

Ana Rita Moura Neves de Matos de Cadima Carvalho

**A DUPLICIDADE DE PAPÉIS DO CORRETOR DE
SEGUROS AO ABRIGO DO NOVO RGPD: RESPONSÁVEL
PELO TRATAMENTO E/OU SUBCONTRATANTE**

Relatório de estágio curricular na MDS RE
com vista à obtenção do grau de Mestre em
Direito e Mercados Financeiros

Orientadores:

Professora Doutora Margarida Lima Rego, Professora da Faculdade de Direito da
Universidade Nova de Lisboa

Dr.^a Ana Cristina Borges, CEO MDS RE

Dezembro 2018

Ana Rita Moura Neves de Matos de Cadima Carvalho

**A DUPLICIDADE DE PAPÉIS DO CORRETOR DE
SEGUROS AO ABRIGO DO NOVO RGPD: RESPONSÁVEL
PELO TRATAMENTO E/OU SUBCONTRATANTE**

Relatório de estágio curricular na MDS RE
com vista à obtenção do grau de Mestre em
Direito e Mercados Financeiros

Orientadores:

Professora Doutora Margarida Lima Rego, Professora da Faculdade de Direito da
Universidade Nova de Lisboa

Dr.^a Ana Cristina Borges, CEO MDS RE

Dezembro 2018

A duplicidade de papéis do corretor de seguros ao abrigo do novo RGPD: Responsável pelo tratamento e/ou subcontratante?

DECLARAÇÃO DE COMPROMISSO ANTIPLÁGIO

Declaro por minha honra que o trabalho elaborado é original e da minha exclusiva autoria. Toda a utilização de contribuições ou textos alheios está devidamente referenciada. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 1 de Dezembro de 2018

AGRADECIMENTOS

Na realização da presente dissertação contei com o apoio de múltiplas pessoas às quais estou profundamente grata. Em primeiro lugar, não posso deixar de agradecer o apoio incondicional dos meus pais, pelo apoio económico e pelo acompanhamento permanente em toda a minha vida pessoal e académica.

Quero também agradecer à Professora Doutora Margarida Lima Rego pela permanente orientação neste desafio. Pela visão crítica e oportuna que em muito contribuíram para a construção desta dissertação. Agradeço também a total disponibilização e as rigorosas notas da Dr.^a Maria da Graça Canto Moniz, especialista em matéria de Proteção de Dados.

Muito agradeço também à equipa da MDS, salientando a Dr.^a Ana Cristina Borges e o meu colega André Vicente pela inteira disponibilidade no auxílio de alguns temas. Por último, não posso deixar de agradecer às minhas colegas e amigas Mariana Justo e Rita Mendes pela sua grande paciência e palavras motivadoras no decorrer desta longa viagem.

*«The only way to achieve the impossible is to
believe it's possible»*

Lewis Carroll

Carlos Carvalho

INDICAÇÕES DE LEITURA

MODO DE CITAÇÃO

As citações utilizadas na presente dissertação fazem-se com a indicação, em primeiro lugar do apelido, e primeiro nome do autor, separado por um hífen do título da obra, que é mencionado em itálico. O último elemento que compõe a nota diz respeito à página, mencionando-se por vezes o endereço eletrónico da obra por forma a facilitar a consulta do leitor. As obras em co-autoria separam os autores do maior para o menor grau de relevância, seguindo a ordem de indicações acima referidas. Nas obras de publicação periódica o título do artigo em questão é mencionado em aspas e separado do título da revista/publicação através da preposição *in*. Em caso de citação indireta, ou seja, uma citação de uma citação, utiliza-se a expressão «apud», que significa «citado por». As expressões em latim ou em língua estrangeira serão apresentadas em itálico. As transcrições são feitas de acordo com a língua em que se encontram escritas. As citações de jurisprudência são feitas pela indicação abreviada do acórdão e número do processo.

A bibliografia contém todos os elementos indicados acima, acrescentado os que a tornam suficiente em termos de localização em motores de busca, nomeadamente, volume, n.º, ano de publicação, consulta e endereço eletrónico.

Esta dissertação foi escrita ao abrigo do Novo Acordo Ortográfico.

Declaro que o corpo da tese ou dissertação, incluindo espaços e notas, ocupa um total de 123 666 caracteres.

LISTA DE ABREVIATURAS

AC - Acordão

AIPD – Avaliação de Impacto sobre Proteção de Dados

ASF – Autoridade de Supervisão de Seguros e Fundos de Pensões

Cap – Capítulo

CC – Código Civil

CEPD – Comité Europeu de Proteção de Dados

Cf – Conferir

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

DDS – Diretiva de Distribuição de Seguros

DL – Decreto-Lei

EEE – Espaço Económico Europeu

EPD – Encarregado de Proteção de Dados

n.º - Número

OCDE - Organização para a Cooperação e Desenvolvimento Económico

p – Página

paras. – Parágrafos

RGPD – Regulamento Geral de Proteção de Dados

ss - Seguintes

STJ – Supremo Tribunal de Justiça

TI – Tecnologia de Informação

UE – União Europeia

vol – Volume

RESUMO

A revolução a que se tem assistido no ecossistema digital tem provocado uma disseminação, sem controlo, dos dados pessoais que se pretende colmatar com as alterações legislativas propostas pelo Regulamento Geral de Proteção de Dados, ao nível dos princípios e direitos, como também as respeitantes às novas obrigações inerentes ao responsável pelo tratamento e ao subcontratante. A necessidade em clarificar os seus conceitos surge para uma correta atribuição das obrigações, auxiliando também em questões de aplicabilidade da lei nacional. Estas alterações legislativas configuram também impactos a um nível mais global em todos os setores de atividade, em especial para o setor segurador pelo tratamento necessário de categoriais de dados especiais.

O objetivo deste estudo é analisar o papel da MDS – Corretor de Seguros no âmbito da sua atividade com os clientes e seguradoras. O estudo incide sobre a classificação da entidade no momento que antecede e sucede à celebração do contrato de seguro. A análise divide-se em três momentos essenciais: O primeiro dedica-se à contextualização do Regulamento Geral de Proteção de Dados, o segundo concentra o seu foco nas figuras do responsável pelo tratamento e subcontratante e o terceiro aborda os impactos provocados pelo regulamento no setor segurador, em especial na categoria do corretor de seguros.

A primeira parte deste relatório de estágio aborda os princípios e os direitos presentes no novo Regulamento Geral de Proteção de Dados. A análise deste primeiro capítulo culmina no estudo dos conceitos de responsável pelo tratamento e subcontratante, destacando-se as principais alterações legislativas, bem como a complexidade da sua atribuição na prática e os impactos que provoca no setor segurador. De seguida o foco centra-se, dentro do ramo segurador, na categoria de corretor de seguros, onde se examina a problemática da duplicidade de papéis, considerando as já expostas linhas orientadoras da

Comissão Nacional de Proteção de Dados e os impactos do regulamento provocados por intermédio do setor segurador, bem como aqueles que dela resultam diretamente.

Palavras-chave: RGPD; Responsável pelo tratamento; Subcontratante; MDS.

ABSTRACT

The revolution witnessed in the digital ecosystem has led to an uncontrolled dissemination of the personal data that it intends to fill with the legislative changes proposed by the General Regulation on Data Protection in terms of principles and rights, as well as those concerning new obligations inherent to the controller and the subcontractor. The need to clarify its concepts arises for a correct assignment of the obligations, also aiding in questions of applicability of the national law. These legislative changes also imply impacts at a more global level in all sectors of activity, especially for the insurance industry by the necessary treatment of special data categories.

The purpose of this study is to analyze the role of MDS - Corretor de Seguros in the scope of its activity with clients and insurers. The study focuses on the classification of the entity at the time before and succeeds to the conclusion of the insurance contract. The analysis is divided into three key moments: The first stage focuses on the contextualization of the General Data Protection Regulation, the second concentrates its focus on the data of the controller and the subcontractor and the third deals with the impacts caused by the regulation in the insurance sector, especially in the insurance broker category.

The first part of this internship report addresses the principles and rights of the new General Data Protection Regulation. The analysis of this first chapter culminates in the study of the concepts responsible for the treatment and subcontractor, highlighting the main legislative changes, as well as the complexity of their attribution in practice and the impacts that it causes in the insurance sector. Next, the focus is on the insurance broker category, where the issue of duplicity of roles is examined, as well as the guidelines of the National Commission on Data Protection and the impacts of the Regulation through the insurance sector, as well as those that directly result from it.

Keywords: RGPD; Controller; Processor; MDS.

INTRODUÇÃO

A palavra privacidade de acordo com o dicionário de Língua Portuguesa, apresenta como definição: «Condição do que é privado, pessoal ou íntimo; Vida privada». Tem origem na palavra grega *privates* que significa separado do resto. Quer isto dizer que, é ao separar-se da sociedade que o indivíduo se pode expressar verdadeiramente. Foi em 1890 com Samuel D. Warren e Louis D. Brandeis que surgiu o primeiro¹ artigo jurídico sobre a privacidade². Inicialmente a utilização da palavra tinha uma função meramente física, baseando-se no isolamento de uma zona como forma de proteção do domicílio da família e do segredo da correspondência.³ O termo foi evoluindo com as alterações provocadas pelos avanços políticos, económicos e sociais. Assim, o direito de privacidade que outrora encontrava a sua fronteira na proteção da propriedade compreende agora uma nova forma de interpretação que coloca a pessoa e o seu desenvolvimento no centro do direito à privacidade. Esta nova asserção configura no Direito Português, nomeadamente na CRP nos seus artigos 26.º, 18.º e 35.º a sua proteção em vários contextos. Ao nível europeu, a sua proteção é também configurada na Convenção Europeia dos Direitos do Homem, a Declaração Universal dos Direitos do Homem, a Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados pessoais e a Carta dos Direitos Fundamentais da União Europeia. Medindo toda esta proteção que é conferida a nível europeu, é notória a sua influência no artigo 1.º da Diretiva n.º 95/46/CE. A definição abrange uma continuidade relativamente ao conceito expresso nas *Guidelines* da OCDE, bem como do Conselho da Europa⁴.

A evolução da sociedade digital tem provocado um crescente grau de exposição dos dados pessoais, resultando numa tensão entre os direitos e liberdades das pessoas

¹ GLANCY, Dorothy J - «*The Invention of the Right to Privacy*», p.1.

² WARREN, Samuel and D. BRANDEIS, Louis D, «The Right to Privacy», p. 193-220.

³ WARREN, Samuel and D. BRANDEIS, Louis D. - «The Right to Privacy», p.3.

⁴ CORDEIRO, António Barreto Menezes - «DADOS PESSOAIS: CONCEITO, EXTENSÃO E LIMITES», p.4.

singulares. O paradigma atual apela pela formação de um quadro legislativo mais sólido de homogeneização. O incremento da fragmentação pode impedir a livre circulação dos dados e criar obstáculos ao exercício das atividades económicas. Nesta senda, a ideia de dar continuidade ao progresso da economia digital resulta do Regulamento Geral da Proteção de Dados que prevê uma contribuição para um mercado único europeu de dados e uma harmonização legislativa ao nível de todos os Estados-Membros da UE, assentando numa lógica de atribuição de um maior controlo dos dados aos seus titulares através da constituição de novos direitos como a portabilidade e o esquecimento e o reforço dos já existentes. Mas, o novo quadro legal traz de um mesmo modo mudanças significativas que impactam também as organizações, consoante a natureza, áreas de atividade, dimensão e tipo de tratamento de dados pessoais. Assim, as novas regras de tratamento dos dados pessoais, otimizam os princípios e dos direitos dos titulares através da atribuição de maiores responsabilidades às entidades responsáveis pelo tratamento, bem como aos seus subcontratantes. As principais alterações legislativas introduzidas são alterações substanciais que requerem uma avaliação criteriosa dos níveis de riscos aceitáveis para as organizações em matérias de proteção de dados pessoais.

Focando o setor segurador, com especial destaque para a figura do corretor de seguros e verificando que as maiores preocupações se prendem com matérias relacionadas com o tratamento de categorias especiais de dados, com a subcontratação e com as novas exigências ao nível do encarregado de proteção de dados, as entidades devem implementar uma metodologia que avalie criteriosamente a respetiva situação atual:

- (i) Identificação das falhas existentes;
- (ii) Elaboração um plano de ação com medidas e prazos concretos de implementação, nomeadamente realização de inventários que identifiquem as áreas que tratam dados pessoais, quais os dados tratados e os prazos de conservação dos mesmos;
- (iii) Revisão dos conceitos normativos para introdução de políticas de privacidade, dever de informação, entre outras;

- (iv) Renovação de acordos no ramo da subcontratação;
- (v) Constituição de um EPD nas atividades que o artigo 35.º do regulamento exige e que serão mais adiante enunciadas e fundamentadas.

Posto isto, a questão objeto deste estudo insere-se na **Duplicidade de papéis que o Corretor de Seguros pode assumir nas fases de intervenção cliente/seguradora: Responsável pelo tratamento e/ou Subcontratante?**

O estudo desta problemática merece especial atenção, uma vez que é ao responsável pelo tratamento que compete a determinação das finalidades e os meios de tratamento dos dados pessoais. Assim, apesar de ser encarado como mero intermediador, o corretor pode ser considerado responsável pelo tratamento, sendo-lhe assim exigido, entre outras obrigações, a prestação de informações aos titulares dos dados, previstas no artigo 13.º, do RGPD.

A análise do tema proposto teve início com uma exausta investigação bibliográfica baseada na intenção de conhecer a fundo a problemática a que se refere a realidade da MDS enquanto corretora de seguros, mas também a realidade subjacente a qualquer entidade que se figure com a mesma discussão. Assim, a abordagem que mais se compatibiliza com a metodologia utilizada para a solução da questão que se coloca «Duplicidade de papéis que o Corretor de Seguros pode assumir nas fases de intervenção cliente/seguradora: Responsável pelo tratamento e/ou Subcontratante?» é a qualitativa. A observação e a interpretação dos estudos realizados permitiram chegar à qualificação da MDS nos seus momentos de intervenção, quer no âmbito dos clientes, quer no âmbito das seguradoras. Este estudo encontra-se assim dividido em quatro momentos, entendendo-se o primeiro como o pilar que permitiu a exposição dos restantes capítulos. Assim, é refletida no primeiro capítulo a análise do trabalho realizado no estágio curricular na MDS RE, que foca, por fases, a implementação do RGPD na empresa. O segundo momento pertence às principais alterações legislativas referentes aos princípios e direitos dos titulares dos dados. A terceira fase deste relatório de estágio afigura a noção dos conceitos responsável pelo tratamento e subcontratante, destacando a complexidade da sua aplicação na prática e a importância da sua clarificação. A análise efetuada converge no seu enquadramento ao

ramo segurador, em especial na figura do corretor de seguros e na questão da duplicidade dos seus papéis na fase que antecede e sucede à celebração do contrato de seguro. Expostas as notas essenciais que originam um melhor entendimento do tema, é elaborado com base na realidade da MDS enquanto corretora de seguros, um estudo de caso sobre a problemática da duplicidade de qualificações que esta entidade pode assumir pelas atividades que lhe estão associadas⁵.

⁵ A importância da celebração de um contrato entre a corretora e a empresa de seguros afigura-se como um dos temas centrais do RGPD, bem como da nova Diretiva de Distribuição de Seguros, visto que incorpora uma maior responsabilidade e uma maior defesa na questão de incumprimento. O requisito de informação prévia à ASF de uma empresa que pretenda subcontratar e do aumento das responsabilidades, obrigações e sanções ao nível do incumprimento, poderão permitir, todavia, de uma mesma forma, colmatar a falta de vínculos contratuais entre as corretoras e empresas de seguros.

CAPÍTULO I

ESTÁGIO CURRICULAR

1.1. MDS

A MDS é uma entidade especializada no desenvolvimento e negociação de soluções de corretagem de resseguro, operando em Portugal, África e Brasil. Foi constituída em 1984 e presta também serviços de consultoria de seguros. É detida pelos grupos Sonae, a maior multinacional portuguesa e pelo grupo industrial brasileiro, Suzano. O grupo é fundador da BrokersLink, uma empresa global de corretagem e acionista da Ed. Brooking (a anterior Cooper Gay Swett & Crawford), considerado o maior corretor de resseguro independente do mundo, e é um Lloyd's Broker. Detém um portfólio diversificado e uma posição relevante a nível mundial, ocupando o ranking dos três melhores corretores mundiais. Quer isto dizer que o seu acesso aos mercados internacionais é pleno, adquirindo, conseqüentemente, uma maior capacidade para alcançar as melhores soluções para os clientes.

A MDS RE é uma sociedade do grupo MDS especializada no desenvolvimento e negociações de corretagem de resseguro, serviços de consultoria de seguros a nível de riscos tradicionais e emergentes. Opera fortemente em Portugal e em África, beneficiando da extensa rede internacional e de acesso privilegiado ao Lloyd's e à Ed, capacitando-a, deste modo, para apresentar um mais vasto e sofisticado leque de soluções para a transferência do risco, combinando com as melhores condições de cobertura e preços.

1.2. MDS RE

Na sequência do protocolo celebrado entre a Universidade Nova de Lisboa e a MDS RE, foi-me concedida a oportunidade de realizar um estágio curricular nesta instituição, com a duração efetiva de quatro meses para a elaboração de um relatório de estágio com vista à obtenção do grau de mestre.

No decorrer do estágio tive a oportunidade de acompanhar e intervir no processo de implementação do RGPD na MDS. O processo de implementação consistiu:

- (i) Elaboração de um diagnóstico para calcular a percentagem de conformidade da MDS face ao RGPD;
- (ii) Elaboração das políticas de privacidade e de *cookies*;
- (iii) Análise dos acordos de confidencialidade elaborados pelos Clientes e Seguradoras;
- (iv) Implementação de medidas de segurança necessárias à proteção dos dados pessoais;
- (v) Estudo da problemática dos novos negócios de forma a torná-los conforme o RGPD.

Na sequência da realização do estágio e sem ter a pretensão de elaborar um relatório meramente descritivo com a identificação apenas das atividades concretizadas, pretendo abordar e investigar a questão da possível duplicidade de sujeitos do Corretor de Seguros. Esta duplicidade configura alguns obstáculos no momento da elaboração de determinados acordos de subcontratação.

CAPÍTULO II

O NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

2. Contextualização

A ponderação da nova legislação sobre a proteção dos dados pessoais resulta, em larga medida, do crescente grau de disseminação, sem controlo, dos dados pessoais, enfatizando o desequilíbrio da pessoa face às entidades empresariais. A concretização de um novo quadro legal que coloque os cidadãos no controlo dos seus dados permite combater a posição de vulnerabilidade em que o respetivo titular agora se encontra. A margem de liberdade em relação ao conteúdo legislativo da qual resultava a Diretiva 95/46/CE, de 24 de outubro de 1995, configurava um panorama de insegurança jurídica que se pretende colmatar com o novo Regulamento Geral de Proteção de Dados. As novas regras de tratamento de dados pessoais, impostas pelo RGPD glorificam com requisitos mais exigentes, o quadro regulatório já apresentado pela Lei 67/98, de 26 de outubro, consubstanciando um acompanhamento das operações de tratamento, independentemente do fundamento jurídico do tratamento⁶.

2.1. Direitos dos titulares dos dados

A cartilha de direitos em que o RGPD assenta consubstancia o ideal de proteção, controlo e transparência desejado pelos titulares. A adaptação do quadro regulatório advém da crescente exposição dos dados pessoais das pessoas singulares e pode resultar em danos significativos para os seus direitos e liberdades. Com o acompanhamento do tratamento dos dados e uma maior transparência do tratamento, que se traduz numa maior clarificação e num maior reforço dos direitos já existentes e na criação de outros, o regulamento proporciona ao titular dos dados meios eficazes para assegurar que estão plenamente

⁶ Commission Staff Working Paper - «*Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*», de 25 de janeiro de 2012, p.53.

informados quanto ao que se sucede aos seus dados pessoais, facilitando igualmente, o exercício dos seus direitos⁷.

2.1.1. Informação

O reforço do direito à informação revela-se na predominância de uma base informativa mais sólida no momento da tomada de decisões por parte dos titulares dos dados. Está consagrada nos artigos 13º e 14º do RGPD e encontra-se subjacente ao dever geral de transparência. Este direito exige por parte do responsável pelo tratamento a prestação da informação de uma forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples⁸. Acresce ainda, a prestação de informação ao titular dos dados, que deve ser concretizada no momento da recolha dos mesmos, seja por escrito ou telefone e realizada junto titular ou não⁹. São configuradas, no entanto, algumas exceções, nomeadamente, em situações que o titular dos dados detenha já conhecimento das mesmas, situações em que se comprove a impossibilidade de disponibilização de informação ou que a empresa tenha que fazer um esforço desproporcional para a concretizar, em casos em que a obtenção e divulgação dos dados esteja expressamente prevista no direito da União ou nos Estados-Membros ou na exigibilidade da confidencialidade em virtude de uma obrigação de sigilo profissional. É de notar ainda, o particular cuidado pelos responsáveis do tratamento no âmbito dos deveres de informação quando o tratamento de dados abrange crianças, uma vez que, representam um grupo societário mais vulnerável.

2.1.2. Direito de acesso

Entende-se este direito como o ponto de partida para a verificação da qualidade dos dados, podendo resultar ou não no exercício dos seus direitos¹⁰. O direito de acesso,

⁷ KUNER, Christopher - «*The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*», de 6 de fevereiro de 2012, p.6.

⁸ Artigo 12.º do RGPD.

⁹ Artigos 13.º e 14.º do RGPD.

¹⁰ COUTINHO, Francisco Pereira e MONIZ, Graça Canto - *O ANUÁRIO DA PROTEÇÃO DE DADOS*, p.17.

consagrado no artigo 15.º do RGPD, confere uma maior transparência no tratamento, permitindo uma análise ponderada e corrigido o desequilíbrio entre a inovação na proteção de dados e a sua exploração¹¹. O acesso pode ter uma regularidade razoável no que diga respeito às razões pelos quais os dados são tratados, quais os dados que são tratados, destinatários a quem sejam divulgados, incluindo entidades localizadas em países fora da União Europeia ou organizações internacionais, sendo neste caso, informado das garantias aplicadas.

2.1.3. Direito à portabilidade

A posição teleológica do direito à portabilidade instituído no artigo 20º do RGPD, configura uma interpretação complexa e multifacetada¹². O instrumento possibilita o indivíduo de solicitar a transmissão dos seus dados para outro prestador de serviços, reutilizando-os para a contratação de outro serviço, facilitando igualmente em caso de incumprimento das regras legais do responsável pelo tratamento. Inserem-se aqui também informações comunicadas ao Responsável pelo tratamento por terceiro (instruções dadas por terceiros da conta bancária do titular dos dados), não excluindo a informação de terceiros prestada ao titular¹³. Em contrapartida, ficam excluídos, para este efeito, os dados que no decorrer da atividade do responsável pelo tratamento sejam derivados ou obtidos por inferência dos respetivos dados originais (por exemplo, dados que delineiam um perfil do consumidor ou histórico de sinistralidade)¹⁴. A importância da criação desta ferramenta implica não só a proteção dos dados pessoais como promove também as transferências de dados, não implicando, todavia, o seu pagamento. O GRUPO DE TRABALHO DO ARTIGO 29.º entende que o direito à portabilidade abrange tanto os dados fornecidos de forma consciente e ativa pelo respetivo titular, bem como os dados pessoais que o titular

¹¹ AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS - Parecer 3/2015. «A grande oportunidade da Europa Recomendações da AEPD sobre as opções da UE para a reforma da proteção de dados», p.4.

¹² CORDEIRO, António Menezes, (coordenador científico), CORDEIRO, António Barreto Menezes e ROCHA, Francisco, (coordenadores executivos) - «I JORNADA DE PROTEÇÃO DE DADOS E EMPRESAS» Primeiro Painel, em 3 de maio de 2018. [consult. 15/11/2018]. Disponível em: <https://www.youtube.com/watch?v=gnmxsKZ4WgU>

¹³ O n.º4 do presente artigo refere que os dados de terceiros podem ser objeto de portabilidade, não podendo, no entanto, o terceiro ser colocado numa posição pior da que atualmente se encontra.

¹⁴ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientações sobre o direito à portabilidade dos dados*, de 5 de abril de 2017, p. 3 e ss. [consult. 15/11/2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf

fornece ao utilizar determinado serviço ou dispositivo (por exemplo, históricos de pesquisa, dados de tráfego ou dados de localização geográfica)¹⁵. O acesso a serviços *online*, requer muitas vezes o fornecimento de informação pessoal com o objetivo de prever comportamentos e elaborar análises de mercado, adaptando os produtos e serviços às necessidades dos consumidores, constituindo, assim, vantagens significativas sobre os concorrentes¹⁶. A ilação que se extrai do n.º1 do artigo, compreende especificidades que devem ser tidas em consideração pelo responsável do tratamento e que se debruçam no recebimento dos dados num formato estruturado, de uso corrente e de leitura automática, possibilitando a sua reutilização. Os termos «estruturado», de «uso corrente» e de «leitura automática», vêm despoletar a ideia da interoperabilidade. Ou seja, ainda que os sistemas das organizações não sejam compatíveis entre si, devem possuir a capacidade de poderem comunicar entre si, permitindo a reutilização dos dados, respeitando assim, o âmbito do regulamento.

Uma última nota a apontar a este direito reconduz-se à sua matéria de riscos. Os abusos que lhe estão inerentes, podem impedir a prestação de serviços e causar tratamento discriminatório. A título de exemplo, configura-se a não celebração do contrato de saúde ou um de vida pelas companhias de seguros, sem que lhes sejam exercidas a portabilidades dos dados médicos, hábitos de vida do tomador do seguro¹⁷.

¹⁵ Cuatrecasas, «PROPRIEDADE INTELECTUAL, MEDIA E TI», de 19 de julho de 2017, p.3. [consult. 15/11/2018]. Disponível em: https://www.cuatrecasas.com/pt/publicacoes/newsletter_propriedade_intelectual_media_e_ti_2_trimestre_2017.html

¹⁶ AUWERMEULEN, Barbara Van Der - «How to attribute the right to data portability in Europe: A comparative analysis of legislations», p.2. [consult. 17/11/2018]. Disponível em: <http://isiarticles.com/bundles/Article/pre/pdf/104675.pdf>

¹⁷ CORDEIRO, António Menezes, (coordenador científico); CORDEIRO; António Barreto Menezes e ROCHA, Francisco, (coordenadores Executivos) - «I JORNADA DE PROTEÇÃO DE DADOS E EMPRESAS» Primeiro Painel, em 3 de maio de 2018. [consultado a 15/11/2018]. Disponível em: <https://www.youtube.com/watch?v=gmxsKZ4WgU>

2.1.4. Direito à retificação e ao esquecimento

O direito de retificação surge da averiguação da qualidade¹⁸ dos dados feita pelo respetivo titular. Assim, na medida em que constate um erro, tem o direito os retificar pelo consagrado no artigo 16.º do RGPD. Está intimamente associado ao direito ao esquecimento apontado no artigo 17.º do RGPD pela possibilidade de flexibilização relativamente à destruição permanente quando constate um dos motivos enumerados nas alíneas do n.º 1 do artigo 17.º. A sua importância surge do acórdão *Google Spain*¹⁹, na medida em que, o Tribunal de Justiça considerou que um operador de um motor de busca recolhe, recupera, regista, organiza, conserva, comunica e coloca informações (muitas delas pessoais) à disposição do público, desenvolvendo desta forma, a atividade de tratamento de dados pessoais, tornando-o responsável por retirar resultados que possam revelar uma ingerência indesejada na vida privada de algum usuário²⁰. Em respeito pelos direitos fundamentais consolidados nos artigos 7º e 8º da Carta de Direitos Fundamentais da União, o indivíduo pode efetivamente requerer que a informação não lhe seja mais associada, referindo apenas a sua exceção em caso de se fundamentar a sua exposição no interesse público²¹.

2.1.5. Direito à limitação

A limitação do tratamento de dados patente no artigo 18.º do RGPD reconduz-se a situações em que não seja claro quando e se os dados pessoais terão de ser apagados. A

¹⁸ COUTINHO, Francisco Pereira e MONIZ, Graça Canto, *O ANUÁRIO DA PROTEÇÃO DE DADOS*, p.17.

¹⁹ CONCLUSÕES DO ADVOGADO-GERAL NIILO JÄÄSKINEN apresentadas em 25 de junho de 2013 (1)

Processo C-131/12, Google Spain SL Google Inc. contra Agencia Española de Protección de Datos (AEPD) Mario Costeja González [pedido de decisão prejudicial apresentado pela Audiencia Nacional (Espanha)]. [consult. 18/11/2018]. Disponível em: <https://www.gedipe.org/website/images/gedipe/jurisprudencia/C-131-12%20MARIO%20COSTEJA%20v.%20GOOGLE%20Opinião%20AG.pdf>, refere-se a matéria de apagamento de um dado pessoal (nome), por parte de um cidadão espanhol, que viu violado o seu direito à honra e bom nome pelo facto de surgir numa lista de resultados de pesquisa do *Google* no âmbito de um processo antigo de dívidas ao fisco. Apesar de solicitar a eliminação do seu nome, a empresa alegou que não tinha o dever de proceder a esse bloqueio, por não se encontrar estabelecida na União Europeia, tendo aí apenas uma sucursal que geria o negócio da publicidade.

²⁰ PLMJ, Sociedade de Advogados - «À PROCURA DO PASSADO: PROTECÇÃO DE DADOS E DIREITO AO ESQUECIMENTO NA INTERNET», p.1-2. [Consult. 24/11/2018]. Disponível em: [https://www.plmj.com/xms/files/newsletters/2014/Maio/Proteccao de Dados e Direito ao Esquecimento n a Internet.pdf](https://www.plmj.com/xms/files/newsletters/2014/Maio/Proteccao%20de%20Dados%20e%20Direito%20ao%20Esquecimento%20na%20Internet.pdf)

²¹ PEREIRA, Alexandre Libório Dias - «BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA»: A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)», p.18.

Comissão determina «limitação» como os dados pessoais que só podem ser tratados, com exceção da sua conservação, com o seu consentimento para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva ou por motivos de interesse público da UE ou de um Estado-Membro da UE²².

2.1.6. Direito à oposição

O titular dos dados goza, nos termos do artigo 21.º do regulamento da faculdade de se opor ao tratamento dos seus dados em qualquer momento com a exceção de o tratamento se fundamentar em razões preponderantes e legítimas para o responsável pelo tratamento²³.

2.1.7. Decisões automatizadas e definição de perfis

As práticas empresariais focam-se no aumento da produtividade, desenhando processos que, na ótica de acautelar o *misseling*, podem incluir a definição de perfis. Os resultados decorrentes do processo podem resultar em riscos significativos para os direitos e liberdades do titular dos dados, reconhecendo como forma de mitigação do risco, a possibilidade de o indivíduo não ficar sujeito a nenhuma decisão automatizada incluindo a definição de perfis²⁴. O processo das decisões automatizadas pode ocorrer com ou sem intervenção humana, podendo resultar ou não na definição de perfis. Assim, aquele que ocorre sem intervenção humana e sem a definição de perfis, consiste na criação de um *output* automatizado com base nos *inputs* recolhidos²⁵. Por outro lado, as decisões

²² Comissão Europeia - «Quando devo exercer o meu direito à limitação do tratamento dos meus dados pessoais?». [consult. 23/11/2018]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_pt

²³ No setor segurador é frequente os dados pessoais serem necessários para a defesa de ações judiciais em caso de medidas anti fraude ou anti branqueamento de capitais. Nesses casos, as companhias de seguros podem recusar-se a atender ao pedido de oposição de uma pessoa com base em motivos que prevalecem sobre os direitos e as liberdades deste.

²⁴ Artigo 22.º do RGPD.

²⁵ O Grupo de Trabalho foi instituído pelo artigo 29.º da Diretiva 95/46/CE e consiste num órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cujas atribuições se encontram previstas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE. Extrai-se do GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientação sobre as decisões*

individuais automatizadas que podem convergir na definição de perfis, resultam da apreciação de comportamentos pessoais²⁶.

Diferentemente dos restantes, o artigo 22.º fundamenta a sua base na proibição, que apesar do rigor que suporta, prevê ressalvas legais que se subsumem no (i) consentimento explícito do titular dos dados que como referido anteriormente, tem de se basear no maior retorno possível de informação por parte do responsável pelo tratamento tanto em relação às finalidades do tratamento como no que diz respeito às possíveis consequências uma vez que, é através de uma base sólida de informação, principalmente em caso de definição de perfis, que o exercício dos direitos dos titulares dos dados pode ser devidamente exercido. (ii) pela necessidade de celebração ou execução do contrato. O envolvimento humano para a quantidade de informação que o responsável pelo tratamento recebe e que tem que dar resposta é tido como ineficiente, sendo deste modo, mais apropriado a adoção de decisões individuais automatizadas. É de salientar contudo que, mais importante que a apropriação do método é a sua necessidade. Quer isto dizer que, se for passível de se adotar um meio menos invasivo a proibição do artigo 22.º é acionada. (iii) autorização dada pela União ou pelo Estado-Membro em casos de branqueamento de capitais e outras justificações legais, designando ainda assim, medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses dos titulares dos dados.

individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 Adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, o exemplo que com aplicação de coimas por excesso de velocidade com base exclusivamente em provas obtidas através de radares de velocidade constitui um processo de decisão automatizada que não implica necessariamente uma definição de perfis.

²⁶ O processo de apreciação de comportamentos pessoais para a venda de seguro de viagem, direcionada aos clientes cuja frequência de voo se considere acima do normal, sugere uma definição de perfis. O fator chave que se deve ter em consideração, é o fundamento da recolha dos dados. Consequentemente e como referido no GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientação sobre as decisões individuais automatizadas e a definição de perfis* para efeitos do Regulamento (UE) 2016/679 Adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, qualquer classificação que implique uma recolha de dados pessoais, mas que não resulte na sua apreciação, não se trata de definição de perfis.

CAPÍTULO III

O RESPONSÁVEL PELO TRATAMENTO E O SUBCONTRATANTE

3. Alterações legislativas

O ecossistema digital tem posicionado a Europa como um espaço geopolítico e geoestratégico. A criação de novas tecnologias, produtos e *softwares* tem levado o legislador a redefinir a arquitetura dos sistemas informáticos com a criação de meios tecnológicos ao nível dos responsáveis pelo tratamento e subcontratante que contribuam para uma melhor gestão do risco²⁷. O alcance destas novas obrigações em matéria de conformidade tem resultado numa aproximação entre as fronteiras do mundo tecnológico e jurídico, permitindo um mundo digital mais seguro e conseqüentemente mais atrativo para os consumidores²⁸.

3.1. O Responsável pelo tratamento

Indicado como um dos principais instrumentos que proporciona a proteção dos dados, a sua definição é, desde logo, indicada no artigo 4.º, alínea 7) do regulamento: «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; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo

²⁷ GUTWIRTH, Serge; LEENES, Ronald and DE HERT, Paul - *Data Protection on the Move: Current Developments in ICT and Privacy/Data*, p.21. [consult. 17/11/2018]. Disponível em: <https://books.google.pt/books?id=JPRcCwAAQBAJ&pg=PR10&lpg=PR10&dq=Gutwirth,+Serge,+Leenes,+Ronald,+De+Hert,+Paul.+%C2%ABData+Protection+on+the+Move:+Current+Developments+in+ICT+and+Privacy/Data%C2%BB,+2016&source=bl&ots=c9CF9p5F9p&sig=gUri4T4kmpjjiLUckFUiSm2LqjBY&hl=en&sa=X&ved=2ahUKEwiEqdmTzdjeAhURgHMKHXLQDtUQ6AEwBXoECAoQAQ#v=onepage&q=Gutwirth%2C%20Serge%2C%20Leenes%2C%20Ronald%2C%20De%20Hert%2C%20Paul.%20%C2%ABData%20Protection%20on%20the%20Move%3A%20Current%20Developments%20in%20ICT%20and%20Privacy%20Data%C2%BB%2C%202016&f=false>

²⁸ CORDEIRO, António Menezes, (coordenador científico), CORDEIRO, António Barreto Menezes e ROCHA, Francisco, (coordenadores executivos) - «I JORNADA DE PROTEÇÃO DE DADOS E EMPRESAS» Quarto Painel, em 3 de maio de 2018. [consult. 17/11/2018]. Disponível em: <https://www.youtube.com/watch?v=k9hZQ3Gr4u4>

tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro». A diferenciação empresarial provocada pelas TIC, bem como pela globalização do tratamento dos dados, torna necessário o recurso às linhas orientadoras da CNPD. O elemento «determinação da finalidade», que respeita à figura que define a atividade e que igualmente decide que dados serão utilizados, quem pode aceder, por quanto tempo serão tratados e conservados é que torna, em princípio, a entidade como responsável pelo tratamento. A incerteza que decorre desta qualificação, resulta da sua aplicação prática, emergindo a necessidade de recorrer ao Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»²⁹. O parecer considera que, independentemente da atribuição do controlo dos dados por lei, é fundamental compreender que ele se baseie numa análise factual e não meramente formal, devendo neste sentido refletir a realidade. Assim, é a empresa que exercer um controlo efetivo dos dados que deve ser indicada como responsável pelo tratamento.

3.1.1. Clarificação dos conceitos e a sua importância nas exigências previstas no RGPD

Desempenhando um papel de chefia relativamente ao subcontratante, orientando-o no tratamento de dados pessoais, o responsável pelo tratamento é considerado também a entidade que estipula a forma de atuação em caso de violação dos dados, assumindo, em primeira instância, o cumprimento do artigo 5.º, n.º2 e 24.º, n.º1 do RGPD.³⁰³¹ Este dever em assegurar e demonstrar a conformidade com o regulamento deve estar incorporado na construção do próprio projeto e acompanhar toda a operação que lhe segue, garantindo a

²⁹ GRUPO DE TRABALHO DO ARTIGO 29.º SOBRE A PROTECÇÃO DE DADOS - Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante». Adotado em 16 de Fevereiro de 2010. [consult. 10/11/2018]. Disponível em: https://www.gdpd.gov.mo/uploadfile/others/wp169_pt.pdf.

³⁰ SALDANHA, Nuno, *NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS. O que é? A quem se aplica? Como implementar?*, p.73.

³¹ Os riscos para os direitos e liberdades dos indivíduos são variáveis. Deste modo e de acordo com o artigo 33.º do RGPD, deve proceder-se a adoção de medidas que mitiguem esse mesmo risco. A Avaliação de Impacto sobre a Proteção de Dados analisa porquanto, a probabilidade da ocorrência de uma violação de dados. Desta forma, caso o tratamento venha a implicar um elevado grau de risco deve-se atender ao disposto no artigo 36.º do RGPD. Caso autorização por parte da Autoridade de Controlo são implementações medidas, quer ao nível técnico como a pseudonimização, quer a definição de políticas como a política de privacidade dos dados, que se encontram patentes no artigo 24.º, n.º 1 e 2 do RGPD. Importando ainda sublinhar o cumprimento dos princípios presentes no artigo 5.º do RGPD.

eficácia do seu princípio *privacy by design*³². «[P]rescribes that we built privacy directly into the design and operation (...)»³³. Na verdade, a ideia aqui subjacente percebe-se a *privacy before design*, na medida em que, considera que a fase do desenvolvimento do produto deve ser aquela em que se afigura o risco para os direitos e liberdades da pessoa singular podendo, no caso de implicar um risco que se sobreponha aos benefícios da sua elaboração, evitar custos desnecessários³⁴. É de notar ainda que as medidas a implementar se norteiam do mesmo modo, a garantir a eficácia do princípio *privacy by default*, conduzindo o tratamento de dados ao estritamente necessário para cada finalidade³⁵. A violação de alguma destas disposições implica, segundo o n.º 5 do artigo 83.º do regulamento, uma coima de €20 000 000 ou, no caso de uma empresa, uma coima até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior consoante o montante que for mais elevado.

O caráter protecionista do *privacy by design* está intimamente associado à confeção de uma abordagem baseada no risco. Quer isto dizer que se constitui o cálculo do impacto das operações de tratamento para os direitos e liberdades das pessoas singulares como ponto de partida na adoção das medidas corretas de mitigação a possíveis violações de dados. Nestes moles, entende-se a AIPD como o elemento propulsor na proteção de dados. A proteção face aos riscos³⁶ expostos nos direitos e liberdades dos titulares dos dados varia

³² A preocupação com a proteção dos dados pessoais deve existir desde o primeiro momento e estar presente ao longo de todo o tratamento considerando-se, todavia que, esta preocupação não pode ser incalculável. O considerando (83) expõe que as medidas de segurança a adotar têm de ter em conta fatores objetivos como os custos de aplicação em função dos riscos e natureza dos dados a proteger.

³³ CAVOUKIAN, Ann - «PRIVACY BY DESIGN: FROM RHETORIC TO REALITY», p.224. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>

³⁴ GUTWIRTH, Serge; LEENES, Ronald and DE HERT, Paul - *Data Protection on the Move: Current Developments in ICT and Privacy/Data*, p.22. [consult. 13/11/2018]. Disponível em: <https://books.google.pt/books?id=JPRcCwAAQBAJ&pg=PR10&lpg=PR10&dq=Gutwirth,+Serge,+Leenes,+Ronald,+De+Hert,+Paul.+%C2%ABData+Protection+on+the+Move:+Current+Developments+in+ICT+and+Privacy/Data%C2%BB,+2016&source=bl&ots=c9CF9p5F9p&sig=gUri4T4kmpjjiLUckFUiSm2LqjBY&hl=en&sa=X&ved=2ahUKEwiEqdmTzdjeAhURgHMKHXLQDtUQ6AEwBXoECAoQAQ#v=onepage&q=Gutwirth%2C%20Serge%2C%20Leenes%2C%20Ronald%2C%20De%20Hert%2C%20Paul.%20%C2%ABData%20Protection%20on%20the%20Move%3A%20Current%20Developments%20in%20ICT%20and%20Privacy%20Data%20BB%2C%202016&f=false>

³⁵ Artigo 25.º, n.º 2 do RGPD.

³⁶ Os riscos podem refletir-se em danos materiais ou imateriais. Muitos dos ataques de *ransomware*, que ocorrem através das fragilidades existentes no sistema operativo dos computadores, permitem a encriptação

consoante o nível de agravamento. Assim, apenas quando o tratamento for «suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares»³⁷³⁸ se torna obrigatória a realização de uma AIPD, acrescentando a este aspeto a obrigatoriedade³⁹ de notificação à autoridade de controlo quando face aos riscos residuais apresentados o responsável pelo tratamento não detenha capacidade de resposta. (Artigo 36º, n.º1 e n.º3, alínea e) do RGPD). Esta abordagem baseada no risco⁴⁰ tem como significado primordial determinar a origem, natureza, particularidade e gravidade do risco, significando isto que as medidas adotadas devem ter atenção à dimensão da operação de tratamento de dados, à sua finalidade, o tipo de dados que vão ser tratados e a possibilidade de transferência.⁴¹⁴² Algumas das medidas de mitigação resultantes da extensão deste elemento reconduzem-se à elaboração de códigos de conduta⁴³, políticas de privacidade e registo de informação relativa aos dados. O âmbito de aplicação deste requisito engloba empresas com mais de 250 trabalhadores,⁴⁴ ou quando as operações possam resultar num risco para os direitos e liberdades dos titulares ou que confirmem o cumprimento das instruções do responsável pelo tratamento se concretizarem mediante a conservação de um registo de todas as categorias de atividades de tratamento realizadas em nome da primeira entidade.

dos dados da pessoa, em que a atribuição de um código que a desbloqueie ocorre mediante a transação de uma quantia monetária, criam para as empresas, bem, como para os titulares dos dados, um *mindset* de gestão de risco.

³⁷ Artigo 35.º do RGPD.

³⁸ Projeto de Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados. Esta lista resulta das recomendações contidas no Parecer 18/2018 do Comité Europeu de Proteção de Dados, bem como das sugestões recebidas no âmbito da consulta pública transmitida pela CNPD.

³⁹ O requisito de obrigatoriedade resulta numa falta de resposta por parte dos responsáveis pelo tratamento, sujeitando o titular dos dados ao perigo direto de uma ocorrência de violação e, conseqüentemente, a possibilidade de danos irreversíveis.

⁴⁰ O conceito, proveniente da orientação do GRUPO DE TRABALHO DO ARTIGO 29.º - *Statement on the role of a risk-based approach in data protection legal frameworks*, de 30 de maio de 2014, era já conhecido pela Diretiva 95/46/CE, designadamente nos seus artigos 17º e 20º. [consult. 14/11/2018]. Disponível em: <https://www.pdp.ie/docs/10046.pdf>.

⁴¹ COUTINHO, Francisco Pereira e MONIZ, Graça Canto, *O ANUÁRIO DA PROTEÇÃO DE DADOS*, p. 50.

⁴² Veja-se a este propósito, *ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 3/2010 on the principle of accountability*. Adopted on 13 July 2010, paras. 45 e 46. [consult. 15/11/2018]. Disponível em: <https://www.dataprotection.ro/servlet/ViewDocument?id=720>.

⁴³ Artigo 24.º, n.º 2 e 3 do RGPD.

⁴⁴ Considerando (13) do RGPD. É, no entanto, configurada uma exceção à exceção no n.º 5 do artigo 30.º do RGPD, verificando a aplicação da regra de registo para empresas com menos de 250 trabalhadores quando seja suscetível de resultar num risco para os direitos e liberdades dos titulares dos dados.

O incentivo anunciado pelo regulamento confere a adoção de políticas de privacidade⁴⁵ e *cookies*⁴⁶ que são parte integrante dos deveres de informação previstos nos artigos 13.º e 14.º do RGPD e que se relacionam com uma base sólida de informação, bem como com a arquitetura de medidas de segurança previstas no artigo 32.º do RGPD tais como (i) atribuição de direitos de acesso de forma restrita e controlada, (ii) atribuição das credenciais de acesso de forma controlada através de um processo formal de gestão do respetivo ciclo de vida, (iii) aplicações do cliente (Android, IOS, WEB), que devem ser desenvolvidas adotando práticas de desenvolvimento seguro, (iv) capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações, (v) revisão de direitos de acesso de utilizadores em intervalos regulares, (vi) revisão de direitos de acesso de utilizadores em intervalos regulares, (vii) capacidade para garantir que os utilizadores fazem uma utilização correta dos dados, (viii) restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil), (ix) automatização dos processos de concessão, revisão, análise e revogação de acesso, (x) procedimentos seguros de início de sessão, (xi) capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis, (xii) inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional⁴⁷. A elaboração de códigos de conduta e procedimentos de certificação que ao abrigo do artigo 24.º, n.º 2 e 3 do regulamento são encarados como medidas complementares de cumprimento ao RGPD. O incumprimento de algum destes deveres implica a aplicação de coimas até €10.000.000, em cada caso individual, tendo a asserção as considerações apresentadas pelo n.º 2 do artigo 83.º do regulamento, ou até 2% do seu volume anual de negócios, no caso de uma empresa⁴⁸. A aplicabilidade de uma coima no valor de €400.000.00 por parte da CNPD, na

⁴⁵ MDS Group – Global Insurance & Risk Consultants, Política de Privacidade de Clientes. Disponível em: <https://www.mdsinsure.com/pt/politica-de-privacidade/>.

⁴⁶ MDS Group – Global Insurance & Risk Consultants, Política de Cookies. Disponível em: <https://www.mdsinsure.com/pt/politica-de-cookies/>.

⁴⁷ Resolução do Conselho de Ministros n.º 41/2018, Diário da República, 1.ª série — N.º 62 — 28 de março de 2018, ANEXO (a que se referem os n.º 1, 3 e 4) Arquitetura de segurança das redes e sistemas de informação Requisitos técnicos.

⁴⁸ Artigo 83.º, n.º 4 do RGPD.

sequência de uma auditoria ao centro Hospital Barreiro-Montijo devido às políticas de acesso às bases de dados, que permitiam que técnicos e médicos consultassem processos clínicos dos doentes sem a devida autorização⁴⁹, tem alertado as empresas para um comportamento mais pró-ativo⁵⁰.

3.2. O Subcontratante

A figura do subcontratante, consagrada no artigo 4.º n.º 8 do regulamento, compreende na sua definição elementos já mencionados na lei 67/98 e na Diretiva 95/46/CE. «Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes» O ator assume assim, um papel de auxílio na execução da atividade do responsável pelo tratamento, assegurando a confidencialidade e a segurança do tratamento, sujeitando as pessoas autorizadas a tratar dos dados pessoais a obrigações legais de confidencialidade, bem como a garantia do cumprimento integral das instruções conferidas pela entidade que o contrata. Por se encontrarem intimamente associados, devem em conjunto com os respetivos colaboradores, formar o «círculo interno do tratamento de dados»⁵¹.

A regulação de novas obrigações ao nível da subcontratação e a expansão de outras, convergem na elaboração de aditamentos contratuais e na criação de contratos de tratamento de dados pessoais, em especial na corretagem de seguros, ou um outro ato jurídico vinculativo em que se estabeleça uma descrição devidamente detalhada sobre os conceitos de responsável pelo tratamento e subcontratante e, conseqüentemente, as instruções de atuação do prestador de serviços.

⁴⁹ SÉNECA, Hugo - «CNPD: Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos» in Exame Informática, 19/10/2018.

⁵⁰ *OPINIONS EUROPEAN DATA PROTECTION SUPERVISOR - Opinion of the European Data Protection Supervisor on the 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», in Official Journal of the European Union, paras. 99 e 100.*[consult. 20/11/2018]. Disponível em: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XX0622\(01\)&from=PL](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XX0622(01)&from=PL).

⁵¹ GRUPO DE TRABALHO DO ARTIGO 29.º SOBRE A PROTECCÃO DE DADOS - Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», Adotado em 16 de Fevereiro de 2010, p.9. [consult. 23/11/2018]. Disponível em: https://www.gdpd.gov.mo/uploadfile/others/wp169_pt.pdf.

3.2.1. Contratos de subcontratação

O recurso a atividades específicas de entidades especializadas, possibilita o auxílio no desenvolvimento das atividades principais ou, mais comum, acessórias, da empresa que subcontrata, passando a estarem economicamente dependentes uma da outra. Entende-se, segundo MARTINEZ, Pedro, a subcontratação como «o negócio jurídico bilateral subordinado a outro contrato (designado por contrato base ou contrato principal) e celebrado por uma das partes nesta última convenção com base nos direitos que da mesma lhe advêm»⁵². A parte contraente encarrega um terceiro a executar parte ou a totalidade das prestações contratuais a que está obrigado. Uma das desvantagens apontadas como preponderantes neste regime é a qualidade do serviço prestado, que pode causar danos graves à entidade contratante. O que o artigo 28.º, n.º 1 do RGPD pretende oferecer é um auxílio em matéria de segurança no tratamento de dados, estabelecendo critérios no momento de eleição de um subcontratante.

Qualificando-se como a empresa que trata os dados por conta do responsável pelo tratamento, a sua relação deverá ser regida por um contrato ou outro ato normativo ao abrigo da União ou dos Estados-Membros. O contrato deve vincular o subcontratante às instruções apontadas pelo responsável no modo de tratamento dos dados pessoais, estabelecendo (i) objeto e a duração do tratamento, (ii) natureza e a finalidade, (iii) categorias, (iv) obrigações e direitos do responsável pelo tratamento e (v) estabeleça que após a conclusão do tratamento, o subcontratante deva apagar ou devolver os dados (a menos que seja exigida a sua conservação). Nesta matéria, importa ainda salientar o compromisso de confidencialidade ou a sujeição a adequadas obrigações legais de confidencialidade a assegurar pela entidade relativamente às pessoas autorizadas a tratar os dados pessoais, bem como, prestar, tendo em conta os custos e a natureza do tratamento, ao responsável pelo tratamento, as medidas técnicas e organizativas e as informações necessárias para demonstrar o cumprimento das obrigações previstas adequadas ao

⁵² MARTINEZ, Pedro Romano – *O Subcontracto*, p.20.

conteúdo subcontratante, bem como as regras respeitantes ao tratamento de subcontratantes ulteriores.

A adoção de medidas técnicas e organizativas que assegurem um nível adequado de proteção, a comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o regulamento é tanto mais robusta, quanto maior for o nível de segurança que ofereça. Assim, o subcontratante que dispuser de certificação⁵³ e de códigos de conduta, assegura a nível empresarial, um maior grau de conhecimento, bem como lhe é atribuído uma vantagem no momento de celebração de contratos de subcontratação⁵⁴. É de notar ainda que o cumprimento dos pressupostos consagrados no artigo 28.º reforçam a proteção a conferir aos dados pessoais, facilitando também na delimitação das responsabilidades de cada entidade.

3.2.2. Contratos de subcontratação – Setor segurador

As regras de subcontratação no setor segurador decorrem do regime aplicável à atividade seguradora. A Lei n.º 147/2015, de 9 de setembro consagra, em matéria de subcontratação, a sua definição no disposto do artigo 5.º, n.º 1, alínea x). «O acordo entre uma empresa de seguros ou de resseguros e um prestador de serviços, quer se trate de uma entidade supervisionada ou não, nos termos do qual o prestador de serviços realiza, diretamente ou mediante nova subcontratação, um processo, serviço ou atividade que de outra forma seria realizada pela própria empresa de seguros ou resseguros». A supervisão por parte da ASF releva-se, de acordo com o artigo 22.º da Lei n.º 147/2015, pela proteção dos tomadores de seguros, segurados e beneficiários. Neste seguimento, torna-se necessário, em matéria de governação, a permanente verificação do correto exercício da atividade e do cumprimento das disposições legais, regulamentares e administrativas pelas empresas de seguros e de resseguros, bem como dos grupos seguradores e resseguradores⁵⁵. Assim, e por forma a eliminar qualquer irregularidade que possa consistir num prejuízo

⁵³ O Regulamento prevê a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados. A certificação é voluntária e está disponível através de um processo transparente. Emitida por organismos de certificação acreditados pelos Estados-membros ou pela Autoridade de controlo competente e tem a duração de três anos.

⁵⁴ Artigo 24.º, n.º 2 e 3 do RGPD.

⁵⁵ Cf. artigo 25.º da Lei n.º 147/2015, de 9 de setembro.

para os tomadores de seguros, segurados e beneficiários, as empresas de seguros e de resseguros devem informar previamente a ASF de todas as estratégias, processos e procedimentos que pretendam realizar⁵⁶.

3.3. Clarificação dos conceitos e a sua importância na classificação da autoridade de controlo principal

É mediante a transferência de dados pessoais para países ou organizações internacionais que urge identificar a autoridade de controlo principal, pois as suas funções repercutem-se ao nível do gerenciamento das atividades de tratamento transfronteiriças de dados. São matérias relacionadas com tratamentos de atividades suscetíveis de causar impactos aos direitos e liberdades dos seus titulares, como comunicações em caso de violações de dados e designações de encarregados de proteção de dados que tornam imperativa a correta designação da autoridade de controlo principal. Na verdade, a sua identificação está intimamente associada à localização do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento⁵⁷ na UE, cujos elementos caracterizadores se encontram previstos nos termos do artigo 4.º, ponto 16, alínea a) do RGPD. Assim, o estabelecimento da união que detenha administração central, competente para decidir e executar as finalidades e os meios de tratamento dos dados pessoais, revela-se como o estabelecimento principal. Acresce ainda a importância do considerando (36) do RGPD em sede de esclarecimento quando não se aplique o fator acima referido. O considerando recorre ao local onde ocorre o exercício efetivo e real das atividades de gestão que determinam as decisões principais quanto às finalidades e aos meios de tratamento mediante instalações estáveis. Quer isto dizer que se socorre da clarificação da entidade responsável pelo tratamento para averiguar a localização do estabelecimento principal e, por sua vez, a autoridade de controlo principal⁵⁸.

⁵⁶ Cf. artigo 28.º, da Lei n.º 147/2015.

⁵⁷ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante*. p.5. [consult. 24/11/2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf.

⁵⁸ Cumpre notar pelo GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do*

3.4. Transferências internacionais de dados

A criação do mecanismo do balcão único dirigido por uma única autoridade de controlo, designada por autoridade de controlo principal, é acionado apenas no âmbito de um tratamento transfronteiriço. Esta garantia de um nível adequado de segurança jurídica é alvo de um controlo periódico pela Comissão, como decorre do artigo 25.º, n.º 6 ou 26.º, n.º4 da Diretiva 95/46/CE e tem de ter em conta os pareceres do Parlamento Europeu e Conselho, bem como de outras fontes legislativas pertinentes. De acordo com o considerando (101) do RGPD, «Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado».

A lógica das transferências para países terceiros assenta em vários momentos. Numa primeira fase é essencial verificar se os dados recolhidos pelas empresas foram cumprindo a legislação aplicável e para as finalidades de recolha originais⁵⁹ para poderem continuar a ser tratados. Feito o diagnóstico ao nível interno, no segundo momento a tarefa consiste em verificar o local da transferência e averiguar as garantias. Significa isto que, caso seja para empresas do mesmo grupo, mas sediadas em território norte-americano e estas estejam certificadas com o *privacy-shield*⁶⁰, os dados podem ser transferidos. Por outro lado, caso o local da transferência seja para o grupo empresarial cujo local seja outro fora da UE e do EEE, tem de se adotar regras vinculativas do *Binding Corporate rules*, que funcionam como um código de conduta que consagra o mesmo nível de proteção oferecido pelo RGPD. Em situação oposta, o grupo empresarial tem de cumprir com algum dos outros fundamentos que garantam um nível adequado de proteção sob pena de os dados não poderem continuar a ser tratados, podendo estes ser: (i) Cláusulas contratuais-tipo que se

subcontratante. p. 5. [consult. 24/11/2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf, que esta identificação pode ser contestada pelas autoridades de controlo interessadas.

⁵⁹ A menos que haja algum fundamento jurídico e/ou novo consentimento.

⁶⁰ Consiste num sistema de auto-certificação, segundo do qual as organizações/empresas americanas se comprometem a respeitar um conjunto de princípios relativos à privacidade de dados pessoais que recebam da União Europeia, incluindo dados relativos à saúde.

traduzem em cláusulas adotadas por uma autoridade de controlo e aprovadas pela Comissão, (ii) procedimentos de certificação, bem como selos e marcas de proteção, (iii) elaboração de códigos de conduta por forma a fazer cumprir a legislação. Note-se que estes fundamentos não prejudicam a adoção de mais medidas de garantias adequadas. Assim, na falta dos fundamentos acima indicados, as transferências internacionais apenas podem ser concretizadas mediante consentimento explícito do titular dos dados, for necessária para a celebração ou execução de um contrato entre as partes, necessário para o interesse do titular dos dados, for necessária por razões de interesse público, for necessária à declaração ou à defesa de um direito num processo judicial, for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, realizada a partir de um registo que se destine a informar o público e se encontre aberto à consulta pública em geral ou de qualquer outra pessoa que possa provar nela ter um interesse legítimo.

3.5. Violações no tratamento de dados pessoais

Em sede de violações de dados, as orientações do GRUPO DE TRABALHO DO ARTIGO 29.º sobre a imposição em caso de violação de dados pessoais, estabelecem recomendações aos responsáveis pelo tratamento e subcontratantes aquando o momento de deteção das mesmas. O entendimento do processo de notificação incorpora, numa primeira abordagem, conhecer o conceito de violação de dados pessoais que ao abrigo do novo regulamento, decorre do artigo 4.º, n.º12. «Uma violação da segurança que provoque, de modo accidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento». Do conceito exposto, subsume-se a existência de uma quebra de segurança que possa ser suscetível de criar riscos significativos para os direitos e liberdades dos indivíduos. As possíveis consequências enfatizadas pelos considerandos (85) e (75) relacionam-se com a adequação de medidas mitigadoras para evitar operações suscetíveis de causar danos físicos, materiais ou imateriais, tais como a discriminação, perdas financeiras, perdas de confidencialidade, prejuízos para a reputação, ou a quaisquer outros prejuízos de natureza económica ou social. Assim e de acordo com o considerando (86), na

sequência de algumas destas violações, o responsável pelo tratamento deve, sem demora injustificada, informar a autoridade de controlo competente, bem como o titular dos dados, proporcionando-lhe tomar as precauções necessárias. Embora aluda, nos termos do artigo 33.º, n.º1 e artigo 55.º do RGPD à notificação à autoridade de controlo, sem demora justificada, o regulamento reconhece também a possibilidade de os responsáveis pelo tratamento não terem acesso à informação necessária respeitante à violação num prazo de 72 horas⁶¹ após terem tomado conhecimento da mesma, possibilitando, desta forma, uma notificação em fases.⁶² Todavia, esta salvaguarda deve apenas respeitar a casos complexos que exigem a determinação completa da natureza da violação e da extensão de titulares afetados.⁶³ Apesar da extensão permitida através do artigo 33.º, n.º4 do RGPD, cumpre notar que a comunicação à autoridade de controlo deve também nestes casos, ser feita sem demora injustificada, resultando numa violação para ambos os casos, quando a falha de notificação não se faça acompanhar dos motivos do atraso. É, no entanto, fundamental compreender que, subjacente à notificação, tem de estar definido um grau de certeza razoável da ocorrência de um dano para os direitos, liberdades e garantias do titular dos dados.⁶⁴

O aumento da responsabilização configurada pelo regulamento ao nível da subcontratação, percebe as obrigações aplicáveis tanto a responsáveis pelo tratamento

⁶¹ Considerandos (85), (87), (89) e artigo 33.º do RGPD. No ramo segurador, o entendimento geral confere um prazo de notificação por parte do subcontratante de 48 horas. Este prazo é tido como mais razoável uma vez que, possibilita um maior grau de detalhe a investigação da violação por parte do IT.

⁶² *ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Personal data breach notification under Regulation 2016/679. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018*, recomenda, nestes casos, que o responsável pelo tratamento, aquando da primeira notificação, deve informar que não dispõe de todos os factos relevantes para a autoridade de controlo ser capaz de, corretamente, exercer o seu poder de correção, nos termos do artigo 58.º, n.º2, alínea e) do RGPD.

⁶³ *ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Personal data breach notification under Regulation 2016/679. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018*, estabelece a título de exemplo, que a probabilidade de notificação em fases é maior em casos de ciberataques, uma vez que se encontra quase sempre subjacente uma investigação criminal. O GRUPO DE TRABALHO DO ARTIGO 29.º, faz salientar ainda que, não deve constituir obstáculo à notificação o facto de o responsável pelo tratamento não ter resultados precisos relativamente a informações relevantes, considerando aceitar aproximações, nos casos de determinação da extensão de indivíduos afetados, visto o ponto fulcral da notificação à autoridade de controlo ser o combate às consequências que resultam da violação.

⁶⁴ *ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Personal data breach notification under Regulation 2016/679* relativo às orientações face à violação de dados pessoais, presenteia na sua pág. 11, exemplo 2, uma clara evidência da ocorrência de uma violação de dados pessoais. *A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorized disclosure.*

como a subcontratantes. A possibilidade de apresentar ação judicial contra os subcontratantes⁶⁵ por violação do regulamento, bem como a possibilidade de receber uma indemnização diretamente do subcontratante⁶⁶ pelos danos sofridos, é uma das mais importantes alterações legislativas resultantes do novo regulamento. O artigo 83.º do RGPD, mostra uma alteração no perfil de risco dos prestadores de serviços que processam dados em nome e por conta dos responsáveis pelo tratamento.

3.6. Clarificação dos conceitos e a sua importância na responsabilidade civil pelo tratamento de dados pessoais

Em matéria de responsabilidade civil o regulamento prevê em caso de violação de direitos pessoais, a possibilidade de o titular dos dados receber diretamente do responsável pelo tratamento ou do subcontratante uma indemnização pelos danos sofridos. Assim, contrariamente à lei 67/98, o regulamento introduz a responsabilidade civil ao nível de ambas as entidades. Contudo, o n.º2, do artigo 82.º do regulamento parece ainda restringir a responsabilidade do subcontratante, respondendo apenas pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações impostas pelo regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento, preconizando a sua isenção de culpa no caso de provar que não deu origem ao dano provocado. A estrutura que se compactua com o universo dos dados pessoais e a sua indissociável relação com o RGPD percebeção, desde logo, uma responsabilidade extracontratual pela identificação da relação entre os diversos direitos de personalidade, num domínio onde se lida com direitos absolutos⁶⁷. Neste sentido, pode haver uma responsabilidade direta da parte do responsável pelo tratamento no caso de se provar que não cumpriu os critérios de eleição na escolha do subcontratante, que pode, no entanto ser afastada mediante a prova de que o subcontratante detinha à data da violação

⁶⁵ Artigo 79.º do RGPD.

⁶⁶ Artigo 825.º do RGPD.

⁶⁷ BARBOSA, Mafalda Miranda - «Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil», p.443. [consult. 24/11/2018]. Disponível em: <https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5aaacd451ae6cf02516c4b66/1521143111492/2018-10.pdf>

um código de conduta aprovado ou um procedimento de certificação aprovado⁶⁸⁶⁹. A facilidade em intentar a ação contra a entidade que no momento lhe convier, permite consolidar a lógica de uma responsabilidade pelo risco, por força do artigo 500.º do CC, na medida em que, não se pressupondo qualquer relação contratual, se prevê assegurar alguma segurança relativamente ao risco originado pelas estruturas piramidais⁷⁰. Todavia, para que o facto danoso fique coberto pela relação comitente/comissário, tem que estar inerente ao exercício das funções do subcontratante, exigindo-se de igual forma que haja a obrigação de indemnizar o comitente⁷¹.

Por outro lado, a estrutura da responsabilidade contratual encontra-se patente no disposto do artigo 28.º do regulamento. Este artigo oferece um importante contributo na relação responsável pelo tratamento e subcontratante, uma vez que estabelece que a mesma deve ser regida por contrato ou outro ato normativo ao abrigo do direito da União ou Estados-Membros que vincule o subcontratante ao responsável pelo tratamento. Assim, configura-se uma responsabilidade direta da parte do subcontratante em tudo o que viole o disposto no contrato. Nota-se, todavia, perante uma violação ao titular dos danos, novamente uma possível analogia à figura do comitente, na medida em que o respetivo titular pode intentar a ação contra o responsável pelo tratamento, cabendo, deste modo, o direito de regresso imposto ao subcontratante.

A abordagem direta (perante uma violação de dados, é) face à figura do subcontratante que o regulamento preconiza em sede de responsabilidade civil perante violação de dados é uma das principais alterações legislativas face à lei 67/98. Consubstancia-se a continuidade em assegurar o risco originado pelas estruturas piramidais, apenas com a ressalva de uma atenuação na esfera da entidade que subcontrata, não comprometendo sempre a possibilidade afetação direta das suas receitas.

⁶⁸ Artigo 82.º, n.º3 do RGPD.

⁶⁹ São entendidas como medidas complementares às que devem assegurar o cumprimento do regulamento, podem ser utilizadas como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

⁷⁰ MORAIS, Nuno - *A RESPONSABILIDADE OBJECTIVA DO COMITENTE POR FACTO DO COMISSÁRIO, A ANÁLISE DO ARTIGO 500 DO CÓDIGO CIVIL —SEUS PRESSUPOSTOS E REGIME*, p.41.

⁷¹ MORAIS, Nuno - *A RESPONSABILIDADE OBJECTIVA DO COMITENTE POR FACTO DO COMISSÁRIO, A ANÁLISE DO ARTIGO 500 DO CÓDIGO CIVIL —SEUS PRESSUPOSTOS E REGIME*, p.60.

CAPÍTULO IV

O CORRETOR DE SEGUROS

4. Enquadramento legal

FERREIRA, Carlos De Almeida, define o conceito de mediação como o «contrato pelo qual uma das partes (o mediador) se obriga mediante remuneração, a promover negociações ou a indicar a contraparte para a formação de um contrato que a outra parte no contrato de mediação (o cliente) pretende celebrar»⁷². Por sua vez, ANTUNES, José Engrácia, enuncia a mediação como «contrato pelo qual uma parte – o mediador – se vincula para com a outra – o comitente ou solicitante – de modo independente e mediante retribuição, prepara e estabelece uma relação de negociação entre este último e terceiros – os solicitados – com vista à eventual conclusão definitiva de negócio jurídico»⁷³. O mediador obriga-se a promover⁷⁴ a celebração do negócio, aproximando o comitente do terceiro, informando-o e esclarecendo-o em relação a aspetos provenientes do negócio, sem, todavia, participar⁷⁵ efetivamente no mesmo.

A expressão «mediação de seguros» foi consagrada na totalidade, pela primeira vez, com o Decreto-Lei n.º 145/79, de 23 de maio, não sofrendo quaisquer alterações até à data. A sua evolução legislativa prossegue-se com o DL n.º 336/85, de 21 de agosto, e, posteriormente, com o DL n.º 388/91, de 10 de outubro que integrou a disciplina comunitária do setor tendo, contudo, sido revogado pelo DL n.º 144/2006, de 31 de julho, cujo relevo advém sobretudo da transposição que fez da Diretiva Comunitária 2002/92/CE

⁷² FERREIRA, Carlos – *Contratos II* 2007, p.203.

⁷³ ANTUNES, José Engrácia, *Direito dos contratos comerciais*, 2009, p. 458.

⁷⁴ Note-se que, de acordo com a anotação do STJ de 4 de janeiro de 2014, tratando-se de um contrato oneroso, o direito à remuneração (comissão) não está dependente dos esforços envolvidos para a promoção do negócio, mas sim da produção de um resultado que se plasma na celebração do contrato de seguro.

⁷⁵ VASCONCELOS, Pedro Pais De, *Direito Comercial*. Volume I. Parte Geral. Contratos Mercantis. Títulos de Crédito, Almedina, Coimbra, 2011, pág. 197. O mediador é encarado como um «facilitador». Nas palavras de MONTEIRO, ANTÓNIO PINTO, *Contrato de Agência* (Anteprojecto), in BMJ, n.º 360, novembro 1986, 43-139, p. 85: «a obrigação fundamental do mediador é conseguir interessado para certo negócio que, raramente conclui ele próprio. Limita-se a aproximar duas pessoas e a facilitar a celebração do contrato.»

de 9/12/2002⁷⁶, não prevendo, no entanto, um modelo contratual em matéria de mediação de seguros.

Centrando a análise na figura do corretor de seguros, cuja definição se apresenta no artigo 8.º, alínea c) do DL n.º 144/2006, de 31 de julho: «categoria em que a pessoa exerce a atividade de mediação de seguros de forma independente face às empresas de seguros, baseando a sua atividade numa análise imparcial de um número suficiente de contratos de seguro disponíveis no mercado que lhe permita aconselhar o cliente tendo em conta as suas necessidades específicas», verifica-se que a sua atividade se desdobra em dois momentos negociais. Em primeiro lugar, averigua-se o estabelecimento de uma relação com o cliente, potencial tomador. O vínculo que lhe está subjacente, pode corresponder a uma mediação, à procura da cobertura ideal para o seu cliente, ficar-se na análise de riscos, ou estender-se à elaboração do contrato, à gestão de sinistros e à intermediação entre as partes durante toda a vida do contrato de seguro⁷⁷, estando-lhe associado o cumprimento dos pressupostos previstos nos artigos 31.º a 33.º do presente diploma. Mas, enquanto profissional independente, não subordinado às instruções da seguradora, exerce a atividade de mediação de seguros «por sua conta e risco»⁷⁸. Por outro lado, o vínculo que resulta da celebração do contrato de seguro entre o cliente e a seguradora faz nascer um recurso à subcontratação da parte da empresa de seguros, nos termos do acompanhamento da gestão contratual. A regulação deste regime de subcontratação está previsto na Lei n.º 147/2015 de 9 de setembro, bem como no novo Regulamento Geral de Proteção de Dados pelo tratamento necessário de categorias de dados sensíveis no ramo segurador, à elaboração de normas que orientem a relação contratual em matéria de subcontratação, permitindo, deste modo, a compreensão dos limites de responsabilidade entre as empresas de seguros e a entidades que esta subcontrata.

4.1. A duplicidade de papéis do Corretor de Seguros

Compreendida a dualidade de atividades inerentes à categoria do corretor de seguros, bem como as linhas orientadoras da CNPD em matéria de conceitos do

⁷⁶ ECLI : PT : STJ : 2016 : 432/08.6 TASCRLI.S1.

⁷⁷ Apud, CASTELO, Hígina - *Contrato de mediação – ESTUDO DAS PRESTAÇÕES PRINCIPAIS*, p. 157.

⁷⁸ ECLI : PT : STJ : 2016 : 432/08.6 TASCRLI.S1.

responsável pelo tratamento e do subcontratante, prevê-se uma capacidade em conectar estes dois temas.

A atividade do corretor de seguros é caracterizada por dois momentos distintos de atuação. O primeiro afigura-se pela fase que antecede à celebração do contrato de seguro. Esta fase é a que faz desencadear a relação corretor/cliente. As funções que se compactuam com a atividade do corretor neste contexto adequam-se com a prestação de serviços de consultoria. Os projetos concretizam-se através de uma análise imparcial de contratos disponíveis no mercado, incluindo operações de simulação e de cotação que têm por base questionários elaborados pelas seguradoras. Mas, apesar de um primeiro entendimento que faz aludir-se à identificação do corretor como subcontratante, a verdade é que este atua de forma independente face às seguradoras, tornando-o, neste primeiro momento de intervenção, responsável pelo tratamento. O momento que sucede à celebração do contrato de seguro assenta na constituição de uma relação entre o cliente e a empresa de seguros. Não sendo parte desta relação, a atividade do corretor neste segundo momento de intervenção, resulta da sua relação com as seguradoras. O auxílio⁷⁹ que presta no acompanhamento da gestão e execução do contrato, em especial em caso de sinistro⁸⁰ torna a entidade compatível com os elementos caracterizadores da subcontratação, já referidos em capítulos anteriores.

Afigurando-se uma única entidade como responsável pelo tratamento e subcontratante, em fases de atuação distintas, as suas exigências prevêm-se ao nível destas duas figuras, tendo por isso de cumprir no primeiro momento de atuação, os pressupostos previstos no artigo 13.º do RGPD e os elementos consagrados no artigo 28.º na fase em que assuma o papel de auxílio do organismo com quem mantém uma relação de subcontratação.

⁷⁹ As funções do corretor nesta fase incluem operações de cobrança de prémios, avisos e renovações e intervenção na regularização de sinistros.

⁸⁰ Cf. artigo 5.º, alínea c) do Decreto-Lei n.º 144/2006 e artigo 2.º, n.º1 da DDS.

4.2. Impactos do RGPD no setor segurador, em especial na categoria do corretor de seguros

A atividade do setor segurador implica necessariamente o tratamento de categorias de dados sensíveis em grande escala. Aplicando-se ao ramo segurador os princípios e as regras do RGPD, as matérias impactadas no âmbito do respetivo setor são: (i) tratamento de categorias de dados sensíveis, (ii) encarregado de proteção de dados e (iii) subcontratação.

O critério referente à primeira situação remete para a celebração do contrato de seguro, cuja recolha de dados do tomador é essencial para a sua celebração e execução. À luz do regulamento, verifica-se que as novas exigências em matéria de consentimento são mais restritas, na medida em que, para o tratamento de dados sensíveis é necessário o consentimento explícito do titular dos dados. O artigo 9.º do regulamento, que diz respeito aos dados de categoria especial, revela uma proteção acrescida face aos restantes dados pessoais, na medida em que, são dados que fazem parte da esfera íntima da pessoa, de tal forma que se encontram também revelados no artigo 35.º da CRP. Constatou-se, neste sentido, que o critério protecionista deste artigo o aciona pela negativa, implicando o preenchimento de algum dos requisitos previstos no presente artigo para que a exceção funcione. Nesta senda, está implícita a revisão de todos os consentimentos prestados até à data, podendo a sua violação levar à suspensão do contrato de seguro. A problemática referente ao consentimento explícito advém da inércia praticada pelos titulares dos dados e é sentida pelas empresas de seguros e consequentemente os mediadores de seguros no âmbito do auxílio da gestão contratual. O consentimento que ao abrigo do artigo 9.º, n.º1 do RGPD passou a ter que ser explícito no que diga respeito a dados sensíveis⁸¹, tem levantado questões relacionadas com a inércia dos próprios titulares dos dados, podendo conduzir à suspensão dos contratos de seguro quando os requisitos⁸² para o consentimento explícito não tenham sido observados.

⁸¹ Artigo 4.º, alínea 15) do RGPD considera «dados relativos à saúde», os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o estado de saúde».

⁸² De acordo com o artigo 4.º, n.º 11 do RGPD, o consentimento apenas é válido quando haja uma manifestação de vontade, livre, específica, informada e explícita, na qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

O contrato de seguro é, tendencialmente, de longa duração, quer porque é estipulado um prazo longo (seguros de vida, que podem estender-se por períodos superiores a 30 anos), quer porque é alvo de renovações periódicas que podem estender-se por largas décadas⁸³. As modalidades de saúde, vida, acidentes pessoais e de trabalho, pela sua natureza de proteção da vida, saúde e integridade física dos titulares dos dados, implicam o tratamento de dados sensíveis. A preocupação ilustrada pela APS ao nível dos constrangimentos sentidos na atividade seguradora, levou à sugestão de uma disposição transitória a considerar na aprovação de legislação nacional, que salvede a possibilidade de se continuar a efetuar o tratamento de dados pessoais, incluindo dados de saúde, relativos aos contratos em vigor, até ao termo da respetiva anuidade, assim como a gestão de sinistros em curso (até à sua conclusão, salvaguardando inclusivamente o exercício de direitos de regresso deles decorrentes), desde que, respetivamente, tenham sido celebrados ou tenham ocorrido antes da entrada em vigor do regulamento⁸⁴. A sugestão legislativa sugerida baseia-se nas propostas da APS, bem como na proposta de lei espanhola, na medida em que, o legislador espanhol foi sensível aos problemas específicos do setor. A adoção desta disposição transitória poderá revelar-se num mecanismo de combate à resolução automática dos contratos e à suspensão da gestão de sinistros, evitando a inércia por parte dos titulares dos dados. Notando a necessidade de tratamento de dados de categorias especiais para a execução do contrato de seguro de vida, saúde ou acidentes, a proposta de alteração da base de licitude do consentimento para a execução do contrato, afigura-se como compreensível. Uma vez que, o âmago da celebração de qualquer um destes contratos se repercute ao nível da «prestação de cuidados ou tratamentos de saúde» e que estes mesmos pressupostos que se encontram expressos no artigo 9.º, n.º2, alínea h) do

⁸³ POÇAS, Luís, *O Dever da Declaração Inicial do Risco no Contrato de Seguro*. [consultado a 18/11/2018]. Disponível em: https://books.google.pt/books?id=gS_RAQAAQBAJ&pg=PT522&lpg=PT522&dq=o+contrato+de+seguro+e+tendencialmente+de+longa+dura%C3%A7%C3%A3o&source=bl&ots=x7nmB28n7y&sig=jB8YweCHkw8FGC88ZhTpPYUmHqc&hl=en&sa=X&ved=2ahUKEwio8qXxrujeAhUtyoUKHRi0BtIQ6AEwAHoECAkQAO#v=onepage&q=o%20contrato%20de%20seguro%20e%20tendencialmente%20de%20longa%20dura%C3%A7%C3%A3o&f=false

⁸⁴ APS – PROCESSO DE CONSULTA PÚBLICA PARA APROVAÇÃO DE LEGISLAÇÃO NACIONAL RELATIVA AO REGULAMENTO GERAL DE PROTECÇÃO DE DADOS.

RGPD, a APS propõe como sugestão legislativa uma solução que desague numa formulação similar à exposta no presente artigo.

O regime em matéria de consentimento, não tem adequação a nível da legislação interna de execução, nomeadamente, no que respeita aos seguros de pessoas, podendo provocar entropias muito significativas nos processos de contratação, renovação e execução dos contratos de seguro, cujo objetivo primordial se prende com a proteção da vida, saúde e integridade física dos titulares dos dados (desde o tomador de seguro, pessoas seguras, beneficiários e até terceiros lesados que não são parte no contrato, como no caso de todos os seguros obrigatórios). Nessa medida, a legislação nacional deverá clarificar alguns destes aspetos, sem colidir com o RGPD, mas que também não resulte num retrocesso na dinâmica da atividade nem prejudique os interesses legítimos dos próprios titulares dos dados, especialmente quando estiverem em causa tratamentos relacionados com dados de saúde⁸⁵.

Em virtude do considerando (77) e do artigo 39.º do RGPD, a figura do encarregado de proteção de dados tem um estatuto de independência⁸⁶ e autonomia dentro da organização e tem como função, tal como o nome indica, a proteção dos dados pessoais. Neste sentido deve: (i) cooperar com a autoridade de controlo aplicável e com os titulares de dados; (ii) monitorizar as AIPD; (iii) informar e aconselhar⁸⁷ o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores no âmbito das suas obrigações em matéria de proteção de dados; (iv) ponto de contacto com a autoridade de controlo; (v) controla a

⁸⁵ APS – PROCESSO DE CONSULTA PÚBLICA PARA APROVAÇÃO DE LEGISLAÇÃO NACIONAL RELATIVA AO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS.

⁸⁶ Tal como expresso no considerado (97) do RGPD, quer seja um prestador de serviços externo ou um colaborador da empresa, o estatuto de independência tem de estar assegurado.

⁸⁷ Segundo o GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientações sobre os encarregados de proteção de dados (EPD)*, Adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, os EPD não são pessoalmente responsáveis pelo incumprimento dos requisitos de proteção de dados. Questão contraditória se aponta em matéria de prestação de informações erróneas ou enganosas. Assim, o encarregado de proteção de dados que, nos termos das suas funções, incumpra o disposto anteriormente, provocando danos a terceiros (empresa) pode, no caso de se qualificar como um prestador externo, em sede de responsabilidade civil profissional, ser-lhe imputada a responsabilidade pelo dano. Questão diversa se aponta no caso de o EPD ser um colaborador da empresa. Neste contexto, poderá qualificar-se a empresa como terceiro, imputando-lhe a responsabilidade civil profissional?

conformidade com outras disposições, nomeadamente, os mecanismos⁸⁸ adotados pelos responsáveis pelo tratamento e subcontratantes que permitam demonstrar o cumprimento do RGPD. A sua designação é, por isso, obrigatória em diversas situações, designadamente quando o tratamento seja: (i) efetuado por uma autoridade ou organismo público; (ii) efetuado em grande escala⁸⁹; (iii) necessário um controlo regular e sistemático⁹⁰ dos titulares dos dados, (iv) dados sensíveis. A nomeação do encarregado de proteção tem de se basear nas qualidades profissionais, nos conhecimentos especializados pelo setor e empresa e na sua capacidade para desempenhar⁹¹ as funções em causa, privilegiando-se a contratação de um colaborador da empresa.

As circunstâncias que implicam a designação obrigatória de um EPD atentam ao preenchimento dos elementos (i) «grande escala» (ii) «monotorização sistemática e de forma regular». Os conceitos de «larga escala» e «controlo regular e sistemático» não estão

⁸⁸ As orientações sobre a execução de medidas adequadas e sobre a comprovação de conformidade pelos responsáveis pelo tratamento ou subcontratantes, tal como previstas no considerando (100), bem como nos artigos 40.º e 41.º do RGPD, poderão ser obtidas nomeadamente recorrendo a mecanismos de certificação ou a elaboração de códigos de conduta. O regulamento prevê a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, reforçando, deste modo, a transparência e o cumprimento do regulamento.

⁸⁹ É o caso das seguradoras e Corretores de Seguros. A omissão de uma definição no que diz respeito ao «tratamento em grande escala» tenta ser combatida mediante o considerando (91) e as orientações sobre o encarregado de proteção de dados, concretizadas pelo GRUPO DE TRABALHO DO ARTIGO 29.º. Com efeito, o seu conteúdo apoia-se em fatores como extensão geográfica da atividade do tratamento, designadamente no tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros.

⁹⁰ A omissão de uma definição no que diz respeito ao «controlo regular e sistemático» tenta ser colmatada mediante o considerando (24) e as orientações sobre o encarregado de proteção de dados concretizadas pelo GRUPO DE TRABALHO DO ARTIGO 29.º. Considera-se assim, «controlo regular e sistemático» todas as formas de seguimento e de definição de perfis na *internet*, nomeadamente, para fins de publicidade comportamental. Este controlo comportamental tem de ser feito de forma específica, periódica, sendo desenvolvido no seguimento de uma estratégia.

⁹¹ O artigo 39.º sugere que o encarregado de proteção de dados tenha que prestar aconselhamento aos titulares dos dados e cooperar com as autoridades de controlo em causa, tomando sempre as medidas adequadas para fornecer aos titulares as informações dos artigos 13.º e 14.º do RGPD. A importância de exercer as suas funções em conjunto com uma equipa que o auxilie resulta da possível ocorrência de uma violação de dados, em caso de um subcontratante ter residência em Estado-Membro diverso do responsável pelo tratamento. A exigência da transparência do tratamento que pressupõe o dever de informação aos titulares dos dados numa linguagem clara e concisa pode, todavia, tornar-se num desafio para o EPD e sua equipa. Como tal, sugere-se a nomeação de um encarregado de proteção de dados, ainda que não obrigatória, quando subcontratações em Estados-Membros diversos, por forma a se superar os obstáculos inerentes às peculiaridades de cada país e respeitar os princípios do tratamento.

explanados de forma clara no RGPD⁹². No entanto, as orientações do GRUPO DE TRABALHO DO ARTIGO 29.º, no que respeita aos encarregados de proteção, bem como o considerando (91) em sede de «tratamento em grande escala» e o considerando (24) em âmbito de «controlo regular e sistemático», proporcionam de forma não exaustiva, linhas orientadoras. Apesar dos requisitos impostos pelo RGPD, em matéria de designação de EPD, fundamentarem a sua não obrigatoriedade nas situações que aí não se enquadrem, a empresa que opte⁹³ pela sua nomeação, garante um nível de cumprimento mais elevado.

Em matéria de subcontratação, a demonstração e o cumprimento dos requisitos previstos no RGPD, obrigam à elaboração de acordos/contratos de subcontratação cujo conteúdo estabeleça os pressupostos do artigo 28.º do regulamento. As preocupações daqui resultantes, compactuam-se, numa primeira linha de ação, com a identificação das partes, que podem variar consoante o contexto da atividade e cuja importância se depreende com as responsabilidades que lhes estão adstritas.

Para os novos modelos de negócios, o impacto que lhes está associado coloca-se, numa primeira abordagem, ao nível da identificação da entidade responsável pelo tratamento, uma vez que cabe a esta entidade a responsabilidade de providenciar o direito à informação previsto nos artigos 13.º e 14.º do regulamento, informando o respetivo titular do exercício dos seus direitos e antes disso, de cumprir com os princípios expostos no artigo 6.º do RGPD, funcionando também como medida de mitigação do risco, incluindo a definição de perfis⁹⁴. A finalidade da atividade deve ter em consideração a recolha dos dados estritamente necessários à sua prossecução, identificando de um mesmo modo os dados sensíveis, uma vez que as exigências que decorrem do artigo 9.º do regulamento conferem

⁹² Linklaters, *The General Data Protection Regulation*, «A survival guide», p. 42. [consult. 13/11/2018]. Disponível em: [file:///C:/Users/arcarvalho/Downloads/TMT_DATA_Protection_Survival_Guide_Singles%20\(8\).pdf](file:///C:/Users/arcarvalho/Downloads/TMT_DATA_Protection_Survival_Guide_Singles%20(8).pdf)

⁹³ Averiguando a necessidade de implementação de medidas que salvaguardem os dados pessoais dos titulares que deem cumprimento em artigo 24.º do regulamento, antecede ao início de qualquer tratamento de dados cuja operação seja suscetível de resultar num elevado risco para os direitos e liberdades da pessoa singular, a realização de uma AIPD. Sendo o grau de risco que as atividades de tratamento de dados constituem variável, a designação, ainda que não obrigatória, de um EPD, comporta benefícios pelas funções que lhe estão inerentes.

⁹⁴ A reforma procura criar uma tendência para o tratamento transparente e como tal, os modelos que envolvam inteligência artificial tem de assentar nos princípios descritos no artigo 6.º do RGPD.

requisitos mais restritos em função dos restantes, como a obrigatoriedade do pedido de consentimento à pessoa titular dos dados. As finalidades cujo tratamento de dados não englobe a categoria de dados sensíveis e para os quais não seja necessário o consentimento do titular por se basear numa fonte de licitude diversa, não legitima a falta de informações ao titular, designadamente a opção de *opt out*⁹⁵.

Os modelos de negócio caracterizados pela atividade do corretor de seguros, englobam, entre outros, (i) consultoria e (ii) acompanhamento da gestão contratual⁹⁶. Assim, integrando a categoria de mediação de seguros, as maiores preocupações prendem-se com:

- Revisão dos consentimentos prestados pelos titulares dos dados e adaptá-los às novas exigências do RGPD;
- Identificação do tratamento de dados sensíveis;
- Revisão dos instrumentos contratuais com os subcontratantes no que respeita à transferência e tratamento de dados;
- Adoção e medidas técnicas e organizativas adequadas.

As novas obrigações ao nível da segurança dos dados preveem uma revisão das condições de segurança dos sistemas de informação e definição de políticas de segurança dos sistemas que cumpram as novas regras impostas pelo regulamento. Neste contexto torna-se indispensável concretizar uma avaliação de impacto de modo a controlar a exposição dos dados ao risco e implementar novas soluções técnicas que permitam detetar violações de dados pessoais. De um modo geral, todas as entidades têm de criar manuais e políticas internas que versem sobre a proteção de dados pessoais⁹⁷, definir novos processos e procedimentos e rever todos os contratos que tenham celebrado com entidades

⁹⁵ Artigo 5.º do RGPD. As obrigações ao nível do responsável pelo tratamento, inserem-se, entre outras em conferir ao titular dos dados o direito de saída, não ficando sujeito a ações de *marketing*.

⁹⁶ A atividade do corretor de seguros envolve um tratamento de dados pessoais e sensíveis, designadamente em operações de cobrança de prémios, avisos e renovações e intervenção na regularização de sinistros.

⁹⁷ Programas de *compliance*, mecanismos de controlo operacional, programas de auditorias regulares, modelos de avaliação de impacto, entre outros.

subcontratadas ou parceiros com o fundamento de cumprimento relativamente às novas regras do regulamento. As alterações face ao atual regime vêm culminar numa maior auto responsabilização por parte dos responsáveis pelo tratamento de dados que deixam de ter que notificar a CNPD que passa a agir como entidade fiscalizadora. Quer isto dizer que, é apenas em casos excepcionais que o responsável pelo tratamento terá de fazer uma consulta prévia junto da CNPD antes de iniciar o tratamento de dados.

A necessidade de suporte tecnológico no que respeita a mecanismos de controlo e acessibilidade dos dados, através das medidas de segurança impostas pelo artigo 32.º, do RGPD como forma de combate à violação de dados, podem implicar, entre outras, (i) configuração de perfis de utilizadores de acesso, (ii) *download* de documentação diretamente nas plataformas das seguradoras, (iii) pseudonomização, (iv) encriptação e (v) rotinas de *backup*. Sublinha-se, no entanto que, os reforços de medidas de combate à fraude implicam custos onerosos para as empresas. Assim, na sequência do vazio legal existente no setor segurador, que tem impacto direto na atividade de mediação de seguros, a adoção de determinadas medidas técnicas encontra-se suspensa.

CAPÍTULO V

CASO DE ESTUDO

Far-se-á neste capítulo a análise da duplicidade de papéis da MDS – Corretor de Seguros, ao abrigo do novo RGPD nas duas fases de intervenção. Trata-se da análise da duplicidade de papéis, responsável pelo tratamento e/ou subcontratante que a MDS pode assumir nas suas fases de intervenção com o cliente e seguradora e que é compatível com as operações de simulação e cotação, bem como com a sua atividade de acompanhamento da gestão contratual. O que sucede pelo seu estatuto de independência face às seguradoras é a sua consideração como responsável pelo tratamento na primeira fase de atuação e a identificação como subcontratante na atividade de auxílio na gestão do contrato de seguro.

5. A duplicidade de papéis do Corretor de Seguros –MDS- ao abrigo do novo RGPD

A consultoria e o acompanhamento da gestão do contrato promovem o auxílio ao cliente, bem como à seguradora. Esta última, especialmente em caso de sinistro, decorre da celebração do contrato de seguro entre o cliente e a seguradora e impacta fortemente a MDS, no sentido de, face ao novo RGPD, ter que se elaborar um contrato de proteção de dados pessoais. É nesta fase que ganha especial enfoque a definição do papel da MDS uma vez que o contrato estipula o modo de atuação do subcontratante relativamente aos dados pessoais do cliente da seguradora. Urge assim, a necessidade de clarificar o papel da MDS nestas fases de atuação: Responsável pelo tratamento ou Subcontratante?

A qualificação da MDS varia consoante o contexto e a atividade de tratamento. Em moldes de análise serão apresentados dois cenários com vista a qualificar o papel da MDS nas duas fases em que intervêm.

FASE I – Relação MDS / Cliente – Anterior à celebração do contrato de

seguro: Uma vez contactada pelo cliente, a MDS, com vista à prossecução de um contrato de seguro, procede a uma análise imparcial de um número de contratos de seguro disponíveis no mercado. O corretor atua, neste contexto, por conta e, em regra, com poderes de representação, do seu cliente. É a sua independência face às seguradoras que o torna responsável na finalidade de mediação, não devendo, por isso, estar abrangidas pelo escopo dos contratos, as atividades de distribuição de seguros compatíveis com: (i) proposta, (ii) aconselhamento ou outros atos preparatórios da celebração de contrato de seguro, designadamente, prestação de informação sobre contratos de seguro na fase pré-contratual, incluindo comparação de preços e pedidos de cotações, bem como a própria conclusão de contratos de seguro. Deste modo, atuando como responsável pelo tratamento, terá de dar cumprimento ao dever de prestar informações ao titular dos dados, facultando um documento que contemple todas as informações previstas no artigo 13.º do RGPD.

FASE II – Relação MDS / Seguradora – posterior à celebração do

contrato de seguro: A fase posterior à celebração do contrato de seguro entre o cliente e a seguradora, não torna a MDS parte no contrato de seguro. As atividades de cobrança de prémios, avisos e renovações e intervenção em caso de sinistro refletem-se no acompanhamento da gestão contratual, mas enquanto corretor independente, têm a sua própria responsabilidade no tratamento dos dados que faça. Todavia, apesar do seu papel independente face às seguradoras, a MDS enquanto corretor de seguros, atua de acordo com as instruções estipuladas pela seguradora. Neste sentido e de acordo com a definição de subcontratante consagrada no artigo 4.º n.º 8 do RGPD e com as diretrizes apontadas nas orientações da CNPS no seu parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», a sua atividade torna-se compatível com os elementos caracterizadores do subcontratante.

Em consonância com a abordagem dos conceitos de responsável pelo tratamento e subcontratante, verifica-se a complexidade de adoção ao caso concreto das definições extraídas do RGPD. Adicionalmente são desenhadas orientações apresentadas pelo GRUPO DE TRABALHO DO ARTIGO 29.º, no seu Parecer 1/2010 e que favorecem um mar de

critérios que possibilita um conceito mais informado, facilitando na aplicação da legislação a adotar.

O caso de estudo revela que apesar do papel da MDS se compactuar com as instruções desenhadas pela seguradora, a sua independência face às mesmas, resulta numa ausência de influência de facto que por si só, classifica a entidade como responsável pelo tratamento⁹⁸. Por outro lado, a segunda fase é baseada numa decisão por parte da seguradora de delegar parte das suas atividades de tratamento à MDS. No que toca a este ponto, é de salientar que são duas as condições básicas para a qualificação como subcontratante: por um lado, ser uma entidade jurídica distinta do responsável pelo tratamento e, por outro, proceder ao tratamento dos dados por conta deste⁹⁹.

Nesta senda, verifica-se ao nível do responsável pelo tratamento, o cumprimento dos deveres de informação previsto nos artigo 13.º do regulamento, bem como o exercício dos restantes direitos, adotando a lógica de atribuição de controlo aos respetivos titulares percecionada pelo RGPD. A qualificação do seu papel como subcontratante, por outro lado, confere o cumprimento dos requisitos previstos no artigo 28.º do regulamento, devendo neste sentido, adotar medidas de segurança adequadas ao cumprimento quer ao nível do regulamento, como ao nível das instruções conferidas pelo responsável pelo tratamento, implicando a imputação de responsabilidade civil pelo tratamento dos dados pessoais aquando a violação de algumas destas disposições. Em termos de impacto no setor segurador e maior acompanhamento do titular, no processo de tratamentos dos seus dados, constata-se no setor segurador uma verdadeira problemática ao nível do artigo 9.º do regulamento pelo seu carácter mais restritivo.

⁹⁸ Pode, contudo, de acordo com os elementos «determinação dos fins» e «meios de tratamento» consagrados no artigo 4.º, alínea 7) do RGPD, surgir alguma divergência em termos de classificação, na medida em que, o corretor, em bom rigor, atua mediante as finalidades estabelecidas pela seguradora. Assim, tendo algumas seguradoras vindo a ignorar o papel independente das seguradoras, baseando-se apenas no elemento «determinação das finalidades», têm classificado o corretor, nesta fase pré-contratual como subcontratante.

⁹⁹ GRUPO DE TRABALHO DO ARTIGO 29.º - Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante». Adotado em 16 de Fevereiro de 2010.

CONCLUSÕES

O tema em que incidiu este estudo de caso focou-se na problemática da duplicidade de funções que a MDS pode assumir na fase anterior e posterior à celebração do contrato de seguro. A análise partiu num primeiro momento do entendimento dos conceitos de responsável pelo tratamento e subcontratante, bem como no exame das alterações legislativas decorrentes do novo Regulamento Geral de Proteção de Dados por influência da globalização.

As atividades de simulação e pedidos de cotação concretizadas ao abrigo da primeira fase de intervenção transformam a MDS em responsável pelo tratamento pelo seu fator independente face às empresas de seguro. Na verdade, o elemento preponderante desta distinção resulta na primeira linha de ação, não da determinação das finalidades, mas deste fator «independente» que caracteriza a categoria da atividade da MDS. A desmistificação dos conceitos possibilita uma verdadeira determinação das obrigações patentes nesta categoria, configurando também a correta aplicabilidade da lei nacional e a imputação ao nível da responsabilidade civil pelo tratamento de dados, incluindo também a possibilidade de designação de um encarregado de proteção de dados. Por outro lado, a segunda fase de atuação que resulta da relação MDS/Seguradora, percebe uma atividade baseada no auxílio do acompanhamento da gestão do contrato de seguro sugerindo um controlo efetivo por parte da seguradora. Adotando a qualidade de subcontratante, a MDS deve cumprir não só as disposições previstas no RGPD que lhe digam diretamente respeito, como também as instruções explanadas nos contratos de subcontratação elaborados com as seguradoras sob pena de incumbir em responsabilidade pelo incumprimento do artigo 28.º do regulamento. Neste contexto, releva-se a importância da ausência de legislação nacional ao nível do setor segurador, bem como de uma disposição transitória que não provoque de forma imediata a suspensão do tratamento das apólices. O problema presente emerge de uma fase de subcontratação em que a MDS trata os dados por conta da seguradora e que, por englobar o tratamento de categorias especiais de dados, tem de fazer prova do artigo 9.º do RGPD.

JURISPRUDÊNCIA

ECLI : PT : STJ : 2016 : 432/08.6 TASCRL1.S1. [Consult. 17/11/2018]. Disponível em: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/816828c216c8cecd80257f8c004e219b?OpenDocument>

BIBLIOGRAFIA

ANTUNES, José Engrácia - *Direito dos contratos comerciais*. Coimbra: Edições Almedina, 2009. ISBN: 9789724039350

APS – PROCESSO DE CONSULTA PÚBLICA PARA APROVAÇÃO DE LEGISLAÇÃO NACIONAL RELATIVA AO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

ARTICLE 29 DATA PROTECTION WORKING PARTY - Opinion 3/2010 on the principle of accountability. [Em linha]. Bruxelas : Comissão Europeia. [consult. 15/11/2018]. Disponível em: <https://www.dataprotection.ro/servlet/ViewDocument?id=720>

ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Personal data breach notification under Regulation 2016/679. [Em linha]. Bruxelas : Comissão Europeia. [Consult. 24/10/2018]. Disponível em: [file:///C:/Users/arcarvalho/Downloads/wp250rev01_enpdf%20\(3\).pdf](file:///C:/Users/arcarvalho/Downloads/wp250rev01_enpdf%20(3).pdf)

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS - Parecer 3/2015. «A grande oportunidade da Europa Recomendações da AEPD sobre as opções da UE para a reforma da proteção de dados». [Em linha]. Bruxelas : Comissão Europeia. [consult 10/11/2018]. Disponível em: https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_pt.pdf

BARBOSA, Mafalda Miranda - *Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil*. [Em linha]. Estudos de Direito do Consumidor : Pedro Manuel de Melo Pais de Vasconcelos. [Consult. 20/11/2018]. Disponível em: <https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>

CASTELO, Higinia – *Contrato de Mediação, Estudo das prestações principais*. [Em linha]. Lisboa : Faculdade de Direito da Universidade Nova de Lisboa, 2013. Tese de Doutoramento.

CAVOUKIAN, Ann - «*PRIVACY BY DESIGN: FROM RHETORIC TO REALITY*». [Em linha]. Toronto: [s.n]. [Consult. 16/11/2018]. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>

Comissão Europeia - «Quando devo exercer o meu direito à limitação do tratamento dos meus dados pessoais?». [Em linha]. Bruxelas : Comissão Europeia. [consult. 23/11/2018]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_pt

CARVALHO, Alberto Arons de; CARDOSO, António Monteiro; FIGUEIREDO, João Pedro - *Direito da Comunicação Social*, 3ª edição, [s.l.], texto editores, 2012. ISBN: 9789724744728

Comissão Europeia. As prioridades da Comissão - «Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?». [Em linha]. Bruxelas. Comissão Europeia. [Consult. 13/11/2018]. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - «PRINCÍPIOS SOBRE A UTILIZAÇÃO DE DADOS BIOMÉTRICOS NO ÂMBITO DO CONTROLO DE ACESSOS E DE ASSIDUIDADE». [Em linha]. Lisboa : CNPD. [Consult 10/10/2018].

Disponível em: <https://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-BIOM-assiduidade-acesso.pdf>

COMMISSION STAFF WORKING PAPER - «Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)». [Em linha]. Bruxelas : Comissão Europeia. [consult. 10/10/2018]. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN>

CONCLUSÕES DO ADVOGADO-GERAL

NILO JÄÄSKINEN

apresentadas em 25 de junho de 2013 (1) Processo C-131/12, *Google Spain SL Google Inc.* contra *Agencia Española de Protección de Datos (AEPD)* *Mario Costeja González* [pedido de decisão prejudicial apresentado pela Audiencia Nacional (Espanha)]. [Em linha]. *Agencia Española de Protección de Datos (AEPD)* : CURIA – documents. [consult. 18/11/2018]. Disponível em:

<https://www.gedipe.org/website/images/gedipe/jurisprudencia/C-131-12%20MARIO%20COSTEJA%20v.%20GOOGLE%20Opinião%20AG.pdf>

CORDEIRO, António Barreto Menezes, «DADOS PESSOAIS: CONCEITO, EXTENSÃO E LIMITES». [Em linha]. Centro de Investigação de Direito Privado : [s.n]. [consult. 13/11/2018]. Disponível em:

https://alvarovelho.net/index.php/component/jdownloads/send/30-educ-para-os-media/519-dadospessoais-conceito-extensao-limites?option=com_jdownloads

CORDEIRO, António Menezes, (coordenador científico) CORDEIRO, António B. M. e ROCHA, Francisco, (coordenadores executivos) - «I JORNADA DE PROTEÇÃO DE DADOS E EMPRESAS» Primeiro Painel, 2018 Lisboa : [consult. 15/11/2018]. Disponível em: <https://www.youtube.com/watch?v=gmxsKZ4WgU>

CORDEIRO, António Menezes, (coordenador científico), CORDEIRO, António B. M. e ROCHA, Francisco, (coordenadores executivos) - «I JORNADA DE PROTEÇÃO DE DADOS E EMPRESAS». Quarto Painel, em 3 de maio de 2018. [consult. 17/11/2018]. Disponível em: <https://www.youtube.com/watch?v=k9hZQ3Gr4u4>

CORDEIRO, António Menezes, (coordenador científico); CORDEIRO, António B. M. e ROCHA, Francisco, (coordenadores executivos), «I JORNADA DE PROTEÇÃO DE DADOS E EMPRESAS» Terceiro Painel, em 3 de maio de 2018. Disponível em: <https://www.youtube.com/watch?v=DNC2rqW4G0c>

Cuatrecasas - «PROPIEDAD INTELLECTUAL, MEDIA E TI». [Em linha]. Lisboa : *Cuatrecasas*. [consult. 15/11/2018]. Disponível em: https://www.cuatrecasas.com/pt/publicacoes/newsletter_propriedade_intelectual_media_e_t_i_2_trimestre_2017.html

DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO. [Em linha]. [s.n]. [Consult. 14/11/2018]. [Em linha]. Espanha : *Agencia Española de Protecceión de Datos*. [Consult. 13/11/2018]. Disponível em: <https://www.aepd.es/media/guias/guia-directrices-contratos.pdf>

DUPLCIDADE DE FUNÇÕES DO CORRETOR DE SEGUROS – RESPONSÁVEL PELO TRATAMENTO E/OU SUBCONTRATANTE? Programa de Regulamento Geral de Proteção de Dados, 2ªedição, 2018. Apresentação do projeto – Grupo I. Lisboa 22 de março de 2018

FERREIRA, Carlos De Almeida - *Contratos*. Reimpressão da 4.ª Edição : Almedina, 2012. ISBN: 9789724063232

GABEL, Detlev and HICKMAN, Tim - «Obligation of controllers - Unlocking the EU General Data Protection Regulation». [Em linha]. White & Case Law firm : White & Case LLP. [Consult. 13/11/2018]. Disponível em: <https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection>

GLANCY, Dorothy J. - «The Invention of the Right to Privacy». *[Em linha]*. [Santa Clara Law Digital Commons] : [Santa Clara Law Digital Commons]. [consult. 10/10/2018]. Disponível em: <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://www.google.pt/&httpsredir=1&article=1318&context=facpubs>

GRUPO DE TRABALHO DO ARTIGO 29.º - *Statement on the role of a risk-based approach in data protection legal frameworks*. [Em linha]. Bruxelas : Comissão Europeia. [consult. 14/11/2018]. Disponível em: <https://www.pdp.ie/docs/10046.pdf>

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - «Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante» [Em linha]. Bruxelas: Comissão Europeia. [Consult. 13/10/2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientações sobre o direito à portabilidade dos dados*. [Em linha]. Bruxelas : Comissão Europeia. [consult. 15/11/2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientação sobre as decisões individuais automatizadas e a definição de perfis*. [Em linha]. Bruxelas : Comissão Europeia. [Consult. 23/11/2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf

GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS - *Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante*. Bruxelas : Comissão Europeia. [consult. 24/11/2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf

GRUPO DE TRABALHO DO ARTIGO 29.º SOBRE A PROTECÇÃO DE DADOS - *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*. [Em linha]. Bruxelas: Comissão Europeia. [consult. 10/11/2018]. Disponível em: https://www.gdpd.gov.mo/uploadfile/others/wp169_pt.pdf.

GRUPO DE TRABALHO DO ARTIGO 29.º SOBRE A PROTECÇÃO DE DADOS - *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*. [Em linha]. Bruxelas : Comissão Europeia. [consult. 23/11/2018]. Disponível em: https://www.gdpd.gov.mo/uploadfile/others/wp169_pt.pdf

Guía DEL Reglamento General DE Protección DE Datos PARA Responsables DE Tratamiento. [Em linha]. Espanha : A Agencia Española de Protecceión de Datos. [Consult. 13/11/2018]. Disponível em: <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>

Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Annex to the Recommendation of the Council of 23rd September 1980. [Em linha]. França : OECD. [consult. 11/11/2018]. Disponível em: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderflowsofpersonaldata.htm>

GUTWIRTH, Serge; LEENES, Ronald and HERT, Paul DE - *Data Protection on the Move: Current Developments in ICT and Privacy/Data*. Bruxelas: Springer, 2016. ISBN 978-94-017-7375-1. Disponível em:

<https://books.google.pt/books?id=JPreCwAAQBAJ&pg=PR10&lpg=PR10&dq=Gutwirth,+Serge,+Leenes,+Ronald,+De+Hert,+Paul.+%C2%ABData+Protection+on+the+Move:+C urrent+Developments+in+ICT+and+Privacy/Data%C2%BB,+2016&source=bl&ots=c9CF9p5F9p&sig=gUri4T4kmpjjLUckFUiSm2LqjBY&hl=en&sa=X&ved=2ahUKEwiEqdmTzdjeAhURgHMKHXLODtUQ6AEwBXoECAoQAQ#v=onepage&q=Gutwirth%2C%20Serge%2C%20Leenes%2C%20Ronald%2C%20De%20Hert%2C%20Paul.%20%C2%ABData%20Protection%20on%20the%20Move%3A%20Current%20Developments%20in%20ICT%20and%20Privacy%20Data%C2%BB%2C%202016&f=false>

<https://www.plmj.com/xms/files/newsletters/2014/Maio/Proteccao de Dados e Direito a o Esquecimento na Internet.pdf>

KUNER, Christopher - «*The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*», *Bloomberg BNA Privacy and Security Law Report*. [Em linha]. (2012). [consult. 10/10/2018]. Disponível em: http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf. ISSN 1538-3423.

Linklaters - *The General Data Protection Regulation - «A survival guide»*. [Em linha]. Inglaterra : Peter Church. [consult. 13/11/2018]. Disponível em: [file:///C:/Users/Ana%20Rita%20Carvalho/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/TMT_DATA_Protection_Survival_Guide_Singles%20\(1\).pdf](file:///C:/Users/Ana%20Rita%20Carvalho/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/TMT_DATA_Protection_Survival_Guide_Singles%20(1).pdf)

MARTINEZ, Pedro Romano – *O SUBCONTRATO*. [s.l.]. Edições Almedina, 1989. ISBN 9789724005423.

MDS Group – *Global Insurance & Risk Consultants*, Política de Cookies. Lisboa. [Consult. 10/10/2018]. Disponível em: <https://www.mdsinsure.com/pt/politica-de-cookies/>

MDS Group – *Global Insurance & Risk Consultants*, Política de Privacidade de Clientes. [Em linha]. Lisboa. [Consult. 10/10/2018]. Disponível em: <https://www.mdsinsure.com/pt/politica-de-privacidade/>

MORAIS, Nuno - *COMITENTE POR FACTO DO COMISSÁRIO, A ANÁLISE DO ARTIGO 500 DO CÓDIGO CIVIL —SEUS PRESSUPOSTOS E REGIME*. [Em linha]. [s.l] : [s.n]. [Consult. 25/11/2018]. Disponível em: <http://julgar.pt/wp-content/uploads/2016/05/04-Nuno-Morais-responsabilidade-objectiva-do-comitente.pdf>

OPINIONS EUROPEAN DATA PROTECTION SUPERVISOR - Opinion of the European Data Protection Supervisor on the 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», in *Official Journal of the European Union*. Disponível em: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XX0622\(01\)&from=PL](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XX0622(01)&from=PL)

OPINIONS EUROPEAN DATA PROTECTION SUPERVISOR - Opinion of the European Data Protection Supervisor on the 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». [Em linha]. Bruxelas : *European Data Protection Supervisor*. [consult. 20/11/2018]. Disponível em: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XX0622\(01\)&from=PL](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011XX0622(01)&from=PL)

COUTINHO, Francisco Pereira e MONIZ, Graça Canto (Coordenadores) - *O ANUÁRIO DA PROTEÇÃO DE DADOS*. Lisboa : CEDIS 2018. ISBN 978-972-99399-5-2.

PEREIRA, Alexandre Libório Dias - *BIG DATA, E-HEALTH E «AUTODETERMINAÇÃO INFORMATIVA»: A LEI 67/98, A JURISPRUDÊNCIA E O REGULAMENTO 2016/679 (GDPR)*. [Em linha]. Coimbra: [s.n]. [Consult. 18/11/2018]. Disponível em: <https://estudogeral.sib.uc.pt/bitstream/10316/48094/1/Big%20data%20ehealth%20autodeterminacao%20informativa.pdf>

PLMJ, Sociedade de Advogados - «À PROCURA DO PASSADO: PROTECÇÃO DE DADOS E DIREITO AO ESQUECIMENTO NA INTERNET». [Em linha]. PMLJ, Sociedade de Advogados : PMLJ, Sociedade de Advogados. [Consult. 24/11/2018]. Disponível em: http://www.plmj.com/xms/files/newsletters/2014/Maio/Proteccao_de_Dados_e_Direito_ao_Esquecimento_na_Internet.pdf

POÇAS, Luís - *O Dever da Declaração Inicial do Risco no Contrato de Seguro*. Almedina, 2013. ISBN: 9789724051970

SALDANHA, Nuno - *NOVO REGULAMENTO GERAL DE PROTECÇÃO DE DADOS. O que é? A quem se aplica? Como implementar?*. Lisboa: FCA, 2018. ISBN 9789727228898.

SÉNECA, Hugo - «CNPD: Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos» [Em linha]. []. [] *Exame Informática*, (2018), []. [consult. 20/11/2018]. Disponível em: <http://exameinformatica.sapo.pt/noticias/mercados/2018-10-19-CNPD-Hospital-do-Barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos>

AUWERMEULEN, Barbara pauVan Der - «How to attribute the right to data portability in Europe: A comparative analysis of legislations». [Em linha]. *Faculty of Law, University of Vienna* : Elsevier Ltd. [consult. 17/11/2018]. Disponível em: <http://isiarticles.com/bundles/Article/pre/pdf/104675.pdf>

VASCONCELOS, Pedro Pais - *Direito Comercial*. Volume I. Edições Almedina, 2011. ISBN: 9789724047218

VELOSO, Mónica - «O Regulamento Geral de Protecção de Dados. Como devem as empresas tratar os dados pessoais que têm na sua posse?». [Em linha]. Área Jurídica da

Unidade Empreendedorismo, Incubação e Aceleração da ANJE : [s.n]. [Consult. 14/1/2018]. Disponível em:

<http://www.anje.pt/system/files/items/781/original/Quickaid18.pdf>

WARREN, Samuel D. and BRANDEIS, Louis D. - «The Right to Privacy». [The Harvard Law Review Association] : [JSTOR archive]. [consult. 10/10/2018]. Disponível em:

<http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>

ÍNDICE

DECLARAÇÃO DE COMPROMISSO ANTIPLÁGIO	4
AGRADECIMENTOS	5
INDICAÇÕES DE LEITURA	9
LISTA DE ABREVIATURAS	10
RESUMO	11
ABSTRACT	13
INTRODUÇÃO	14
CAPÍTULO I.....	18
ESTÁGIO CURRICULAR	18
1.1. MDS	18
1.2. MDS RE	18
CAPÍTULO II	20
O NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS	20
2. Contextualização	20
2.1. Direitos dos titulares dos dados.....	20
2.1.1. Informação	21
2.1.2. Direito de acesso	21
2.1.3. Direito à portabilidade.....	22
2.1.4. Direito à retificação e ao esquecimento	24
2.1.5. Direito à limitação.....	24
2.1.6. Direito à oposição.....	25
2.1.7. Decisões automatizadas e definição de perfis	25
CAPÍTULO III.....	27
O RESPONSÁVEL PELO TRATAMENTO E O SUBCONTRATANTE.....	27
3. Alterações legislativas.....	27
3.1. O Responsável pelo tratamento.....	27
3.1.1. Clarificação dos conceitos e a sua importância nas exigências previstas no RGPD	28
3.2. O Subcontratante	32
3.2.1. Contratos de subcontratação.....	33

3.3. Clarificação dos conceitos e a sua importância na classificação da autoridade de controlo principal.....	35
3.4. Transferências internacionais de dados	36
3.5. Violações no tratamento de dados pessoais	37
3.6. Clarificação dos conceitos e a sua importância na responsabilidade civil pelo tratamento de dados pessoais	39
CAPÍTULO IV	41
O CORRETOR DE SEGUROS	41
4. Enquadramento legal.....	41
4.1. A duplicidade de papéis do Corretor de Seguros	42
4.2. Impactos do RGPD no setor segurador, em especial na categoria do corretor de seguros	44
CAPÍTULO V	51
CASO DE ESTUDO	51
5. A duplicidade de papéis do Corretor de Seguros –MDS- ao abrigo do novo RGPD.....	51
CONCLUSÕES.....	54
JURISPRUDÊNCIA	55
BIBLIOGRAFIA.....	56
ÍNDICE	66

