação que recai sobre várias empresas sediadas no território nacional de manter a seu dispor dados durante 7 anos por motivos da legislação de combate ao branqueamento de capitais e financiamento de capitais. Outras ordens jurídicas poderão dispor diferentemente, na medida em que a lei portuguesa transpõe uma Diretiva europeia que só impõe, no mínimo, 5 anos de período de conservação.

[166] As regras vinculativas aplicáveis às empresas destinadas a subcontratantes tinham já sido previstas pelo Grupo de Trabalho do Artigo 29 em junho de 2012 (*cfr.* WP195*).*

[167] ARTICLE 29 WORKING PARTY – Explanatory Document on the Processor Binding Corporate Rules, p. 6.

[168] *Ibidem.*

[169] *Ibidem,* p. 17.

O Regulamento também promove alterações relativamente aos procedimentos de cooperação anteriormente descritos. Na medida em que o Regulamento prescreve que a autoridade de controlo competente para agir como autoridade principal é a autoridade de controlo do estabelecimento principal[170][171] do grupo empresarial, já não será necessário que o grupo de empresas designe uma autoridade de controlo competente; o próprio "Procedimento de Reconhecimento Mútuo" deixa de ter qualquer razão de existir, em consequência destes desenvolvimentos legislativos[172].

A autoridade de controlo com autoridade principal será a encarregada de aprovar as regras vinculativas aplicáveis às empresas do grupo empresarial em causa. A aprovação das regras vinculativas aplicáveis às empresas, bem como outras medidas[173], está sujeita ao procedimento de controlo de coerência, previsto no artigo 63º do Regulamento.

Este procedimento de controlo de coerência é um mecanismo que obriga, em certos casos, à cooperação das autoridades de controlo, de forma a "contribuir para a aplicação coerente do presente regulamento em toda a União" (art. 63º).

Ora, nos termos do disposto do Regulamento e no âmbito deste procedimento de controlo de coerência, o Comité Europeu de Proteção de Dados[174] (que vem substituir o Grupo de Trabalho do Artigo 29, doravante "Comité") deverá emitir o seu parecer no prazo máximo

---

[170] O Regulamento, através do seu Considerando 36, informa como se deverá proceder à determinação do que constitui esse estabelecimento principal:
"*O estabelecimento principal de um responsável pelo tratamento na União deverá ser o local onde se encontra a sua administração central na União, salvo se as decisões sobre as finalidades e os meios de tratamento dos dados pessoais forem tomadas noutro estabelecimento do responsável pelo tratamento na União. Nesse caso, esse outro estabelecimento deverá ser considerado o estabelecimento principal. O estabelecimento principal de um responsável pelo tratamento na União deverá ser determinado de acordo com critérios objetivos e deverá pressupor o exercício efetivo e real de atividades de gestão que determinem as decisões principais quanto às finalidades e aos meios de tratamento mediante instalações estáveis. Esse critério não deverá depender do facto de o tratamento ser realizado nesse local. (...) Sempre que o tratamento dos dados seja efetuado por um grupo empresarial, o estabelecimento principal da empresa que exerce o controlo deverá ser considerado o estabelecimento principal do grupo empresarial, exceto quando as finalidades e os meios do tratamento sejam determinados por uma outra empresa*" (sublinhado nosso).

[171] Assistimos assim a uma consagração do princípio do país de origem relativamente à jurisdição.

[172] MOEREL – cit. 79, p. 116.

[173] Outras medidas tomadas pela autoridade de controlo competente que estão sujeitas ao procedimento de controlo da coerência: adoção de uma lista das operações de tratamento sujeitas à exigência de proceder a uma avaliação do impacto sobre a proteção dos dados; adoção dos critérios de acreditação de códigos de conduta; adoção de critérios de organismos de certificação; determinação de cláusulas contratuais-tipo; autorização de cláusulas contratuais *ad hoc* (*cfr.* art. 64º n.º 1 do Regulamento).

[174] Órgão independente, dotado de personalidade jurídica (*cfr*. Considerando 139 do Regulamento).

de oito semanas quanto ao projeto apresentado[175], por maioria simples dos membros que o compõem (art. 64º, n.º 3). Caso os membros do Comité não tenham respondido ou levantado objeções no referido prazo de oito semanas, presume-se que estes estão de acordo com o projeto de regras vinculativas aplicáveis às empresas apresentado.

Como se poderá compreender, em resposta às várias críticas feitas ao anterior sistema, o processo de aprovação das regras vinculativas aplicáveis às empresas foi substancialmente simplificado. O reconhecimento expresso no Regulamento deste mecanismo, e o facto de já não carecer de autorização específica de todas as autoridades de controlo dos Estados-Membros onde empresas do grupo estão estabelecidas, constitui um fator igualmente essencial para o potencial incremento da adesão de multinacionais.

O facto de uma multinacional ter de cooperar, sob as novas normas previstas no Regulamento, apenas com uma autoridade de controlo é também um potencial aliciante para aquela, na medida em que é provável que já tenha interagido com tal autoridade de controlo noutras instâncias. Mesmo que não seja esse o caso, poderá a multinacional criar relações de confiança com a autoridade de controlo, facilitando o processo[176].

O reconhecimento das regras vinculativas aplicáveis às empresas para responsáveis para tratamento e subcontratantes, bem como a simplificação do regime de aprovação destas, demonstram também a desejável abordagem pragmática do legislador europeu face ao clássico *trade-off* entre o manter a sua postura protecionista dos direitos fundamentais dos cidadãos europeus e responder às necessidades do mercado. Através destas inovações legislativas o legislador europeu manifesta igualmente a necessidade de se encontrar uma solução flexível e com reflexos reais na prática.

[175] A autoridade de controlo deverá enviar ao Comité "as informações que forem pertinentes, incluindo, consoante o caso, um resumo dos factos, o projeto de decisão, os motivos que tornam necessário adotar tal medida, bem como as posições das outras autoridades de controlo interessadas." (*cfr.* art. 64º n.º 4 do Regulamento)

[176] PIETRZAK, Sylwia - Transborder Data Flows: Binding Corporate Rules As A Global Transfer Mechanism and Trusted Data Processing Area, p. 22.

5.2. Requisitos das Regras Vinculativas Aplicáveis às Empresas no Regulamento 2016/679

Os requisitos presentes no Regulamento não surgem *ex novo*, de um vácuo regulatório; são, parcialmente, uma codificação dos requisitos prescritos pelo Grupo de Trabalho do Artigo 29, tendo sido ajustados a certas novas realidades constantes do Regulamento. Um exemplo é a adoção de pressupostos que estejam de acordo com o novo princípio da responsabilidade (art. 5º, n.º 2).

As regras vinculativas aplicáveis às empresas para responsáveis pelo tratamento devem conter no próprio documento ou no formulário a apresentar à autoridade de controlo competente[177], sob pena de rejeição, os seguintes elementos[178]:

i) O dever de assegurar o cumprimento das regras, vinculando todas as empresas do grupo e seus funcionários a esta obrigação (arts. 47º n.º 1 al. a) e 47º n.º 2 al. c));

ii) Demonstração de como, na prática, estas regras vinculam as entidades e indivíduos referidos no número anterior (arts. 47º n.º 1 al. a) e 47º n.º 2 al. c)), seja através de acordos intra-grupo, seja através de qualquer outro meio desde que essa vinculação seja efetivamente alcançada e demonstrável (quanto às empresas do grupo); quanto à vinculação dos funcionários, se está é feita, por hipótese, através de cláusulas individuais em cada contrato de trabalho com sanções previstas em caso de incumprimento, acordo avulso individual com sanções, acordo coletivo com os trabalhadores, etc;

iii) A criação de direitos de terceiro beneficiário para os titulares dos dados, incluindo a possibilidade de estes interporem uma queixa perante os tribunais competentes ou perante a autoridade de controlo (arts. 47º n.º 1 al. b) e 47º n.º 2 al. c)). As regras vinculativas aplicáveis às empresas do responsável pelo tratamento deverão expressamente prever os direitos dos titulares dos dados, fazendo menção expressa aos

[177] Será feita menção expressa de quando algum requisito deva constar do formulário, mas não no próprio texto das regras vinculativas aplicáveis às empresas

[178] Lista baseada no ARTICLE 29 WORKING PARTY - Working Document Setting up a Table with the Elements and Principles to be Found in Binding Corporate Rules

variados direitos que lhes assistem, bem como do direito que estes têm de recorrer ao tribunal ou à autoridade de controlo competente para obter compensação ou obrigar à reparação por qualquer incumprimento das obrigações nelas elencadas;

iv) Aceitação, por parte do estabelecimento principal do grupo empresarial ou do designado membro europeu com tais tarefas delegadas, da responsabilidade por toda e qualquer violação das regras vinculativas aplicáveis às empresas por parte de uma entidade envolvida que não se encontre estabelecida na União (art. 47º, n.º 2 al. f)). Assim, as regras deverão prever que mesmo em caso de violação por parte de uma empresa coberta pelas regras vinculativas aplicáveis às empresas estabelecida num país terceiro, o titular dos dados poderá exercer os seus direitos perante um tribunal ou autoridade de controlo desse membro estabelecido na União Europeia que aceitou a responsabilidade.

O Grupo de Trabalho do Artigo 29 fez já saber que, nos casos em que esta estrutura de responsabilidade não possa ser observada, as regras vinculativas aplicáveis às empresas poderão prever que cada membro estabelecido na União Europeia que exporte dados pessoais para empresas do grupo em países terceiros, poderá ser responsável por qualquer violação que ocorra após essa exportação em particular;

v) As empresas que aceitarem responsabilidade, nos termos do número anterior, terão de demonstrar que dispõem de suficientes ativos[179] na eventualidade de terem que pagar qualquer compensação por danos que resultem da violação das regras vinculativas aplicáveis às empresas[180];

vi) Declaração de que o ónus de prova recai sobre as empresas e não sobre o individuo. Poderão, porém, as empresas em causa exoneradas de qualquer responsabilidade se conseguirem demonstrar que os danos ou prejuízos referidos pelo titular dos dados afetado não lhe podem ser imputados (art. 47º, n. º2 al. f));

vii) Prever obrigações de transparência e fácil acesso às regras vinculativas aplicáveis às empresas para os titulares dos dados (art. 47º, n.º 2 al. g)). Os titulares dos dados deverão ser informados detalhadamente dos direitos que lhes assistem, nomeadamente de terem direitos de terceiro beneficiário e os meios que poderão destes fazer uso, nos

[179] ARTICLE 29 WORKING PARTY - WP74 (*cfr.* para. 5.5.2) e WP108 (*cfr.* para. 5.17).

[180] Esta menção só terá que constar do formulário e não do texto das regras vinculativas aplicáveis às empresas.

termos do número 1.3 do presente capítulo. Deverão também precisar que partes das regras vinculativas aplicáveis às empresas deverão ser transmitidas aos titulares dos dados, bem como do meio de publicação (por exemplo, em casos que os titulares dos dados sejam exclusivamente os trabalhadores das empresas do grupo, não fará sentido publicar estas regras no *site* das empresas);

viii) Existência de programas adequados de treino e ações de formação dirigido às pessoas que tenham acesso a dados pessoais ou que estejam envolvidas no desenvolvimento ou criação de ferramentas tecnológicas destinadas ao tratamento de dados pessoais (art. 47º, n.º 2 al. n)). O programa de treino e ações de formação deverá ser especificado no formulário a apresentar à autoridade de controlo competente;

ix) Existência de procedimentos internos de reclamação (art. 47º, n.º 2 al. i)), de forma a que o titular dos dados possa exercer os seus direitos de reclamação a qualquer das empresas cobertas pelas regras vinculativas aplicáveis às empresas. Neste documento deverão estar especificadas de que forma é que se processam os referidos procedimentos, bem como das obrigações legais de resposta e dos prazos consignados no Regulamento (art. 12º, n.º 3) e das consequências da não observação dos prazos e/ou de tais reclamações serem válidas e que devam promover uma alteração dos padrões de comportamento das empresas, entre outras informações;

x) Existência de programas de auditorias (art. 47º, n.º 2 al. j)), que devem ser feitas de forma regular – quer internamente quer por entidade acreditada externa – de forma a assegurar a conformidade da atuação das empresas com as regras vinculativas que regem as transferências de dados pessoais intra-grupo. Devem também estar previstas formas de implementar eventuais medidas corretivas das deficiências identificadas em sede de auditoria. Nas regras vinculativas aplicáveis às empresas deverá também ser garantido às autoridades de controlo o acesso aos resultados das auditorias, devendo igualmente providenciar relativamente à possibilidade de as autoridades de controlo poderem realizar as suas próprias auditorias em qualquer das empresas abrangidas pelas regras, se justificado;

xi) Designação do encarregado de proteção de dados (art. 37º), articulado com a determinação das suas funções e competências (47º, n.º 2 al. h)). Se o grupo empresarial criar uma rede de encarregados de proteção de dados locais deverá descrever de forma breve as estruturas internas e alocação de funções e competências. Deverá também

constar das regras vinculativas aplicáveis às empresas que o encarregado de proteção de dados responde diretamente a direção ao mais alto nível (art. 38º, n.º 3);

xii) Dever de todas as empresas do grupo cooperarem com as autoridades de controlo (art. 47º, n.º 2 al. l)), principalmente quanto às obrigações relacionadas com as auditorias.

xiii) Descrição do âmbito material das regras vinculativas aplicáveis às empresas (art. 47º, n.º 2 al. b)). Deverá constar deste documento uma descrição geral das transferências ou conjunto de transferências de dados pessoais, em particular, as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão, de forma a que a autoridade de controlo competente poder avaliar a atuação concreta das empresas e atestar da conformidade com o definido nas regras vinculativas aplicáveis às empresas;

xiv) Descrição do âmbito geográfico das regras vinculativas aplicáveis às empresas e especificação da estrutura e os contactos do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta e de cada uma das entidades que o compõe (art. 47º, n.º 2 al. a)).

Este documento deverá indicar se é aplicável apenas aos dados pessoais exportados para fora da União Europeia pelas empresas do grupo ou se é aplicável a todas operações de tratamento prosseguidas pelas empresas do grupo;

xv) Introdução de procedimentos de elaboração de relatórios e de registo de alteração às regras (art. 47º, n.º 2 al. k)). As regras vinculativas aplicáveis às empresas podem ser alteradas – por exemplo, na hipótese de uma mudança da estrutura do grupo – mas tais modificações têm de ser devidamente comunicadas, num prazo razoável, a todas as empresas do grupo vinculadas a este documento, aos titulares dos dados afetados e às autoridades de controlo, através da autoridade de controlo competente.

No caso de mudança do elenco das empresas de grupo vinculadas, nenhuma transferência de dados pessoais pode ser feita para um novo membro, enquanto este não estiver efetivamente vinculado à observação das regras vinculativas aplicáveis às empresas, por algum dos métodos referidos *supra* em ii);

xvi) Elenco de direitos que taxativamente deverão ser observados pelas empresas do grupo e aplicação dos princípios gerais de proteção de dados (art. 47º, n.º 2 al. d)), nomeadamente a limitação das finalidades, a minimização dos dados, a limitação dos

prazos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas (i.e. que garantias deverão ser observadas em tais transferências).

As definições e a letra das regras vinculativas aplicáveis às empresas em sede de cumprimento deste requisito deverão estar em conformidade com as definições e letra constantes do Regulamento.

xvii) Previsão dos mecanismos de cumprimento das obrigações em sede do princípio da responsabilidade, incluindo a manutenção de um registo todas as operações de tratamento sob a sua responsabilidade (art. 30º); quando justificado pelos elevados riscos que uma específica operação de tratamento possa representar na esfera dos direitos fundamentais e liberdades dos indivíduos, proceder a uma avaliação de impacto sobre a proteção de dados, nos termos do artigo 35º do Regulamento, entre outros.

xviii) Previsão de mecanismos de comunicação, à autoridade de controlo competente, de todos as normas legais que alguma empresa do grupo empresarial deverá observar num país terceiro que sejam passíveis de ter forte impacto negativo nas garantias dadas pelas regras vinculativas aplicáveis às empresas (art. 47º, n.º 2 al. m)). Tal compromisso só será aplicável se não existir algum requisito legal impeditivo, como por exemplo a confidencialidade de uma investigação criminal, que impeça a referida divulgação.

5.2. Requisitos das Regras Vinculativas Aplicáveis às Empresas no Regulamento 2016/679

As regras vinculativas aplicáveis às empresas tiveram a sua origem como um código de conduta interno, i.e., uma forma de auto-regulação, relativamente às políticas de tratamento de dados pessoais efetuadas no seio de multinacionais ou grupos de empresas, incluindo as transferências estabelecidas entre as várias empresas e filiais.

Com o regime introduzido pelo Grupo de Trabalho do Artigo 29, o que era um sistema de auto-regulação interno foi articulado com o poder decisório das autoridades de controlo, de forma a assegurar que tal instrumento vincula as empresas à observação das garantias adequadas previstas na então vigente Diretiva 95/46/CE, como condição para as transferências de dados pessoais para países terceiros. Desta forma e face ao regime de aprovação e validação de adequação por parte do poder regulatório na matéria, as regras vinculativas aplicáveis às empresas passaram a consubstanciar um esforço co-regulatório, um sistema híbrido de cooperação institucional entre o público e o privado.

Vários autores afirmam que é salutar pensar em códigos de conduta voluntários e regulação diretamente ditada pelo Estado como polos opostos no *continuum* regulatório, com a maior parte dos esquemas de auto-regulação a cair algures entre estes dois polos[181],[182].

Rubinstein refere ainda que a "*co-regulação, incluindo os portos seguros de privacidade, são um instrumento político eficiente e flexível, se adequadamente definido, oferecendo diversas vantagens em comparação com a falsa dicotomia das voluntárias diretrizes da indústria vs a regulação prescritiva emanante do governo*"[183].

Tem sido apontado como falhas da rígida prescrição da legislação tradicional o facto de ser "*cara, deficiente, intrusiva, desconsidera os interesses específicos e únicos interesses*

[181] RUBINSTEIN – cit. 1, p. 357.

[182] No Rand Report relativo a eventuais opções para a eficiência da auto- e co-regulação na internet é apresentada uma escala de auto- e co-regulação, que vai desde o nível 0 "Pura auto-regulação" sem intervenção governamental, até ao nível 11 onde essa co-regulação é "governamentalmente imposta". Poderá considerar-se que as regras vinculativas aplicáveis às empresas recaem algures entre o nível 8 e 9 desta escala – sendo o nível 8 "Auto-regulação aprovada pelo governo com reconhecimento/aprovação e o 9 "Co-regulação obrigatória aprovada" em que o envolvimento do governo envolve "discussão dos princípios. Abrange sanções e auditorias". Não é necessariamente integrável nesse último nível pelo facto de as regras vinculativas aplicáveis às empresas não serem obrigatórias, mas também não se enquadra perfeitamente com o nível 8 por este não fazer referência a sanções e auditorias.

[183] RUBINSTEIN – cit. 1, p. 358.

das organizações, em favor de uma solução rígida global que falha em canalizar o conhecimento da indústria e reprime a inovação"[184].

Ainda assim é necessário que exista algum mecanismo governamental que restrinja o interesse próprio económico, como diz Rubinstein:

"*As soluções de co-regulação, que combinam um mecanismo de auto-regulação com alguma forma de intervenção estatal, são mais resistentes e eficazes do que a auto-regulação isoladamente considerada*"[185].

Em muitos domínios do direito têm sido testados sistemas mais flexíveis de regulação que permitem, dentro de determinados limites e mediante um regime-quadro mais ou menos abrangente, às empresas prosseguir os fins subjacentes ao impulso regulatório, mas através da definição individual de políticas, conforme as suas necessidades específicas. O poder estatal (ou europeu) e os seus representantes conservam o papel de responsáveis pela adequação e eficácia do controlo dos referidos sistemas internos. Tais mecanismos foram já usados em áreas tão dispares quanto: saúde e segurança, segurança alimentar, mercados financeiros, proteção ambiental, entre outros[186].

As autoridades de controlo desempenham também um papel relevante na aplicação da normativa relativa a proteção de dados internacionalmente, coadjuvando as empresas e grupos de empresas nesse âmbito.

O Grupo de Trabalho do Artigo 29 permitiu a existência deste mecanismo, não só pela pressão exercida pelas multinacionais interessadas, mas também porque reconheceu que, na prática, o poder de supervisionar e aplicar as disposições da Diretiva pelas autoridades de controlo não estavam a ser suficientes para forçar o cumprimento desta pelas empresas, resultando de um miríade de problemas intercruzados: a falta de cooperação entre Estados-Membros, falta de ferramentas e mecanismos de aplicação coerciva da lei ao dispor das autoridades de controlo, falta de recursos das autoridades de controlo, quer a nível de pessoal

[184] *Idem, ibidem*, p. 367.
[185] *Idem, ibidem*, p. 368.
[186] GILAD, Sharon - It runs in the family: Meta-regulation and its siblings, p. 1.

quer a nível de orçamento, e o avultado volume de incumprimento da lei em matéria de proteção de dados[187].

Face a tais ineficiências estruturais, o Grupo de Trabalho do Artigo 29 não teve outra hipótese senão reconhecer a mais-valia prática em que se poderia traduzir este mecanismo, na medida em que fomenta o cumprimento das empresas, constituindo uma via interessante de legitimação de transferências internacionais (e um símbolo de confiança para os consumidores, por exemplo). As autoridades de controlo podem, assim, modelar tal ímpeto de cumprimento, condicionando a aprovação das regras vinculativas aplicáveis às empresas à observação de certos critérios e requisitos – abordados no subcapítulo anterior – que asseguram um mínimo indispensável nível de proteção para o tratamento de dados pessoais mesmo para empresas do grupo fora da União Europeia.

Desta forma, empresas estabelecidas na União Europeia, ao transferir dados pessoais para empresas do grupo em países terceiros, funcionam também como uma espécie de *missionário institucional* contemporâneo, levando a mensagem da proteção dos dados pessoais e da necessidade de garantia dos direitos fundamentais para países com deficitária legislação na área em causa.

Embora tal sistema seja extremamente comum em vários países, especialmente nos Estados Unidos da América, muitos partilham da visão de que a aplicação das leis europeias em matéria de proteção de dados não pode ser deixada à decisão e discricionariedade do mercado, devendo a supervisão da sua aplicação pelas entidades privadas ser guiada por mecanismos governamentais[188]. A co-regulação, neste aspeto, acaba por ser um reconhecimento das falhas do controlo governamental e do direito público quanto a certas matérias, combinado com reconhecimento da capacidade de auto-governação das empresas.

Este tipo de atividade regulatória demonstra também um certo pragmatismo na forma como se abordam as condições em que as empresas efetivamente procuram cumprir com as responsabilidades legais que lhes assistem. Demonstra também o reconhecimento de que estas, em relação a certas matérias, têm uma maior capacidade, conhecimento e experiência para efetivamente saber quais são os fatores e catalisadores que regem a sua atuação – e não o Estado. Mais facilmente se encontra assim um caminho para a observação material das regras.

[187] MOEREL – cit. 79, p. 22.
[188] *Idem, ibidem,* p. 51.

Articulando as circunstâncias acima mencionadas com as dificuldades sentidas pelos Estados quanto à aplicação da lei em matérias que extravasam as suas fronteiras, mais necessário se torna existirem mecanismos que procurem, na prática, dar resposta aos problemas sentidos pelos cidadãos.

Dessa forma, regular a auto-regulação ("meta-regulação" como lhe chama Lokke Moerel[189]) das empresas que procedem ao tratamento dos dados poderá ser um método muito mais eficaz para assegurar materialmente o cumprimento das normas e princípios existentes em matéria de proteção de dados, na medida em que os objetivos regulatórios tradicionais enformam e operacionalizam a inerente capacidade auto-regulatória das empresas.

O objetivo desta meta-regulação, nestes termos, é a criação de estruturas formais de governação e sistemas de gestão que terão de ser usados e modelados pelas empresas conforme a sua capacidade e necessidades, de forma a promover uma cultura de responsabilidade na prática[190].

É também um facto de que, em variadas áreas, as empresas tem instituídos procedimentos internos de melhores práticas (quer seja financeira, quer em matérias de ambiente), e o reconhecimento pela literatura relativamente a definição de políticas públicas que as legislações que demonstram um caráter marcadamente prescritivo (i.e., leis que procuram extensivamente determinar o comportamento que os visados deverão adotar) têm "*limitações inerentes para atingir os objetivos regulatórios subjacentes, devido ao acesso imperfeito dos "reguladores" à informação factual e a conhecimento teórico (por exemplo, das soluções que possam mitigar de forma mais efetiva e eficiente os riscos para os objetivos regulatórios)*"[191].

Têm sido também apontadas como falha grave da legislação com tais características o facto de ser pouco flexível e adaptável em face de circunstâncias imprevisíveis[192], particularmente comuns no mundo contemporâneo, correndo o risco de ficar funcionalmente desadequada num curto espaço temporal. Uma abordagem mais casuística, em que as normas sejam pensadas de forma mais abstrata e com a definição de princípios e objetivos gerais destas,

[189] *Idem, ibidem,* p. 79.
[190] *Idem, ibidem*, p. 179.
[191] *Ibidem.*
[192] GILAD – cit. 186, p. 489.

poderá revelar-se um meio mais profícuo de assegurar o real envolvimento das empresas na procura de soluções para os problemas que possam eventualmente surgir.

Com efeito, os desenvolvimentos tecnológicos referidos ao longo do presente estudo e as inúmeras possibilidades em aberto quanto às experiências no horizonte digital, e a velocidade em que todo o panorama se altera e transforma, dificilmente a letra da lei, quando demasiado prescritiva e restritiva, poderá acompanhar a realidade que pretende regular.

Nesse sentido, os legisladores não fariam um controlo da utilização concreta dos mecanismos e sistemas adotados *ex ante*, mas "*em vez disso, fazer os seus juízos com base na avaliação contínua das organizações sobre (...) os resultados das mudanças que introduzirem*"[193].

Face aos referidos avanços tecnológicos, a "*flexibilidade dos quadros regulatórios revestirá uma importância fundamental em garantir que os reguladores tendem às necessidades atuais e futuras do mercado e mantêm a confiança dos consumidores através da proteção dos interesses públicos*"[194].

O Regulamento, como já referido, veio consagrar definitivamente as regras vinculativas aplicáveis às empresas, codificando (ainda que não totalmente) o regime previsto pelo Grupo de Trabalho do Artigo 29. Tal decisão não se esgota na sua necessidade prática, mas também se insere num contexto superior de mudança legislativa a nível da União Europeia.

Em 2003 foi exarado o Acordo Interinstitucional sobre legislar melhor (que, entretanto, foi revisto e substituído por outro Acordo[195]), que é um acordo que visa "*melhorar a forma como a União Europeia legisla e garantir que a legislação da UE serve melhor os cidadãos e as empresas*"[196].

Este acordo vincula as instituições da União Europeia (o Parlamento Europeu, o Conselho Europeu e a Comissão Europeia) a vários princípios que deverão ser observados no processo legislativo, tais como a subsidiariedade, proporcionalidade, segurança jurídica e, mais

[193] MOEREL – cit. 79, p. 182.
[194] MARSDEN, Christopher – Co- and Self-regulation in European Media and Internet Sectors: The Results of Oxford University's Study, p. 78.
[195] Acordo Interinstitucional Entre O Parlamento Europeu, O Conselho Da União Europeia E A Comissão Europeia Sobre Legislar Melhor de 13 de abril de 2016.
[196] http://www.consilium.europa.eu/pt/policies/better-regulation/ [consultado em 27/04/2018].

importante para o estudo em causa, a simplificação. Sob a alçada deste último princípio procura-se promover instrumentos de regulamentação mais eficazes, a fim de evitar o excesso de regulamentação e os encargos administrativos.

Ora, o Acordo Interinstitucional referido diz que "*a UE legisla apenas quando é necessário. Por vezes, é útil recorrer a mecanismos de regulação alternativos, como a corregulação ou a autorregulação*."

Os efeitos vinculativos deste tipo de acordos são claros[197].

Também a Comissão Europeia refere que considerará o uso de mecanismos de co-regulação quando constituir um meio eficiente de atingir os objetivos da União Europeia[198].

Portanto, as regras vinculativas aplicáveis às empresas encontram aqui mais um fator de legitimidade, na medida em que a própria União Europeia reconhece a potencial falibilidade dos instrumentos clássicos de regulação em determinadas matérias, e o valor acrescentado que este tipo de mecanismos podem representar.

Com efeito, tem sido reconhecido que este tipo de iniciativas, a cooperação direta e formalmente estruturada de entes privados com as figuras de direito público e europeu, pode "*gerar um maior grau de adesão, ser mais eficientes e eficazes, ser de melhor qualidade, o processo de criação de normas ser mais transparente e democrático e, portanto, mais legítimo, e o cumprimento ser menos problemático*"[199].

Como expõe Karmel e R. Kelly: "O cumprimento resulta do interesse próprio e da legitimidade"[200].

Embora o sucesso dos instrumentos de co-regulação em matéria de proteção de dados tenha sido relativamente limitado[201], tal deverá mudar com o início da aplicação do Regulamento, na medida em que vários problemas que afastavam as empresas de introduzir estes mecanismos, deixarão de se verificar. Como se pode ler no Rand Report: "(…) *para que*

[197] CAFAGGI, Fabrizio – Private Law-making and European Integration: Where do They Meet, When do They Conflict? p. 211.
[198] COMMISSION OF THE EUROPEAN COMMUNITIES - European Governance: A White Paper, p. 21.
[199] MOEREL – cit. 79, p. 231.
[200] KELLY, Claire – The Hardening of Soft Law in Securities Regulation, p. 15.
[201] "*Resulta claro de que os mecanismos de auto e co-regulação não estão a desempenhar um papel relevante nas práticas de proteção de dados europeias" - cfr.* Rand Report, p. 9.

a auto ou co-regulação sejam eficazes, fatores como a transparência, responsabilidade, prevenção das assimetrias de informação, alinhamento dos interesses das instituições de auto-regulação ou de co-regulação com aqueles do público, supervisão, monitorização (pelo governo e pelas partes interessadas) e cumprimento são absolutamente necessários[202].

Na medida em que as regras vinculativas aplicáveis às empresas constituem um documento, que incorpora toda a política de tratamento de dados pessoais de um determinado grupo de empresas e estando todas as empresas do grupo vinculadas a estas, pode considerar-se cumprido o requisito da transparência avançado no Rand Report. A satisfação desse princípio é reforçada pelo facto de o Regulamento prescrever exatamente, em moldes gerais, os requisitos necessários e a existência do procedimento de coerência, onde as decisões da Comissão terão de ser publicadas.

Uma vez que existe um requisito destas regras relativamente à responsabilidade que impende sobre as empresas, também se terá de considerar este fator observado.

Na medida em que estas regras têm como *ratio* o assegurar das garantias adequadas quanto ao tratamento de dados pessoais relativamente aos direitos fundamentais dos cidadãos, os requisitos respeitantes ao alinhar dos interesses entre as instituições e o público (e sendo que tais direitos, como o direito de acesso e retificação, reduzem as assimetrias de informação) parecem estar observados.

Apenas surgem como incógnitas, dos vetores apontados no Rand Report, o que se relaciona com a efetividade da supervisão, fiscalização e capacidade de fazer cumprir a lei em matéria de proteção de dados pelas autoridades de controlo, face à falta de recursos monetários e humanos destas[203].

Porém, este fator é extremamente relevante e determinante do sucesso das regras vinculativas aplicáveis às empresas. O referido sucesso só se poderá verificar caso tenha lugar uma operacionalização prática das realidades teóricas constantes da legislação de proteção de dados[204], que produzam efeitos reais na esfera dos protegidos. Nesse sentido, Caffaggi refere:

---

[202] RAND REPORT – cit. 3, p. 10.

[203] "*Recursos adequados são um elemento chave do sucesso da auto-regulação*" (*cfr.* MARSDEN – cit. 168, p. 87).

[204] Cafaggi diz também que a existência de mecanismos de co-regulação "*reflete uma mudança de foco relativamente à relação existente entre a legislação e os atores privados: da legitimidade à eficácia*" (*cfr.* CAFAGGI– cit. 197, p. 215).

"*A eficácia* [de sistemas de co-regulação] *não é medida apenas pela conformidade dos regulados, mas examina também os efeitos do processo de regulamentação nos beneficiários finais.*".

Releva também considerar que a co-regulação está estritamente conexa ao princípio de responsabilidade previsto no Regulamento, na medida em que as empresas têm de demonstrar que as suas diretrizes e regras internas de atuação estão em conformidade com os parâmetros definidos pelo poder regulatório. Assim, as empresas são obrigadas a introduzir mecanismos de responsabilidade, de forma a poder demonstrar a adequação dos *meios* escolhidos para atingir os objetivos e *fins* estabelecidos pelo legislador ou pelo poder supervisor. Como diz Gilad:

"*A meta-regulação, em particular, requer que as organizações providenciem aos reguladores uma contínua auto-avaliação da relação entre os seus sistemas de conformidade e os resultados esperados*"[205].

Um dos principais problemas relativamente a estes mecanismos de co-regulação, porém, é uma das razões anteriormente apontadas como justificativas da sua consagração legal: o facto de as empresas, relativamente a certas matérias, disporem de informações que o legislador não tem acesso. Tal poderá significar, na ótica pessimista, que o regulador não terá acesso às informações necessárias para efetivamente julgar se dada empresa está a cumprir (ou não) as disposições constantes do Regulamento e as regras a que se vinculou.

É, porém, defensável que perante a existência do princípio da responsabilidade e face aos ónus que recaem sob a empresa sob a égide deste princípio (como a demonstração da conformidade e a necessidade de registo das operações de tratamento), tal risco seja, na prática, diminuto.

[205] GILAD, Sharon – cit. 186, p. 493.

5.4. As Regras Vinculativas Aplicáveis às Empresas e o Princípio da Responsabilidade

O propósito essencial do princípio da responsabilidade é a utilização da lei vigente em matéria de proteção de dados de forma a vincular as empresas às suas responsabilidades através de vários mecanismos que encorajam ou forçam tais empresas a integrar sistemas e estruturas de governação na sua orgânica interna. O Regulamento consagra expressamente este princípio (art. 5º, n.º 2). O Grupo de Trabalho do Artigo 29º e o Rand Report tinham já recomendado que este princípio fosse introduzido no novo instrumento legislativo.

Como já referido em capítulo anterior[206], o Regulamento adotou uma abordagem baseada no risco quanto à aplicação de várias das suas disposições: emulando, assim, a forma como as empresas, na sua maioria, formam as suas estratégias no que respeita à conformidade com várias das suas obrigações, incluindo no domínio da proteção de dados[207].

Estas decisões quanto à prioridade dada, em termos de cumprimento das obrigações em matéria de proteção de dados no terreno, são tomadas a nível central (normalmente, pela empresa-mãe) e impostas às restantes empresas do grupo.

Ora, tal abordagem baseada no risco é compatível com o princípio da responsabilidade em matéria de proteção de dados pessoais, na medida em que este princípio consubstancia um exemplo de uma abordagem baseada no risco – o legislador europeu foca-se assim mais no resultado das ações da empresa alvo de regulação através da regulação dos processos instaurados pelas empresas e na concreta demonstração continuada do respeito pelas regras, do que nas notificações *ex ante* de tratamento de dados pessoais, que se tornaram uma forma genérica de cumprimento da lei, sem que haja uma real cultura de cumprimento vigente.

Tal desenvolvimento legislativo também se coaduna perfeitamente com a prescrição de mecanismos de co-regulação, na medida em que ambas novidades do Regulamento "*representam um passo decisivo na direção de abandonar mecanismos regulatórios estaduais de «comando e controlo» a favor de uma «regulação reativa», que permite a introdução de programas de auto-regulação*"[208].

[206] *Cfr*. Capítulo 3. pp. 32 e 33.
[207] MOEREL – cit. 79, p. 97.
[208] *Idem, ibidem*, p. 98.

Ambos desenvolvimentos tiveram como *ratio* a ideia, reconhecida pelo Grupo de Trabalho do Artigo 29, que a legislação vigente em matéria de proteção de dados não estava a ter sucesso em garantir que os princípios e requisitos de proteção de dados tivessem tradução prática e com materiais efeitos na proteção dos cidadãos[209].

No âmbito do Regulamento, o princípio de responsabilidade obriga o responsável pelo tratamento a implementar as medidas técnicas e organizativas que forem adequadas de forma a garantir os princípios relativos ao tratamento de dados pessoais na prática, e deverá poder comprová-lo, devendo ter em atenção a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis (art. 24º, n.º 1), conforme a abordagem baseada no risco.

A necessidade de conseguir demonstrar à autoridade de controlo o cumprimento deste princípio irá facilitar de forma notória a aplicação da lei e supervisão por parte das autoridades de controlo[210].

É importante referir que o princípio da responsabilidade não constitui um novo princípio *per se*, procurando antes o material e efetivo cumprimento dos princípios já existentes.

Com efeito, este princípio surge pelo reconhecimento do Grupo de Trabalho do Artigo 29º de que não existe, a nível das empresas, uma verdadeira cultura de cumprimento da lei vigente em matéria de proteção de dados pessoais: os gerentes e os membros do Conselho de Administração de várias empresas não estão ao corrente das obrigações que recaem sob as empresas neste âmbito, nem aspetos de privacidade e proteção de dados enformam os processos tecnológicos e os sistemas informáticos das organizações[211]. Neste âmbito, o Grupo de Trabalho acrescenta que, a menos que os princípios e obrigações comecem a permear os valores e práticas das organizações e que as responsabilidades comecem a ser expressamente alocadas, violações da lei e dos direitos fundamentais dos cidadãos continuarão a ter lugar e a confiança do público nas empresas e nos administradores públicos será fortemente abalada[212].

[209] ARTICLE 29 WORKING PARTY – cit.31, p. 7.
[210] ARTICLE 29 WORKING PARTY – cit. 31 p. 20.
[211] *Idem, ibidem*, p. 19.
[212] *Ibidem.*

Outro exemplo de mecanismo que num diagrama de Venn seria o resultado de uma justaposição relativa entre a abordagem baseada no risco e o princípio da responsabilidade previsto pelo Regulamento seria a necessidade de, quando um certo tipo de tratamento for suscetível de implicar um elevado risco para os direitos e liberdades dos cidadãos, o responsável pelo tratamento proceder a uma avaliação do impacto das operações de tratamento previstas sobre a proteção dos dados pessoais (art. 35º, n.º 1). Tal avaliação de impacto só terá lugar caso a empresa em causa identifique riscos relevantes associados, ficando responsável pela sua determinação[213].

Uma das falhas mais relevantes do Regulamento, tendo o legislador europeu rejeitado a recomendação feita pelo Grupo de Trabalho do Artigo 29º[214] nesse sentido, resulta do facto de o cumprimento das obrigações sob a égide do princípio da responsabilidade não constituir um fator mitigante na determinação de sanções; muito embora o Regulamento tenha, de facto, seguido a recomendação do Rand Report e tenha instituído uma abordagem baseada no risco nas sanções e coimas[215].

Com efeito, um dos fatores a considerar, aquando da determinação de coimas, é a "iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares" (art. 83º, n.º 2 al. c)). Este é o fator mitigante que mais se aproxima do princípio da responsabilidade. Ora, tal vetor parece ter um pendor *post factum*, não constituindo uma medida de prevenção dos riscos associados ao tratamento de dados pessoais, como seria corolário deste princípio.

Diga-se que este princípio da responsabilidade não é propriamente novo, sendo já aplicado em vários campos do direito. Mesmo dentro do domínio da proteção de dados pessoais, este princípio encontra-se presente em diversos instrumentos normativos: Diretrizes da OCDE, Regime-quadro quanto à Privacidade da APEC, os princípios de privacidade previstos na lei australiana, entre outros.

---

[213] Sem prejuízo da possibilidade de as autoridades de controlo compilarem listas de operações de tratamento que deverão, necessariamente, ser alvo de uma avaliação de impacto sobre a proteção de dados, o que se prevê que aconteça.

[214] MOEREL – Cit. 79, p. 58.

[215] Veja-se, por exemplo, um dos fatores que uma autoridade de controlo deverá considerar aquando da determinação de uma coima a aplicar: "A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos" (*cfr*. art. 83º, n.º 2 al. a)).

Embora não tenham feito o seu caminho até à versão final, na Proposta de Regulamento[216], a anterior versão deste artigo (art. 22º da Proposta de Regulamento) continha uma listagem não taxativa de medidas de demonstração do princípio da responsabilidade, que proporcionavam alguma claridade. Essas medidas incluíam: conservar a documentação; aplicar requisitos de segurança; realizar uma avaliação de impacto sobre a proteção de dados; respeitar as obrigações relativas à autorização ou consulta prévias da autoridade de controlo; e o dever de designar um delegado para a proteção de dados (art. 22, n.º 2).

Compreende-se, porém, que tal lista não tenha sido consagrada no texto final do Regulamento. Tais requisitos do princípio de responsabilidade foram criticados por serem demasiado específicos - correndo o risco de indevidamente condicionar o cumprimento da lei. O legislador europeu reconheceu, assim, a mais valia que representa a definição de um princípio geral, que permita às empresas definir as suas próprias políticas de cumprimento, conforme as suas necessidades e sistemas estabelecidos[217].

As regras vinculativas aplicáveis às empresas, na medida em que constituem um código de conduta que estabelece, com relativo detalhe (por força dos requisitos definidos em sede do Regulamento), as políticas seguidas por um dado grupo de empresas em matérias de proteção

[216] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), de 25 de janeiro de 2012.

[217] O Grupo de Trabalho do Artigo 29 tinha já indicado que os tipos de medidas a tomar sob a égide deste princípio não deveriam ser especificados no texto da disposição geral, mas através de diretrizes subsequentes (*cfr*. para. 30 GRUPO DE TRABALHO DO ARTIGO 29º - Cit. 196).

Este Grupo de Trabalho elencou, porém algumas medidas ilustrativas, sem tal lista ser exaustiva. Veja-se então que medidas seriam essas: "*Estabelecimento de procedimentos internos antes da criação de novas operações de tratamento de dados pessoais (revisão interna, avaliação, etc); Adopção de políticas de protecção de dados formais e vinculativas a ter em conta e a aplicar às novas operações de tratamento de dados (por ex. conformidade com a qualidade dos dados, avisos, princípios de segurança, acesso, etc), que devem ser disponibilizadas às pessoas em causa; Descrição dos procedimentos de forma a assegurar a adequada identificação de todas as operações de tratamento de dados e gestão de um inventário dessas operações; Designação de um encarregado de proteção de dados e outras pessoas com responsibilidade pela protecção de dados; Disponibilização de uma proteção de dados adequada, e de formação adequada nesta matéria aos colaboradores. Deve abranger as pessoas que tratam (ou são responsáveis pelo) tratamento de dados pessoais (como os directores de recursos humanos), mas também gestores de TI, criadores e directores de unidades operacionais. Devem ser atribuídos recursos suficientes para a a gestão da proteção da privacidade, etc; Criação de procedimentos para gerir os pedidos de acesso, de correcção e de supressão, que devem ser transparentes para as pessoas em causa; Estabelecimento de um mecanismo interno de gestão de reclamações; Realização de avaliações de impacto sobre a privacidade em circunstâncias específicas; (...)*" Como se poderá ver, vários destes requisitos estão efetivamente presentes nas previsões relativamente às regras vinculativas aplicáveis às empresas.

de dados pessoais, representam exemplarmente o princípio da responsabilidade. Tal facto foi reconhecido pelo Grupo de Trabalho do Artigo 29º, que refere que:

"*As regras vinculativas aplicáveis às empresas são códigos de conduta, elaborados e seguidos por organizações multinacionais, que contêm medidas internas designadas para implementar os princípios de proteção de dados (como auditorias, programas de formação, sistema de tratamento de reclamações)*"[218].

Com a adoção de regras vinculativas aplicáveis às empresas um determinado grupo de empresas compromete-se e vincula-se à adoção e observação dos princípios gerais de proteção de dados pessoais (art. 47, n.º 2 al. d)) , põe em funcionamento procedimentos de reclamação (art. 47º, n.º 2 al. i)), assegura os direitos dos titulares dos dados (art. 47º, n.º 2 al. e)) e instaura procedimentos para assegurar o cumprimento das regras vinculativas aplicáveis às empresas, independentemente de onde as empresas do grupo estejam localizadas no mundo. Estamos, assim, perante um mecanismo jurídico que necessariamente orbita, em toda a sua extensão, em volta do princípio da responsabilidade.

Como muitas vezes referido, devido ao seu diagnóstico como princípio nuclear enformador das alterações legislativas por ora estudadas, a proteção de dados tem de passar da teoria à prática[219]. Como o Grupo de Trabalho do Artigo 29 estabelece:

"*Os requisitos jurídicos têm de ser traduzidos em medidas reais de proteção dos dados. O quadro jurídico da UE em matéria de proteção de dados necessita de mecanismos adicionais para incentivar a proteção dos dados na prática"*[220]

Ora, consistindo o princípio de responsabilidade num princípio vinculativo juridicamente que exige expressamente dos responsáveis pelo tratamento e subcontratantes a aplicação de medidas adequadas e eficazes para pôr em prática as obrigações e princípios postulados na legislação vigente em matéria de proteção de dados, facilmente se vê as regras vinculativas aplicáveis às empresas como uma manifestação casuisticamente determinada – moldada conforme as especificidades reais da empresa, *inter alia* motivos de cultura interna, volume e categorias de tratamento de dados pessoais, as finalidades procuradas – deste princípio. Essa proporcionalidade é, também, manifestamente um fator relevante do princípio da responsabilidade (e da abordagem pelo risco): as medidas específicas a aplicar, de forma a

[218] MOEREL – Cit. 79, p. 58.
[219] GRUPO DE TRABALHO DO ARTIGO 29º - Parecer 3/2010 sobre o Princípio da Responsabilidade, p. 199.
[220] *Ibidem.*

introduzir o princípio da responsabilidade numa entidade, deverão ser "*determinadas em função dos factos e das circunstâncias de cada caso particular, com especial atenção para o risco associado ao tratamento e ao tipo de dados*"[221].

Uma determinação genérica das obrigações, por parte do legislador europeu, que recaem sob as empresas nesta matéria levá-los-ia a adotar estruturas inadequadas e, por fim, acabaria por falhar[222]. Outra vantagem da prescrição mais lata do conceito é a possibilidade de se manter atual durante mais tempo, num contexto de constante mudança, que necessita de ser suficientemente flexível de forma a permitir a previsão de rápidas mudanças na tecnologia, nas técnicas comerciais, estruturas de empresas e necessidades do cidadão[223].

Essa flexibilidade também se reflete na maior capacidade modeladora que assiste às empresas para alocar os seus recursos de forma mais eficaz nas operações de tratamento que demonstrem constituir mais riscos para a privacidade dos seus clientes e funcionários, conforme a abordagem pelo risco à proteção de dados pessoais[224].

Por outro lado, a necessária flexibilidade que assiste o conceito pode levar a uma definição muito aberta, como poderá ser considerado o caso, correndo o risco de gerar insegurança jurídica[225].

O Grupo de Trabalho do Artigo 29 expõe também que muitas das obrigações decorrentes deste princípio da responsabilidade têm, como elemento integral, a transparência, pelo facto da observação deste princípio conduzir a uma maior responsibilização das entidades envolvidas no tratamento de dados pessoais[226]. Exemplifica tal argumento com sugestões como a publicação de políticas de privacidade na Internet, a transparência nos procedimentos internos de reclamação e a publicação de relatórios anuais.

Na medida em que as regras vinculativas aplicáveis às empresas constituem um código de conduta que poderá ser disponibilizado aos interessados e afetados, para além de existir uma

[221] GRUPO DE TRABALHO DO ARTIGO 29º - Cit. 158, p. 13.
[222] *Ibidem.*
[223] CENTRE FOR INFORMATION POLICY LEADERSHIP – Accountability: A Compendium for Shareholders, p. 8.
[224] *Idem, ibidem,* p. 9.
[225] Circunstância que o Grupo de Trabalho do Artigo 29º reconhece, no seu parecer sobre o princípio da responsabilidade (cit. 158).
[226] GRUPO DE TRABALHO DO ARTIGO 29º - Cit. 158, p. 13.

"publicidade" dos termos em que o grupo procede ao tratamento de dados, prevê mecanismos que assistem a tais interessados em caso de incumprimento, sendo um fim em si mesmo.

Nesse sentido, as regras vinculativas aplicáveis às empresas são o exercício da discricionariedade de um grupo empresarial, quanto à adequação da concreta aplicação do princípio da responsabilidade às transferências intra-grupo, legitimada pelas autoridades de controlo competentes em matéria de proteção de dados pessoais.

Com efeito, as regras vinculativas aplicáveis às empresas assumem, neste âmbito, o papel de um programa de conformidade de um dado grupo de empresas, prevendo os mecanismos utilizados e os meios de comprovação da sua efetividade na prática, bem como das garantias determinadas em caso de incumprimento. Constituem, aliás, programas de conformidade com especial legitimidade, face ao processo de aprovação à escala europeia a que estão sujeitos, nos termos do art. 47º do Regulamento.

É ainda importante notar que o cumprimento da lei em matéria de proteção de dados não é o único fator determinante, o único *business driver* da decisão de implementação de um mecanismo de co-regulação como as regras vinculativas aplicáveis às empresas: a real e efetiva observação do princípio da responsabilidade resulta também numa potencial vantagem competitiva e maior confiança por parte dos cidadãos e clientes. Ou melhor, o cumprimento da lei não é, nesses termos, um fim em si mesmo, contendo externalidades económicas positivas. Recupera-se aqui o já anteriormente citado: "*O cumprimento resulta do interesse próprio e da legitimidade*"[227].

Uma boa governação dos interesses nestas matérias, através da existência de mecanismos adequados constitui, no fundo, uma eficaz tradução e adaptação dos princípios e obrigações da legislação em matéria de proteção de dados para o *habitat* auto- e co-regulatório de um determinado grupo de empresas (e a sua demonstração) cria uma imagem de confiança para o exterior e para as partes interessadas da empresa, como os acionistas e consumidores.

Reputação é, portanto, um fator relevante motivador do cumprimento. Nem o facto de as empresas procederem à subcontratação, mitiga a responsabilidade que diretamente lhes é

[227] Cit. 174.

atribuída, num fenómeno denominado de "*brand boomerang"*[228], numa espécie de culpa *in eligendo* comercial.

Porém, tem sido referido que "*a adoção de compromissos de privacidade não parece mais ser uma vantagem, mas sim a não adoção uma desvantagem*"[229].

Existem também razões de eficiência procedimental a serem consideradas. Na medida em que após a aprovação, nos termos acima descritos, das regras vinculativas aplicáveis às empresas de um determinado grupo empresarial, mais nenhuma aprovação específica de tratamento de dados no seio das empresas vinculadas, no contexto do fluxo de dados internacionais entre elas encetado, será necessária. Tal eficiência poderá refletir-se positivamente na esfera dos clientes e de todas as partes interessadas.

[228] MOEREL – Cit. 79, p. 93.
[229] MOEREL – Cit. 79, p. 99.

5.5. Recomendações quanto à Implementação das Regras Vinculativas Aplicáveis às Empresas no Atual Panorama Global de Proteção de Dados

Perante a importância nuclear dos dados pessoais no contexto internacional, quer no domínio comercial quer na esfera de proteção dos cidadãos, e face à potencial onerosidade e mais efetivo controlo que o Regulamento promete impor às empresas relativamente aos massivos e estruturados fluxos de dados pessoais, e perante o papel que mecanismos como as regras vinculativas aplicáveis às empresas poderão desempenhar no contexto internacional, decorrentes da sua natureza, cumpre analisar a hipótese da existência de um *standard* de proteção dos dados pessoais à escala mundial, através da convergência – interoperabilidade - de sistemas de proteção de dados existentes. Tal hipótese tem sido definida como a forma mais prática e efetiva de procurar uma solução global para os problemas e riscos (também eles globais) gerados pela atual realidade de tratamento de dados pelas empresas[230].

Lokke Moerel assevera que o facto de as multinacionais, naturalmente, não se encontrarem estabelecidas apenas em países da União Europeia significa que o reconhecimento das regras vinculativas aplicáveis às empresas deveria também ser procurado nesses países[231], recomendando que a União Europeia entre em negociações oficiais com países terceiros tendo em vista o mútuo reconhecimento e supervisão do cumprimento da lei destes instrumentos[232].

Poderia pensar-se que esta hipótese avançada por Moerel não apresenta qualquer utilidade prática; que, muito embora existam atualmente 121 países no mundo com legislação vigente em matéria de proteção de dados[233], sempre se diria que ao estar em conformidade com as regras da União Europeia, sendo esta a mais restritiva das legislações vigentes por força do seu pendor de proteção de direitos fundamentais e a força politica e histórica que detém para as apresentar e coagir ao cumprimento, já se estaria a observar um nível de proteção que corresponderia a cumprimento a nível global.

[230] U.S. CHAMBER OF COMMERCE - Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity, p. 32.
[231] MOEREL – Cit. 79, p. 8.
[232] *Idem, ibidem*, p. 129.
[233] GREENLEAF – Cit. 11, p. 2.

Não é assim, porém: como qualquer outra matéria regulatória, a legislação relativa à proteção de dados pessoais reflete toda uma cultura legislativa, com as especificidades e necessidades que resultam num produto necessariamente único.

Não significa isto, porém, que interoperabilidade e iniciativas conjuntas entre diferentes sistemas sejam um objetivo inatingível, pelo contrário. Apesar das suas falhas, a já supramencionada Decisão que institui o "porto seguro" entre a União Europeia e os Estados Unidos da América (tendo nascido das suas cinzas o "Escudo de Privacidade") representa uma solução de compromisso e de "ponte" entre sistemas jurídicos e culturais muito diferentes. Pode ser que esse pragmatismo institucional gere mais decisões conjuntas entre sistemas, desde que não envolvam sacrifícios sérios para a proteção dos cidadãos. A proteção de dados pessoais dos cidadãos não tem, necessariamente de constituir um *jogo de soma zero*.

Atente-se, no âmbito da eventual cooperação entre sistemas regionais de proteção de dados, pela sua relevância internacional, ao regime pela APEC (em português: Cooperação Económica Asia- Pacifico), um fórum para facilitar o comércio e o investimento na área geopolítica da Asia-Pacifico[234].

Em 2005 os Estados membros[235] da APEC (que inclui os Estados Unidos da América, China, Japão, Austrália, Canadá, Rússia, entre outros[236]) adotaram a o Regime-Quadro relativo à Privacidade da APEC[237], que pretende estatuir uma base legal para os fluxos internacionais de dados pessoais ao mesmo tempo que prevê um nível de proteção de dados pessoais (atendendo à específica cultura regulatória, com a tónica em *privacidade*), reconhecendo a importância da proteção da informação e da manutenção dos fluxos de dados pessoais entre as economias da região Asia-Pacífico e com os seus parceiros comerciais. Este regime-quadro é profusamente inspirado nas Diretrizes da OCDE.

A relevância da adoção dos 21 países que integram a APEC de políticas estruturais comuns não pode ser ignorada: as economias representadas nesta organização conjuntamente

[234] POUNDER, Chris – Why the APEC Privacy Framework is Unlikely to Protect Privacy, p. 2.
[235] Sob a designação de *Member Economies*, para demonstrar a enfase económica e não uma holística política de cooperação.
[236] Brunei, Indonésia, Coreia do Sul, Malásia, Nova Zelândia, Filipinas, Singapura, Tailândia, Taiwan, Hong Kong, México, Papua Nova Guiné, Chile, Peru e Vietname.
[237] Na versão original, em inglês: "*APEC Privacy Framework*".

representam mais de um terço da população mundial, metade do PIB global, e perto de metade do comércio mundial[238].

Embora este Regime-Quadro relativo à Privacidade preveja princípios materiais semelhantes às regras europeias, tais como o dever de dar conhecimento das operações de tratamento de dados pessoais aos respetivos titulares (para. 15), a existência de medidas de segurança adequadas (para. 22) e o direito de acesso e retificação (para. 23), várias circunstâncias parecem indicar que não cumprirá, na sua atual formulação, o nível de proteção adequado requerido na legislação europeia em matéria de proteção de dados.

O Regime-Quadro relativo à Privacidade prevê, porém, várias e explícitas exceções aos princípios acima referidos que põe em risco a sua efetiva observação na prática. Por exemplo, o direito de acesso e retificação poderá ser negado ao titular dos dados caso "(i) o encargo ou custo de prover o acesso e retificação não for razoável ou proporcionado em relação aos riscos para a privacidade do individuo em causa; (ii) a informação não possa ser divulgada por razões legais ou de segurança ou de forma a proteger informação comercial confidencial; (iii) a privacidade de outras pessoas para além do indivíduo em causa possa ser violada" (para 24).

Tais exceções poderão ser exploradas pelas empresas de forma a não responder aos titulares dos dados, diminuindo o verdadeiro alcance da norma.

Quanto aos princípios importa referir que este regime-quadro prevê, tal como o novo Regulamento de proteção de dados europeu, o princípio da responsabilidade (para. 26), tendo por inspiração as Diretrizes da OCDE (para. 14 Diretrizes OCDE de 1980).

Este princípio, no âmbito do referido regime-quadro, determina que o responsável pelo tratamento deverá, aquando da transferência de dados (quer domesticamente quer internacionalmente) para outra pessoa ou entidade, procurar obter o consentimento do titular dos dados ou fazer as diligências razoáveis para assegurar que o recipiente dos dados irá proceder ao seu tratamento de forma consistente com os princípios do regime-quadro.

Este princípio inclui algumas limitações. Parece decorrer do comentário explicativo junto ao princípio que este só se aplica quando exista uma contínua relação comercial ou de outro tipo, entre o responsável pelo tratamento e o terceiro a quem os dados serão enviados.

[238] GREENLEAF, Graham – Five Years of the APEC Privacy Framework: Failure or Promise? p. 1.

Nesse caso exemplificativo, o titular dos dados não teria qualquer via judicial ou extrajudicial de forma a valer os seus direitos para com o responsável pelo tratamento exportador.

De qualquer das formas, sempre se dirá que o facto de atualmente quer o Regulamento quer o Regime-Quadro relativo à Privacidade da APEC preverem o princípio da responsabilidade constitui necessariamente uma aproximação e harmonização *quasi*-global dos sistemas em causa. Como já referido, o princípio da responsabilidade não substitui nem prejudica a observação das disposições legais vigentes em matéria de proteção de dados; simplesmente, constitui um mecanismo que visa o cumprimento dessas normas pelos devidos responsáveis. Assim, tal princípio, de forma isolada, não pode contribuir para a aproximação substancial dos dois sistemas considerados.

Greenleaf considera que nenhuma das economias da APEC introduziu na sua legislação os princípios específicos previstos no Regime-Quadro relativo à privacidade, ou seja, os que não sejam comuns às Diretrizes da OCDE ou já presentes na normativa relativa a proteção de dados produzida pela União Europeia[239].

A sua efetividade na prática poderá também ser diminuta no sentido em que a adesão aos princípios expostos no Regime-Quadro em questão é feita numa base voluntária pelas economias da APEC, não tendo qualquer estatuto legal[240].

Os desenvolvimentos legislativos pós- Regime-Quadro relativo à Privacidade da APEC não tem refletido os seus princípios e disposições: países como China e a Região autónoma de Macau decretaram legislação em matéria de proteção de dados em que a influência da legislação europeia é notória[241] - particularmente notória na lei macaense por se ter explicitamente baseado na lei portuguesa[242].

Em 2011, a APEC desenvolveu um sistema de regras e políticas que permitem o fluxo além-fronteiras de dados pessoais entre as economias representadas na APEC. Tais regras adotadas pelas empresas terão de estar em conformidade com os princípios previstos no

[239] https://twitter.com/grahamgreenleaf
[240]GREENLEAF – Cit. 215, p. 2.
[241] *Idem, ibidem*, p.6.
[242] *Ibidem.*

Regime-Quadro relativo à Privacidade da APEC, sendo tal conformidade avaliada por uma entidade independente que tenha poderes reconhecidos para o efeito[243].

Atualmente, só cinco das economias da APEC aderiram a este sistema: Estados Unidos da América, México, Japão, Canadá e Coreia do Sul.

Ao contrário, porém, das regras vinculativas aplicáveis às empresas, não se aplicam apenas a transferências intra-grupo, sendo tal certificação extensível a todas as transferências de dados feita para qualquer empresa dentro da região em causa, mesmo fora de um eventual grupo empresarial.

Porém, outros problemas existem. Primeiro, a certificação conseguida tem que ser intentada em cada uma das economias da APEC que adotaram o presente sistema, sendo que a adoção deste sistema não derroga a aplicação das leis internas em matéria de proteção de dados, as quais requerem frequentemente um nível de proteção mais elevado que o decorrente do Regime-Quadro.

Na medida em uma lei interna ultrapasse o nível de proteção previsto no Regime-quadro, a adoção destas regras não trará, assim, grandes benefícios às empresas.

Estes problemas relevantes destas regras, articulados com as expostas fragilidades do Regime-Quadro que subjaz à sua aplicação, obstam a que o material nível de proteção garantido por este sistema seja minimamente semelhante ao que resulta das regras aplicáveis na União. Tal facto é exposto num documento informal de referência[244] criado por um grupo de trabalho que juntou especialistas do Grupo de Trabalho do Artigo 29 e do Sub-Grupo da Proteção da Privacidade das Economias membro da APEC.

O objetivo deste documento é " *constituir uma lista de verificação pragmática e informal para organizações que apresentam pedidos de autorização de regras vinculativas para empresas (RVE) e/ou de certificação de regras de privacidade transfronteiriças (RPT), facilitando deste modo a conceção e a adoção de políticas de proteção de dados pessoais em conformidade com cada um dos sistemas*"[245]. Dessa forma constitui um documento que poderá servir de referência

[243] Quanto às características deste sistema, ver melhor: GREENLEAF, Graham - APEC's cross-border privacy rules system: A house of cards?.

[244] GRUPO DE TRABALHO DO ARTIGO 29º – Parecer 2/2014 sobre os parâmetros de referência dos requisitos aplicáveis às regras vinculativas para empresas (RVE) apresentadas às autoridades nacionais de proteção de dados da UE e às regras de privacidade transfronteiriças (RPT) apresentadas aos agentes de responsabilização da Cooperação Económica Ásia-Pacífico (APEC) .

[245] *Idem, ibidem*, p. 2.

para empresas que pretendam a certificação em cada um dos sistemas apresentados, e não constitui uma declaração de intenções no sentido do reconhecimento mútuo[246], até porque, as regras definidas pela APEC carecem de certificação em cada uma das economias aderentes para onde pretendem transferir dados pessoais.

Este documento, embora de interesse para perceber a real e efetiva clivagem entre os dois sistemas, não poderá ser a pedra de toque de uma eventual decisão de interoperabilidade. Para além do facto de dificilmente o sistema fixado no Regime-Quadro relativo à Privacidade da APEC representar um nível adequado de proteção nos termos do Regulamento, as regras vinculativas aplicáveis às empresas dizem, neste momento, respeito exclusivamente às transferências dentro de um grupo empresarial, sendo as Cláusulas Contratuais-tipo o instrumento usado na Europa para transferências de dados pessoais para países terceiros.

Como diz Greenleaf, isto significa que "*parâmetros de referência entre as cláusulas contratuais-tipo e as regras de privacidade transfronteiriças seriam também necessárias, antes de qualquer caminho para total «interoperabilidade» poder começar*"[247].

Na medida em que, para já, se afigura difícil a criação de um sistema global de proteção de dados, resta perceber de que forma é que as regras vinculativas aplicáveis às empresas poderiam protagonizar um papel mais relevante no cenário internacional, atendendo à sua natureza e características já apontadas.

[246] *Ibidem.*
[247] GREENLEAF – Cit. 220, p. 2.

5.6. Potencial futuro das Regras Vinculativa Aplicáveis às Empresas?

As regras vinculativas aplicáveis às empresas constituem um mecanismo de responsabilidade que, sujeitas à aprovação das autoridades de controlo competentes, representam um nível adequado de proteção de dados pessoais para transferências internacionais.

O escopo de aplicação destas regras reduz-se, porém, a transferências internacionais de dados pessoais entre as empresas integrantes de um determinado grupo empresarial. Não resulta óbvio porque é as regras vinculativas aplicáveis às empresas deverão continuar sujeitas a esta limitação: na medida em que constituem uma espécie de redoma de proteção que espelha a normativa europeia onde quer que se encontre, estando previstos todos os direitos que assistem aos titulares dos dados, recurso aos tribunais, *inter alia*.

Atendendo a tal quadro factual, o próximo passo lógico da perspetiva regulatória deste mecanismo, seria o permitir a livre circulação de dados pessoais entre empresas que não sejam do mesmo grupo empresarial, mas que tenham ambas adotado (e sido aprovadas) regras vinculativas aplicáveis às empresas. Na medida em que ambas apresentam um nível de proteção adequado através das regras vinculativas aplicáveis às empresas, não se descortinam razões para considerar que os dados pessoais dos respetivos titulares não estarão suficientemente protegidos, e que seria necessário a celebração de um contrato com cláusulas contratuais-tipo para que essa transferência fosse válida e legítima.

Fazendo uso do mesmo silogismo, poderia considerar-se que o mesmo se poderia dizer da transferência de qualquer empresa, ainda que não vinculada às regras sob estudo, para uma empresa sujeita à observação das regras vinculativas aplicáveis às empresas.

O mesmo se poderia aplicar, por extensão lógica, à relação comercial ou institucional existente entre uma empresa subcontratante e uma empresa pertencente a um grupo empresarial coberto por regras vinculativas aplicáveis às empresas que figure como responsável pelo tratamento. Ainda que que a empresa subcontratante não tenha regras suas, desde que se vincule contratualmente à observação das regras vinculativas aplicáveis às empresas do responsável pelo tratamento, deveria àquela ser permitida a transferências de dados pessoais dentro do seu grupo empresarial.

Tais transferências, face à existência de regras vinculativas aplicáveis às empresas, não parecem apresentar riscos e ausência de aplicação das leis europeias na matéria em toda a sua extensão, mantendo a União Europeia a sua sombra regulatória sob tais transferências.

Não seria necessário, sequer, uma relevante alteração legislativa para que o atual regime abarcasse as possibilidades enunciadas acima: o Regulamento dispõe que as regras vinculativas aplicáveis às empresas são "*regras internas de proteção de dados pessoais aplicadas (...) dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta*" (art. 4º, 20); sublinhado nosso).

Nem o Regulamento nem qualquer parecer da Comissão ou do Grupo de Trabalho do Artigo 29º parecem esclarecer em que casos é que se poderá considerar que há um grupo de empresas envolvidas numa atividade económica conjunta *de facto*; não parece constituir um entendimento que ultrapasse, injustificadamente, os limites da interpretação, a possibilidade de o Regulamento tacitamente permitir o desenvolvimento futuro das regras vinculativas aplicáveis às empresas nessa direção.

Cumpre também referir que a Comissão tem poderes para emitir diretrizes, recomendações e melhores práticas relativamente aos "*critérios os critérios e requisitos aplicáveis às transferências de dados baseadas em regras vinculativas aplicáveis às empresas aceites pelos responsáveis pelo tratamento e em regras vinculativas aplicáveis às empresas aceites pelos subcontratantes, e outros requisitos necessários para assegurar a proteção dos dados pessoais dos titulares dos dados em causa*" (art. 70º, n.º 1 al. i)), podendo vir a prover esclarecimentos quanto a está matéria, e a conduzir a interpretação da letra da lei *de facto*, sem que seja necessário qualquer adenda ou modificação do Regulamento.

6. Conclusões

O novo Regulamento Geral de Proteção de Dados tem posto a proteção de dados pessoais, finalmente, na superfície das preocupações empresariais e dos cidadãos, numa escala sem precedentes. Fatores endógenos do Regulamento, como as elevadas multas previstas, têm sustentado o *quasi*-pânico generalizado que este instrumento legislativo tem provocado – ao mesmo tempo que a sua urgência e adequação tem encontrado legitimação em vários casos recentes, como as violações de dados pessoais na instituição financeira norte-americana *Equifax* ou a ingerência do *Facebook* em instâncias políticas, através da não autorizada venda de dados pessoais que estes terão alegadamente empreendido a organizações como a *Cambridge Analytica.*

Por várias ordens de razões, a Diretiva foi pensada e conceptualizada para proteger o cidadão num *statu quo* completamente diferente, não estando esta à altura de corresponder aos atuais desafios (mais ainda dos vindouros) em matéria de proteção de dados pessoais. Ainda assim, e apesar de não ser o instrumento certo para cumprir os abstratos objetivos prosseguidos, os seus fundamentos são ainda sólidos, e o Regulamento aproveita-os extensivamente, assegurando que se trata de uma evolução e não uma completa revolução quanto aos pressupostos da política de proteção de dados europeia. O legislador europeu procurou não alterar, assim, as fundações da proteção de dados, mas os meios e mecanismos que os operacionalizam, na procura de uma maior eficácia prática e material observação e cumprimento dos seus princípios.

Procurou apresentar-se as regras vinculativas aplicáveis às empresas como um dos mecanismos que poderá ativamente contribuir para que a material proteção de dados do cidadão seja, efetivamente, uma realidade mais concreta. Embora historicamente este mecanismo tenha sofrido de processos de aprovação morosos e caros, o que se traduziu num baixo nível de adesão pelas empresas, assim já não acontece em sede do novo Regulamento.

Constituindo as regras vinculativas aplicáveis às empresas um extensivo programa de conformidade com a lei em matéria de proteção de dados, sendo ainda um fator que legitima a transferência de dados para países "não adequados" em matéria de proteção de dados, ao mesmo tempo que cumpre com o relevante ónus de demonstrar a conformidade com a lei (tal como disposto no novo princípio da responsabilidade), este mecanismo poderá ser extremamente relevante no horizonte legislativo europeu. Tal tese não obsta, porém, à

identificação de potenciais instâncias de melhor interpretação e operacionalização prática do conceito: defende-se, na presente dissertação, que o escopo de instrumento de co-regulação poderá ser alargado, nomeadamente, devendo as transferências de dados entre empresas com regras vinculativas aplicáveis às empresas ser permitidas, sem qualquer ónus adicional.

Referências Bibliográficas

A. Monografias e Artigos

ACQUISTI, Alessandro - Privacy and Security of Personal Information: Economic Incentives and Technological Solutions. In **The Economics of Information Security.** Kluwer, 2014.

BLACK, Julia – The Role of Risk in Regulatory Process. In **The Oxford Handbook of Regulation**. Oxford: Oxford Academic, 2010. ISBN: 9780199560219. P. 209 – 242.

BOMHOFF, Jacco e MEUWESE, Anne – The Meta-regulation of Transnational Private Regulation. In **Journal of Law and Society**. 2011. Vol. 38, 1, p. 138 – 162.

CAFAGGI, Fabrizio – New Foundations of Transnational Private Regulation. In **Journal of Law and Society**. Cardiff: Cardiff University Law School, 2011. ISSN:1467-6478. Vol 38, p. 20 – 49.

CAFAGGI, Fabrizio - Private Law-making and European Integration: Where Do They Meet, When Do They Conflict?. In **The Regulatory State: Constitutional Implications**. Oxford: Oxford University Press, 2010. ISBN-13: 9780199593170. P. 201 – 228.

CENTRE FOR INFORMATION POLICY CENTRE - **Response to the Consultation by the Irish Data Protection Commissioner on the Topics of Transparency and International Data Transfers under the GDPR**. Hunton & Williams LLP, 2017. [Consultado a 1/05/2018] Disponível em <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_irish_dpc_consultation_on_transparency_and_international_data_transfers_under_the_gdpr.pdf

CENTRE FOR INFORMATION POLICY CENTRE – **The Role of Risk Management in Data Protection**. Hunton & Williams LLP, 2014. [Consultado a 1/05/2018] Disponível em https://www.hunton.com/files/Uploads/Documents/Centre/Role_of_Risk_Management_in_Data_Protection.pdf

CENTRE FOR INFORMATION POLICY LEADERSHIP – **Accountability: A Compendium for Shareholders**. Hunton & Williams LLP, 2011. [Consultado a 1/05/2018] Disponível em

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_2011_.pdf

CENTRE FOR INFORMATION POLICY LEADERSHIP – **Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy**. Hunton & Williams LLP, 2017. [Consultado a 1/05/2018] Disponível em https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf

CENTRE FOR INFORMATION POLICY LEADERSHIP - **The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society**. Hunton & Williams LLP, 2015. [Consultado a 1/05/2018]] Disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf

EUROPEAN COMMISSION - **Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union**. COM/2010/0609 final. 2010.

GILAD, Sharon - It runs in the family: Meta-regulation and its siblings. In **Regulation & Governance**. John Wily & Sons Australia, Ltd, 2010. ISSN 1748-599. Vol. 4, p. 485 - 506.

GREENLEAF, Graham - APEC's Cross-Border Privacy Rules System: A House of Cards?. In **Privacy Laws & Business International Report**. Sydney: University of New South Wales, 2014. Vol. 128, p. 27-30.

GREENLEAF, Graham – Data Protection Convention 108 Accession Eligibility: 80 Parties Now Possible In **Privacy Laws & Business International Report**. 2017. ISSN 2046-844X. Vol. 148, p. 12-16.

GREENLEAF, Graham - Five years of the APEC Privacy Framework: Failure or Promise?. In **Computer Law & Security Review**. Tilburg: Tilburg Institute for Law, Technology, and Society, 2009. Vol. 25, 1, p. 28 - 43.

HUSTINX, Peter - EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. In **New Technologies and EU Law**. ISBN-13: 9780198807216. Oxford: Oxford Academic, 2017. ISBN-13: 9780198807216. P. 123 – 173.

HUSTINX, Peter – The Role of Data Protection Authorities In **Reinventing Data Protection?**. Dordrecht: Springer, 2009. ISBN 978-1-4020-9497-2. P. 131 – 137.

KARMEL, Roberta e R. KELLY, Claire – The Hardening of Soft Law in Securities Regulation. In **Brooklyn Journal of International Law**. Brooklyn, 2009. Vol. 34, 3, p. 884 – 951.

KIRBY, Michael – The History, Achievement and Future of the 1980 OECD Guidelines on Privacy In **International Data Privacy Law**. 2011. ISSN 2044-3994. Vol. 1, p. 6–14.

KISS, Attila e SZŐKE, László - Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. In **Reforming European Data Protection Law**. Dordrecht; Springer, 2015.. ISBN 978-94-017-9385-8. P. 311-332.

KOBRIN, Stephen – Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. In **Review of International Studies**. 2004. Vol. 30, p. 111-131.

KOOPS, Bert-Jaap – The Trouble with European Data Protection Law. In **International Data Privacy Law**. Oxford: Oxford Academic, 2014. ISSN 2044-3994. Vol. 4, 4, p. 250-261.

KULESZA, Joanna - Transboundary data protection and international business compliance. In **International Data Privacy Law**. Oxford: Oxford Academic, 2014. ISSN 2044-3994. Vol. 4, 4, p. 298 – 306.

KUNER, Christopher – Developing an Adequate Legal Framework for International Data Transfers. In **Reinventing Data Protection?**. Dordrecht: Springer, 2009. ISBN 978-1-4020-9497-2. P. 263 - 273.

KUNER, Christopher - **Transborder Data Flows and Data Privacy Law**. 1ª ed. Oxford: Oxford University Press, 2013. ISBN: 9780199674619.

KUNER, Christopher *et al* – Editorial: Risk Management in Data Protection. In **International Data Privacy Law**. Oxford: Oxford Academic, 2015. ISSN 2044-3994. Vol. 5, 2, p. 95 – 98.

LACHAUD, Eric - The General Data Protection Regulation and the rise of certification as a regulatory instrument. In **Computer Law & Security Review**. Tilburg: Tilburg Institute for Law, Technology, and Society, 2018. Vol. 34, 2, p. 244-256.

LYNSKEY, Orla – **The Foundations of EU Data Protection Law**. 1ª ed. Oxford: Oxford University Press, 2015. ISBN 978–0–19–871823–9.

MARSDEN, Christopher - Co- and Self-regulation in European Media and Internet Sectors: The Results of Oxford University's Study. In **The Media Freedom Internet Cookbook.** Vienna, 2004. P. 76 – 101.

MCBARNET, Doreen - **Corporate Social Responsibility Beyond Law, Through Law, for Law**. Edimburgo: U. of Edinburgh School of Law Working Paper No. 2009/03, 2009.

MESAIKOU, Evangelia - **Examining the Binding Corporate Rules as the most promising solution for the cross border data transfers of multinational companies under the EU Data Protection Directive: A comparative study with the Cross Border Privacy Rules developed in the APEC**. Tilburg: Tilburg University, 2008. Dissertação de mestrado.

MOEREL, Lokke – **Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers**. 1ª ed. Oxford: Oxford University Press, 2012. ISBN 978–0–19–966291–3.

MOEREL, Lokke - **The Implications of the *Schrems* judgment of the European Court for data transfers to the US**. [Consultado a 1/05/2018] Disponível em https://media2.mofo.com/documents/160913-implications-schrems-data-transfers.pdf

MOEREL, Lokke e Prins, Corien - **Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things**. SSRN Electronic Journal, 2016. [Consultado a 1/05/2018]. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123

PADOVA, Yann - The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?. In **International Data Privacy Law**. Oxford: Oxford Academic, 2016. ISSN 2044-3994. Vol. 6, 2, p. 139 – 161.

PIETRZAK, Sylwia - **Transborder Data Flows: Binding Corporate Rules as a Global Transfer Mechanism and Trusted Data Processing Area**. Tilburg: Tilburg University, 2017. Dissertação de mestrado.

POUNDER, Christopher – **Why The APEC Privacy Framework is Unlikely to Protect Privacy**. 2017. [Consultado a 1/05/2018]. Disponível em https://www.out-law.com/page-8550

PRINS, Corien - Should ICT Regulation Be Undertaken at an International Level?. In **Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners**, Haia: T.M.C. Asser Press. Vol. 9, p. 293 – 244.

PROUST, Olivier e Bartoli, EMMANUELLE - Binding Corporate Rules: A Global Solution for International Data Transfers. In **International Data Privacy Law**. Oxford: Oxford Academic, 2012. ISSN 2044-3994. Vol. 2, 1, p. 35 – 39.

PURTOVA, Nadezha – **Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency**. 2017. Tilburg Law School Research Paper No. 2017/21**.**

PURTOVA, Nadezhda - Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain Informatisation, and Ambient Intelligence. In **Computers, Privacy and Data Protection: An Element of Choice.** Dordrecht: Springer, 2011. 978-94-007-0641-5. P. 39 - 64.

RAAB, Charles e KOOPS, Bert-Jaap – Privacy Actors, Performances, and the Future of Privacy Protection In **Reinventing Data Protection?**. Dordrecht: Springer, 2009. ISBN 978-1-4020-9497-2. P. 207 - 221.

ROUVROY, Antoinette e POULLET, Yves - The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In **Reinventing Data Protection?**. Dordrecht: Springer, 2009. ISBN 978-1-4020-9497-2. P. 45-76.

RUBINSTEIN, Ira – Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes. In **A Journal of Law and Policy for the Information Society**. 2010. Vol. 6, p. 355 – 423.

TERWANGNE, Cécile de – Is a Global Data Protection Regulatory Model Possible?. In **Reinventing Data Protection?**. Dordrecht: Springer, 2009. ISBN 978-1-4020-9497-2. P. 175 - 189.

WUGMEISTER, Miriam, RETZER, Karin e RICH, Cynthia - Global solution for cross-border data transfers: making the case for corporate privacy rules. In **Georgetown Journal of International Law**. Georgetown, 2007. Vol 38, p. 449 – 498.

ZARSKY, Tal – Incompatible: The GDPR in the Age of Big Data. In **Seton Hall Law Review**. 2017. Vol. 47, p. 995 – 1020.

B. Relatórios, Pareceres, Documentos, Opiniões e Recomendações

ARTICLE 29 WORKING PARTY - **First orientations on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy (WP4)**

ARTICLE 29 WORKING PARTY - **Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? (WP7)**

ARTICLE 29 WORKING PARTY - **Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (WP74)**

ARTICLE 29 WORKING PARTY - **Model Checklist: Application for approval of Binding Corporate Rules (WP102)**

ARTICLE 29 WORKING PARTY - **Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules" (WP107)**

Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules (WP108)

ARTICLE 29 WORKING PARTY - **Working Document Setting up a framework for the structure of Binding Corporate Rules (WP154)**

ARTICLE 29 WORKING PARTY - **Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules (WP155)**

ARTICLE 29 WORKING PARTY - **The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168)**

ARTICLE 29 WORKING PARTY - **Adequacy Referential (WP254)**

EUROPEAN COMMISSION – **European Governance: A White Paper**. 2001. COM(2001) 428 final.

EUROPEAN DATA PROTECTION SUPERVISOR - **EDPS Opinion on coherent enforcement of fundamental rights in the age of big data.** 2016. Disponível em

https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf [Consultado a 1/05/2018]

EUROPEAN DATA PROTECTION SUPERVISOR - **EDPS recommendations on the EU's options for data protection reform.** 2015. Disponível em https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_en_0.pdf [Consultado a 1/05/2018]

EUROPEAN DATA PROTECTION SUPERVISOR - **Preliminary Opinion on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy"**. 2009. Disponível em https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en [Consultado a 1/05/2018]

GRUPO DE TRABALHO DO ARTIGO 29º - **Documento de Trabalho: Observações preliminares relativas ao uso de cláusulas contratuais no contexto da transferência de dados pessoais para países terceiros (WP9)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Transferência de dados pessoais para países terceiros: aplicação dos artigos 25º e 26º da Directiva comunitária relativa à protecção dos dados (WP12)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Privacidade na Internet: Uma Abordagem integrada da UE no domínio da protecção de dados em linha (WP37)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Parecer 8/2003 sobre o projecto de cláusulas contratuais-tipo apresentado por um grupo de organizações empresariais ("modelo de contrato alternativo") (WP84)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Declaração do grupo de trabalho do artigo 29.º sobre a aplicação da lei (WP 101)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Documento de trabalho sobre uma interpretação comum do n.º 1 do artigo 26.º da Directiva 95/46/CE de 24 de Outubro de 1995 (WP114)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Parecer 4/2007 sobre o conceito de dados pessoais (WP136)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Parecer 3/2010 sobre o princípio da responsabilidade (WP173)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Parecer 05/2012 relativo a computação em nuvem (WP196)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Parecer 1/2010 sobre os conceitos de "responsável pelo tratamento" e "subcontratante" (WP169)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Documento explicativo sobre as regras vinculantes para empresas destinadas aos subcontratantes (WP204)**

GRUPO DE TRABALHO DO ARTIGO 29º - **Parecer 2/2014 sobre os parâmetros de referência dos requisitos aplicáveis às regras vinculativas para empresas (RVE) apresentadas às autoridades nacionais de proteção de dados da UE e às regras de privacidade transfronteiras (RPT) apresentadas aos agentes de responsabilização da Cooperação Económica Ásia-Pacífico (APEC) (WP212)**

PARLAMENTO EUROPEU, CONSELHO DA UNIÃO DA EUROPA E COMISSÃO EUROPEIA - **Acordo Interinstitucional Entre o Parlamento Europeu, o Conselho Da União Europeia e a Comissão Europeia Sobre Legislar Melhor de 13 de abril de 2016**

RAND REPORT – **Options for and Effectiveness of Internet Self- and Co- Regulation.** Santa Monica: RAND Corporation, 2008.

RAND REPORT – **Review of the European Data Protection Directive**. Santa Monica: RAND Corporation, 2009.

Índice