



UNIVERSIDADE D
COIMBRA

Nídia Simões Cristino

**INSURTECH: A APLICAÇÃO DA
TECNOLOGIA AO SETOR DOS SEGUROS**

**Dissertação no âmbito do Mestrado em Ciências Jurídico-
Empresariais/ Menção em Direito Empresarial orientada pelo
Professor Doutor Alexandre Libório Dias Pereira e apresentada à
Faculdade de Direito da Universidade de Coimbra.**

Outubro de 2020



FACULDADE DE DIREITO
UNIVERSIDADE DE
COIMBRA

InsurTech: A Aplicação da Tecnologia ao Setor dos Seguros

InsurTech: Applying Technology to the Insurance Industry

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Especialização em Ciências Jurídico-Empresariais/ Menção em Direito Empresarial

Nídia Simões Cristino

Orientador: Professor Doutor Alexandre Libório Dias Pereira

Coimbra, 2020

“Mudam-se os tempos, mudam-se as vontades,
Muda-se o ser, muda-se a confiança;
Todo o mundo é composto de mudança,
Tomando sempre novas qualidades.”

— Luís Vaz de Camões

AGRADECIMENTOS

Ao Professor Doutor Alexandre Libório Dias Pereira, por ter aceitado guiar-me neste projeto, dando-me liberdade para que pudesse crescer academicamente e orientação para que pudesse fazer progredir o meu trabalho.

Aos meus pais que sempre me ensinaram que todo o esforço tem a sua recompensa. Em especial, à minha Mãe, por ouvir todos meus lamentos, sem nunca me deixar desistir.

À minha irmã, a quem agradeço o companheirismo e a irreverência de sempre, que tanto me tem ensinado.

RESUMO

A tecnologia promete transformar a oferta dos produtos de seguro, tendo surgido uma série de empresas *Insurtech*. Os produtos de seguro oferecidos pelas empresas *Insurtech* integram tecnologias como *Blockchain*, *Big Data* e Inteligência Artificial, conferindo-lhes valor que os recursos humanos não conseguem conferir.

Este estudo consiste, sobretudo, numa análise de como e em que medida a tecnologia afetou o setor dos seguros. Para tanto, estarão em foco as tecnologias-chave da *Insurtech*, designadamente a possibilidade de celebrar contratos de seguro automatizados, as consequências do recurso à tecnologia para efeitos de aferição do risco e a criação de novos produtos de seguro.

Apesar da flexibilidade e dinamização trazidas à contratação do seguro, escondem-se aqui inúmeras questões, nomeadamente em sede de proteção dos dados, questão que está na ordem do dia.

Palavras-chave: Tecnologia; *Insurtech*; *Blockchain*; *Smart contracts*; *Big Data*; Internet das Coisas; Inteligência Artificial; Seguros; Dados Pessoais

ABSTRACT

The technology promises to transform the offer of insurance products, having emerged a series of *Insurtech* companies. The insurance products offered by *Insurtech* companies integrate technologies such as *Blockchain*, *Big Data* and *Artificial Intelligence*, giving them value that human resources cannot confer.

This study consists, above all, in an analysis of how and to what extent the technology has affected the insurance sector. To this end, *Insurtech's* key technologies will be in focus, namely the possibility of concluding automated insurance contracts, the consequences of using technology for risk assessment purposes and the creation of new insurance products.

Despite the flexibility and dynamism brought to the contracting of insurance, countless issues are hidden here, particularly in terms of data protection, an issue that is on the agenda.

Keywords: *Technology; Insurtech; Blockchain; Smart contracts; Big Data; Internet of Things; Artificial Intelligence; Insurance; Personal Data*

SIGLAS E ABREVIATURAS

Ac. – Acórdão

Al./Als. - Alínea, alíneas

Art./Arts. - Artigo, artigos

ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões

B2C/b2c – Business to consumer

CCiv. – Código Civil

CE – Comissão Europeia

Cfr. - Confira

CMVM - Comissão do Mercado de Valores Mobiliários

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

CSC – Código das Sociedades Comerciais

DCE – Diretiva sobre o Comércio Eletrónico

DDS – Diretiva da Distribuição de Seguros

DL – Decreto-lei

DLT - Distributed Ledger Technology / Distributed ledger technologies

E.g. - *exempli gratia*

EDI/TED - *Electronic Data Interchange*, Intercâmbio Eletrónico de Dados, Transferência Eletrónica de Dados

eIDAS - Regulamento (UE) 910/2014, que revogou a Diretiva 1999/93/CE

UE – União Europeia

EUA – Estados Unidos da América

LCE – Lei do Comércio Eletrónico

N.º/n.ºs - Número, números

P. - Página/Páginas

P2P/p2p – *Peer to peer*

Proc. – Processo

RGPD – Regulamento Geral da Proteção de Dados

RJCS – Regime Jurídico do Contrato de Seguro

RJDEAD – Regime Jurídico dos Documentos Eletrónicos e da Assinatura Digital

TRL – Tribunal da Relação de Lisboa

V. - Vide, Veja-se

Vol. – Volume

NOTA PRÉVIA

Na redação da presente dissertação, foram respeitadas as regras do Novo Acordo Ortográfico, exceto nas citações bibliográficas que foram reproduzidas com respeito pela ortografia utilizada pelos autores.

Índice

Introdução	10
1. <i>Insurtech</i> : Considerações Iniciais	12
1.1 O Acesso ao mercado segurador.....	14
1.2 Financiamento das <i>startups</i>	18
2. Contratação Eletrónica e Contratação Automatizada	19
2.1 Contratação Eletrónica	19
2.2 Contratação Automatizada.....	22
2.2.1 Terminologia e construção do conceito “smart contract”	22
2.2.2 Breve enquadramento histórico dos Smart contracts: De Hero aos dias de hoje	26
2.2.3 Smart insurance products.....	27
3. O contrato de seguro automatizado	29
3.1 A imutabilidade dos <i>Smart contracts</i>	33
3.2 Smart contracts e blockchain	37
3.2.1 Distributed Ledger Technologies e Blockchain.....	37
3.2.1.1 Noção.....	37
3.2.1.2 Características da tecnologia <i>Blockchain</i>	38
3.2.2 Desafios legais da contratação automatizada.....	44
3.2.2.1 Requisitos formais do contrato de seguro.....	44
4. <i>Big Data</i> e Internet das Coisas (<i>IoT</i>).....	47
4.1 O Recurso à <i>IoT</i>	50
4.1.2 <i>IoT</i> e Proteção de Dados: Aplicação da Legislação em vigor	53
4.1.3 Princípios relativos ao tratamento de dados pessoais.....	56
4.1.4 As fontes de licitude do tratamento de dados	60
4.1.4.1 O Consentimento do titular de dados	60
4.1.4.2 Outras fontes de licitude	62

4.2	O Responsável pelo Tratamento de Dados.....	68
4.3	Deveres de Informação do Segurado e a Aferição do Risco no seio da <i>Insurtech</i>	70
4.4	As práticas discriminatórias.....	79
5.	Inteligência Artificial e <i>Robot-Advisors</i>	85
5.1	Deveres de Informação do Segurador	87
5.2	Responsabilidade Civil dos <i>Robot-Advisors</i>	90
6.	Novos modelos de seguros	97
6.1	Seguros Baseado no Uso	97
6.2	<i>On-demand insurance</i>	98
6.3	Seguros colaborativos ou P2P.....	99
	Conclusão	103
	Bibliografia	105

Introdução

A tecnologia tem mergulhado de tal forma na sociedade que representa uma forte referência na História. Não obstante, a forma como a utilizamos é suscetível de gerar quer vantagens, quer desafios.

Desde que se banalizou relativamente o recurso à Internet, os hábitos e pretensões dos consumidores encontram-se em mutação, grande parte devido à penetração de novas tecnologias e dispositivos móveis no seu dia-a-dia. De facto, hoje podemos falar de um “novo” consumidor, consciencializado para atuar “no virtual”, com acesso a mais informações e que é cada vez mais exigente com os serviços que procura. Felizmente para as empresas, surgem constantemente novas tecnologias que visam colmatar as lacunas dos produtos mais antigos e que preenchem as necessidades dos consumidores.

É num contexto de crise financeira que o recurso à tecnologia se alastrou a vários setores e esta se tornou uma aliada forte na comercialização de diversos produtos e serviços. Em contrapartida, o mercado dos seguros é uma indústria antiga e altamente regulamentada. Precisamente por isso, o mercado tem sido adverso à adoção das novidades que a tecnologia propõe quando feita a comparação a outros setores. O contrato de seguro, pela complexidade que lhe é subjacente, ainda está sujeito a processos lentos e burocráticos, nos quais é crucial a intervenção humana. Ainda hoje, os clientes se deparam com papelada e burocracia demoradas no momento de receber um reembolso ou solicitar uma nova apólice de seguro. Além disso, muitas vezes os clientes acabam por pagar mais pelo seguro, porque as apólices não são adaptadas às suas necessidades exclusivas.

Nos últimos anos, tem-se começado a notar um esforço global por parte das companhias de seguros para introduzir novos produtos e adotar novos canais de distribuição, nomeadamente com recurso à Inteligência Artificial, à Internet da Coisas (*IoT*), entre outras...

Neste âmbito, o recurso às novas tecnologias tem como principal missão auxiliar na formulação de novos produtos, novos modelos de negócio e proporcionar maior rapidez e mais segurança no processo de comunicação dos sinistros.

Um dos maiores desafios que as seguradoras enfrentam prende-se com a fraude contra seguros. Na fase de negociação, os segurados tendencialmente enaltecem atributos positivos para ficarem sujeitos a taxas mais baixas e, posteriormente, relatam danos agravados para receberem valores mais altos de compensação pelo sinistro e, por vezes, registam várias vezes a queixa do mesmo incidente para obter lucro. O setor de seguros despense uma quantidade considerável de recursos para combater a fraude, o que obriga a impor prémios mais altos de apólice para cobrir o aumento dos custos administrativos, procedimentos de subscrição, processamento de reclamações e resolução de disputas.

O presente estudo iniciar-se-á pela compreensão dos novos *players* no mercado dos seguros, as empresas *Insurtech* e a dificuldade que elas possam enfrentar aquando da sua entrada no mercado. Segue-se um estudo sobre a celebração de contratos de seguro inteligentes, passando por uma análise da tecnologia *Blockchain* e uma reflexão sobre a possibilidade destas tecnologias alterarem a forma como o contrato de seguro é celebrado. De seguida, abordamos o recurso às tecnologias *Big Data* e Internet das Coisas, analisando, em primeiro lugar, que implicações decorreram a nível da proteção de dados; depois, de que modo a informação recolhida pelas novas tecnologias pode ser considerada pela atividade seguradora e, por fim, de que forma é que o risco passa a ser avaliado.

Posteriormente, é feita uma breve exposição sobre a Inteligência Artificial e as implicações que traz a nível dos deveres de informação a cargo do segurado e a responsabilidade dos *Robot-Advisors* por conselhos.

A final são dados a conhecer alguns dos novos produtos de seguros, cuja criação foi possibilitada pelas novas tecnologias

Durante a exposição, tentaremos fazer uma reflexão tendo em vista a legislação aplicável em vigor.

Note-se, contudo, que na presente lide, não se pretende abordar o tema de um ponto de vista técnico, mas antes espelhar as principais questões jurídicas decorrentes do uso de determinadas tecnologias.

1. *Insurtech*: Considerações Iniciais

Embora a globalização e a digitalização tenham já contribuído para uma transformação substancial de muitas outras indústrias, tem-se, contudo, constatado que a indústria dos seguros se revelou bastante relutante à “invasão” tecnológica, embora tenha um grande potencial que merece ser explorado.

Como refere ALEXANDRE DIAS PEREIRA, houve uma migração das atividades económicas tradicionais para o meio eletrónico¹. Na generalidade, as empresas começaram por adotar soluções derivadas das novas tecnologias, tais como a publicidade na Internet e lojas *online*. No setor dos seguros, deram-se os primeiros passos com a aparição de *sites* comparativos de seguros e depois com a banalização da contratação eletrónica no geral. Entretanto, foram surgindo empresas a oferecer os seus produtos através da Internet até que se têm visto, cada vez mais frequentemente, empresas que operam exclusivamente *online*.

É, contudo, com a emergência das *Insurtech* que se observa o maior impacto da tecnologia no setor segurador. Em particular, a relação empresa-segurado transforma-se de tal forma que se pode mesmo afirmar que “o mercado segurador, como quase todos, está a ser colonizado pela tecnologia”^{2,3}.

Apesar de ainda não existir uma definição unânime, as empresas *Insurtech*, cujo termo resulta da junção da palavra “seguro”, em inglês, com a palavra “tecnologia”, visam sobretudo o desenvolvimento de sistemas digitais destinados a flexibilizar todo o processo inerente à celebração e execução do contrato de seguro, através do recurso a tecnologias como a análise de dados, *blockchain* e *smartcontracts* para exercer a atividade seguradora diretamente ou por intermédio de uma seguradora já existente. Neste sentido, distinguem-se as

¹ Alexandre Dias Pereira, *Empresa, comércio eletrónico e propriedade intelectual*, in *Nos 20 anos do Código das Sociedades Comerciais, Homenagem aos Professores Doutores A. Ferrer Correia, Orlando de Carvalho e Vasco Lobo Xavier, Volume I - Congresso Empresas e Sociedades*, p. 450-453

² Paula Ribeiro Alves, *Os Desafios digitais no mercado segurador*, in *Fintech – Desafios da Tecnologia Financeira*, p. 34

³ Neste sentido, faz, Michael Nwogugu, a distinção entre *Insurtech 1.0* e *Insurtech 2.0*, aquele corresponde ao movimento que se verificou numa primeira fase de recurso às novas tecnologias, o que inclui, a contratação e pagamento do seguro através da Internet, a denúncia do sinistro por meios telemáticos e o uso da Internet para fins de publicidade, etc. Por sua vez, *Insurtech 2.0*, além de comportar os desenvolvimentos trazidos pela *Insurtech 1.0*, diz ainda respeito àquilo que está em foco neste trabalho, e portanto, à criação de aplicações para *smartphones*, o uso de dispositivos “monitorizadores” de comportamento, como teremos oportunidade de estudar. Vide *Corporate Governance, Financial Stability and evolving Insurtech: The Case of Insurance Australia Group (2011-2016)*, disponível em: <https://ssrn.com/abstract=2980133>

Insurtech B2C que fornecem o produto diretamente ao consumidor final, seja ele uma pessoa singular ou uma pessoa coletiva, das *Insurtech* B2B que fornecem o seu produto inovador e mais eficiente a empresas de seguro já estabelecidas.

Na sua maioria, estas empresas *Insurtech* constituem empresas *startup*, pois tratam-se de empresas na sua fase inicial de atividade que, mesmo que não tenham ainda iniciado a comercialização dos seus serviços, já se encontram numa fase de desenvolvimento da atividade profissional. Simultaneamente, estas empresas destacam-se pelo uso da tecnologia e desenvolvimento de modelos de negócio verdadeiramente inovadores.⁴

Em 2012, a Portaria n.º 432/2012, que cria a medida de apoio à contratação de trabalhadores por empresas *startup*'s, define-as como empresas que cumpram os seguintes requisitos: (1) ser uma pessoa singular ou coletiva⁵ de natureza jurídica privada, com ou sem fins lucrativos; (2) regularmente constituída e registada; (3) ter obtido certificação de PME (pequena ou média empresa), nos termos do Decreto-Lei n.º 372/2007, de 6 de novembro; (4) ter iniciado atividade há menos de 18 meses e (5) ser uma empresa baseada em conhecimento, com potencial de exportação ou de internacionalização.

⁴ A própria definição que nos é dada pelo Dicionário *online* de Língua Portuguesa Priberam reflete essas características. Segundo o Dicionário, uma *startup* é uma “empresa ou negócio novo ou em fase de arranque, geralmente de carácter inovador e ligado à tecnologia”, in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2020, <https://dicionario.priberam.org/startup>

⁵ Enquanto pessoas coletivas, estas empresas não só operam através de meios eletrónicos, como podem escolher concretizar-se apenas no “mundo virtual”. J. M. Coutinho de Abreu, *Empresas Virtuais (Esboços)*, in *Estudos em homenagem ao Professor Doutor Inocêncio Galvão Telles*, vol. IV, Almedina, Coimbra, 2003, p. 599-610. Muitas delas têm a natureza de verdadeiras empresas virtuais, que não comercializam produtos corpóreos, nem detêm lojas físicas, são desprovidas de elementos materiais.

Não obstante, há, entre nós, uma tendência para utilizar sinonimicamente os termos estabelecimento e empresa.

Coutinho de Abreu apresenta uma noção de empresa virtual, enquanto “unidade jurídica fundada em organização de meios essencialmente informáticos que constitui um instrumento relativamente autónomo para produzir bens imateriais (serviços) trocáveis (apenas) na Internet”. O Autor expõe os vários tipos de empresas virtuais. De forma resumida, encontramos a empresa virtual enquanto empresa potencial; enquanto organização de meios informáticos (aquele tipo que aqui desenvolvo) e enquanto empresa convencional-codificada.

A empresa virtual, neste sentido, aproxima-se do conceito de empresa em sentido objetivo, com a particularidade de ter como meios empresariais meios informáticos, produtos imateriais, troca de produtos meramente *online*. Recorde-se o conceito de empresa que na sua vertente objetiva é tida como “instrumento ou estrutura produtivo-económica objeto de direitos e de negócios”. Vide Jorge Manuel Coutinho de Abreu, *Curso de Direito Comercial: Volume 1*, p. 215 e 216, 220 e 221, 602 e 603.

Em regra, as *startup's* são constituídas sob a forma de sociedades por quotas, o que se compreende tendo em conta a sua pequena dimensão e flexibilidade (necessidade de uma grande dinâmica e pouca burocracia).⁶

Normalmente, para além da sua formalização em termos societários (contrato de sociedade), as *startup's* são criadas através de um acordo entre os seus fundadores, no qual podem constar as seguintes estipulações: o objetivo global do negócio, as consequências da saída de um ou mais dos fundadores, a duração mínima de permanência de cada fundador e a natureza da contribuição de cada fundador para o desenvolvimento do projeto, são os chamados acordos parassociais, regulados no art. 17.º do CSC.⁷

Quando empresas *startups* pretendem operar como seguradoras, estas devem cumprir determinados requisitos específicos. De antemão, impõem-se requisitos a nível do capital mínimo que devem ser cumpridos para que estas obtenham autorização administrativa para operar enquanto seguradoras.

1.10 Acesso ao mercado segurador

Embora as apostas tecnológicas no setor segurador tenham vindo principalmente de empresas já consolidadas no mercado e que estavam habituadas a trabalhar com os produtos “tradicionais”, já se têm visto nascer empresas com o intuito de oferecer soluções totalmente digitais.

Sucintamente, algumas das tendências que se têm verificado e que são aqui objeto de estudo prendem-se, principalmente com a criação de novos modelos de seguro, como são os seguros baseados no uso (*Used Based Insurance, UBI*)⁸, seguros a pedido (*Insurance on Demande, IoD*) e até mesmo seguros colaborativos (P2P).

⁶ A recordar, estas podem ser constituídas por um só sujeito (sociedades unipessoais), art. 270.º-A do CSC e, não estando sujeitas a um valor mínimo para o seu capital social, apenas ao mínimo de 1€ por cada quota, poderão ser constituídas sociedades com apenas 1€, no caso de serem unipessoais.

Hoje, com a opção "Empresa Online", para constituir uma sociedade por quotas, basta aceder ao *site* <https://eportugal.gov.pt/servicos/criar-uma-empresa-online> e fazer o pedido, apresentando os elementos elencados no art. 6º do DL n.º 125/2006, seguindo posteriormente a tramitação enunciada no art. 12º do mesmo diploma. Coutinho de Abreu, *Curso de Direito Comercial: Volume II – Das Sociedades*, p.93

⁷ Vide João Vieira dos Santos, *Aspetos jurídicos das startups*, in Revista da Ordem dos Advogados. - Lisboa : O.A.. - A. 77, n.º 1-2 (jan.-jun. 2017), p. 239-277

⁸ Este modelo, ele mesmo, com várias modalidades, como *pay-as-you-drive* ou *pay-as-you-live*, que teremos oportunidade de conhecer mais adiante.

Como consequência do desenvolvimento das novas tecnologias, surgem algumas questões que merecem melhor análise, nomeadamente em que termos podem as *startups* de *Insurtech* exercer atividade seguradora.

Segundo um Relatório da OCDE sobre a Tecnologia e Inovação no setor segurador, muito poucas empresas iniciantes da *InsurTech* conseguiram licença para subscrever seguros e a maioria possui licenças de corretor.

Estes obstáculos ao exercício da atividade profissional das *startups* na *Insurtech* podem traduzir-se numa estagnação da inovação tecnológica.⁹

Em Portugal, a influência da tecnologia no mercado segurador revela um impacto promissor. Embora ainda pouco desenvolvida, tem-se verificado a criação de algumas iniciativas que podem acelerar o desenvolvimento das empresas *Insurtech*, de entre as quais se destacam a criação da Associação Portugal *Fintech*¹⁰ e a Associação *Fintech* e *Insurtech* Portugal¹¹. Aquela apresenta como seus principais objetivos o empoderamento do ecossistema *Fintech* e gerar valor pela cooperação do mercado. Esta última foca-se em angariar recursos e potencial nacional para promover os sectores *FinTech* e *InsurTech*, melhorando a posição competitiva das suas empresas.

A atividade de distribuição de seguros só pode ser exercida pelas entidades elencadas no nº 1 do art. 3.º da Lei n.º 147/2015, de 9 de setembro¹², são elas: sociedades anónimas; mútuas de seguros; sucursais de empresas de seguros com sede em outro Estado membro, desde que cumpridos os requisitos exigidos; sucursais de empresas de seguros de um país terceiro,

⁹ OCDE (2017), *Technology and innovation in the insurance sector*, disponível em: <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf>

¹⁰ <https://www.portugalfintech.org/>

¹¹ <https://afip.pt/en/>

¹² Que aprova o regime jurídico de acesso e exercício da atividade seguradora e resseguradora, bem como o regime processual aplicável aos crimes especiais do setor segurador e dos fundos de pensões e às contraordenações cujo processamento compete à Autoridade de Supervisão de Seguros e Fundos de Pensões, transpondo a Diretiva 2009/138/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, procede à quinta alteração ao Decreto-Lei n.º 12/2006, de 20 de janeiro, à primeira alteração ao regime jurídico do contrato de seguro, aprovado pelo Decreto-Lei n.º 72/2008, de 16 de abril, à segunda alteração ao Decreto-Lei n.º 40/2014, de 18 de março, e revoga o Decreto de 21 de outubro de 1907 e o Decreto-Lei n.º 90/2003, de 30 de abril, alterada pela Lei 7/2019, de 16 de janeiro que aprova o regime jurídico da distribuição de seguros e de resseguros, transpondo a Diretiva (UE)2016/97, altera a Lei n.º 147/2015, de 9 de setembro, que aprova o regime jurídico de acesso e exercício da atividade seguradora e resseguradora, bem como o regime processual aplicável aos crimes especiais do setor segurador e dos fundos de pensões e às contraordenações cujo processamento compete à Autoridade de Supervisão de Seguros e Fundos de Pensões, e revoga o Decreto-Lei n.º 144/2006, de 31 de julho.

quando autorizadas; empresas de seguros ou empresas de resseguros públicas ou de capitais públicos, criadas nos termos da lei portuguesa, desde que tenham por objeto a realização de operações de seguro ou de resseguro em condições equivalentes às das empresas de direito privado.

Por sua vez, a atividade seguradora ou resseguradora pode também ser exercida por empresas de seguros e de resseguros que adotem a forma de sociedade europeia, nos termos da legislação que lhes for aplicável (n.º2).

A atividade seguradora ou resseguradora em Portugal em regime de livre prestação de serviços só pode ser exercida por empresas de seguros ou de resseguros com sede em outro Estado membro, desde que cumpridos os requisitos exigidos na Diretiva 2009/138/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (n.º3).

Quanto ao capital social mínimo, este varia consoante a categoria através da qual a sociedade pretende exercer a atividade, nomeadamente, para efeitos de inscrição no registo na categoria de agente de seguros, a Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF, doravante) entende que continua a ser exigível um capital social mínimo de 5 000 euros, dispõe o art. o Decreto-Lei n.º 144/2006, de 31 de julho.

Para as categorias de corretor de seguros e mediador de resseguros o capital social mínimo exigido é de 50 000 euros, como consta do art. 19.º do Decreto-Lei n.º 144/2006, de 31 de julho.¹³

Vale a pena ainda referir que a Diretiva 2016/97/EU, do Parlamento Europeu e do Conselho, de 20 de Janeiro de 2016, transposta para o nosso ordenamento jurídico pela Lei n.º 7/2019, de 16 de janeiro, que veio introduzir um conceito amplo de distribuição de seguros.

Encontra-se explanado no art. 2.º/1 da Lei n.º 7/2019, que a atividade de distribuição de seguros consiste em: “em prestar aconselhamento, propor ou praticar outros atos preparatórios da celebração de contratos de seguro, em celebrar esses contratos ou em apoiar a gestão e a execução desses contratos, em especial em caso de sinistro, incluindo a prestação de informações sobre um ou mais contratos de seguro, de acordo com os critérios selecionados

¹³ <https://www.asf.com.pt/NR/exeres/BDAD6D42-CBB1-41E1-AAEC-5DF27BEE4452.htm>

pelos clientes através de um sítio na Internet ou de outros meios e a compilação de uma lista de classificação de produtos de seguros, incluindo a comparação de preços e de produtos ou um desconto sobre o preço de um contrato de seguro, quando o cliente puder celebrar direta ou indiretamente um contrato de seguro recorrendo a um sítio na Internet ou a outros meios”.

Pelo exposto, é possível aferir que o conceito de distribuição de seguros introduzido pelas normas comunitárias é bastante abrangente, o que, como (bem) nota MAFALDA MIRANDA BARBOSA, teve como objetivo compreender o máximo de agentes que operam no setor dos seguros, para que, por sua vez, houvesse igualdade no tratamento desses operadores e, conseqüentemente se garantisse a proteção dos consumidores, independentemente do canal de distribuição a que recorreram.¹⁴

Neste sentido, as *Insurtech* poderão introduzir-se no mercado enquanto mediadores de seguros, que a Lei.º 7/2019, de 16 de janeiro define como sendo “uma pessoa singular ou coletiva, com a exceção de empresas de seguros ou resseguros e dos seus empregados e mediadores de seguros a título acessório, que inicie ou exerça, mediante remuneração, a atividade de distribuição de seguros” (art. 4.º/c)). Para tal, além da autorização administrativa que estas empresas têm que receber de acordo com o art. 5.º/1/a) da Lei n.º 147/2015, a Lei n.º 7/2019, no seu art. 11.º, enuncia vários requisitos para que as pessoas singulares se possam inscrever enquanto mediadores de seguros, de resseguros e de seguros a título acessório, entre os quais figura a necessidade de ter qualificação adequada às características da atividade de distribuição que pretendem exercer.

Ainda, o art. 14.º da Lei n.º 7/2019 impõe a idoneidade das pessoas que pretendam exercer a sua atividade no mercado.

Além disso, os mediadores de seguros, assim como os corretores de seguros estão sujeitos a condições específicas e processos de inscrição próprios, conforme estabelecem os arts. 16.º, 17.º, 18.º e 19.º da Lei n.º 7/2019, respetivamente.

Neste sentido, apesar de sujeitas a um controlo apertado, revela-se favorável às *Insurtech*, não só o facto de lei permitir o acesso ao mercado de distribuição de seguros a um

¹⁴ *Diretiva de distribuição de seguros: os sujeitos*, in *Revista de Direito Comercial*, disponível em: <https://www.revistadedireitocomercial.com/diretiva-de-distribuicao-de-seguros-os-sujeitos>

leque tão vasto de *performers*, como a garantia de que os produtos oferecidos são aprovados pela ASF.

1.2 Financiamento das *startups*

Os moldes nos quais se dá o financiamento das *startups* são extremamente importantes para garantir a sobrevivência das mesmas e a continuidade da inovação.

O financiamento das *startups* pode ser feito com recurso a capitais próprios ou com recurso a capitais alheios, de terceiros e divide-se em várias fases.

Em primeiro lugar, a chamada fase de investimento semente, na qual se dá um investimento inicial, usualmente designado de investimento 3 F's (pois é, em regra, realizado por fundadores, família e amigos – *friends* – ou, informalmente *family, friends and fools*). Este investimento tem como objetivo estabelecer o rumo e os objetivos da empresa, “dar-lhe um empurrãozinho” de modo a que esta possa desenvolver a sua atividade comercial. Depois, na fase do “vale da morte”, as *startups* necessitam de “injeções de capitais”, na fase de investimento A. Quando se começam a verificar receitas capazes de cobrir todos os custos mensais fixos e variáveis, as empresas atingem o *breakeven*. É nesta fase que a empresa “se torna um investimento interessante para empresas de *venture capital*”, podendo ocorrer, posteriores investimentos (B, C, D). Sendo bem-sucedida, a empresa pode ser vendida a uma outra empresa ou abrir o seu capital ao investimento da bolsa.¹⁵

Tem-se verificado, no âmbito das *Insurtech*, uma grande interação com as empresas de seguros ditas “tradicionais”. As *startups*, ora são incorporadas por empresas de maior dimensão, ora ingressam em parcerias com essas grandes empresas já estabelecidas. Esta última opção abre novas oportunidades às *startups*, que passam a ter acesso a um mercado e a transações que, provavelmente, só mais tarde conseguiriam atingir, sem pôr em risco a sua independência^{16,17}.

¹⁵ Vide Ana Perestrelo de Oliveira, *O papel das startups na Fintech e o ciclo de financiamento de startups*, in *Fintech ...cit.*, p. 259 Para mais desenvolvimento, vide também Diogo Pereira Duarte e João Freire de Andrade, *Breves notas sobre o financiamento de startups e a sua regulação*, in *Fintech II – Novos Estudos sobre a Tecnologia Financeira* p. 221-224

¹⁶ Vide João Vieira dos Santos, *Aspetos Jurídicos... cit.*

¹⁷ Por exemplo, a empresa Habit, que antes se identificava como Muzzley e se dedicava ao fornecimento de produtos *IoT* para o consumidor final, hoje dedica-se à criação de soluções para as seguradoras tradicionais

Algumas *startups* recorrem, ao invés, a plataformas de *crowdfunding*. Esta é uma fonte de financiamento alternativa relativamente recente e que JOÃO VIEIRA DOS SANTOS define como sendo “uma forma de financiamento de projetos e empreendimentos, geralmente com recurso à Internet, através de um convite ao investimento do público (*crowd*)”.

Isto acontece também porque da parte das grandes empresas, que têm mais meios para investigar e suportar os riscos dessa investigação e inovação, não há, muitas vezes, interesse em explorar as inovações tecnológicas, precisamente pelos custos elevados e incerteza que acarretam.

Acontece, contudo que muitas *startups* não conseguem sobreviver, sendo raras aquelas que são bem-sucedidas e, por isso, apelidadas de *startup* unicórnio. Algumas *Insurtech* unicórnio, como a chinesa Zhong An, ou as estadunidenses Oscar e CloverHealth podem ser avaliadas até aos 900 milhões de dólares

2. Contratação Eletrónica e Contratação Automatizada

2.1 Contratação Eletrónica

A contratação à distância não é um fenómeno novo, pois já há muito que se realizam contratos por catálogo, telefone ou mesmo através da televisão. Contudo, é com a Internet que se verifica a expansão da contratação à distância. É a Internet que se identifica como mecanismo propulsor da contratação eletrónica, que aqui se deve entender como uma forma de contratar à distância, seja através de lojas virtuais (alojadas em *sites* de Internet), seja por contacto pessoal por correio eletrónico.

Ao passo que inicialmente a Internet surgiu como ferramenta de apoio à gestão da atividade das empresas, na proliferação da sua imagem através da publicidade, por exemplo, hoje esta viabiliza a contratação de diversos bens e serviços tais como pagamentos eletrónicos (*home banking*), comércio de ações, serviços de transporte e alojamento e a contratação de seguro, que aprofundamos nesta disposição.¹⁸

(nomeadamente a Allianz), baseadas em dados extraídos pela tecnologia *IoT*. As seguradoras ficam encarregadas de contactar o cliente final, e a Habit ajuda a seguradora a ter mais pontos de contacto com o cliente, nomeadamente se a pilha do alarme da casa está a acabar.

¹⁸ No caso do seguro em concreto, verificou-se um maior desenvolvimento da contratação pelos meios eletrónicos, a Internet e o telefone, entre 2007 e 2008, com o lançamento da primeira marca de seguros que comercializava os seus produtos *online* e por telefone e das primeiras marcas que comercializavam os seus produtos exclusivamente pelos meios eletrónicos. O investimento em empresas *Insurtechs* aumentou a partir

Com a contratação eletrônica de seguros a ganhar proporções cada vez mais relevantes, torna-se necessário estudar o regime legal em vigor.

Em sentido amplo, a contratação eletrônica traduz-se na celebração de um negócio jurídico com recurso a meios eletrônicos. Se se verifica intervenção humana, estamos perante contratação eletrônica *strictu sensu*. Neste caso, as declarações de vontade são formuladas pelas partes através dos meios eletrônicos, tais como o endereço eletrónico. Estes servem a mera função de meio de comunicação. Já na contratação automatizada, os contratos são celebrados sem intervenção humana¹⁹ - e, por isso, considerados “inteligentes” - através da transferência eletrônica de dados (TED)²⁰ ou com recurso a um agente eletrónico inteligente, os agentes de *software*^{21, 22}.

de 2015 e a inovação tecnológica também. Cfr. Paula Ribeiro Alves, *Contrato de seguro à distância. O Contrato eletrónico*, p. 140-142 e Jovan Savicevic, *Impact potential of the innovations*, disponível em: www.etd.ceu.edu

¹⁹ Embora, em boa verdade e como refere Paula Ribeiro Alves em *Contrato de seguro à distância. O Contrato eletrónico*, “na realidade não existe contratação sem intervenção humana. A contratação pressupõe a emissão de declarações de vontade e só a pessoa humana é possuidora de vontade juridicamente relevante. O que acontece neste tipo de contrato é que no momento da celebração, em que são transmitidas as declarações de vontade, não estão presentes os seres humanos a quem são atribuíveis, mas sim computadores que comunicam diretamente entre si”, v. p. 81. Por isto, vai preferir-se, ao longo deste trabalho, a expressão “contrato inteligente” ou “smart contract”.

²⁰ Ou EDI (*Electronic Data Interchange*).

²¹ Também este termo é suscetível de induzir em erro. Usamos aqui um termo traduzido da expressão inglesa *software agents*. Ora, o termo *agent* no direito anglo-saxónico aproxima-se mais da figura de “representante” ou “procurador” no nosso ordenamento jurídico, pelo que não podemos compreender estes agentes no sentido técnico acolhido entre nós. Daniel Batalha, *Criptocontratação: uma nova forma de contratação automatizada?*, Dissertação de Mestrado, disponível em: <http://hdl.handle.net/10316/85817> p. 21 e 22 e Francisco Pereira Coelho, *Contratação Automatizada e Execução contratual automatizada: dos “software agents” aos “smart contracts”*, in *Direito e Robótica*, Actas do Congresso. Nestes casos, o que temos são “dispositivos eletrónicos ou programas de *software* capazes de atuar materialmente de forma automática (sem intervenção humana contemporânea), de acordo com critérios constantes da sua programação, em interação com outros dispositivos eletrónicos (quer tomando a iniciativa de agir, quer reagindo a estímulos recebidos).” V. David de Oliveira Festas, *A contratação eletrónica automatizada*, in *Direito da Sociedade da Informação* (VI), p. 415

²² Francisco Pereira Coelho define-os como sendo “no essencial, programas de computador que, de modo contínuo e autónomo, realizam uma certa atividade, naturalmente em nome de um sujeito utilizador, atividade que, no nosso caso, consiste justamente na celebração de contratos”. V. *Contratação Automatizada*, *ob. cit.* Cfr. ainda David de Oliveira Festas, *cit.*, p. 411, V. tbm. Hugo Ramos Alves, *Smart contracts: entre a tradição e a inovação*, p. 186 e 187, v. ainda Paula Costa e Silva, *A Contratação Automatizada*, in *Direito da Sociedade da Informação*, vol. IV, p. 290 Em sentido diferente, V. Miguel Ascencio, *Derecho Privado de Internet*, p. 332

Por sua vez, em sentido legal, a contratação eletrónica abrange os contratos celebrados por via eletrónica ou informática²³, os contratos executados imediatamente em linha e os contratos sem intervenção humana.

Os contratos executados imediatamente em linha serão aqueles em que, nos termos do art. 29.º, a encomenda que foi feita é imediatamente entregue através do meio eletrónico utilizado. Serão exemplos disso, a aquisição de músicas no iTunes, em que a música é imediatamente descarregada para o aparelho que serviu à celebração do contrato.

Na contratação eletrónica em sentido estrito, temos uma declaração eletrónica de vontade ou declaração de vontade eletronicamente transmitida, na contratação automatizada, como veremos, temos uma declaração automatizada ou computadorizada²⁴.

O contrato celebrado por meios eletrónicos *online* é geralmente um contrato estandardizado, constituído principalmente por cláusulas contratuais gerais a que o consumidor anui. Neste caso, os meios eletrónicos são utilizados como meros meios de comunicação da vontade das partes. Por sua vez, o contrato automatizado não só dá o primeiro passo para o cumprimento autónomo da ordem, como ainda, se não for possível o cumprimento do contrato, procede à penalização do devedor. Nestes últimos casos, é muito reduzida a intervenção humana. Contudo, há também casos em que a contratação é automatizada apenas de um lado, i.e., unilateral, em que de uma das partes temos, um computador, mas do outro lado uma pessoa.

Ora, a contratação eletrónica é regulada pela Lei do Comércio Eletrónico²⁵, que, no seu art. 25.º consagra o princípio da liberdade de celebração de contratos por via eletrónica, vigorando ainda o princípio da equiparação plena da contratação eletrónica à contratação dita “tradicional”, com as exceções do art. 9.º/2 da Diretiva sobre o Comércio Eletrónico (DCE), no art. 3.º/3, da Diretiva relativa aos direitos dos consumidores, no art. 2.º do DL n.º 7/2004, de 7 de janeiro (com as alterações introduzidas pelo DL n.º 62/2009, de 10 de março, e pela Lei n.º 46/2012, de 28 de agosto).

²³ Entende-se por contratação pela via informática a contratação efetuada através de computadores e pela via eletrónica a contratação efetuada por quaisquer meios eletrónicos. V. Paula Ribeiro Alves, *Contrato de Seguro...*, p. 81.

²⁴ Paula Costa e Silva, *A contratação automatizada...*, p. 290

²⁵ DL 7/2004, de 07 de janeiro alterada pelo DL n.º 62/2009, de 10 de março e pela Lei n.º 46/2012 de 29 de agosto, que transpôs a Diretiva n.º 2000/31/CE, de 8 de junho.

2.2 Contratação Automatizada

No nosso ordenamento jurídico, a contratação automatizada ou sem intervenção humana está prevista no art. 33.º da Lei do Comércio Eletrónico, que determina que lhe é aplicável o regime comum, salvo nas situações em que este prevê uma atuação.

Em primeiro lugar, importa esclarecer a parte final do art. 33.º. Cremos que, quando o legislador refere «salvo quando este pressupuser uma atuação», este quis dizer que à contratação eletrónica automatizada sem intervenção humana será aplicável o regime geral do Código Civil. E, nos casos em que para a conclusão do contrato seja exigível uma atuação humana, aplicar-se-á outro regime. Porém, o legislador não esclarece qual o regime aplicável nestes casos. Conclui-se contudo que não é “congruente que não seja aplicável o regime geral à contratação eletrónica com intervenção humana, por força do princípio da especialidade, previsto no art.º 7.º, n.º 3, do Código Civil”. Neste sentido, o regime geral é aplicável a toda a contratação eletrónica, salvo derrogação por parte de lei especial.

Assim, e nas palavras de OLIVEIRA DE ASCENSÃO, “toda a vez que a lei contiver uma disposição que se baseie na vontade humana, ela é inaplicável à contratação automatizada, ou pelo menos terá que ser adaptada”, portanto e como teremos ocasião de apreciar infra, cabe fazer uma recondução dos preceitos do regime geral ao programador do computador, quando essas disposições versem sobre a atuação do computador.²⁶

Ora, além da Lei do Comércio Eletrónico e do regime geral do Código Civil, e, porque, na maioria das vezes, a contratação automatizada segue parâmetros rígidos, impondo a contratação nos termos determinados pelo prestador de serviços através de cláusulas contratuais gerais, aplicar-se-á, também o DL n.º 446/85, de 25 de outubro.

2.2.1 Terminologia e construção do conceito “smart contract”

Os contratos sem intervenção humana, por de forma automática executarem os termos do contrato, têm sido referidos como contratos inteligentes ou *smart contracts*. Todavia, esta é uma terminologia suscetível de induzir em erro. Por um lado, Autores há que afirmam que

²⁶ José de Oliveira Ascensão, *Contratação Eletrónica*, in Sep de: *Direito da Informação*, Volume 4 (2003), p.66.

estes contratos não são inteligentes na sua essência.²⁷ Por outro, também os há que duvidam da natureza dos *smart contracts* enquanto verdadeiros contratos.

Quanto à “inteligência” do contrato, em boa verdade, deve dizer-se que os *smart contracts* devem o seu funcionamento ao conjunto de instruções predefinidas no programa informático que seguem, i.e., assentam “na execução de uma ordem programada”^{28,29}.

Com efeito, adoção do termo ‘smart’ (ou inteligente na nossa língua) não envolve necessariamente o recurso à inteligência artificial, mas antes pretende indicar que aquele contrato é dotado de determinadas funções ou capacidades que, devido à sua natureza intrínseca, os contratos ‘tradicionais’ não possuem. Nomeadamente, a possibilidade de proceder autonomamente à cobrança do cumprimento das obrigações das partes.

Deve preferir-se contudo, a justificação mais completa que nos apresenta RORY UNSWORTH, segundo o qual um contrato é inteligente, por ser “capaz” de transformar um código de computador num DLT e executar-se “a si mesmo” tendo em conta determinados dados inseridos na rede. O Autor compara um contrato inteligente a uma folha Excel, cuja fórmula permite que se ajuste automaticamente determinados dados nela inseridos porque é para isso que está programada.³⁰

Em suma, a inteligência do contrato “deve-se” precisamente à sua capacidade para reagir ao estímulo que é a colocação de dados na rede e executar-se a si mesmo.³¹

Por sua vez, discute-se a própria natureza do contrato inteligente enquanto verdadeiro contrato. Vejamos.

Entre nós, tem-se definido um contrato como um “acordo vinculativo, assente sobre duas ou mais declarações de vontade contrapostas mas perfeitamente harmonizáveis entre si, que visam estabelecer uma composição unitária de interesses”.³²

²⁷ David Arroyo Guardado, Jesús Díaz Vico e Luis Hernández Encinas, *Blockchain*, p. 76

²⁸ Hugo Ramos Alves, *Smart contracts: entre a tradição e a inovação*, in *Fintech II - Novos Desafios sobre a Tecnologia Financeira*, p. 196.

²⁹ No mesmo sentido, Riccardo de Caria, *The Legal Meaning of Smartcontracts*.

³⁰ *Smart Contract This! An Assessment of the Contractual Landscape*, in *Legal Tech, Smart Contracts and Blockchain*, p. 20

³¹ David Arroyo Guardado, Jesús Díaz Vico e Luis Hernández Encinas, *Blockchain*, p. 77 e 78

³² Antunes Varela, *Das Obrigações em Geral – Volume I*, p. 212

Em defesa da tese de que não estamos perante verdadeiros contratos, JAVIER JIMÉNEZ entende tratem-se de “meros” mecanismos automáticos de execução de instruções dadas por um programa informático que podem ser pensadas com vista à execução de determinados contratos, não deixando, contudo de ser um ato com consequências legais. De tal maneira que os *smart contracts* podem ser empregues em transações comerciais e civis.³³

Por esta lógica, o *smart contract* seria apenas o meio de execução de um contrato.

Por outro lado, HUGO RAMOS ALVES defende que o *smart contract* deverá ser percebido como um “acordo, vertido em formato digital, autoexecutável e autoimplementável na *blockchain*”, no qual o código informático que traduz os termos contratuais é uma parte ou a totalidade do contrato. Por outras palavras, “o código não constitui um contrato, mas corresponde a um acordo que lhe dá significado e ao qual serve como expressão”³⁴.

Nesta concomitância, o que classificará um *smart contract* como um verdadeiro contrato será o acordo prévio entre as partes, que se traduzirá para uma linguagem informática, binária³⁵. O que acontece é que as partes celebram um contrato em linguagem natural e, nesse mesmo contrato, acordam o recurso a meios de execução autónomos e automáticos.

Aliás, um *smart contract* pode até representar apenas “uma parte” de um contrato. A título de exemplo, um contrato de crédito à habitação pode ser composto por uma cláusula que prevê o ajuste automático do valor da hipoteca em função da taxa de juros de referência. Neste tipo de situações, o *smart contract*, enquanto instrumento através do qual se executam automaticamente determinadas instruções representadas criptograficamente, representa apenas uma parte do contrato e embora implique uma oferta, aceitação e contraprestação, não contém em si programadas questões com vista à resolução de litígios, não identifica a propriedade sobre a qual incide a hipoteca, etc.

De facto, tem-se verificado o uso do termo “smart contract” para duas situações distintas³⁶, o *smart legal contracts* e o *smart contract code*. No primeiro caso, referir-nos-emos a

³³ *Cuestiones jurídicas en torno a la cadena de bloques («blockchain») y a los contratos inteligentes («smart contracts»)*, in *Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, nº 101, 2017, disponível em: <https://revistas.comillas.edu/index.php/revistaicade/article/view/8407>

³⁴ *Smartcontracts: entre a tradição e a inovação, in Fintech II – Novos Estudos sobre a Tecnologia Financeira*, p. 205

³⁵ *Ibidem*, p. 205 e 206

³⁶ Vide Stéphane Blemus, *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*, in *Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review)* RTDF

um verdadeiro contrato no seu sentido legal, com força jurídica. A segunda situação, por sua vez, reporta ao código sob o qual está escrito o *smart legal contract*, que traduz as suas condições e que faz desenrolar a execução do contrato. Enquanto a primeira vertente apura a legalidade do contrato inteligente, a segunda vertente é meramente informática, técnica.

Numa tentativa de incorporar estas duas aceções, STÉPHANO DIVINO define *smart contract* como negócio unilateral ou bilateral, quase inviolável, imperativo, previamente pactuado escrita ou verbalmente, sob a forma de algoritmos e expresso num termo digital que representará *ipsis litteris* o anteriormente acordado, armazenado e executado numa base de dados descentralizada (numa *blockchain*), que irá geri-lo autónoma e automaticamente desde a sua formação à sua extinção, incluindo as condições, os termos, encargos e eventuais despesas judiciais, e sob a aplicação de princípios jurídicos e económicos compatíveis com a relação contratual instaurada.³⁷

RICCARDO CARIA, de forma mais simples, define *smart contract* como qualquer acordo digital, que é escrito num código de computador que se serve da tecnologia *blockchain* ou uma similar tecnologia de “prontuários digitais” e que é automaticamente executado sem qualquer intervenção humana. Consequentemente, o contrato implica um “pedaço de software”, é descentralizado e é inteligente.³⁸

Facto é que a máquina, por muita autonomia que tenha, vai proceder conforme foi programada e vai operar “com o grau de autonomia que na programação lhe tiver sido conferido”, assim, qualquer negócio jurídico celebrado por uma qualquer máquina, terá por de trás de si, a declaração de vontade humana.³⁹

Em função do exposto, entendemos que “apenas será um *vero* contrato – mesmo na hipótese de ambas as partes recorrerem a programação- na eventualidade de ser precedido de um concreto acordo prevendo a sua utilização”⁴⁰.

nº4, dezembro de 2017, disponível em: <https://ssrn.com/abstract=3080639>, v. tbm Hugo Ramos Alves, ob. cit., p. 195 e 196, Eliza Mik, *Smart contracts: terminology, technical limitations and real world complexity*, *Law, Innovation and Technology*, in p. 269-300, disponível em: <https://doi.org/10.1080/17579961.2017.1378468>.

³⁷ Vide *Smartcontracts*, p. 2788 (18)

³⁸ *Ibidem*, p. 737

³⁹ *Ibidem*, p. 423

⁴⁰ Hugo Ramos Alves, ob. cit. p. 205 e 206

2.2.2 Breve enquadramento histórico dos Smart contracts: De Hero aos dias de hoje

Em 1994, NICK SZABO lançava a primeira ideia em torno da construção do conceito de *smart contract*, almejando que, através das emergentes ciências da criptografia e da computação, se viesse a atingir, um dia, a propriedade inteligente⁴¹ e as transações automatizadas, como seriam os pagamentos a baixo custo com grande segurança e confidencialidade.

À altura, o jurista e informático definiu *smart contract* como um protocolo de transação informatizado que executa os termos de um contrato, nomeadamente as condições de pagamento, ónus, confidencialidade e mesmo a execução. SZABO apresentava desde logo, como vantagens a minimização da necessidade de intermediários de confiança, a redução de perdas por fraude, custos de arbitragem e execução.⁴²

Ao mesmo tempo, SZABO fazia uma comparação entre *smart contracts* e as máquinas de vendas automáticas. E se assim for, a origem do *smart contract* remonta a Hero um matemático Grego que, no ano 62 a.C, escreveu sobre uma máquina automática que dispensava água benta nos templos em troca de moedas cujo peso correspondesse ao que estava determinado para a saída da água.

Mas será possível que os contratos inteligentes de que aqui falamos possam ter precedente nas máquinas de venda automáticas? Ao descrevê-las como um “ancestral dos contratos inteligentes”, SZABO olvida que estas nada mais são que a execução de algoritmos pré-programados para libertar o item selecionado quando for inserida uma determinada quantia de dinheiro e introduzido o número correspondente ao produto pretendido. Carecem, portanto, de capacidade técnica para executarem todos os termos da transação, sendo que ainda que possa expor as cláusulas do contrato – muitas vezes em autocolantes no exterior da máquina -, não as conseguirá fazer executar.⁴³

⁴¹ Enquanto propriedade inteligente, Szabo referia-se à incorporação de contratos inteligentes em objetos físicos. Os protocolos incorporados, ou seja, uma representação das condições acordadas do contrato serviriam de orientação ao *software* para dar automaticamente o controlo das chaves de um automóvel por exemplo, ao agente que possui a propriedade por direito, com base nos termos do contrato. Assim, se um empréstimo fosse contratado para comprar o carro e o proprietário não fizesse os pagamentos, o contrato inteligente poderia invocar automaticamente uma garantia, que devolve o controlo das chaves do carro ao banco.

⁴² <https://nakamotoinstitute.org/smart-contracts-glossary/>

⁴³ V. Sthéfano Bruno Santos Divino, *Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios*, in Revista Jurídica Luso-Brasileira, ano 4 (2018), nº 6, http://www.cidp.pt/revistas/rjlb/2018/6/2018_06_2771_2808.pdf

Além do mais, as máquinas de venda automática envolvem sempre uma intervenção manual humana, pelo menos da parte do consumidor, para a inserção da moeda e seleção do produto.

Um ano mais tarde, SZABO desenvolveu o seu conceito de *smart contract*, admitindo que este seria um conjunto de promessas em formato digital, incluindo protocolos que as partes devem cumprir e que são geralmente implementados através de programas de computador.⁴⁴

“Apesar das incontáveis definições trazidas por técnicos e estudiosos da área, a característica intrínseca que SZABO quis dar aos contratos inteligentes e que em grande parte é suprimida na elaboração desses conceitos é a própria essência contratual e capacidade de criar um acordo legalmente exigível”⁴⁵.

2.2.3 Smart insurance products

The Digital Insurer explica a jornada do proponente no processo de celebração um contrato de seguro de habitação automatizado.⁴⁶

Em primeiro lugar, o cliente procura um prestador de serviços de seguro, como tal, acede ao sítio da Internet da seguradora e inscreve-se na sua plataforma com o seu endereço de e-mail, senha e detalhes do seu imóvel. Após a inscrição, recebe uma ordem pública e uma chave privada, que deve guardar. Esta chave é sua exclusiva e é usada para assinar transações ou confirmar acontecimentos importantes.

No momento da inscrição na plataforma, o cliente terá que concordar com os termos e condições aplicáveis, o que pode implicar, nomeadamente, a instalação de um equipamento de deteção de inundação ou incêndio à prova de adulteração.

⁴⁴ <https://nakamotoinstitute.org/smart-contracts-glossary/>

⁴⁵ Idem.

⁴⁶ *Smart insurance Contracts: A discussion paper by Pinsent Masons and Applied Blockchain*
https://www.the-digital-insurer.com/wp-content/uploads/2017/10/980-FinTech_Smart_Insurance_Contracts_Flyer.pdf

Esses dispositivos podem possuir a sua própria chave privada, um localizador GPS, uma câmara embutida e a capacidade de detetar e comunicar o nível da água.

Esses dados são criptografados e armazenados com segurança dentro do *software* do contrato inteligente na rede *blockchain*, como parte da conta do cliente, usando a chave privada do dispositivo.

De seguida, o cliente expressa a sua vontade de receber uma oferta de uma seguradora, e assim solicita um orçamento, permitindo que as seguradoras na plataforma acedam aos seus dispositivos de deteção de inundação e quaisquer informações pessoais que possam influenciar o valor do prémio que vão receber, ou seja, quaisquer informações que são consideradas necessárias à apreciação do risco.

Em vez de fornecer apenas informações básicas, ou muitas informações que não são relevantes para a avaliação do risco, o cliente (através dos dispositivos) disponibiliza informação de forma dinâmica e apenas relativa aos itens específicos de dados que são relevantes e durante o período de tempo exigido pela seguradora para avaliar o risco do cliente e elaborar um orçamento.

O *software* do contrato inteligente celebrado entre a seguradora e o cliente combina todos os dados do cliente com os critérios de avaliação do risco pré-definidos da seguradora, resultando num modelo perfeitamente adaptado ao Cliente que é emitido automaticamente para o cliente pela seguradora.

O cliente seleciona manualmente o seu plano ou, se a plataforma tiver sido projetada para isso, o melhor plano é automaticamente selecionado para o cliente, com base nas suas próprias preferências. O cliente, então, confirma a sua aceitação da oferta, assinando a transação com a sua chave privada *blockchain*. Isso pode até ser feito por meio de autenticação biométrica (como TouchID no iPhone) se a chave estiver armazenada no dispositivo.

Assim que confirmado, o contrato inteligente inicia o débito direto do valor mensal acordado.

Vários meses depois, a casa do cliente é inundada e o sistema faz uma análise automatizada de imagens e dos dados introduzidos e armazenadas na rede *blockchain* diretamente pelo dispositivo. Esses dados com registo de data e hora, juntamente com a localização GPS

constituem uma prova imutável de que o evento de deteção de água ocorreu num determinado dia e hora.

Ao automatizar os pagamentos e garantir que os segurados são pagos na sequência do evento que, tal como ficou firmado no contrato, determinaria o pagamento da indemnização, os contratos inteligentes contribuem para o aumento da confiança entre as partes. Por um lado, as queixas válidas são processadas e pagas automaticamente, e por outro lado, a tecnologia inerente ao contrato inteligente facilita a investigação direcionada, o que permite detetar e negar relatos de sinistros fraudulentos mais facilmente, mormente quando aliados ao bem segurado estão aparelhos sensores, como veremos infra.⁴⁷

3. O contrato de seguro automatizado

O Regime Jurídico do Contrato de Seguro vigente não apresenta uma definição de contrato de seguro, ocupa-se, contudo, de balizar o seu “conteúdo típico” no seu art. 1.º:

“Por efeito do contrato de seguro, o segurador cobre um risco determinado do tomador do seguro ou de outrem, obrigando-se a realizar a prestação convencionada em caso de ocorrência do evento aleatório previsto no contrato, e o tomador do seguro obriga-se a pagar o prémio correspondente”.

É possível observar que a apresentação que o diploma nos faz de contrato de seguro consiste numa “descrição dos traços típicos do contrato de seguro, que, ao mesmo tempo que fornece um argumento legal para a compreensão unitária do tipo contratual, não tem a pretensão de ser exaustiva.”⁴⁸

Na senda de ANTUNES VARELA, concebemos o contrato de seguro enquanto negócio jurídico através do qual uma das partes, a seguradora, se obriga a cobrir o risco que certo facto futuro e incerto, que consiste num sinistro, constitui para a outra parte, o segurado, mediante uma prestação certa e periódica, denominada de “prémio”.⁴⁹

⁴⁷ Vide *Smart Contracts in Insurance...* cit.

⁴⁸ Maria Inês de Oliveira Martins, *Regime Jurídico do Contrato de Seguro em Portugal*, in *Actualidad Jurídica Iberoamericana*, ISSN 2386-4567, IDIBE, núm. 5 ter, dic. 2016, disponível em: <http://www.revista-aji.com/articulos/2016/num6-ter/199-231.pdf>

⁴⁹ *Das Obrigações em Geral*, volume I, 10.^a ed., Almedina Coimbra, 2008, p. 703

Nesta concomitância, constatamos que o contrato de seguro é um contrato aleatório, pois a vantagem patrimonial que dele resulta para cada uma das partes é incerta. Neste caso a aleatoriedade reside no facto de, embora a obrigação principal – a de pagar o prémio - do tomador/segurado seja certa, não o é a do segurador - de indemnizar o segurado *se e quando* ocorra o sinistro (cfr. art. 51.º do RJCS).⁵⁰

Nestes termos, o segurador é a entidade que acolhe o risco a troco de uma remuneração, o prémio. De facto, o contrato de seguro tem como função “a transferência das consequências económicas de um risco – ou seja, de um modo mais explicativo, de transferência das consequências económicas desfavoráveis que um evento incerto é apto a provocar”⁵¹.

Em princípio, esse risco alude à esfera jurídica do tomador, mas poderá incidir sobre uma outra pessoa. Desta feita, a figura do tomador pode não coincidir com a figura do segurado.

Tendencialmente, o contrato de seguro é um contrato de longa duração que pode ser celebrado por um longo período, como o seguro de vida ou celebrado por um ano com possibilidade de renovação.

Pelas características acima enunciadas, o contrato de seguro tem implicado processos lentos e burocráticos, nos quais é crucial a intervenção humana.

Por essa razão também, se tem verificado alguma relutância do setor em explorar as novas tecnologias, embora desde cedo que o legislador comunitário tenha reconhecido a importância dos meios de comunicação à distância como canais de distribuição de produtos e serviços.

A título de exemplo, a Diretiva 97/7/CE que contemplava alguns meios como o correio eletrónico e as televendas, não foi, capaz de prever a sua aplicação no mercado de produtos financeiros, nem considera a possibilidade de surgirem novos meios de comunicação ao longo do tempo.

⁵⁰ Luís Poças, *Problemas e Soluções de Direito dos Seguros*, p. 15

⁵¹ Maria Inês Viana de Oliveira Martins, *Contrato de Seguro e Conduta dos sujeitos ligados ao risco*, Tese de Doutoramento em Ciências Jurídico-Empresariais apresentada à Faculdade de Direito da Universidade de Coimbra, p. 31.

Nas palavras de PAULA RIBEIRO ALVES, os meios elencados no art. 2.º/4 da Diretiva nº 97/7/CE tornaram-se praticamente obsoletos. Talvez por isso, refletindo sobre a possibilidade de celebrar o contrato de seguro de forma automatizada, a Autora conclui que esta via se verifica pouco adequada para a celebração de um contrato como este que está sujeito a tais particularidades.

De facto, o contrato de seguro envolve processos complexos ao longo de toda a relação contratual. Na celebração de um contrato de seguro, enfrentamos várias decisões que carecem de uma ponderação cuidada, como a escolha de cobertura adequada de entre a variedade existente, a apreciação do risco, o volume de informação que deve ser transmitidos de uma parte para a outra justificam a relutância em abandonar a celebração dita “tradicional”, com recurso ao papel. Naturalmente que a automatização do contrato de seguro agrava a dificuldade de contacto entre as partes que é tão importante neste caso.

Em boa verdade, é de concordar com PAULA RIBEIRO ALVES no que toca à execução do contrato de seguro em linha. É que este não poderá ser executado diretamente em linha, porquanto a sua execução passa necessariamente pela realidade, i.e., os acontecimentos que poderão dar origem ao pagamento de uma indemnização ocorrem no mundo real (um incêndio, um acidente rodoviário, etc...). Neste sentido, a construção do sistema que suporta o contrato inteligente tornar-se-á muito mais complexa.⁵²

Como será possível aferir, por ser objeto de desenvolvimento adiante, os contratos inteligentes funcionam com base num sistema de declarações condicionais (“se x, então y”). O contrato inteligente seguro pode ser “redigido” de forma a que se ocorrer um evento previsto no contrato, como a ocorrência de um desastre natural, o sistema despoletará o determinado pagamento de uma determinada quantia pré-definida.

Para tanto será necessário introduzir, no sistema do contrato, a informação da ocorrência desse evento. É essa a tarefa dos “oráculos”. *In casu*, os oráculos podem ser as entidades públicas de dados climáticos.

De tal forma, tem-se fomentado a intervenção de outras partes. Imagine-se que no contrato ficou firmado que a indemnização só seria devida se o veículo fosse reparado em determinada oficina. Nesse caso, as seguradoras podem encarregar os mecânicos de introduzir

⁵² Vide *Contrato de Seguro à distância*, ob. cit., p. 81, em concreto, nota de rodapé 203.

a transação na plataforma *blockchain*, o que despoletará o pagamento do valor devido. Ou, por outro lado, o contrato inteligente pode ser programado para acionar diferentes franquias, dependendo de a reparação ser ou não realizada por determinadas oficinas, com as oficinas a serem obrigadas a introduzir essa informação na rede.

Mas é também possível que as empresas de seguros comecem a conectar-se com outros terceiros como hospitais ou outras autoridades públicas que registariam informações relevantes na rede *blockchain*, para que os prêmios possam ser calculados automaticamente através do código de *software* dos contratos inteligentes, com base na informação fornecida, e.g., o registo dos tratamentos ao paciente ou antecedentes criminais.

Nestes casos, e como se dizia, não se pode dizer que o contrato é completamente automatizado. Na verdade, quantas mais transações estiverem envolvidas, mais longe estamos de um *smart contract*, no sentido em que a execução automática da obrigação de indemnizar vai ser “menos instantânea”.⁵³

Por outro lado, a informação da ocorrência do evento desencadeador da indemnização pode ser introduzida na rede por via da *IoT*.

Uma aplicação interessante dos *smart contracts* é a do reembolso imediato de bilhetes de avião do segurado quando se verifique o cancelamento ou mesmo o atraso do voo, pela intercomunicabilidade da plataforma que alberga a informação dos voos e a plataforma que suporta o contrato.⁵⁴

Na opinião de ANGELO BORSELLI, se todo o contrato for automatizado, e portanto se não se tiver verificado a intervenção humana, a complexidade do contrato e a sua incerteza, levam a que as partes despendam de valores muito mais elevados na previsão de todos os cenários possíveis e na sua tradução para a codificação do *smart contract*, mormente quando são utilizados termos como a “boa-fé”, “diligência” e “razoabilidade”, termos que permitem, com flexibilidade, que as partes tomem em conta as circunstâncias de uma determinada situação, mas que são de difícil tradução para a forma automatizada.

⁵³ Cfr. Borselli A., *Smart Contracts in Insurance: A Law and Futurology Perspective*, in *InsurTech: A Legal and Regulatory View*, disponível em: https://link.springer.com/chapter/10.1007/978-3-030-27386-6_5#citeas

⁵⁴ Este modelo foi implementado pela *startup Insureth* e pela seguradora AXA, baseando a informação do cancelamento do voo, na informação fornecida pelos “nós” confiáveis.

Com base em todo o exposto, concluímos que independentemente de o contrato ser celebrado pessoalmente, *online* ou de maneira mais geral à distância, estará inevitavelmente implícito um contrato tradicional.

3.1A imutabilidade dos *Smart contracts*

Os *smart contracts* têm uma natureza condicional, uma vez que assentam na regra de que o código que foi programado realiza uma ação posterior, de forma automática, com base no que foi configurado, o que se traduz, esquematicamente em declarações condicionais, ou seja, o código é redigido de forma a que se X pagar o valor A, então Y há de conceder-lhe o item B.⁵⁵

Com efeito, é comum o recurso a cláusulas taxativas, de modo a que o contrato seja executado exatamente nos termos em que foi redigido. Nos contratos inteligentes não existe a flexibilidade que é inerente à negociação entre as partes na contratação “tradicional”, estes restringem-se aos procedimentos de liquidação e execução para que foram programados.

Assim, se por algum evento inesperado uma das partes não conseguir cumprir a obrigação a que se propôs, a negociação com a outra parte em nada impede a exequibilidade dos termos das cláusulas, ou seja, verificando-se o incumprimento por uma das partes, o *software* vai automática e imediatamente proceder em conformidade com o que foi programado para a situação de incumprimento.

Embora esta característica da exequibilidade acarrete consigo a vantagem inerente de minimização dos litígios entre os contraentes e a redução significativa (para zero, i.e.) dos custos com vista à execução coerciva do contrato, há que ponderar em que medida se consegue efetivamente pugnar pelo equilíbrio contratual.⁵⁶

Cumpre, então questionar se a desconsideração de eventos exteriores ao contrato leva a que a contratação pela via eletrónica configure uma renúncia ao direito à revisão contratual, à cláusula *rebus sic standibus*.⁵⁷

⁵⁵ Sthéfano Bruno Santos Divino, *Smart Contracts...*

⁵⁶ Diferentemente do que considera Javier W. Ibáñez Jiménez, *Cuestiones...* ob. cit.

⁵⁷ Esta máxima configura uma exceção ao princípio *pacta sunt servanda*, e pugna pela manutenção do contrato enquanto as circunstâncias se mantêm iguais, ou seja, desde que mantidas as mesmas condições quando da celebração do contrato para todas as partes envolvidas. Ora, havendo excessiva onerosidade para uma das partes, poderá o referido contrato ser revisto e ter alteradas suas cláusulas, visando manter-se o equilíbrio idêntico ao do momento em que o contrato foi firmado.

Naturalmente que a alteração do contrato, na eventualidade de ser impossível proceder ao cumprimento, e com acordo das partes, é possível. Porém, para modificar um contrato inteligente, é necessário atravessar um processo muito demorado e com um custo muito alto, quando um contrato dito tradicional poderia ser alterado verbalmente, fortalecendo até as relações de confiança entre as partes.

A título de exemplo, os *smart contracts* poderão ser comparados a caixas hermeticamente fechadas. Para que possam ser abertos (modificados) serão necessárias uma ou mais chaves, mas que são isoladas do mundo exterior, isto porque as transações dependem de uma chave criptografada pública, que ela própria é composta por uma chave pública e outra particular que são geradas juntamente através de um algoritmo e que “garantirá a independência e ausência de conexão entre a chave pública e a privada”⁵⁸. A chave pública funciona, então, como um número de conta bancária que permanece público aguardando a solicitação para uma transação. A chave privada funcionará como um PIN, uma senha. Assim, sendo enviada a solicitação para transigir para a chave pública, apenas a pessoa com acesso à chave privada poderá ter acesso a esse convite.

É indubitavelmente um ponto negativo em comparação com os contratos tradicionais. Atente-se, contudo, que não se critica, naturalmente, o postulado pelo princípio *pacta sunt servanda*⁵⁹, mas antes a “sua dura inflexibilidade e poder de atuação nos *smart contracts*”.⁶⁰

Parece, pois, que a adesão ao *smart contract* consubstancia uma renúncia tácita ao direito de revisão contratual extrajudicial.

Assim, de modo a evitar estas situações, impõe-se que, as partes, prevejam e traduzam para o contrato o maior número de hipotéticas situações para que o próprio *software* possa considerar esses eventos. Afigura-se, contudo, muito difícil que, a “redação” de um contrato no código que será lido pelo computador preveja todas as situações suscetíveis de influenciarem o cumprimento das obrigações.

⁵⁸ Eliza Mik, *Smart contracts: terminology, technical limitations and real world complexity*, in *Law, Innovation and Technology*, 9:2, 269-300, disponível em: <https://doi.org/10.1080/17579961.2017.1378468>

⁵⁹ Este princípio explica a força vinculativa do contrato e a regra da imodificabilidade do contrato de forma unilateral, servindo de proteção das legítimas expectativas das partes. Este princípio estabelece que os sujeitos devem cumprir pontualmente o contrato a que se vincularam voluntariamente e que, em regra, o contrato é imodificável por vontade de apenas um dos contraentes. Vide Antunes Varela, *Das Obrigações em Geral – Volume I*, p. 227

⁶⁰ *Smart contracts*...cit, p. 31.

Por outro lado, as partes podem, *a priori* inserir, no contrato, uma operação para os casos em que seja necessária essa renegociação. Ainda assim esta não se verifica uma situação ideal, pois apenas se verifica a transladação dos custos de uma fase para o momento anterior e não a sua minimização.

Por outro lado ainda, impõem-se um grande cuidado na linguagem a usar no código do *smart contract*. É impossível “representar de forma equivalente a transcrição de determinadas aceções conceituais e termos jurídicos específicos na linguagem computacional”, a título de exemplo, as expressões “boa-fé” e “razoável” requerem que sejam incrivelmente detalhadas quando traduzidas para linguagem informatizada que apenas faz executar ações de forma taxativa. Por outro lado, poderá ser necessário criar um programa que seja capaz de ler, i.e., interpretar as “nuances da linguagem jurídica”.⁶¹

Em consequência, a linguagem acaba por ter que ser ambígua, o que permite alguma flexibilidade no que toca ao cumprimento e na execução contratual, pois possibilita a avaliação do comportamento da parte contrária e a reação da outra parte sem ter que alterar o acordo feito ou ter que celebrar um novo.

Vejamos. Geralmente, no caso de não cumprimento por uma das partes, é possível arguir a exceção de não cumprimento (*exceptio non adimpleti contractus*).

A exceção de não cumprimento do contrato encontra-se prevista no art. 428.º do CCiv, cujo n.º 1 estabelece que “se nos contratos bilaterais não houver prazos diferentes para o cumprimento das prestações, cada um dos contraentes tem a faculdade de recusar a sua prestação enquanto o outro não efetuar a que lhe cabe ou não oferecer o seu cumprimento simultâneo”.

Nestes termos, é atribuída a qualquer das partes a faculdade de recusar realizar a sua prestação enquanto a contraparte não efetuar a que lhe compete.

A exceção de não cumprimento do contrato não nega o direito ao cumprimento da prestação nem afasta o dever de a cumprir, consagrando-se apenas o efeito dilatatório de um dos

⁶¹ Sobre o processo de criação e transformação de um contrato “tradicional” num contrato inteligente, vide *Smartcontract this! An assessment of the contractual landscape* e Sthéfano Bruno Santos Divino, *Smart Contracts*, p. 25 e ss

contraentes realizar a sua prestação em momento posterior, isto é, quando receber a contra-prestação a que tem direito.

Isto porque, cada uma das partes assume obrigações tendo em vista as obrigações da outra parte. Ora, se uma das partes pudesse exigir o cumprimento da outra parte sem ter cumprido a sua prestação, romper-se-ia o equilíbrio contratual, que assenta na reciprocidade entre as obrigações.

Note-se que mesmo estando o cumprimento das obrigações sujeito a prazos diferentes, a exceção de não cumprimento do contrato poderá ser sempre invocada pelo contraente cuja prestação deva ser efetuada depois da do outro, apenas não podendo ser oposta pelo contraente que deva cumprir primeiro.

Contudo, no caso em que a execução do contrato se dá de forma automática, não há espaço para o incumprimento. Assim, surge a questão de saber se a celebração de um contrato com recurso aos *smart contracts* implica ou não uma renúncia à *exceptio non adimpleti contractus*.

Pode parecer que sim, mas analisando questão, concluímos pela negativa. No âmbito do contrato inteligente, a execução automática é uma resposta a um evento (verificando-se o pagamento do valor X, o contrato executará a ordem correspondente, a entrega do bem). Segundo MARINA SÁENZ, o que a parte renúncia é o "direito de violar", seja qual for a situação em que se encontra no mundo real.⁶²

Todos os factos que impossibilitem o cumprimento da obrigação e que sejam suscetíveis de afetarem a justiça contratual e que sejam supervenientes à confirmação de uma obrigação contratual já realizada serão irrelevantes para o sistema executor do contrato, pois uma vez autenticado, a *Blockchain* deverá executar a próxima ordem, só podendo tomar em consideração fatores exteriores através de uma alteração contratual.

⁶² Apud Sthéfano Bruno Santos Divino, *Smart Contracts: Conceitos...ob. cit.*

3.2 Smart contracts e blockchain

3.2.1 Distributed Ledger Technologies e Blockchain

3.2.1.1 Noção

A tecnologia *Blockchain* recebe notoriedade com a introdução, no mercado, da criptomoeda *Bitcoin*, sendo que era através daquela que esta era emitida.

Hoje a *Blockchain* acolhe inúmeras aplicações, suscitando novas e complexas questões.

Blockchain, o vocábulo que é literalmente traduzido como corrente de blocos, diz respeito à tecnologia comumente conhecida como uma espécie de “prontuário digital ou eletrônico” onde estão registados dados e transações de vários tipos e que pode ser acessado através de um computador⁶³.

É, por isto, muitas vezes confundida com a própria tecnologia de registos distribuídos ou *Distributed Ledger Technologies* (doravante DLT). No entanto, estas não coincidem. Na verdade, todas as tecnologias *Blockchain* são tecnologias DLT, mas nem todas as tecnologias DLT são tecnologias *Blockchain*. A *Blockchain* configura assim um tipo de DLT, com a particularidade de armazenar os seus dados na forma de uma corrente de blocos.

Por outro lado, a DLT consiste numa tecnologia digital de registos, cujos dados relativos a várias transações são armazenados, protegidos e validados. Estes dados são disseminados por vários participantes da rede, “os nós”⁶⁴, sem intervenção de uma qualquer entidade centralizada. Todos os nós recebem cópias idênticas dos dados transcritos, pelo que a tecnologia dos registos descentralizados, no geral, assenta num sistema de “livro razão”, que é “descentralizado, aberto e público”⁶⁵, como teremos oportunidade de analisar.

⁶³ Descreve-a assim a Goldman Sachs, no seu artigo *Blockchain – The New technology of Trust*, disponível em <https://www.goldmansachs.com/insights/pages/blockchain/index.html> e o Financial Times em *Blockchain believers hold fast to a utopian vision*, disponível em <https://www.ft.com/content/a12d7476-bc6a-11e6-8b45-b8b81dd5d080>

⁶⁴ Estes utilizadores são identificados por uma “direção”, uma morada na rede e uma chave secreta, podendo ser baseadas em pseudónimos, como nas redes *Bitcoin* e *Ethereum*. Cfr. Pedro J. Ponce de León, *Blockchain, un nuevo patrón tecnológico*, in *Blockchain: aspectos tecnológicos, empresariales y legales*, p. 36 e 37.

⁶⁵ Vide Daniel Augusto de Senna Fernandes Batalha, *Criptocontratação – Uma nova forma de contratação automatizada* e Javier Wenceslao Ibañez Jiménez, *Blockchain: primeras cuestiones en el ordenamiento español*, p. 15 e 16

Tem-se revelado extremamente difícil encontrar uma noção de *Blockchain*, pois esta não é uma “descrição ou definição monolítica”.⁶⁶

O Parlamento Europeu, reconhecendo o potencial de aplicação das DLT transversalmente a vários mercados, assume que a falta de conhecimento sobre o potencial das DLT desencoraja o recurso às mesmas. Entre as aplicações mencionadas, destacam-se o potencial para o registo e administração de veículos, a verificação das distâncias percorridas, os seguros inteligentes, o intercâmbio e interoperabilidade de dados de saúde, a verificação da identidade e a distribuição de medicamentos, bem como, no que diz respeito à utilização de dados pelas companhias de seguros, permitir aos segurados selecionar que dados partilhar.

De modo a incentivar o desenvolvimento e utilização das DLT na Europa, o Parlamento Europeu defende que um qualquer processo legislativo desta matéria deve “ser favorável à inovação, permitir um sistema de passaporte e pautar-se pelos princípios da neutralidade tecnológica e da neutralidade do modelo empresarial”. Para tal, defende a formação das autoridades nacionais de modo a que estas adquiram competências técnicas especializadas e recomenda a promoção, pela Comissão, de iniciativas relacionadas com as DLT.

O PE sublinha ainda que “a União não deve regulamentar as DLT *per se*, mas que deve procurar eliminar os atuais obstáculos à implementação de cadeias de blocos”.⁶⁷

Observemos, então, as suas características.

3.2.1.2 Características da tecnologia *Blockchain*

I. Segurança

O funcionamento da tecnologia *Blockchain* desdobra-se em várias fases. Num primeiro momento, ocorre a recolha, organização e compilação da informação relativa a determinada transação⁶⁸, que é registada e partilhada com os restantes nós presentes na rede. De seguida,

⁶⁶ Nomeadamente, foi graças à descentralização do registo de titularidade inerente à tecnologia *Blockchain* que se resolveu o problema da dupla alienação (double spending). Vide Francisco Mendes Correia, *A tecnologia descentralizada de registo de dados (Blockchain) no setor financeiro*, in *Fintech – Desafios da Tecnologia Financeira*, p. 83 e 84 e Robert Heiran, *Regulating Blockchain*, p. 16

⁶⁷ Vide *Resolução do Parlamento Europeu, de 3 de outubro de 2018, sobre tecnologias de cadeia de blocos e aplicações de cifragem progressiva: reforçar a confiança através da desintermediação (2017/2772(RSP))*, disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_PT.html

⁶⁸ Como transação entende-se qualquer intercâmbio de valor entre dois usuários, desde uma transferência monetária, até à transferência de dados. V. *Goldmansachs*

as transações vão ser “arrumadas” num bloco, a que será aposto um “selo temporal”, com indicação da hora da transação. Desta forma, a informação é colocada sequencialmente, evitando entradas duplas.⁶⁹

De seguida, e através da criptografia⁷⁰, os blocos são alinhados e acrescentados à corrente. Cada bloco é representado por um *hash*, uma direção digital⁷¹, que é formado cada vez que os dados de uma transação são adicionados. Assim, cada novo bloco é representado por um novo *hash* que contém o *hash* anterior, sendo dependentes dos dados das transações anteriores.⁷²

Ao operar desta forma, torna-se a tecnologia da *Blockchain* resistente a alterações da informação introduzida. Para que se fizesse uma alteração, seria necessário chegar ao bloco com a informação que se pretende alterar e alterar todos os *hashes* inseridos nos blocos posteriores àquele com a nova informação.

Isso implica que o nó tivesse que enviar todos esses blocos novos para toda a rede e que estes fossem aceites por todos os restantes utilizadores/nós, os seus *peers*. Sendo assim, não basta simplesmente recolocar o bloco na rede, pois a rede reconheceria que aquela nova corrente de informação não é válida, uma vez não corresponder àqueles blocos que já tinham sido autenticados.

Para culminar, o funcionamento da *Blockchain* revela-se um meio seguro de manter informação face ao ataque dos *hackers*. Mesmo um ataque informático, ao ser operado contra apenas um dos nós, tornar-se-á ineficaz, por via da necessidade de consenso entre vários deles. Como a falsificação de uma única cópia da *blockchain* num dos nós não faz sentido, seria necessário que um ataque ganhasse o controlo de mais de 50% do poder dos nós.⁷³

⁶⁹ Goldman Sachs.... cit. Presume-se que a informação foi introduzida naquele dia àquela hora (art. 3.º/33 e 34 e 41.º do eIDAS).

⁷⁰ O uso da criptografia permite que a informação seja “incrustada” e posteriormente possa ser aberta e relida e de forma mais segura. Todos os dados aparecem em todos os nós simultaneamente e de forma necessariamente idêntica para todos os servidores conectados.

⁷¹ Um *hash* é uma expressão alfanumérica das funções criptográficas gerada automaticamente e aleatoriamente.

⁷² *Blockchain: primeras cuestiones...*, p. 21

⁷³ Isto porque, como se constatará já no próximo ponto, o registo de dados e transações funciona através de consenso. Joachim Schrey e Thomas Thalhofer, *Rechtliche Aspekte der Blockchain*, in *Neue Juristische Wochenschrift*, vol. 70, n.º 20, 2017, p. 1432

Desta forma, a tecnologia *Blockchain* prima pela segurança e imutabilidade da informação que alberga e funciona como uma garantia contra fraudes nos seguros ou qualquer tipo de manipulação de dados e informações.

Ademais, a *Blockchain* pode ser um mecanismo muito útil às seguradoras. O cruzamento de dados previamente registados na rede de forma imutável pode ajudar a identificar padrões de comportamento fraudulento de transações anteriores por parte de determinados utilizadores. Vejamos: uma vez que as informações são introduzidas de forma imutável na rede, é possível avaliar todo o historial de transações do participante, ainda na fase de negociação. Além disso, a rede *Blockchain* funciona como um registo de auditoria permanente dos dados necessários para a avaliação de sinistros e serve de suporte à implementação e desenvolvimento dos contratos inteligentes, no sentido em que é o instrumento onde se vão registar todas as transações inerentes ao cumprimento do contrato (os pagamentos realizados, a ocorrência do sinistro...). Ora, o cruzamento de dados, nomeadamente daqueles que são recolhidos em tempo real, contribui para otimizar a eficiência do contrato, agilizando todo processo de avaliação do sinistro, desde a queixa até ao pagamento.

II. Registo descentralizado e Consenso da rede

A tecnologia *Blockchain*, como referido, é uma tecnologia descentralizada, na medida em que prescinde de uma identidade central responsável hierarquicamente superior.

As redes *Blockchain* distinguem-se pela sua forma de organização. Existem redes de *Blockchain* públicas (ou *permissionless*) e redes privadas (ou *permissioned*).

Nas redes *permissionless*, todo o trabalho de mineração dos dados na rede *Blockchain* é operado pelos nós, i.e., os próprios utilizadores da rede que podem entrar livremente no sistema, sem qualquer restrição.

Por sua vez, as redes *permissioned*, assentando na confiança entre as partes, conferem aos nós dominantes na rede a possibilidade de escolher os novos nós intervenientes. Estas são frequentemente usadas no setor financeiro, pois conferem maior segurança aos registos.

Não obstante, a todas as redes *blockchain*, é comum o recurso a protocolos de consenso, que consistem na concordância entre os vários intervenientes em relação aos registos efetuados. Estes mecanismos são usados para garantir comportamentos honestos por parte dos nós, evitar a colocação ou adulteração de informações na rede e portanto garantir a validade

das transações registadas, funcionando ainda como forma de compensar o utilizador pelo trabalho de computação desempenhado.

Entre os vários sistemas usados, devem referir-se os dois mais comuns: os mecanismos de prova de trabalho (*proof of work*) e os de prova de interesse (*proof of stake*). Nas redes *permissionless*, funciona usualmente, o protocolo de consenso *proof of work*, no qual os nós são compensados com base no trabalho de computação desempenhado, premiando-se o primeiro nó a resolver a função matemática que permite introduzir um novo *hash* e a criar um novo bloco.

Por sua vez, redes privadas como a Ethereum baseiam os seus protocolos de consenso no sistema de *proof of stake*. Nestes, o utilizador é sorteado para introduzir os dados, sendo que os nós com mais blocos criados têm maior probabilidade de ser eleitos e criar novos blocos.⁷⁴ Este sistema parte do princípio de que quem tem depositado mais interesse e tem realizado mais operações no sistema, provavelmente tem mais motivos para querer garantir o seu correto funcionamento, sendo mais confiável. Este interesse traduzir-se-á numa moeda interna do sistema *blockchain* em questão.⁷⁵

Atente-se ainda que só se permitirá a introdução de um bloco se for feita por um nó cujas transações sejam todas válidas, e cujas assinaturas eletrónicas envolvidas sejam válidas.

Assim, a validade dos registos decorre da coerência entre as inscrições individuais de cada membro. “Uma vez atingido [o] consenso multilateral, a nova informação é acrescentada à base de dados, e a partir daí não pode ser alterada ou eliminada, senão com base num novo consenso”⁷⁶.

Neste sentido, o consenso é não mais do que o efeito prático de cada adição de dados.⁷⁷

⁷⁴ Cfr. *Blockchain : aspetos tecnologicos, empresariales y legales*, p. 53-59, vide também David Arroyo Guardado, Jesús Diaz Vico... *Blockchain*, p. 86 e 87

⁷⁵ Este sistema foi proposto, pela primeira vez Cynthia Dwork, em 1992, como parte de uma solução para o correio eletrónico *spam*. Para consultar a exposição da Autora, vide <http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf>

⁷⁶ Francisco Mendes Correia, *A tecnologia descentralizada de registo de dados (Blockchain) no setor financeiro*, in *FinTech: Desafios da Tecnologia Financeira*, p.85

⁷⁷ Javier Wenceslao Ibañez Jiménez, *Blockchain, primeras cuestiones en el ordenamiento español*, p. 2

Estas características “tornam os *Blockchain* especialmente robustos e resistentes a tentativas de corrupção de dados, oferecendo assim um grau muito considerável de (imutabilidade e) fiabilidade da informação”.⁷⁸

III. Dependência à *blockchain*

O recente crescimento e interesse pelos *smart contracts* é, em grande, parte devido ao seu desenvolvimento através da tecnologia *blockchain*, que proporciona o mecanismo de execução automática das condições do contrato.

Tal como alude HUGO RAMOS ALVES, a *blockchain* é o habitat natural do *smart contract*, ainda que seja possível que este “ganhe vida fora da *blockchain*”, este é o “ambiente suscetível de promover o seu desenvolvimento”^{79, 80}

É, como vimos, característico do funcionamento das cadeias de *blockchain*, que as informações introduzidas sejam imutáveis. Assim, a *blockchain* apresenta-se como ferramenta fundamental para garantir o integral cumprimento de qualquer acordo. Neste sentido, o contrato inteligente concretiza-se enquanto postulado do princípio *pacta sunt servanda*. A natureza dos *smart contracts* impede o incumprimento da obrigação a que cada uma das partes está adstrita, uma vez que a execução da obrigação se dá automática e autonomamente, sendo impossível interromper esse ato de execução da obrigação.

Na circunstância de uma das partes estar perante algum evento imprevisível ou mesmo numa situação que é, para si, excessivamente onerosa, esta só pode modificar ou procurar adaptar o contrato, o que é, só por si, muito dispendioso ou recorrer aos Tribunais. Não obstante, tal como remata STÉPHANO DIVINO, “ainda que os custos dessa [via] possam ser menores, seriam incomparáveis com as modificações e alterações extrajudiciais que poderiam ser realizadas em um contrato não inteligente”.

⁷⁸ *A Tecnologia Descentralizada de Registo de Dados*, p.85

⁷⁹ *Ob. cit.*, p.198 e 199

⁸⁰ Até no Relatório de setembro de 2019, o EU Blockchain Observatory and Forum, perceciona os contratos inteligentes à luz da *blockchain*, entendendo que estes se traduzem num código de computador armazenado numa rede *blockchain* e que pode ser acedido por uma ou mais partes. Esses programas geralmente são auto-executáveis e fazem uso de propriedades das *blockchain*, o que permite a resistência a violações, processamento descentralizado e similares, disponível em: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

A Ethereum foi a primeira plataforma *blockchain* desenhada para a celebração destes tipos de contratos, especificamente, a Ethereum é um sistema descentralizado no qual os nós, i.e., computadores ou usuários que o compõem comunicam, formando uma rede P2P, na qual estes se encontram “de igual para igual”, sendo, por isso, um sistema descentralizado, à semelhança do que acontece com a Bitcoin.

O contrato documentado na *blockchain* por meio da criptografia e o próprio contrato inteligente são, por si, eletrônicos por natureza e podem ser concluídos como contratos solenes, na medida em que não prejudiquem o cumprimento da função legal que normalmente executa a forma contratual no suporte por escrito, i.e., o facto de a instrumentação do conteúdo contratual ser feita pela transmissão de dados na rede não é uma razão substancial para conceder ao negócio uma classificação legal mais baixa, assim como discriminar ou limitar sua eficácia por motivos de insuficiência formal, previsto no art. 33.º da LCE.

Não obstante esta indeterminação quanto à natureza dos contratos inteligentes, é desde logo possível perceber as vantagens que lhes são adjacentes. Desde já, revelam-se particularmente convenientes quando se pretendem implementar medidas coercitivas, nomeadamente penalizações como sanções pecuniárias compulsórias, se estiverem previstas no contrato e em caso de violação das cláusulas.⁸¹

Em vez de simplesmente esperar que as partes se rejam pelo princípio da boa-fé, cumprindo as suas obrigações, os contratos inteligentes são concebidos, de forma a se atinja o cumprimento integral do contrato e se garanta o cumprimento das legítimas expectativas das partes.

Por outro lado, estes contratos também não se concretizam meramente no plano digital. Aliás, como diz MARIA INÊS DE OLIVEIRA MARTINS, “o risco e a sua transformação de mera possibilidade em efetividade decorrem, pois no mundo-da-vida: é neste plano que decorrem os processos cuja proteção dá sentido ao contrato”⁸². Se um contrato inteligente condiciona o pagamento à ocorrência de um evento exterior ao mundo virtual, será necessário envolver um terceiro, um oráculo, que reconheça a ocorrência ou não do evento. Esses

⁸¹ Javier Jiménez, *Cuestiones jurídicas*, p. 3

⁸² *Contrato de Seguro e condutas dos sujeitos ligados ao risco*, p. 32.

terceiros, os chamados “oráculos”, que dispõem de uma chave privada para tal, introduzem um *script* quando um evento fora da cadeia é estabelecido como verdadeiro.

3.2.2 Desafios legais da contratação automatizada

3.2.2.1 Requisitos formais do contrato de seguro

Embora o RJCS não faça depender a validade do contrato de seguro da observância de forma especial, estatui, no seu art. 32.º/2 a obrigatoriedade de o segurador formalizar o contrato num instrumento escrito, a apólice do seguro e entrega-la ao tomador de seguro.

O art. 34.º do mesmo diploma acrescenta que se houver acordo entre as partes nesse sentido, o segurador pode entregar a apólice ao tomador em suporte eletrónico duradouro, sem prejuízo de o segurado pedir que a mesma seja entregue em papel.

Por suporte duradouro, entende-se “aquele que permita armazenar a informação dirigida pessoalmente ao consumidor, possibilitando no futuro, durante o período de tempo adequado aos fins a que a informação se destina, um acesso fácil à mesma e a sua reprodução inalterada” (art. 11.º/5 do DL n.º 95/2006), podendo ser uma chave Universal Serial Bus (USB), um CD-ROM, um DVD, um cartão de memória ou um disco rígido de computador, desde que tal permita ao consumidor ou ao fornecedor de bens ou prestador do serviço armazenar informações que lhe sejam pessoalmente dirigidas, e, mais tarde, aceder-lhes pelo tempo adequado à finalidade das informações, e que possibilite a respetiva reprodução inalterada. Naturalmente que a apólice deve cumprir as menções obrigatórias expressas no art. 37.º do RJCS, acrescido da necessidade de cumprimento do dever de informação do segurador ou dever de esclarecimento das cláusulas do contrato, conforme dita o art. 18.º.

É já claro que a apólice pode ser transmitida ao segurado através de correio eletrónico, desta forma ficando preenchida a necessidade de entrega da apólice em formato duradouro. Naturalmente que a apólice deve chegar ao segurado já assinada, carimbada e datada.⁸³

Neste ensejo, cumpre indagar sobre o valor jurídico do código de computador que representa o contrato, o que implica necessariamente recordar que vigora entre nós o princípio da admissibilidade e equiparação dos contratos eletrónicos aos contratos celebrados pela via

⁸³ Vide Paula Ribeiro Alves, *Contrato de Seguro...* ob. cit., p. 169.

eletrónica, segundo o qual as declarações eletrónicas equiparam-se às declarações automatizadas.

Assim, sempre que seja exigida a forma escrita para uma declaração eletrónica, esta exigência considera-se satisfeita sempre que o seu conteúdo seja suscetível de representação como declaração escrita.⁸⁴

A utilização de um aparelho sofisticado “não implica uma rejeição dos princípios voluntaristas subjacentes à autodeterminação e à autonomia privada, nem impede que o ato material levado a cabo pelo computador deva ser juridicamente considerado um ato do explorador do autómato”.

Pode, desta sorte, concluir-se que “a declaração automatizada é uma autêntica declaração de vontade e o fundamento da vinculação do utilizador do computador pela declaração automatizada emitida é a sua vontade, expressa na programação”⁸⁵.

Neste sentido, a contratação eletrónica automatizada tem por base uma vontade negocial que se “exprime em moldes diversos”, “exprime-se fundamentalmente na programação da máquina e na sua preparação para a emissão de declarações negociais”⁸⁶.

Acontece, porém, que no *smart contract*, o contrato (assim como outros atos necessários à execução do contrato) é inscrito e assinado eletronicamente na plataforma. Ademais, o remetente da declaração negocial emitida não corresponde verdadeiramente ao autor da mensagem⁸⁷.

⁸⁴ Paula Costa e Silva, *A contratação automatizada*, p. 300

⁸⁵ “Significa isto que em última análise, a declaração automatizada pode ser sempre reconduzida a uma vontade negocial humana, expressa na programação da máquina, sendo os aparelhos eletrónicos apenas formas sofisticadas de prolongamento da vontade humana”.

⁸⁶ *Idem*, p. 420

⁸⁷ Há autores que negam a natureza de declarações negociais às declarações automatizadas, isto porque são manifestadas por um computador, que não é dotado de autodeterminação. Entende contudo, a doutrina maioritária que estamos efetivamente perante verdadeiras declarações de vontade, emitidas por aquilo que David de Oliveira Festas apelida de “sistemas complexos de manifestação de vontade negocial”, no sentido em que a declaração automatizada é “reconduzida à vontade do seu utilizador”, é-lhe imputada. Nesta concomitância, a vontade negocial não é contemporânea à celebração do negócio jurídico, i. e., ela foi previamente expressa “através da programação da máquina”, uma vez que a intervenção humana não se verifica no momento da celebração do negócio jurídico, mas sim previamente, aquando da escolha, reparação e programação do equipamento eletrónico, o meio de emissão das declarações negociais”. Por outras palavras, declaração negocial emitida pela máquina representa a vontade negocial de alguém, i. e., “a declaração emitida pela máquina tem um autor: o programador, funcionando o autómato como uma longa *manus* da vontade humana” e o computador funciona como mero um meio de veicular a vontade do contraente. Vide Hugo Ramos Alves, *Smart contracts...* cit, p. 193.

Ora, o art. 3.º, n.º 1 do Decreto-Lei n.º 290-D/99, de 2 de agosto (doravante RJDEAD) prevê a satisfação do requisito legal de forma escrita dos documentos eletrônicos quando o seu conteúdo seja suscetível de representação como declaração escrita⁸⁸.

Por esta razão, torna-se patente que não é possível prescindir do contrato “tradicional”, seja ele celebrado através de meios eletrônicos ou não, pois o código de *software* que constitui o *smart contract* não é suficiente enquanto instrumento regulador do contrato.

A contratação eletrónica torna-se assim, muito impessoal. A carência de uma relação de confiança entre as partes impõe o recurso a mecanismos que nos permitam confirmar a identidade da pessoa com quem pretendemos contratar. Por isso é usada a assinatura eletrónica, cujo regime está consagrado no RJDEAD⁸⁹.

Ora, a assinatura eletrónica pode ser concretizada de diversas formas. O código secreto consiste na combinação de algarismos ou letras que constitui um PIN. Este PIN é usado em conjunto com um cartão magnético. A assinatura digitalizada consiste numa digitalização da assinatura do autor copiada para os documentos eletrónicos. A chave biométrica baseia-se no reconhecimento de características físicas do indivíduo, tais como impressões digitais, face, íris do olho, etc., por um equipamento que identifique o seu titular. Por fim, a assinatura digital ou criptográfica divide-se em duas modalidades: a criptografia simétrica com chave única diz respeito a uma chave que funciona para o emitente e recetor da mensagem e que serve para codificá-la e descodificá-la; a criptografia assimétrica com chave pública ou assinatura digital em sentido restrito utiliza uma chave pública e uma chave privada. Introduzindo-se uma mensagem no sistema, este gera um selo eletrónico que é acrescentado a uma mensagem e que gera e atribui uma chave pública e uma chave privada ao titular.

Quando assina um documento, o titular utiliza a sua chave privada e o destinatário vai verificar essa assinatura através da chave pública correspondente, que será compatível apenas se tiver sido gerada em conjunto com a chave privada.

⁸⁸ Por sua vez, a força probatória do documento eletrónico será distinta conforme seja aposta (i) uma assinatura eletrónica simples ou avançada, caso em que os documentos eletrónicos serão apreciados nos termos gerais do direito ou uma assinatura eletrónica qualificada ou assinatura digital: situação em que passam a funcionar as presunções de autoria, vontade e inalterabilidade previstas nas als. a) a c) do n.º 1 do art.º 7.º do RJDEAD.

⁸⁹ *Ibidem*, p. 299 e 300

Ao utilizar a assinatura eletrónica atribui-se-lhe o mesmo valor legal que uma assinatura manuscrita consoante a assinatura eletrónica que se use. Para tanto, deve a assinatura eletrónica ser qualificada nos termos do art. 7.º do RJDEAD, descritos acima.

Por outro lado, o recurso à *Blockchain*, como vimos, permite a aposição de um selo de tempo aos atos eletrónicos introduzidos na rede. A aposição de uma data a um documento eletrónico está prevista na al. u) do art.º 2.º do RJDEAD. Neste sentido, segundo DANIEL BATALHA, se o documento eletrónico contiver uma assinatura eletrónica qualificada, a sua expedição poderá ser equiparada à carta registada, quando seja feita por via de telecomunicação que assegure a sua efetiva receção. Por outro lado, se à receção corresponder o envio de uma mensagem de confirmação subscrita com assinatura eletrónica qualificada e dirigida ao remetente, equivalerá à carta registada com aviso de receção.⁹⁰

Por sua vez, o selo temporal aparece regulado nos arts. 3.º, n.ºs 33 e 34, e 41.º e ss do ReIDAS⁹¹, que preveem que, com a sua aposição, opera a presunção legal da exatidão da data e hora em que se produz a transação e a presunção de confiança na assinatura eletrónica e na sua segurança, integridade, completude e imutabilidade dos dados registados, não lhe podendo ser negados efeitos jurídicos.

Por fim, o próprio conceito de transação passa a significar uma série de operações técnicas na rede e não necessariamente a celebração de um negócio jurídico. Neste sentido, a introdução da comunicação de um sinistro consubstancia, em si, uma transação.

4. *Big Data*⁹² e Internet das Coisas (*IoT*)

A *Big Data* tem sido explicada como o conjunto de informação em larga escala compreendida em três dimensões, “três V’s”: volume, englobando o volume de dados gerados a cada segundo; variedade, uma vez que a informação recolhida provem de diferentes fontes;

⁹⁰ Ob. cit.

⁹¹ Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

⁹² De novo, é utilizada uma expressão inglesa, por ser não se verificar tão frequentes as traduções do termo para a nossa língua (como são os “megadados” ou “dados em massa”). Similarmente, e tal como Ana Alves Leal, iremos adereçar o artigo definindo “a” para nos referirmos à tecnologia, e todos os processos que engloba (a *Big Data*). Por outro lado, sempre que for necessário referirmo-nos aos dados incluídos, utilizaremos o artigo definido “os” (os *Big Data*). Vide p. 94, em particular nota 13.

e velocidade de atualização, já que o conteúdo dos dados está a ser recolhido de forma constante.⁹³

Já mais tarde foram identificadas as dimensões da veracidade e do valor, isto porque muita da informação que está à disponibilidade das empresas não é verdadeira e carece de filtração.

Só mais recentemente é que se verificou que a informação sofre atualizações ao longo do tempo, o que implica também a atualização das análises feitas à informação. Resulta assim um total de “sete V’s”, os que caracterizam a *Big Data*, juntando-se aos já supracitados, a Variabilidade e a Visualização.⁹⁴

O conjunto de dados que constitui a *Big Data* é o resultado da utilização de dispositivos ligados à Internet⁹⁵ e da navegação na Internet através de um *browser*, correspondendo a um rasto de dados deixado pelo utilizador que serão armazenados e processados por uma determinada entidade.

O grande objetivo do tratamento de dados pela *Big Data* reside na dedução de conclusões a partir dos dados recolhidos com o propósito de servirem de guia à tomada de decisões. Para tanto, os dados recolhidos são sujeitos a um processo de mineração de dados, ou *data mining*, que consiste na “conversão de fluxos de dados num conhecimento altamente específico”.

Este processo de conversão pode desenvolver-se com base em diferentes modelos de análise que visam dar resposta a diferentes questões. Uma análise descritiva visa dar resposta às questões “o que aconteceu” e “porque aconteceu”; uma análise preditiva procura responder à questão “o que irá ou poderá acontecer”; por fim, uma análise prescritiva baseia-se nos resultados obtidos pelos outros dois modelos e tem como objetivo responder à pergunta “o que se deverá fazer”.⁹⁶

⁹³ Ana Alves Leal, *Aspetos jurídicos da análise de dados na Internet (big data analytics) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação*, in *Fintech - Desafios da Tecnologia Financeira*, p. 93

⁹⁴ V. Paula Ribeiro Alves, *Os desafios...*p. 43

⁹⁵ Fala-se aqui de dispositivos como *smartphones*, computadores, etc., que recolhem informação da atividade do utilizador da Internet, nomeadamente de transações *online*, e-mails, vídeos e imagens visualizadas, histórico de navegação e registos de localização.

⁹⁶ *Ibidem*, p. 94 e 95

A recolha e tratamento da informação é, nas mais das vezes, feito por empresas de comércio de dados, os *data brokers*, cuja atividade profissional corresponde ao tratamento da informação e a venda do resultado desse tratamento. Esta informação tem-se afigurado valiosa, sendo, cada vez mais, vista como “uma nova categoria de ativo”.⁹⁷

Se não, vejamos: no que toca à análise preditiva, em particular, esta consegue “prever resultados ou tendências futuros; a informação assim obtida poderá ser útil ao decisor – que, querendo, se pode adaptar no presente àquilo que serão comportamentos, eventos, e preferências no futuro”, apresentando-lhe a decisão que deve tomar. Por sua vez, à análise descritiva recorrem sobretudo empresas com o intuito de direcionar os seus produtos ou serviços a uma parte da população. Porque esta se centra numa descrição de factos e comportamentos passados, permite a criação de categorias ou perfis de clientes aos quais as empresas podem especialmente dedicar ofertas personalizadas e descontos mais interessantes, garantindo uma taxa de retorno do investimento mais alta.⁹⁸

No que toca ao contrato de seguro, compreende-se facilmente que o segurador não possa deixar de tratar dados pessoais. Desde o início, o cliente está obrigado a declarar as circunstâncias que possam ser significativas para a apreciação do risco pelo segurador. E, posteriormente, quando se dá o sinistro, a prestar informação detalhada sobre as circunstâncias em que este ocorreu, sendo que o segurador terá de inteirar-se da gravidade dos danos que decorram do sinistro acedendo, nomeadamente, a relatórios clínicos, quer se trate, por exemplo, de um seguro de saúde ou de um seguro de responsabilidade automóvel.

No âmbito dos seguros também é possível tirar partido da *Big Data*, numa primeira fase, o recurso à *Big Data* permite uma maior oferta de produtos, através dos perfis criados pelas análises a dados⁹⁹, consegue abordar-se potenciais clientes e ajustar a oferta dos produtos às necessidades e ambições desses Clientes. Por exemplo, para determinar o preço adequado da apólice para cada cliente, pois é possível fazer uma análise mais adequada ao risco: sa-

⁹⁷Madalena Perestrelo de Oliveira, *Definição de Perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados*, in *Fintech II*, p. 71 e 72.

⁹⁸ Idem, p. 95

⁹⁹ Estes perfis permitem a organização de (potenciais) clientes em categorias, em função de determinadas características, mas permite também a criação de perfis únicos e exclusivos através de um processo que passa pelo *tracking*, *scoring* e *personalizing*. Para mais desenvolvimento cfr. Ana Alves Leal, *Aspetos Jurídicos...* cit, p. 98 e 99

bendo que determinado indivíduo tem inclinação para desportos de risco, podemos tirar conclusões para obter um perfil de risco diferente daqueles que preferem passar as suas tardes em leituras.

4.10 Recurso à *IoT*

Esta nova tecnologia tem sido apontada como o fenómeno que tem vindo a “transformar a Internet”, e através do qual a Internet “deixa de estar só nos computadores e, depois, nos telefones e passa a estar em *chips* integrados em potencialmente tudo, em todo o lado”, uma vez que passa a estar conectada a objetos e até pessoas ou animais, cujos comportamentos são de tal modo monitorizados que é gerada informação detalhada sobre cada indivíduo. Posteriormente, e sem necessidade de qualquer intervenção humana, esta informação é transmitida a um responsável pelo tratamento com vista a determinadas finalidades.

É através da tecnologia *Internet of Things* (doravante *IoT*) que grande parte da informação que compõe os *Big Data* é gerada. Não só são recolhidos os dados resultantes da utilização da Internet e de aplicações para *smartphones* ligadas à Internet, como também da utilização vários tipos de aparelhos, ou objetos que contém, em si inseridos, sensores.

HÉLDER FRIAS explica a tecnologia *IoT* como

“uma rede ou sistemas de equipamentos que servem uma finalidade específica, sendo dotados de sensores eletrónicos/informáticos interrelacionados, que possuem um identificador único e que podem comunicar com humanos (*man to machine* ou *M2H*) e/ou entre equipamentos (*machine to machine* ou *M2M*) através da rede, mediante transmissão de informação”.

A *IoT* caracteriza-se, assim, pelo uso de equipamentos dotados de sensores destinados a extrair informação relativa ao seu utilizador. A este respeito, tal como explica o Autor, não é na utilização de equipamentos¹⁰⁰ interligados entre si que encontramos a inovação, mas sim no facto de estes se ligarem também à Internet. Estes aparelhos ficam, assim, encarregados de, não só, recolher determinados dados (que podem variar desde a localização do usuário, como o peso, o número de horas de sono, etc) em tempo real, como combiná-los

¹⁰⁰ De entre os vários equipamentos, encontramos, por exemplo, paquímetros, termóstatos, equipamentos de monitorização de saúde e de exercício físico, os chamados *wearables* e prateleiras de supermercado

com outros dados, provenientes de outras fontes, procedendo ao seu processamento e organização em função da finalidade que tiver sido atribuída.

Enumerando apenas algumas das possíveis aplicações das *IoT*, destacam-se na área da saúde cinco tipos de sensores¹⁰¹: (1) dispositivos de bancada (como monitores de pressão arterial ou balanças); (2) *wearables* (como as pulseiras FitBit ou Apple Watch que medem valores como a distância percorrida, o ritmo cardíaco e mesmo a qualidade do sono); (3) sensores de contacto íntimos (como adesivos ou tatuagens eletrónicas), criados para, por exemplo, medir a temperatura de um paciente em tempo real, os níveis de hidratação e a exposição aos raios solares; (4) sensores ingeríveis (comprimidos eletrónicos que contém sensores desenhados para monitorizar o corpo do seu interior que, quando conjugados com os sensores-adesivos, possibilitam vigiar a conformidade com a prescrição médica); e (5) sensores implantáveis (como um monitor de saúde cardíaca ou sanguínea, e.g. *pacemakers*), dentro dos quais encontramos dispositivos que conseguem medir a glucose, a pressão arterial, ou *pacemakers* que são capazes de telefonar para o número de emergência se detetarem sinais de ataque cardíaco, fornecendo a localização do paciente. Estando, hoje em dia, a serem desenvolvidos sensores que permitem até detetar a rejeição pelo corpo humano de um órgão transplantado.¹⁰²

No setor automóvel, vale a pena referir (1) os EDR's (i.e., Event data Recorders), uma espécie de caixa preta, que já vem incluída na maioria dos automóveis vendidos nos EUA nos últimos 20 anos e que capta informação sobre a condição do veículo, a velocidade, o uso de cinto de segurança no momento de um acidente rodoviário; (2) sensores automóveis que em conjunto com um *smartphone* monitorizam o estado do automóvel e os hábitos de condução do condutor e que alertam o condutor, pelo *smartphone*, quando é necessária alguma intervenção no veículo; que bloqueiam chamadas no caso de o condutor estar em condução, conseguindo, inclusive, fazer chamadas de emergência verificada a ocorrência de um acidente; (3) dispositivos telemáticos que são fornecidos pelas próprias seguradoras e que são cada vez mais frequentes nos EUA. Estes dispositivos recolhem os dados por cerca de 30 dias, ao final dos quais calculam uma pontuação para cada condutor com base no seu estilo

¹⁰¹ No âmbito deste trabalho, deve entender-se “sensor”, como qualquer “dispositivo que permite adquirir, ler ou transmitir uma informação”, “sensor”, in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2020, <https://dicionario.priberam.org/sensor>

¹⁰² Vide também Carolina Cunha, *Proteção de Dados e Aplicações Móveis na Área da Saúde: um diagnóstico sumário*, in *Revista Online Banca, Bolsa e Seguros*, nº 3 – 2018, p. 31 – 50.

de condução e que acaba por ser usado como um fator na determinação do risco e do prémio de seguro e poderá, posteriormente ser adaptado, verificada uma mudança comportamental do condutor.

Por fim, refiram-se os dispositivos existentes para a habitação, desde termostatos e detetores de fumo a dispositivos que detetam fugas de água ou portas abertas, passando pelos frigoríficos que detetam a falta de certos alimentos e fazem a encomenda dos mesmos através de um *site* de supermercado, a redes elétricas inteligentes que permitem um gasto de energia mais sustentável. Todos estes dispositivos podem ainda servir ao responsável pelo tratamento para perceber os hábitos do habitante, tais como, quão frequentemente cozinha, toma banho, vê televisão ou quantas vezes passa férias durante um ano. As informações recolhidas, quando combinadas entre si e com outras informações, podem revelar-se muito valiosas para os mais variados tipos de empresas, nomeadamente para as empresas de seguros. Estas podem conter respostas muito relevantes a questões como quais as condições económicas do consumidor, se este é privado do sono, se sai atrasado para o trabalho, com que frequência faz a limpeza da casa, se se exercita frequentemente, etc..¹⁰³

É, em grande medida, o surgimento da *IoT* o responsável pela inovação tecnológica no setor segurador, em particular pelo surgimento de novos produtos de seguro. O maior impacto proveniente do uso de *IoT* verificar-se-á a nível da informação a que a empresa seguradora tem acesso diretamente. Como se tem dito, os dispositivos ligados entre si e à Internet permitem à empresa aceder, em tempo real a um extenso volume de informação detalhada sobre o segurado. Naturalmente, sem o recurso aos equipamentos dotados de sensores, não seria possível registar o comportamento dos usuários de forma constante. Mas a importância da *IoT* não se reflete apenas no volume de informação a que o segurador tem acesso, como também na veracidade da informação, pois este último deixa de estar consignado à versão do tomador sobre os factos do risco.

Ora, a partir daqui, as seguradoras conseguirão concretizar avaliações de risco mais exatas, conceder tarifas adequadas a cada segurado e flexibilizar o processo de regularização

¹⁰³ Para uma completa exposição sobre o funcionamento e exemplos destes sensores, vide Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, in *Texas Law Review*, disponível em <http://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>, p. 98-117.

dos sinistros. Tenha-se por exemplo o já aludido cenário no qual dado o atraso ou cancelamento de um voo de avião para o qual o titular contratou um seguro, o beneficiário recebe, de imediato, o valor do mesmo.

Por outro lado, haverá uma evidente diminuição do número de sinistros, consequência da mudança comportamental dos indivíduos que sabem estar a ser vigiados. Estes passarão a adotar comportamentos mais diligentes, tais como uma “condução mais defensiva, melhor manutenção da habitação ou maiores cuidados de saúde ou de exercício físico”.¹⁰⁴

A UE regula a comercialização de dispositivos conectados. Estes devem atender aos requisitos essenciais e características de segurança estabelecidos pela legislação.

Os equipamentos que usam o espectro de radiofrequência devem atender aos requisitos da Diretiva 1999/5/CE do Parlamento Europeu e do Conselho, de 9 de Março de 1999, relativa aos equipamentos de rádio e equipamentos terminais de telecomunicações e ao reconhecimento mútuo da sua conformidade revogada pela Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014 relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado. Além de que devem cumprir com as imposições decorrentes da Diretiva 2011/65 / UE sobre a restrição do uso de determinadas substâncias perigosas. É importante ainda atender a essas imposições, na medida em que, quando um produto, embora fabricado por terceiros, é colocado no mercado com as marcas registadas das empresas *InsurTech*, é suscetível de ser chamada à colação a responsabilidade do fabricante. Com efeito, esta aplica-se também a qualquer pessoa singular ou coletiva que monta, embala, processa ou rotula produtos prontos e os coloca no mercado com seu próprio nome ou marca comercial.

4.1.2 IoT e Proteção de Dados: Aplicação da Legislação em vigor

Pudemos já analisar que os dados em que as seguradoras se baseiam para aferir o risco provêm de diversas fontes (tanto são fornecidos pelo próprio proponente, como podem surgir da navegação deste na Internet e da utilização de dispositivos, como acabámos de verificar).

¹⁰⁴ Hélder Frias, *A Internet de Coisas (IoT) e o mercado Segurador*, p. 240 e ss.

Estes dados servirão sobretudo para guiarem as empresas na tomada de decisões quanto à celebração (ou não) do contrato de seguro e os moldes em que este será executado (nomeadamente para determinar o valor do prémio).

Em virtude de estes aparelhos estarem interligados entre si, a “vigilância” a que o segurado está sujeito aumenta significativamente, mormente porque, pela ligação à Internet, a recolha de dados se dá em tempo real, a um ritmo verdadeiramente frenético. Em boa verdade, os aparelhos *IoT* permitem traçar um mapa quase completo da vida do usuário, o que poderá suscitar algumas questões a nível da proteção dos dados pessoais. De entre elas, distingue-se a necessidade de encontrar uma fonte de licitude do tratamento contínuo dos dados pessoais.

Em princípio¹⁰⁵, merece aqui aplicação o RGPD¹⁰⁶, pois a informação recolhida corresponde à definição de dados pessoais presente no art. 4.º/1 do RGPD, no sentido em que se trata de “informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)”¹⁰⁷.

Todavia, se “os dados recolhidos no equipamento não forem transmitidos nem acedidos externamente, sendo apenas processados no próprio aparelho pelo utilizador, então estaremos fora do âmbito de aplicação do RGPD”, ou seja, sendo a recolha de dados feita por “pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas”, como sucede quando alguém baixa uma *app* onde regista o seu peso e o seu objetivo final, assim como a quantidade de passos que dá num dia com o “mero” objetivo de monitorizar os seus

¹⁰⁵ Dizemos “em princípio”, pois nem todos os dados recolhidos no seio da *Big Data* são dados pessoais. Nomeadamente, não o serão os dados relativos a pessoas coletivas ou dados que não permitem a identificação de pessoas. E, neste contexto não terá lugar a aplicação do RGPD. Cfr. Ana Alves Leal, *Aspetos jurídicos...*cit, p. 122 e 127. A Autora faz uma clara exposição sobre a anonimização dos dados pessoais e a sua distinção em relação à “pseudonimização”.

¹⁰⁶ Além da Lei n.º 41/2004, de 18 de agosto sobre a proteção de dados pessoais e privacidade nas telecomunicações e a Lei n.º 34/2013, de 16 de maio

¹⁰⁷ É considerada “identificável” uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular”. Por sua vez, a informação pode ser recolhida e tratada por um terceiro ou pelo próprio prestador de serviços, assumindo este o papel de responsável pelo tratamento (art. 4º/7). Naquele primeiro caso, o prestador de serviços ao consumidor final assume, antes, o papel de subcontratante (art. 4º/8), vide *Proteção de Dados e Aplicações móveis na área da saúde: Um Diagnóstico Sumário*, p. 35-39

próprios hábitos, não estaremos perante uma situação que reclame a proteção conferida pelo RGPD, conforme dispõe o art. 2.º/2/c).¹⁰⁸

Por outro lado, para efeitos do mencionado diploma, boa parte desta informação estará ainda compreendida na categoria específica dos dados relativos à saúde (art. 4.º/15), que são dados sensíveis e consequentemente estão sujeitos a um regime especial.

São, então, 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 seu estado de saúde. Desta feita, quaisquer dispositivos destinados a medir a glicémia, tensão arterial e *apps* associadas a esses dispositivos ou *apps* para registo de toma de medicamento, etc, recolhem e armazenam informação que se consubstancia em dados relativos à saúde. Inequivocamente são dados relativos à saúde “os que incidem sobre a condição de saúde física ou psíquica e que são gerados num contexto médico-profissional, incluindo os recolhidos por *apps* ou equipamentos, desde que relativos a doenças, patologias história clínica e tratamentos”.

Mas já não serão abarcados nesta categoria, os dados recolhidos através de *apps* de bem-estar, como aquelas suprarreferidas que recolhem informação sobre a frequência com que o sujeito pratica exercício físico ou as que servem para registar estados de espírito ou horas de sono.

Atente-se, contudo que, no contexto em que os estudamos, estes dados são, geralmente, combinados com outros dados recolhidos por outras *apps* e sensores durante um longo período de tempo e utilizados para tirar conclusões sobre o estado de saúde do titular dos dados (a título de exemplo, a falta de *inputs* para a prática de exercício físico combinada com o registo de peso elevado ao longo de várias semanas, permite concluir sobre o estilo de vida sedentário da pessoa, e assim aferir sobre os riscos ligados a vários problemas de saúde).

É, por isso, relevante distinguir aquelas *apps* que fazem uma recolha de dados “em bruto” e que não são combinados com outros dados e/ou usados para a criação de perfis relativos às condições de saúde do titular de dados.

Assim, atentem-se as considerações que tece CAROLINA CUNHA:

¹⁰⁸ Ibidem, p. 39 e 40.

“o que está em causa, para efeitos de tutela jurídica, é a possibilidade de retirar conclusões sobre o estado de saúde, independentemente do acerto dessas conclusões. Por outro lado, é indubitável que há um elemento de escala envolvido na apreciação: pode dizer-se que uma aplicação que registre durante meses ou anos padrões de sono, exercício, peso, dieta, pulsação e outros parâmetros vitais está a processar dados de saúde”.¹⁰⁹

Importa, então investigar em que medida o RGPD serve de proteção aos dados pessoais tratados no âmbito do contrato de seguro, que, como tivemos ocasião de assinalar, se consubstancia a um tratamento feito em larga escala. Servem, nesse sentido, os próximos pontos para expor os principais desafios da aplicação da legislação em atualmente em vigor ao tratamento operado no seio da contratação de seguro quando existe recurso às novas tecnologias.

4.1.3 Princípios relativos ao tratamento de dados pessoais

O RGPD, no seu art. 5.º/1, elenca os princípios relativos aos dados pessoais, são eles: a licitude, lealdade e transparência; a limitação das finalidades; a minimização dos dados, a exatidão; a limitação da conservação e a integridade e confidencialidade.

O responsável pelo tratamento de dados, como estudaremos infra, é o encarregado por garantir o cumprimento destes princípios, dos deveres inerentes a eles e do respeito pelos direitos de que são detentores os titulares dos dados.¹¹⁰

O princípio da licitude, lealdade e transparência determina que os dados pessoais sejam objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (al. a)).

¹⁰⁹ Carolina Cunha, *Proteção de dados...* cit, p. 39

¹¹⁰ Alexandre Dias Pereira, *O responsável pelo tratamento de dados segundo o Regulamento Geral de Proteção de Dados (RGPD)*, in *Boletim da Faculdade de Direito da Universidade de Coimbra*, vol. 95, n.º 2, 2019, p. 1162

No que toca ao princípio da exatidão (al. d)), este determina que os dados pessoais são exatos e atualizados sempre que necessário e que devem ser adotadas todas as medidas adequadas para que os dados inexatos sejam apagados ou retificados sem demora, tendo em conta as finalidades para que são tratados.

O princípio da limitação da conservação, na al. e)) do art. 5.º/1, estabelece que os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados, podendo ser conservados por períodos mais longos nos termos da al. e) do art. 5.º, n.º 1.

De seguida, de acordo com o princípio da integridade e confidencialidade, os dados pessoais devem ser tratados de modo a garantir a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (al. f) do art. 5.º, n.º 1).

Em referência ao princípio da limitação das finalidades, na alínea b) do artigo supramencionado, que tal como o princípio da minimização dos dados aqui requer maior exposição, impõe-se referir que este é o princípio ao abrigo do qual os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades.

De seguida, o princípio da minimização dos dados, vertido na al. c), estatui que os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.

Assim, no âmbito do estudo que ora nos ocupa, o segurador pode ter acesso aos dados que considere necessários e indispensáveis à apreciação do risco do proponente. Atente-se, porém, que essa informação deve limitar-se à “estritamente necessária à realização das diligências pré-negociais ou da execução” (art. 5.º/1/b e c)).

Não obstante, a lei não salvaguarda os interesses dos titulares dos dados das considerações subjetivas e das preferências das entidades com que contrata. Por outras palavras, se para determinada instituição foi necessário um determinado dado em função do seu plano negocial e para outra não, a informação não deixa de ser essencial para a primeira instituição. Em boa verdade, o princípio da autonomia privada, refletido no art. 450.º do nosso CCiv., admite que as partes, no exercício da sua vontade autónoma, autorregulem os seus interesses

na negociação contratual, portanto, aquilo que consideram essencial à celebração de determinado contrato.

Neste sentido, ANA ALVES LEAL sugere a demarcação da informação objetivamente útil e necessária à consecução de um contrato e a informação que se destina à prossecução de interesses legítimos da empresa e que deveria estar sujeita ao teste de ponderação estabelecido no art. 6.º/1/f) do RGPD.¹¹¹

Ainda que se reconheça o mérito a esta sugestão, teremos sempre dificuldades em delimitar o que será essa informação. De facto, como sublinha LUIS POÇAS “ao permitir uma aferição mais rigorosa do risco (aproximando o risco estimado do real), o domínio dessa informação pode revolucionar a atividade seguradora, possibilitando uma melhor segmentação do risco beneficiando, dessa forma, o segurado consumidor e a própria mutualidade segura”. Em referência aos testes genéticos que revelam o risco de uma pessoa desenvolver uma determinada doença LUÍS POÇAS refere que, ainda que se possam considerar elementos fundamentais para a avaliação do risco pelo segurador, a verdade é que podem sempre ser dispensados, em virtude de a empresa não querer investir em recursos, pelo menos numa fase inicial, mais dispendiosos.

Além disso, e tal como acontece com os testes genéticos – talvez estes sejam até mais precisos do que os dados que aqui enunciamos -, a existência de indícios sobre a probabilidade de ocorrência do risco, não significa necessariamente a sua efetivação.

Isto significa que uma maior informação sobre o risco poderá, ao invés de consubstanciar a mitigação do risco, permitir o “desenvolvimento de medidas preventivas que contrariem essas vulnerabilidades” (as vulnerabilidades relativas à saúde de certos indivíduos).¹¹²

Pode sempre a seguradora alegar ser excessivamente onerosa a recolha de informação junto do Cliente, sobretudo quando comparada essa informação com o volume de informação que é possível recolher e tratar com o recurso à tecnologia *Big Data*.

Na senda do supracitado, o objeto do contrato resume-se à cobertura do risco. No caso dos seguros de pessoas, esse risco pode estar associado à vida da pessoa, à sua saúde ou à

¹¹¹ Cfr. *Aspetos Jurídicos...* cit, p. 176

¹¹² V. Luís Poças, *O Dever...* ob. cit., p. 743 e 744.

sua integridade física (175º./1 do RJCS). Neste sentido, os dados de saúde revelam-se indispensáveis à apreciação do risco e decisão do segurador de se vincular ou não através do contrato, e, posteriormente, avaliação do dano resultante do sinistro.

Facilmente se concebe a necessidade de aceder aos antecedentes clínicos do proponente, assim como a exames médicos que traduzam o seu estado de saúde atual. Será, contudo de questionar se se verifica indispensável o recurso à *Big Data*.

De facto, o tratamento de dados tal como é feito no seio da *Big Data* confere às empresas uma visão mais detalhada sobre o atual estado de saúde do proponente, permitindo o acesso a dados que de outra forma não estariam ao alcance da seguradora. A título de exemplo, e porque a atividade das seguradoras não deixa de ter escopo lucrativo, e porque a venda de produtos de seguro depende de um juízo de valor positivo sobre o risco relativo ao segurado, é o segurador que está em melhores condições para determinar as informações sobre as quais pretende ponderar quando está em vista a celebração de um contrato. Neste sentido, poderá revelar-se estritamente necessário, a determinada empresa, saber os hábitos do proponente enquanto condutor, tais como se ultrapassa os limites de velocidade, se efetua travagens bruscas e não apenas quantos acidentes já teve; ainda, será, certamente útil saber que o proponente revela antecedentes de depressão, porém, a somar a esse facto, será determinante para a seguradora saber que, nos últimos meses este ganhou algum peso e não tem dormido um espectáculo para o indivíduo médio.

Ademais, sendo o contrato de seguro um contrato de tendencial longa duração, é provável que se verifique um agravamento ou uma melhoria do estado de saúde do segurado, o que pode ser de interesse para o segurador. Isto pode ser facilmente colmatado com o recurso à *big data*. Com o recurso a esta tecnologia, é possível haver uma intercomunicabilidade dos dados entre o segurado e o segurador muito mais forte.

Por outro lado, o facto de o contrato de seguro ser um contrato de longa duração poderá levar a que, no momento de consentir, não haja ainda informação suficiente sobre as finalidades que poderá vir a ter o tratamento de dados, o que pode não só dever-se ao facto de o responsável pelo tratamento não ter conhecimento dos algoritmos utilizados no tratamento dos dados, como também pode dever-se à impossibilidade de determinação das finalidades do tratamento, uma vez que estes podem vir a ser reutilizados posteriormente e por diferentes

responsáveis pelo tratamento. Neste último caso, há uma total impossibilidade de o responsável informar o titular dos dados sobre os fins do seu tratamento e, naturalmente, uma impossibilidade de prestar o consentimento informado (e válido) quando está em causa o tipo de tratamento operado pela *Big Data*.

Tal como explana ANA ALVES LEAL, seria melhor se se tivesse criado um regime próprio para o tratamento de dados na *Big Data*, porquanto o recurso a esta tecnologia, implicando, na sua génese, uma recolha massiva de dados, seguida da sua análise através de mecanismos automatizados e, por fim, o emprego desses dados para propósitos diferentes dos visados pelos seus titulares aquando da sua divulgação na Internet, coloca desde logo em causa alguns dos princípios base do regime de proteção de dados supracitados.¹¹³

Em síntese, verificamos a verdadeira desadequação das disposições do RGPD no que toca à utilização da *Big Data*, no sentido em que estas não dão resposta aos desafios (futuros) colocados por esta tecnologia.

4.1.4 As fontes de licitude do tratamento de dados

4.1.4.1 O Consentimento do titular de dados

Nos últimos anos, tem sido reconhecido o controlo dos dados ao seu titular. Este controlo manifesta-se no RGPD, em grande parte, através do consentimento que consta, no diploma, como uma das fontes de licitude de que depende o tratamento dos dados (art. 6.º/1/a) e art. 7.º). Uma vez estar em causa o direito à autodeterminação informativa, cabe ao titular dos dados permitir o tratamento destes.

Na aceção do art. 4.º/11, o consentimento é uma manifestação de vontade do titular dos dados, naturalmente, livre, específica, informada e explícita, pela qual este aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.¹¹⁴

Em primeiro lugar, cumpre esclarecer que o consentimento do titular se dirige ao tratamento dos dados para uma ou mais finalidades específicas. Devendo, ainda o titular dos

¹¹³ Ana Alves Leal, ob cit, p. 154

¹¹⁴ O consentimento deve ser explícito (art. 9.º/1), não bastando, por isso, a falta de reação à declaração da intenção de processar os dados. Deve ser

dados estar devidamente informado sobre a dimensão da recolha, armazenamento e tratamento de dados pessoais (art. 13.º)¹¹⁵.

Acontece que um dos maiores desafios no recurso à *IoT* é precisamente o de transmitir ao usuário dos dispositivos a informação sobre a privacidade e segurança no uso dos mesmos e modo de exercício do consentimento em função das características específicas destes dispositivos¹¹⁶. Se não vejamos, um dispositivo de *IoT* é, geralmente, pequeno e, se o tiver, composto por um pequeno ecrã, carecendo de teclado ou painel eletrónico tátil, e.g., uma pulseira rastreadora de atividade desportiva (como a FitBit) não possibilita o acesso às políticas de privacidade e segurança e muito menos o exercício do consentimento de forma personalizada e detalhada, por parte do titular dos dados, pois não permitem, na generalidade, introduzir informação ou modificá-la.

Desta sorte, a informação sobre a privacidade e o consentimento terá que vir, as mais das vezes, exposta num outro lugar, nomeadamente, no manual de instruções do dispositivo, no *site* de Internet do produtor do aparelho ou nos termos e condições de uso da *app* para o telemóvel associada ao dispositivo, se a houver.¹¹⁷

Esta questão torna-se ainda mais preocupante, tendo em consideração que muitos desses dispositivos estão à venda em lojas tradicionais *brick-and-mortar* e não apenas diretamente junto do produtor, o que pode levar a que o consumidor que adquira esse dispositivo sem qualquer aviso prévio de que estará sujeito a uma política de privacidade.¹¹⁸

De todo o modo, se o titular dos dados solicitar pela retirada do consentimento, esta deve ser, para o titular dos dados, tão fácil de exercer, como foi dar o seu consentimento para o

¹¹⁵ *Aspetos Jurídicos...*, p. 158 e 159.

¹¹⁶ Note-se que, para que o consentimento seja informado o titular dos dados sujeitos a tratamento tem que estar esclarecido quanto a) à informação exata que o dispositivo recolhe e através de que tipo de sensores o faz; b) ao lugar onde é que a informação é armazenada, se na *cloud*, no próprio dispositivo, etc; c) ao facto de a informação ser encriptada ou não; d) se é possível ou não alterar os termos do consentimento, etc. Cfr. Scott R. Peppet, ...cit. p. 161

¹¹⁷ Atente-se que para os casos em que o consentimento é dado no contexto de uma declaração escrita, como são as políticas de privacidade comuns em aplicações de *smartphones* ou *sites* de Internet, impõe o art. 7.º/2 que o pedido de consentimento seja apresentado de uma forma que o distinga claramente de outros assuntos na declaração de modo inteligível e de fácil acesso e numa linguagem clara e simples.

¹¹⁸ Neste caso, torna-se imperativo que estes divulguem em que termos, uma terceira parte, *in casu*, os seguradores, têm acesso aos seus dados. Cfr. Scott R. Peppet, *Regulating the Internet of Things...*cit, p. 140 e 161.

tratamento de dados e deve garantir o apagamento de todos os dados do titular que são controlados por aquele responsável, em cumprimento do disposto no art. 17.º do RGPD.

4.1.4.2 Outras fontes de licitude

De entre os casos de tratamento de dados pessoais sem o consentimento do titular, o art. 6.º/1/b) consagra a possibilidade de proceder a esse tratamento, verificando-se a sua necessidade para a execução de um contrato no qual o titular dos dados seja parte, ou para diligências pré-contratuais a pedido do titular de dados.

No contrato de seguro, de facto, verifica-se essa necessidade de tratar os dados pessoais do tomador/segurado. Só dessa forma o segurador consegue avaliar o risco e decidir, de forma informada, se quer contratar ou não com aquele cliente, qual o valor do prémio a implementar, assim como o âmbito da cobertura e análise ao sinistro.

É essencial, antes de mais, esclarecer que este tratamento “à revelia do titular” deve ser moderado e deve ter em conta a voluntariedade do titular dos dados na celebração do contrato. Daqui podemos deduzir que se ele se autocolocou na situação negocial ou pré-negocial, não irá, posteriormente, opor-se à divulgação ou tratamento da informação, pois compreende que ao vincular-se contratualmente, isso implicará, necessariamente o tratamento dos seus dados pessoais. Entende-se, assim, estarmos perante um “consentimento implícito”¹¹⁹.

Quanto aos dados de saúde, porém, dizendo respeito a uma categoria especial de dados merecem proteção legal acrescida. Não encontramos, no art. 9.º do RGPD, semelhante base legal que legitime o tratamento dos dados no seio da execução do contrato de seguro. Desta sorte, poderá não haver lugar ao tratamento de dados de saúde no âmbito dos contratos de seguro.¹²⁰

Torna-se assim imperativo que o segurador obtenha o consentimento explícito do proponente, na celebração de um contrato de seguro que implique o tratamento de dados de

¹¹⁹ Luís Poças, *Problemas e Dilemas do Setor Segurador*, p. 257 e 277-278.

¹²⁰ No mesmo sentido, v. o Parecer n.º 20/2018 da CNPD, de 02/05/2018, disponível em: <http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d46446232317063334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&In-line=true>

saúde, o que pode conduzir ao entendimento de que este artigo configura um requisito adicional para a licitude do tratamento de dados.¹²¹

LUÍS POÇAS destaca que impondo a necessidade de obtenção do consentimento para legitimar o tratamento dos dados de saúde estar-se-á a potenciar uma atuação abusiva por parte do titular dos dados. Imagine-se o titular de dados, que previamente concedeu o seu consentimento, e que omitiu determinadas informações ou introduziu outras erroneamente sobre o seu estado de saúde e que vem, mais tarde, obstar, revogando o seu consentimento nos termos do art. 7.º/3 do RGPD, a que o segurador investigue com alguma profundidade as suas declarações.

A retirada do consentimento determina, assim, a impossibilidade de realizar a prestação, na medida em que o tratamento dos dados de saúde é indispensável à execução do contrato. Se assim não for, não se deve deixar de notar que, nos termos do art. 116.º do RJCS pode haver lugar à resolução por justa causa por, na senda de LUÍS POÇAS, deixar o segurador numa posição vulnerável a práticas fraudulentas, como a simulação de ocorrência de um sinistro, por exemplo.¹²²

Não obstante, é possível constatar que este tratamento é indispensável, quer na fase pré-contratual, quer durante a execução do contrato. Neste sentido, considera LUÍS POÇAS que as empresas de seguros enfrentam uma “notória dificuldade de preenchimento dos requisitos do consentimento, tal como resultam atualmente do RGPD”, pugnando pela desconsideração da necessidade do “consentimento” para o tratamento dos dados de saúde no âmbito da execução do contrato quando seja impossível preencher os requisitos da sua validade.

Torna-se patente que a exigência do consentimento nos termos do RGPD, como forma de garantir ao titular dos dados o controlo sobre eles, não se coaduna com a realidade sobre a qual incide.¹²³

Nomeadamente havendo o recurso às tecnologias *IoT* e o tratamento de dados no seio da *Big Data*, é muito difícil, se não, impossível, a prestação de um consentimento válido por parte do titular dos dados. Primeiramente porque, neste âmbito, é muitas vezes absoluta-

¹²¹ Cfr. Luís Poças, *Problemas e Soluções do setor dos seguros*, p. 271.

¹²² *Idem*, p. 280 e 281.

¹²³ *Ibidem*, p. 283 e 284. No mesmo sentido, v. também., Ana Alves Leal, *Aspetos...cit*, p. 163 e 164.

mente vedado o uso de um *site* ou de uma aplicação para o telemóvel, quando, nomeadamente, o titular dos dados não concorda, nem que seja apenas parcialmente, com as políticas de recolha e tratamento de dados. Depois, porque se tem visto como prática corrente o uso de linguagem técnica e de complexa compreensão para o “mero” consumidor, de tal forma que este é desincentivado a ler as condições de uso, dando o seu consentimento sem ler as suas consequências. Ademais, no momento anterior à prestação do serviço ou ao uso da aplicação, “não há ainda informação suficiente sobre o tratamento e suas finalidades que possa ser prestada ao titular dos dados para que se considere que teve acesso à informação essencial para se autodeterminar e, assim, prestar um consentimento informado”.¹²⁴

É o exemplo do contrato de seguro que por ser celebrado tendencialmente a longo prazo torna “impossível ao segurador saber, no momento de recolha do consentimento (início do contrato), quais as circunstâncias concretas de tempo, lugar e modo em que irá proceder ao tratamento de dados que vinham sendo requeridos pela CNPD”.¹²⁵

De facto, as relações contratuais em causa protelam-se no tempo, impossibilitando a especificação *à priori* de todas as finalidades da recolha e tratamento dos dados que possam vir a tornar-se importantes na ótica da empresa, também porque a própria inovação tecnológica leva à criação de novas aplicações para os dados recolhidos.¹²⁶

Numa interpretação demasiado generosa, nestes casos, BRUNO RICARDO BIONI considera que o titular dos dados consente “acerca da relação que se protrairá no tempo e, com ela, as variantes de tratamento dos dados pessoais que devem estar adequadas ao contexto da relação” e portanto, o consentimento terá que ter em conta “o uso secundário dos dados”, sempre garantindo, porém, o tratamento de acordo com as legítimas expectativas¹²⁷ do titular dos dados.

Por outro lado, afirma o Autor que “mesmo nas situações em que não se recorre a uma declaração de vontade do titular para usos ulteriores das suas informações [e, portanto, nos

¹²⁴ *Ibidem*, p. 164

¹²⁵ Luís Poças, *Problemas e Soluções de Direito dos Seguros*, p. 273

¹²⁶ Vide Bruno Ricardo Bioni sobre o seguro de saúde, e como teremos oportunidade de desenvolver, *Proteção de dados pessoais...cit*, p. 243 e 244

¹²⁷ Segundo Bruno Ricardo Bioni, o titular dos dados mantém o controlo sobre eles, pois sabe que o responsável pelo tratamento, em cumprimento do dever de boa-fé, fará uso e partilha dos dados apenas no contexto da relação pré-estabelecida, *cfr. ob cit.*, p. 246-248.

casos do art. 6.º/1/b)], não se perde de vista lhe assegurar controlo sobre o fluxo informacional”.¹²⁸

De facto, faria sentido não ser necessário proceder à obtenção de “um” consentimento por cada situação que prescindia do tratamento de dados de saúde, mormente nas áreas que implicam o regular tratamento de dados, como são a do seguro de saúde. Tal seria “impraticável, pela ineficiência, complexidade e demora que passaria a afetar a regularização dos processos de sinistro”. Parece, contudo, não ser nesse sentido que aponta o art. 9.º/2/a) (e do art. 6.º/1/a)) do RGPD. O consentimento deve ser relativo a cada uma das finalidades perseguidas pelo responsável pelo tratamento, não bastando um “consentimento genérico”.¹²⁹

Não obstante, na senda de LUÍS POÇAS, é de notar que a necessidade de o consentimento ser específico relativamente a cada finalidade do tratamento de dados inibe a sua obtenção e a consequente legitimação do tratamento dos dados de saúde.¹³⁰

Por outro lado, revelando-se necessário para o exercício de direitos ou para o cumprimento de obrigações do titular dos dados ou da entidade responsável pelo tratamento no âmbito da legislação de segurança social, laboral ou da proteção social, a recolha, tratamento e conservação pelas seguradoras dos dados relativos à saúde é (ou deveria ser) permitida à luz do art.º 9.º. n.º 2, al.) b) do RGPD.

No caso dos seguros obrigatórios, como é o seguro obrigatório de responsabilidade civil e o seguro obrigatório de acidentes de trabalho, LUÍS POÇAS encontra no referido artigo a fonte de licitude do tratamento dos dados de saúde. O normativo dispõe que o tratamento de dados de saúde é lícito, se “for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados”.

¹²⁸ Vide *Proteção dos dados pessoais* ...ob. cit., p. 245 e 246.

¹²⁹ Cfr. Deliberação nº 51/2001 da CNPD, nota 38 concretamente relativa ao caso dos seguros, disponível em: <https://www.cnpd.pt/home/orientacoes/DEL51-2001-ACESSO-DADOS-SAUDE.pdf> e Luís Poças, *Problemas*...cit, p. 272-275.

¹³⁰ *Idem*, p. 275.

Ora, de facto, na senda do que se tem vindo a analisar o tratamento dos dados de saúde, no seio dos contratos de seguro obrigatório revela-se necessário, para tal entendimento contribuindo ainda os artigos 35.º, 37.º e 39.º do Regime do Sistema de Seguro Obrigatório de Responsabilidade Civil Automóvel¹³¹ e a Lei dos Acidentes de Trabalho¹³² que aludem à necessidade de tratar dados de saúde no âmbito daqueles contratos. Além disso, o tratamento é, efetivamente feito, no caso do seguro obrigatório de acidentes de trabalho, em cumprimento de obrigações do responsável pelo tratamento impostas pela Lei dos Acidentes de Trabalho.

O tratamento dos dados de saúde revela-se necessário, não apenas na fase pré-contratual, mas também durante a execução do contrato, inclusive as seguradoras estão adstritas ao dever de seleção criteriosa do risco subscrito, sobre o qual versa o art. 72.º/1 do RJASR (Lei n.º 147/2015), de 9 de setembro. De acordo com o disposto no artigo, as empresas de seguros devem dispor de um sistema de gestão de riscos criterioso de tal modo que lhes permita, a todo o tempo, identificar, mensurar, monitorizar, gerir e comunicar os riscos, de forma individual e agregada, a que estão ou podem vir a estar expostas e as respetivas interdependências.

Este sistema de gestão incidirá (também), por força do n.º 4, al. a) do mesmo artigo, sobre a subscrição, o que implica uma “seleção criteriosa do risco subscrito, para o que não pode, no caso dos seguros de pessoas, deixar de tratar os dados de saúde indispensáveis a tal análise e seleção”.¹³³

Ainda, o art. 102.º/1 do RJCS determina que o segurador é obrigado a satisfazer a obrigação a que se submeteu, assim que se confirmar a ocorrência do sinistro e das suas causas, circunstâncias e consequências, o que carece, necessariamente do tratamento dos dados de saúde.

¹³¹ DL n.º 291/2007, de 21 de agosto de 2007.

¹³² Lei n.º 98/2009, de 4 de setembro de 2004.

¹³³ Vide Luís Poças, *Problemas...*, p. 292

Além do exposto, entende LUÍS POÇAS que o valor da proteção social¹³⁴ é subjacente a todos os contratos de seguro, o que justifica o tratamento dos dados nos termos do art. 9.º/2/b) do RGPD. No mesmo sentido advoga FILIPE ALBUQUERQUE MATOS.¹³⁵

Como explica LUÍS POÇAS, o consentimento passou a representar um “papel subsidiário” enquanto fonte de licitude do tratamento de dados. Isto porque, quando o responsável pelo tratamento tem possibilidade de optar por qualquer uma das fontes, preferi-la-á ao consentimento, por este estar sujeito a requisitos apertados e por implicar que “quando o responsável pelo tratamento disponha cumulativamente de vários fundamentos de licitude de que possa lançar mão e opte por fazer o tratamento com base no consentimento, não poderá posteriormente (e de forma retroativa) invocar outro fundamento” a que tem direito.¹³⁶

Sem prejuízo do que se acabou se explanar, não será, naturalmente, permitida a venda de informação, por parte do responsável pelo tratamento de dados dos usuários da FitBit a uma empresa seguradora. Já aqui falámos do princípio da limitação das finalidades do tratamento que, ao abrigo do art. 5.º/1/b), sujeita o tratamento dos dados a uma limitação ao nível das finalidades do tratamento, no sentido em que estas devem ter uma ligação relevante com as funcionalidades da *app*.¹³⁷

¹³⁴ *Ibidem*, p. 285 e 286

¹³⁵ “Neste domínio, embora a regulação dos seguros facultativos de pessoas não surja propriamente em legislação de segurança social, cremos ser pacífico (...) que tais seguros se destinam precisamente a complementar o regime de proteção social consagrado pelo Sistema Previdencial de Segurança Social”. Neste sentido, convoca, o Autor, o art. 84.º da Lei de Bases da Segurança Social (Lei n.º4/2007, de 16 de janeiro), o art. 76.º/3 do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social e os art. 2.º-A/1/a) e b) e art. 43.º/2 do Código do IRC, *idem*, p. 289-291. No mesmo sentido, expõe Filipe Albuquerque de Matos que não se afigura exclusivo das entidades públicas a prossecução da proteção social. Ademais, através dos seguros obrigatórios, as seguradoras têm um papel com uma forte dimensão social. “Basta pensar no seguro de responsabilidade civil automóvel, onde a tutela do interesse público assume uma particular relevância, condicionando indelevelmente o regime jurídico corresponsivo, ao ponto de obrigar as seguradoras a intervir em situações onde a lógica contratual não justificava a respetiva atuação (ex: art.º 15.º, n.º3 do Decreto Lei n.º 291/2007). No fundo, a disciplina jurídica positiva reservada a tais seguros (no caso do Decreto Lei n.º 291/2007), exprime claramente a influência regulativa de exigências de justiça distributiva e não apenas a necessidade de acautelar os interesses dos particulares, cuja tutela tem fundamentalmente subjacentes razões de justiça comutativa”. Cfr, o *Regulamento de Proteção de Dados Pessoais [2016/679] no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde*, in *Revista Online Banca, Bolsa e Seguros*, nº 3, p. 114-121.

¹³⁶ *Ibidem*, p. 270, em especial, nota 552

¹³⁷ Carolina Cunha, *Proteção de Dados...*, p.42 e 43.

Por tudo que temos vindo a enunciar, afigura-se absolutamente necessário “(re)pensar e (re)avaliar um quadro regulatório” de modo a que o titular dos dados se situe verdadeiramente como um sujeito autónomo “capaz de exercer tal esfera de controlo e, em última análise, desempenhar por si próprio a proteção das suas informações”¹³⁸.

4.2 O Responsável pelo Tratamento de Dados

Enquanto entidade que determina as finalidades e os meios (i.e., o *para quê e como*) de tratamento de dados pessoais, a seguradora será considerada, nos termos do art. 4.º/7 do RGPD, como a responsável pelo tratamento de dados ou *data controller*. Este “é o principal sujeito de deveres e obrigações aí [no RGPD] estabelecidos”. A seguradora poderá fazê-lo isoladamente ou em conjunto com outras entidades.

Por outro lado, a empresa responsável pelo tratamento de dados pode contar com uma outra entidade, seja ela pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta daquele, o subcontratante. Nesta conformidade, ambos realizarão o tratamento de dados.

Todo o capítulo IV do RGPD é dedicado à figura do responsável pelo tratamento de dados, expondo as suas obrigações e deveres, alguns dos quais em análise de seguida.

É ao responsável pelo tratamento de dados que cabe o respeito pelos princípios relativos ao tratamento de dados pessoais e garantir a licitude do tratamento dos dados nos termos supradescritos.

Desta sorte, por respeito ao direito do titular de dados à transparência das informações das comunicações e das regras para o exercício dos direitos dos titulares dos dados, cabe ao responsável pelo tratamento prestar informações por escrito de forma concisa, transparente, inteligível e de fácil acesso, gratuita, utilizando uma linguagem clara e simples e de acordo com os arts. 13.º e 14.º do RGPD. Também assim, deverá transmitir ao titular dos dados que dados, para que fins, durante quanto tempo, de que modo, é feito o tratamento e a quem se destinam os dados (art. 15.º).

Do mesmo modo, manifestando o titular de dados a intenção de ver apagados ou retificados os seus dados nos termos do art. 16.º do RGPD, ou limitado o tratamento dos dados

¹³⁸ Pelo menos por enquanto, mesmo que este seja proativo na procura de informação sobre o funcionamento dos dispositivos *IoT*, nomeadamente procure informar-se sobre o modo de recolha e do tratamento dos dados que é feito, o próprio mercado tem o poder de criar novas tecnologias para neutraliza-lo. Bruno Ricardo Bioni, ob. cit., p. 155

nos termos dos arts. 17.º e 18.º do RGPD ou de se opor, de todo, ao seu tratamento e a decisões automatizadas ao abrigo do art. 21.º do RGPD, deve o responsável pelo tratamento mobilizar os meios para aplicar essas medidas, bem como comunicar, de acordo com o art. 19.º do Diploma, “a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16.º, o artigo 17.º n.º 1, e o artigo 18.º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado”. Ainda, se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários.¹³⁹

Entre outros deveres a que o responsável está adstrito, contamos o dever de manter um registo das atividades efetuadas no seio do tratamento de dados, no qual devem constar as informações elencadas no art. 30.º do RGPD. De acordo com o n.º 5 daquele artigo, porém, as *startups* poderão estar isentas de manter este registo, já que o normativo excetua a sua aplicação às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o art. 9.º/1, ou dados pessoais relativos a condenações penais e infrações referido no art. 10.º.

Ainda neste âmbito, o responsável pelo tratamento tem o dever de assegurar pela segurança dos dados pessoais, podendo aplicar medidas como “pseudonimização” e a cifragem de dados, a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, e um processo para testar, apreciar e avaliar regularmente a eficácia dessas medidas (art. 32.º).¹⁴⁰

Por fim, o Responsável pela Proteção de Dados, quando for autoridade ou organismo público ou quando exerça atividade que exija o controlo de titulares de dados ou o tratamento de dados em grande escala, designadamente no que toca às entidades relacionadas com o presente estudo¹⁴¹, deve, de acordo com o disposto no art. 37.º/1/al. b) e c), designar um Encarregado de Proteção de Dados.

¹³⁹ Vide Alexandre Libório Dias Pereira, *O responsável ...cit.*, p. 1161-1188.

¹⁴⁰ *Ibidem*, *O Responsável...cit.*, p. 1177

¹⁴¹ Não é possível quantificar um número determinante para a classificação do tratamento dos dados em massa. De acordo com o Considerando 91 do RGPD, seriam incluídas as «operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um

Esta é uma figura nova, introduzida pelo Regulamento, cuja função é essencialmente de zelar pelo cumprimento das normas de proteção de dados pessoais e auxiliar o responsável pelo tratamento de dados e o subcontratante relativamente às suas obrigações (art. 39.º).¹⁴²

4.3 Deveres de Informação do Segurado e a Aferição do Risco no seio da *Insurtech*

A celebração de um contrato pressupõe uma relação de confiança que deve ser fomentada desde o momento anterior à sua celebração, portanto desde a fase da negociação. Para que possam celebrar um contrato, as partes devem estar devidamente informadas e formar a sua vontade de forma livre e esclarecida. No contrato de seguro em particular, por estarmos perante um contrato que é geralmente qualificado de *uberrima fides* ou de máxima fé, impõe-se, de forma especial, esse dever de informação sobre as circunstâncias relevantes para a apreciação do risco, as circunstâncias determinantes da vontade negocial da seguradora e uma especial tutela desta, que se traduz no grau de reprovação quando se verifique o incumprimento do tal dever.

Esta classificação decorre da existência de uma assimetria informativa entre as partes e da natureza aleatória do contrato de seguro.¹⁴³

O contrato de seguro caracteriza-se tendencialmente por esta assimetria entre as partes, uma vez que é o proponente quem detém as informações que são relevantes à apreciação do risco, que são informações sobre si ou circunstâncias que a si dizem respeito.

O segurador não tem acesso a essa informação, o que provoca este “desnível”. Esta inacessibilidade pode ser material, no sentido em que a informação pertence ao espaço de acesso reservado ao cliente; legal, quanto a factos que respeitem à vida privada do proponente e sobre os quais incide especial proteção, os dados pessoais; ou económica, pois, ainda que alguns dados sejam acessíveis ao segurador, a procura dos mesmos pode ser muito onerosa ou demorada.¹⁴⁴

elevado risco». Por outro lado, é excluído do tratamento de dados em grande escala, o tratamento dos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado». Cfr. *Orientações sobre os encarregados da proteção de dados (EPD) - Grupo do Artigo 29.º para a proteção de dados*. https://www.cnpd.pt/home/rgpd/docs/wp243rev01_pt.pdf

¹⁴² Alexandre Dias Pereira, *O Responsável...*, p. 1179 e 1180.

¹⁴³ Vide Filipe de Albuquerque Matos, ...cit. p. 51. Vide também Luís Poças, *Problemas...*cit., p. 16 e 17.

¹⁴⁴ V. Luís Poças, *Problemas e Soluções de Direito dos Seguros*, p. 13

Desta sorte, o segurador vê-se obrigado a confiar nas declarações do proponente¹⁴⁵. Nas palavras de FILIPE ALBUQUERQUE MATOS,

“configurando-se a seguradora como a parte económica-técnica e socialmente mais forte na relação contratual, a verdade é que, paradoxalmente, do ponto de vista das informações tidas por relevantes para a avaliação do risco, a mesma se encontra particularmente dependente do acervo informativo que lhe seja atribuído pelo proponente do seguro”.

Em contrapartida, pagando o prémio, o segurado confia que o segurador, cumprirá o seu dever de indemnização quando ocorrido o sinistro.

Neste contexto, LUÍS POÇAS fala de uma confiança forçada, “num constrangimento, numa necessidade ou inevitabilidade de entrega à parte contrária”.

Em função desta assimetria, afigura-se imperativo garantir o equilíbrio da relação contratual. É neste ensejo de “homenagem à boa-fé (...) que a lei obriga o proponente (e mais tarde, durante a execução do contrato, o segurado) a participar à seguradora todos os factos e circunstâncias relativas ao risco”.¹⁴⁶

Por outro lado, recorde-se o que se disse sobre o contrato de seguro ser um contrato aleatório. O equilíbrio informacional permite evitar a “viciação especulativa daquela *alea*”¹⁴⁷.

Por outro lado ainda, o incumprimento do dever de declaração inicial de risco acarreta sanções - a anulabilidade do contrato no caso de omissão ou inexatidão dolosa (art. 25.º/1 da RJCS) ou alteração ou cessação do contrato no caso de atuação negligente (art. 26.º/1 da RJCS)¹⁴⁸.

¹⁴⁵ Luís Eduardo Meurer Azambuja, *Direito Securitário e Boa fé: o dever de informação nos contratos de seguros* - Dissertação de Mestrado em Ciências jurídico – Civilísticas II, p. 194 e 195.

¹⁴⁶ *Ibidem*, p. 195.

¹⁴⁷ Luís Poças fala numa espiral de seleção adversa: por haver uma discrepância entre o prémio pago e o risco incorrido pelo segurador, as seguradoras vêem-se obrigadas a aumentar o valor dos prémios no geral, de modo a compensar os sinistros. Acontece, porém que o aumento dos prémios afasta os segurados com riscos mais baixos, que contratarão a seguradora com o prémio mais baixo, que sempre haverá. Isto posto, as seguradoras que aumentaram os seus prémios concentram, em si, os riscos mais elevados. Vide, *ob. cit.*, p. 15.

¹⁴⁸ Neste último caso (art. 26.º), o segurador pode, dentro do prazo de três meses a contar do conhecimento da inexatidão, propor a alteração do contrato, apenas podendo optar diretamente pela cessação quando demonstre que em caso algum celebra contratos para a cobertura de riscos relacionados com o facto que foi declarado de forma inexata. Se o Cliente rejeitar essa alteração, o contrato cessará os seus efeitos, devendo o segurador devolver o prémio na proporção do risco não coberto. Na eventualidade de, entretanto ocorrer um sinistro

Atente-se ainda que, no seio do contrato de seguro, o dever de informação não tem como objetivo a proteção da parte contratual mais débil, “pois ninguém assim considera uma empresa seguradora”, tratar-se-á, ao invés, de uma “exigência extrajurídica da técnica seguradora”.¹⁴⁹

Isto posto, no caso do tomador ou do segurado, impende sobre ele o dever de declaração inicial do risco, um dever instrumental abarcado pelos arts. 24.º a 26.º da RJCS.

Antes da celebração do contrato, na fase de negociação, e por determinação do art. 24.º, o proponente está adstrito ao dever de declarar com exatidão todas as circunstâncias que conheça e razoavelmente¹⁵⁰ deva ter por significativas para a apreciação do risco pelo segurador.

Segundo JOANA GALVÃO TELES, entende-se por declaração de risco, “o conjunto de informações que devem ser unilateralmente prestadas pelo tomador de seguro ou pelo segurado ao segurador na proposta de seguro, as quais visam permitir que o último, mediante o cálculo exato do risco e do correspondente valor do prémio e a apreciação das restantes cláusulas contratuais, decida aceitar ou recusar tal proposta”¹⁵¹.

Na aceção de LUÍS POÇAS, o dever de declaração inicial do risco corresponde ao dever do proponente de “informar o segurador, de forma completa e exata, antes da conclusão do contrato, sobre as características do risco por si proposto, de modo a que o segurador possa

influenciado pelo facto declarado de forma inexata, o segurador deverá efetuar a sua prestação, reduzida na proporção da diferença entre o prémio pago e o que seria devido caso o risco tivesse sido corretamente declarado. Por sua vez, se o segurador demonstrar que de modo algum teria celebrado o contrato se tivesse conhecido a circunstância incorretamente declarada, fica exonerado do dever de prestar, mas tem que devolver o prémio até então pago.

Diferentemente, no caso de incumprimento doloso, o segurador pode, dentro do prazo de três meses a contar do conhecimento da inexatidão, anular o contrato com efeitos retroativos, mantendo, porém, o direito a receber o prémio devido até ao final desse prazo de três meses; caso o segurado tenha atuado com dolo agravado, i.e., com o propósito de obter uma vantagem, o segurador tem o direito a receber o prémio até ao termo do contrato. Estes deveres devem ser transmitidos ao segurado sobre o dever em causa, assim como as consequências do seu incumprimento. Maria Inês de Oliveira Martins, *Regime Jurídico do Contrato de Seguro...*

¹⁴⁹ Luís Eduardo Meurer Azambuja, *Direito Securitário e Boa fé...*cit, p. 196

¹⁵⁰ Portanto, as circunstâncias que o homem médio considera significativas para a apreciação do risco.

¹⁵¹ Joana Galvão Teles, *Deveres de Informação das partes*, in *Temas de Direito dos Seguros a propósito da Nova Lei do Contrato de Seguro* e Ac. do TRL de 22/05/2014, disponível em: <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/cdda74afea44b63680257ce7002f28fe>

determinar a sua vontade negocial e estabelecer as condições contratuais – mormente, tarifárias – equivalentes à probabilidade e intensidade desse risco.”¹⁵²

Por seu turno, o risco é explicado por MENEZES CORDEIRO enquanto a “vertente negativa da álea: a do perigo de um mal”¹⁵³. JOSÉ VASQUES apresenta-o “como o evento futuro e incerto cuja materialização constitui o sinistro”¹⁵⁴. E para MARIA INÊS DE OLIVEIRA MARTINS, o risco traduzirá “as consequências económicas desfavoráveis que um evento incerto é apto a provocar”¹⁵⁵.

Tendo em vista estas conceções, ainda que estas nos despertem para evidências distintas, constatamos que todas elas traduzem o objetivo do contrato de seguro como o de prevenir as consequências negativas da ocorrência do evento que constitui o sinistro. Como é possível observar, também pela leitura do art. 1.º e do art. 44.º do RJCS (cuja epígrafe é a “inexistência do risco”), o risco é um elemento essencial do contrato de seguro, sendo graduado em função da possibilidade de ocorrência do evento tido como sinistro.¹⁵⁶

A despeito do risco, cumpre ainda referir que, por força do art. 51.º do RJCS, o risco manifestar-se-á no valor do prémio, i.e., o prémio deve ser ajustado ao risco que o proponente pretende ver protegido.

Em conformidade, a prática do setor tem-nos ensinado que os riscos mais altos são segurados por preços mais altos ou estão sujeitos a piores condições contratuais. No extremo, alguns proponentes terão os seus riscos avaliados como tão altos que o preço ser-lhes-á inacessível, isto se não virem mesmo as seguradoras recusarem fornecer-lhes cobertura. Por exemplo, é provável que pessoas com maior risco de inundação e que mais necessitam de cobertura também são aquelas com maior probabilidade de não ter seguro para isso. A questão da inacessibilidade é agravada pelo facto de que frequentemente as áreas com os prémios mais altos são aquelas com os níveis de renda mais baixos. Em resposta ao aumento dos

¹⁵² Luís Poças, *Aproximação económica à declaração do risco no contrato de seguro*, in *Revista de Direito e de Estudos Sociais*, 57 (2016), p. 279 e ss.

¹⁵³ Ainda que não se reporte necessariamente a um evento infeliz, podendo, nomeadamente traduzir-se na natalidade. *Direito dos Seguros*, p. 539 e 540.

¹⁵⁴ José Vasques, *Contrato de Seguro (Notas para uma teoria geral)*, Coimbra: Coimbra Editora, p. 127.

¹⁵⁵ *Contrato de Seguro e Conduta dos Sujeitos Ligados ao Risco*, p. 31.

¹⁵⁶ *Ibidem*.

preços, algumas pessoas podem tentar mitigar ou evitar o risco. Outros, aqueles para os quais os prémios de seguro são inacessíveis, passam a ter que assumir o risco.¹⁵⁷

O impacto poderá até traduzir-se no desinteresse da seguradora no próprio risco.¹⁵⁸ O evento incerto, no contexto do contrato de seguro, corresponde a um acontecimento com consequências negativas para o sujeito a quem esse evento diz respeito, quer seja o aumento de despesas, quer seja uma diminuição do seu ativo patrimonial.¹⁵⁹ A prossecução da atividade das empresas de seguro, assim como a prossecução de qualquer atividade profissional, não deixa de ter como objetivo a prossecução de lucro, por esse motivo e em consonância com o princípio da autonomia contratual, as empresas devem poder decidir se pretendem celebrar determinado contrato e em que termos, o que implica necessariamente fazer uma análise cabal do risco, de modo a garantir as provisões necessárias para fazer face aos sinistros. Não se pode impor às seguradoras que aceitem prémios desproporcionais aos riscos em vista proteger.

Por outro lado, os princípios da técnica seguradora assentam na correta análise de risco de todas as situações que lhe sejam propostas, de modo a que a empresa de seguros aceite ou recuse a contratação ou agrave um prémio de acordo com o risco que está em causa. Por essa razão, está o tomador obrigado a declarar com exatidão as circunstâncias que considera necessárias à celebração do contrato e, sendo caso disso, das alterações a essas circunstâncias que ocorram durante a vigência do contrato (arts. 24.º/1 e 91.º).

Ora, no nosso Ordenamento Jurídico, por força do art. 24.º/2 do RJCS, vigora um sistema de questionário aberto¹⁶⁰, segundo o qual o tomador ou segurado «tem o dever ou o ónus de declarar espontaneamente, de forma exata e completa, os factos e circunstâncias que conheça e que razoavelmente deva ter por significativos para a apreciação do risco pelo segurador, mesmo que “a sua menção não seja solicitada em questionário eventualmente fornecido pelo

¹⁵⁷ Cfr. Angelo Borselli, *Smart Contracts in Insurance...* cit.

¹⁵⁸ E neste caso, verificada a recusa por, pelo menos, três empresas de seguros, o proponente de seguro pode recorrer ao Instituto de Seguros de Portugal para que este defina as condições especiais de aceitação (art. 18.º do DL n.º291/2007, de 21 de agosto).

¹⁵⁹ Maria Inês Oliveira, *Contrato de seguro...* cit., p. 31

¹⁶⁰ V. Joana Galvão Teles, *Deveres de Informação...*cit., p.259 e 260. Em sentido diferente, Luís Poças, *Problemas*, ob. cit., p. 23. V. também Ac. do TRL de 22-05-2014, (relator: Ondina Alves), disponível em www.dgsi.pt

segurador para o efeito”», uma vez que este serve apenas como guia na recolha de informação significativa para apreciação.¹⁶¹ Diferentemente, o sistema de questionário fechado impõe o ónus à seguradora de “elaborar um questionário claro e completo, ao qual o tomador de seguro e o segurado possam responder, de forma clara e completa, declarando, assim, os factos e circunstâncias relevantes para a análise do risco a cobrir pela primeira”.¹⁶²

Atente-se, porém, que não se impõe ao proponente “que investigue, estude e analise meticolosamente a informação antes de poder contratar com segurança”, mas *tão-pouco* se lhe impõe o dever de informar sobre aquelas circunstâncias que este conheça e que “possam influir na apreciação do risco ou mesmo a decisão de (não) celebrar o contrato por parte do segurador”¹⁶³.

É precisamente no que toca à informação necessária ao processo de aferição do risco que se tem verificado a grande influência das novas tecnologias. Se anteriormente a seguradora só possuía o conhecimento indireto dos factos que caracterizam o risco, hoje pode ter acesso (em tempo real) a esses factos.

Foi já referida a possibilidade de hoje, ao invés de se recorrer somente à declaração inicial do risco tratamento dos dados recolhidos, a seguradora se valer das tecnologias que permitem efetuar uma avaliação dos riscos e criação de um perfil do segurado. Estas trazem vantagens não só para o profissional, que determina de forma mais precisa o nível de risco do segurado, mas também para o cliente, porque permitem o acesso a produtos personalizados à medida do “seu” risco.

Conforme tivemos ocasião de analisar, a *Big Data* permite traçar um mapa quase completo da vida de alguém.

¹⁶¹ A redação do questionário deve fornecer uma orientação ao segurado de que matérias são relevantes para o segurador. Vide Joana Galvão Teles, *Deveres...* cit. Vide também Maria Inês de Oliveira Martins, *Regime Jurídico do Contrato de Seguro em Portugal...*

¹⁶² No sistema que acolhemos deve, contudo, partir da seguradora, o controlo do preenchimento do formulário, de modo a que não restem perguntas por responder ou respostas incompletas ou demasiado genéricas, ou mesmo contradições, sob pena de este não poder prevalecer-se do regime do incumprimento do dever da declaração inicial de risco.

Por outro lado, se a informação omitida pelo tomador ou segurador incidir sobre factos conhecidos do segurador ou factos de conhecimento geral, também este não pode prevalecer-se da omissão por parte do tomador ou segurado.

¹⁶³ Maria Francisca Rodrigues Santos, *Deveres de informação do tomador do seguro ou do segurado na fase pré-contratual. A informação na contratação eletrónica* - Dissertação de Mestrado em Direito, na Área de especialização de Direito Privado, p. 12 e 13

E se para alguns o recurso à *Big Data* implica ponderadas considerações sobre a legitimidade da seguradora em exigir o acesso aos dados retirados de dispositivos monitores – na opinião de SCOTT R. PEPPEY poderá ser demasiado invasivo permitir que as seguradoras requeiram este tipo de informação detalhada para a celebração de um contrato¹⁶⁴ - entendemos que estas poderão colmatar algumas dificuldades do setor ou, pelo menos, trazer-lhe algumas vantagens. São elas, entre outras, uma maior seleção dos riscos, aplicação de tarifas mais precisas e a criação de produtos adequados às necessidades do cliente.

Ora, neste contexto, surgem algumas questões que merecem alguma ponderação.

Em primeiro lugar, é oportuno indagar se o segurado está obrigado ao dever de informar, quando a informação resulte dos dados recolhidos na Internet. Aliás, há que apurar se o Cliente, ao inibir-se de prestar essa informação, estará a incorrer no incumprimento do seu dever. Do mesmo modo, poderá o segurado ver cumprido o seu dever de comunicar quaisquer fatores que possam ser relevantes para o risco se o plano de seguro a que está vinculado confere acesso direto (i.e., ao vivo) aos seus dados? Isto porque os dispositivos *IoT* têm capacidade de detetar alterações no risco e comunicar essa informação ao contrato inteligente. Falamos aqui daqueles sensores como os medidores de glucose ou pressão arterial, já mencionados.

Na opinião de ANA ALVES LEAL, esta não é uma questão relevante, visto que o resultado da prestação da informação “seria atingido de outra forma e a instituição financeira, afinal, não se encontra em estado de carência informativa”¹⁶⁵.

Por outro lado, é importante apurar qual o valor da informação a que a seguradora tem acesso através destas tecnologias.

De facto, como sublinha LUIS POÇAS “ao permitir uma aferição mais rigorosa do risco (aproximando o risco estimado do real), o domínio dessa informação pode revolucionar a atividade seguradora, possibilitando uma melhor segmentação do risco beneficiando, dessa forma, o segurado consumidor e a própria mutualidade segura”. Em referência aos testes genéticos que revelam o risco de uma pessoa desenvolver uma determinada doença LUÍS POÇAS refere que, ainda que se possam considerar elementos fundamentais para a avaliação

¹⁶⁴ Scott R. Peppet, p. 154 e 155.

¹⁶⁵ Ob. cit. p., 196.

do risco pelo segurador, a verdade é que podem sempre ser dispensados, em virtude de a empresa não querer investir em recursos, pelo menos numa fase inicial, mais dispendiosos.

Além disso, e tal como acontece com os testes genéticos – provavelmente estes até mais precisos do que os dados que aqui enunciamos, a existência de indícios sobre a probabilidade de ocorrência do risco, não significa necessariamente a sua efetivação.

Isto significa que uma maior informação sobre o risco poderá, ao invés de consubstanciar a mitigação do risco, permitir o “desenvolvimento de medidas preventivas que contrariem essas vulnerabilidades” (as vulnerabilidades relativas à saúde de certos indivíduos).¹⁶⁶

Por outro lado, e desta vez, tomando em consideração o caso específico dos seguros de responsabilidade civil automóvel, imagine-se que alguém contrata um seguro automóvel, instalando vários sensores que captam diferentes informações sobre as condições nas quais se deu um sinistro. A questão que se coloca é a de saber qual o valor da informação que é detalhadamente registada e transmitida à seguradora no âmbito de um sinistro quando confrontada com os dados de alguém que não disponha de tão detalhada informação, em função de não ter sensores associados ao serviço.¹⁶⁷

Na esteira de FILIPE ALBUQUERQUE MATOS, constatamos que a regulamentação em vigor dificulta o acesso da informação que as seguradoras consideram como necessária para decidirem de forma livre, sã e esclarecida e, conseqüentemente, de se valerem dessas informações para adequarem o valor do prémio. De certo modo, poderá obstar à aplicação e desenvolvimento da tecnologia no setor¹⁶⁸.

Não só a nível da proteção de dados verificamos essa dificuldade, uma vez que, na medida do estudado, só é permitido o tratamento dos dados quando houver consentimento expresso do titular nesse sentido; como também devido à imposição, ao segurado de um dever de informação.

Ora, o aparecimento da Internet das Coisas, se desenvolvido, vem em grande medida distorcer os termos em que é exercido esse dever. De facto, afigura-se uma mudança na detenção da informação que passa do tomador/segurado para o segurador, os equipamentos “monitorizadores” permitem que o segurador tenha o conhecimento direto da situação do tomador/segurado, sem que este tenha que servir de intermediário.

¹⁶⁶ V. Luís Poças, *O Dever de Declaração Inicial do Risco no contrato de Seguro*, p. 743 e 744.

¹⁶⁷ Paula Ribeiro Alves, *Os desafios digitais no mercado segurador*, in *Fintech – Desafios da tecnologia Financeira*, p. 47

¹⁶⁸ *O Regulamento de Proteção de Dados Pessoais... cit*, p. 114

Assim, tendo a seguradora a possibilidade de ter um contacto direto com a informação sobre o risco, é de questionar se o proponente se encontra, ainda adstrito à obrigação inicial de declarar o risco e às que decorrem da alteração do risco já no decorrer do contrato (art. 91.º da RJCS), i.e., em que termos pode considerar a seguradora a informação por si recolhida pela Internet ou pelos aparelhos dispositivos se esta não foi prestada diretamente pelo segurado.

E ainda, que relevância terá a informação fornecida pelo cliente quando confrontada com a informação recolhida pelos dispositivos? Em princípio, a seguradora poderá “atribuir à informação obtida (...) a relevância que bem entender no contexto daquilo que sejam as suas preferências subjetivas”¹⁶⁹, salvo regulamentação em contrário. A despeito da veracidade da informação deve, por um lado, ter-se em atenção que a informação providenciada por dispositivos *IoT* sempre será mais fiável, na medida em que é recolhida por dispositivos não sujeitos à parcialidade que o próprio segurado terá sobre si; e, por outro lado, que estes dispositivos de recolha de informação, como denota HÉLDER FRIAS, e bem, “tipicamente são equipamentos pouco sofisticados que não gozam dos mesmos mecanismos de segurança de um computador pessoal (antivírus, combate ao *malware*, atualizações periódicas, etc)”¹⁷⁰.

Não obstante, quando a informação atravessa um processo de tratamento, como acontece com os *Big Data*, é possível, porque baseada numa análise preditiva, que esta não seja a mais precisa em relação a todo e qualquer utilizador.

Desta sorte, deve sempre ser possível, para o segurado, que este, verificando a imprecisão da informação recolhida, possa refutá-la.

Uma tentativa de responder às questões supraexpostas, requererá sempre uma ponderação entre o direito à autodeterminação informativa (art. 35.º da CRP) dos segurados e a carência que as empresas seguradoras têm de aceder à informação considerada necessária para a determinação da celebração do contrato com determinado proponente, sem descuidar o desenvolvimento tecnológico do setor.

No nosso entender, e tendo também em vista a inovação do mercado segurador, ao segurador deve ser dada a possibilidade de decidir tomar ou não tomar em consideração as

¹⁶⁹ Ana Alves Leal, *Aspetos...* cit., p. 209

¹⁷⁰ Hélder Frias, *A Internet das coisas...* cit., p. 250 e 251.

informações pré-contratuais disponibilizadas pelo proponente quando confrontadas com as informações extraídas pelas tecnologias da *IoT* e da *Big Data*.

Não obstante, consideramos ser necessária alguma flexibilização na regulação deste tema, de modo a fomentar a progressão da tecnologia.

4.4 As práticas discriminatórias

Já se referiu a capacidade que a tecnologia *Big Data* tem para, após a recolha de dados, organizá-los em categorias, de tal modo que a vida de uma pessoa pode ser toda retratada em dados.¹⁷¹

Esta prática consubstancia uma subcategoria do tratamento de dados pessoais que opera de forma automatizada, a definição de perfis. Retratada no n.º 4 do art. 4.º do RGPD, esta categoria de tratamento, diz respeito a “qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações”.¹⁷²

Os resultados deste tratamento de dados apresentam previsões para o futuro através da utilização de técnicas de *machine learning* que consistem essencialmente em algoritmos preparados para detetar padrões comportamentais na informação recolhida e fornecida pelo titular dos dados ou terceiros, até. Estas deduzem as preferências de determinadas categorias da população com base numa “amostra” dessa categoria. Por outras palavras, tiram conclusões sobre os titulares de dados. Significa que são recolhidos dados provenientes de várias fontes para deduzir algo sobre alguém, com base nas características ou comportamentos de outras pessoas que, estatisticamente, parecem semelhantes por se encontrarem na mesma faixa etária, serem do mesmo sexo, ou por terem comportamentos de navegação na Internet semelhantes.

¹⁷¹ Bruno Ricardo Bioni, *Proteção de Dados Pessoais: a função e os limites do consentimento*, p. 87

¹⁷² Segundo o art. 4.º/2 do RGPD, o tratamento de dados consiste numa “operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição”.

Esta informação será posteriormente usada com vista à orientação na tomada de decisões pelo responsável pelo tratamento de dados.

Acontece, porém que o tratamento dos dados nestes termos potencia práticas discriminatórias contra os titulares de dados. Na senda do que se tem vindo a explicar, a definição de perfis, prevista no n.º 4 do art. 4.º do RGPD, consiste fundamentalmente na categorização de pessoas, acabando por restringi-las às (potenciais) preferências apresentadas como resultado da análise dos dados.

A título de exemplo, um estudo revelou que a *LexisNexis*, uma empresa que presta serviços jurídicos através de tecnologias como *machine learning* e inteligência artificial, usava vários dados pessoais não relacionados com a condição de saúde da pessoa para prever os seus custos médicos que teria. Tais informações variavam, desde números de telefone de pessoas, antecedentes criminais, registos de propriedades, segurança do bairro onde habitavam, etc. Tinha-se vindo a notar que informações como a habitação em bairros mais pobres ou bairros de cor, que traduzem o aumento das despesas com assistência médica resultavam, no aumento dos prémios dos seguros de saúde, ou mesmo na recusa de celebração do contrato para os sujeitos implicados. Outros fatores a ter em conta seriam, por exemplo, a compra, por uma mulher, de roupas *plus size*, o que, segundo o algoritmo, era indicador de risco de depressão mais elevado e do conseqüente aumento dos custos de saúde, porque já se tinha confirmado que um determinado número de mulheres, na mesma faixa etária e com os mesmos comportamentos sofria de depressão.¹⁷³

A este respeito e em função do supracitado no ponto anterior, cumpre ressaltar que a adaptação, só por si, do prémio do seguro ao segurado que comporte um risco mais elevado não configura uma prática discriminatória. Vejamos.

De modo a obviar as práticas supramencionadas, o legislador introduziu alguns diplomas relevantes. Em primeiro lugar, a Lei n.º 46/2006, de 28 de Agosto proíbe e pune a discriminação em razão da deficiência e da existência de risco agravado de saúde.

Também o DL n.º 72/2008, de 16 de Abril, que estabelece o Regime Jurídico do Contrato de Seguro consagra, no art. 15.º, a proibição de práticas discriminatórias em violação do

¹⁷³Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, disponível em: <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>

princípio da igualdade nos termos previstos no artigo 13.º da Constituição da República Portuguesa e em relação a todos os seguros. Em função do disposto no n.º 2 do art. 15.º, “são consideradas práticas discriminatórias, em razão da deficiência ou em risco agravado de saúde, as ações ou omissões, dolosas ou negligentes, que violem o princípio da igualdade, implicando para as pessoas naquela situação um tratamento menos favorável do que aquele que seja dado a outra pessoa em situação comparável”, exceto práticas e técnicas de avaliação, seleção e aceitação de riscos próprias do segurador que sejam objetivamente fundadas e tenham por base dados estatísticos e atuariais rigorosos considerados relevantes nos termos dos princípios da técnica seguradora (n.º 3).

Depois, a DDS regula a distribuição de todos os tipos de produtos de seguros por todos os tipos de distribuidores, reforçando o dever do distribuidor de seguros de adequar o produto ao segurado (art. 20.º/1), mas impedindo práticas discriminatórias de venda, nomeadamente quando o uso da análise de *big data* as possa proporcionar (arts. 8.º/4 e 9.º/1).

A Diretiva 2004/113/CE do Conselho de 13 de Dezembro de 2004¹⁷⁴, que pugna pelo tratamento igual entre homens e mulheres no acesso a bens e serviços e seu fornecimento, expõe, no seu art. 4.º, o princípio da igualdade de tratamento, sob o qual se proíbe qualquer discriminação direta e indireta em função do sexo.¹⁷⁵

Ainda, em função do art. 5.º, “os Estados-Membros devem assegurar que, em todos os novos contratos celebrados (...) a consideração do sexo enquanto fator de cálculo dos prémios e das prestações para efeitos de seguros e outros serviços financeiros não resulte, para os segurados, numa diferenciação dos prémios e prestações. Atente-se, ainda na Lei n.º 9/2015, de 11 de fevereiro, esta veio implementar no nosso ordenamento jurídico a decisão do Acórdão do Tribunal de Justiça da União Europeia, de 1 de março de 2011 (Processo C-236/09, «Test-Achats»)¹⁷⁶ que considerou inválido o n.º 2 do artigo 5.º da Diretiva n.º 2004/113/CE do Conselho, de 13 de dezembro.

¹⁷⁴ Transposta pela Lei n.º 14/2008, de 12 de março.

¹⁷⁵ É, então, oportuno esclarecer que se entende haver discriminação direta quando, em função do sexo, uma pessoa for sujeita a tratamento menos favorável do que aquele que é dado a outra pessoa em situação equivalente. A Diretiva ainda esclarece que as diferenças entre homens e mulheres na prestação de serviços de saúde resultantes das suas diferenças físicas não se referem a situações equivalentes, pelo que não constituem discriminação.

¹⁷⁶ O acórdão pode ser consultado em: <http://curia.europa.eu/juris/document/document.jsf?jsessionid=B9024BDB1A0672FFD7D8652A8F72B385?text=&docid=80019&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=3354866>

Na situação em concreto, a Associação Belga dos Consumidores considerava que o art. 5.º/2 da Diretiva era contrário ao princípio da igualdade entre homens e mulheres. Em apreciação das questões, invocou-se o décimo oitavo considerando da Diretiva que enuncia que a consideração do sexo enquanto fator atuarial não deve resultar numa diferenciação nos prémios e benefícios individuais. Contudo, o considerando seguinte reconhece uma derrogação ao princípio da igualdade de tratamento entre homens e mulheres, a faculdade de os Estados-Membros não aplicarem a regra dos prémios e das prestações unissexo.

Ora, era precisamente no art. 5.º/2 da Diretiva que residia essa derrogação. O artigo permitia diferenciações proporcionadas nos prémios e benefícios individuais sempre que a consideração do sexo fosse um fator determinante na avaliação de risco com base em dados atuariais e estatísticos relevantes e rigorosos. Nestas circunstâncias, existia o risco de que a derrogação à igualdade de tratamento entre homens e mulheres prevista no artigo 5.º/2, da Diretiva fosse indefinidamente permitida pelo direito da União, i.e., sem limite temporal.

Considerou, assim, o Tribunal que esta disposição deveria ser considerada inválida com efeitos a 21 de dezembro de 2012.

Vale ainda referir a Norma Regulamentar n.º 8/2008-R, de 6 de Agosto, emitida pelo Instituto de Seguros de Portugal. Segundo a Norma, as empresas de seguros que pretendam introduzir ou manter diferenciações nos prémios e prestações individuais de seguros devem elaborar, atualizar e publicar no sítio da Internet ou entregar em suporte papel quando solicitado, os rácios do custo do risco entre os sexos e identificar os dados em que basearam a avaliação do risco nos termos previstos.

Do exposto resulta que qualquer diferenciação no tratamento deve ser baseada numa análise do risco fundada em cálculos objetivos. Na verdade, é no art. 51.º da RJCS que esta prática é legitimada: “o prémio é a contrapartida da cobertura acordada e inclui tudo o que seja contratualmente devido pelo tomador do seguro, nomeadamente os custos da cobertura do risco, os custos de aquisição, de gestão e de cobrança e os encargos relacionados com a emissão da apólice”. Ou seja, o risco reflete-se no prémio, assim, quanto mais alto for o risco, compreensivelmente, mais alto será o valor a pagar pelo segurado.

Por outro lado, se pretender recusar celebrar contrato com determinado Cliente ou agravar o prémio em função de deficiência ou de risco agravado de saúde, a seguradora deve

prestar informação ao proponente sobre o rácio entre os fatores de risco específicos e os fatores de risco de pessoa em situação comparável mas que não esteja afetada por aquela deficiência ou risco agravado de saúde, nos termos dos n.ºs 3 a 6 do art. 178.º, implicando a comunicação do resultado de exames médicos e dos efeitos desses resultados que resultam na recusa da celebração do contrato ou agravamento do prémio (art. 15.º/4 da RJCS)¹⁷⁷.

Da leitura dos preceitos, observa-se que o condicionamento da celebração do contrato de seguro a um determinado preço mais elevado, baseado no facto de o Cliente ser suscetível de desenvolver uma determinada doença, por exemplo, não resulta numa prática discriminatória, porquanto, na verdade, uma análise objetiva dos fatores relevantes para a apreciação do risco demonstram que a verificação deste era mais provável relativamente a este segurado.

Assim, para que se verifiquem práticas discriminatórias, devem sempre observar-se dois elementos: a violação do princípio da igualdade e a recusa ou penalização¹⁷⁸ na celebração do contrato.

Por fim, ao abrigo do RGPD, a definição de perfis está regulada no art. 22.º, que confere ao titular de dados o direito “de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.”

Segundo ANA ALVES LEAL, este direito corresponde a “uma situação de imunidade do titular dos dados à tentativa de outra pessoa (o decisor) alterar a sua esfera jurídica através de uma ação (a tomada de decisão)”.¹⁷⁹

Assim, pode requerer a intervenção humana no tratamento dos dados, o titular dos dados que tenha sido sujeito a uma decisão tomada de forma automatizada ou de uma decisão com intervenção humana, mas cuja motivação assente nos resultados do tratamento automatizado de dados.

¹⁷⁷ Para mais desenvolvimento, v. *A discriminação e a avaliação do risco nos seguros*, in *Revista de Direito e Estudos Sociais*, ano LII (XXV da 2ª série), julho/dezembro, ano de 2011, nº 3-4, p. 245-250.

¹⁷⁸ E com penalização, deve entender-se quer agravamentos do prémio, quer limites de indemnizações, por exemplo. *Ibidem*, p. 223

¹⁷⁹ *Idem*, p. 153

Desconstruindo estes requisitos, é necessário que se verifique: i) uma decisão tomada por meios exclusivamente tecnológicos, sem qualquer intervenção humana; ii) dirigida a uma pessoa concreta; iii) que produza efeitos na esfera jurídica dessa pessoa ou que o afete significativamente ou de forma similar.

Relativamente ao primeiro requisito, só não estamos perante uma decisão automatizada quando se verifique uma “real influência humana no resultado final do processo de tomada de decisão” relativamente a uma pessoa individual.

Este segundo requisito impõe que a decisão seja individual, mas não requer que a definição do perfil o seja. “Assim, pode existir uma definição de perfis relativa a um grupo que, por seu turno, resulte numa decisão com impacto num específico titular dos dados”.¹⁸⁰

Por fim, a decisão deve ser suscetível de produzir efeitos na esfera jurídica do titular dos dados ou afetá-lo significativamente de forma similar, no sentido em que os efeitos sentidos pelo titular dos dados sejam “suficientemente relevantes ou importantes para merecerem atenção” e que a decisão tenha “o potencial para influenciar de forma significativa as circunstâncias, comportamento ou escolhas da pessoa visada”, o que inclui as situações “em que as decisões automatizadas afetem (...) os seus [do titular dos dados] direitos num contrato”.¹⁸¹ Não é imperativo que o impacto seja negativo, vigorando o princípio *invito non datur*, i.e, ninguém pode ser beneficiado contra a sua vontade.¹⁸² Ademais, de modo a proteger o titular dos dados nos casos em que haja um prejuízo da dignidade, integridade ou reputação, entende-se que os efeitos da decisão automatizada a verificarem-se na esfera da-quele poderão ser imateriais.

Na esteira de MADALENA PERESTRELO DE OLIVEIRA, consideramos ser essencial fazer-se uma análise casuística “que considere o contexto e objetivo do tratamento, bem como o tipo de dados envolvidos”.¹⁸³

Não obstante, deve reter-se que as informações trazidas pela *Big Data* fazem um tratamento automatizado de dados comportamentais de uma fração da população que apresenta semelhanças entre si. Decerto que dentro daquela “fatia” existem exceções. Neste sentido,

¹⁸⁰ Madalena Perestrelo de Oliveira, *Definição...cit*, p.77

¹⁸¹ Ibidem, p. 76

¹⁸² Madalena Perestrelo de Oliveira, *Definição...cit*, p. 76, vide também Ana Alves Leal, ob. cit., p. 138

¹⁸³ Ibidem, p. 77

ANA ALVES LEAL considera ainda a possibilidade de o visado poder desvincular-se, re-
futando aquelas informações que, relativamente ele, não são verdadeiras.¹⁸⁴

Em alternativa, o titular dos dados tem direito a opor-se ao tratamento dos seus dados
pessoais quando estes sejam utilizados para fins de comercialização direta, nos termos do
art. 21.º do RGPD.

Concluindo, pode ainda dizer-se que “em caso de dúvida, a ratio subjacente ao Regula-
mento impõe que se decida a favor do titular dos dados e se conceda direito a intervenção
humana no processo de tomada de decisão”¹⁸⁵.

Além disso, o titular dos dados pode fazer-se valer dos meios de defesa constantes no
RGPD¹⁸⁶, tais como o direito de retificação, no art. 16.º, o direito ao apagamento dos dados,
no art. 17.º e o direito à limitação do tratamento, no art. 18.º.

5. Inteligência Artificial e *Robot-Advisors*

Ainda não se verifica unânime o conceito de Inteligência Artificial. A OCDE avança
que a Inteligência Artificial (IA) é a inteligência exibida pelas máquinas. Sendo assim, uma
máquina seria considerada "inteligente" quando tem em consideração o seu ambiente e toma
medidas otimizadoras da sua performance.¹⁸⁷ Recentemente, a Comissão Europeia, adiantou
que a IA se resumia ao “conjunto de tecnologias que combinam dados, algoritmos e capaci-
dade computacional”.¹⁸⁸

Com o recurso à IA as empresas seguradoras conseguem obter uma gestão mais célere
dos sinistros e eficiente. É possível receber e analisar um grande número de relatos de ocor-

¹⁸⁴ *Aspetos jurídicos...* p. 196

¹⁸⁵ *Ibidem*, p. 77

¹⁸⁶ Ora, o recurso a estes meios de defesa não implica necessariamente que o tratamento dos dados seja
proibido. Tal como refere Ana Alves Leal, o tratamento de dados pressupõe a declaração unilateral do titular
de dados ao responsável pelo tratamento e só após essa autorização se dá a constituição do direito de oposição
e o direito de apagamento dos dados, o que “permite antever que em causa estão meios de defesa do titula dos
dados também perante condutas lícitas do responsável pelo tratamento”. Em boa verdade, “sendo o tratamento
proibido (...) o responsável pelo tratamento estaria já (independentemente de qualquer impulso de defesa por
parte do titular dos dados) obrigado a não praticar nenhum comportamento tendente a esse tratamento”. Ana
Alves Leal, *ob. cit.*, p. 146 e 147

¹⁸⁷ OECD (2017), *Technology and innovation in the insurance sector*.

¹⁸⁸ *Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a
confiança*, Bruxelas, 19.2.2020 COM(2020) 65 final, disponível em: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf

rências e selecionar aquelas que exigem uma investigação mais profunda e aquelas que merecem cobertura, uma vez que tem a capacidade de reconhecer padrões e fazer previsões em função dessa informação. Será, contudo, o aconselhamento prestado pela IA e os desafios que as seguradoras enfrentarão com a sua utilização que serão o foco da análise que se segue.

Os *robot advisors* ou *robots* consultores consistem, essencialmente, numa modalidade de consultoria financeira automática que envolve uma reduzida intervenção humana.¹⁸⁹ Segundo MAFALDA MIRANDA BARBOSA, o “aconselhamento automatizado é visto como a prestação de serviços de consultoria para investimento ou de gestão de carteiras através de um sistema automatizado ou semi-automatizado utilizado como ferramenta de utilização direta pelo cliente, sem intervenção humana”¹⁹⁰.

Os *robot advisors*, através do recurso a algoritmos matemáticos, conseguem fornecer uma orientação financeira adaptada às necessidades do proponente a custos reduzidos¹⁹¹, após a recolha de informações junto do cliente e avaliação das suas necessidades e pretensões. O aconselhamento pode incidir sobre vários elementos, primeiramente poderá culminar numa avaliação às apólices atuais do cliente com vista a informá-lo sobre a sua cobertura e desenvolver um (novo) plano adaptado ao cliente. Posteriormente, os *robot advisors* poderão operar no sentido de implementar esse plano, nomeadamente, abrir contas, transferir ativos e, no decorrer da relação contratual, ajustar esse plano em função das várias análises que se vão fazendo, das atualizações de mercado, etc.

Além de o consumidor conseguir obter aconselhamento sobre um produto a custos reduzidos, a consultoria robótica é, geralmente mais acessível, prescindindo da deslocação a uma agência, o que, em consequência deixa o consumidor mais “à vontade” para discutir a situação monetária em que se encontra.¹⁹² Para o prestador de serviços, esta tecnologia permite-lhe atingir um maior número de (potenciais) clientes e melhorar os serviços que oferece.¹⁹³

¹⁸⁹ António Barreto Menezes Cordeiro, *Inteligência Artificial e consultoria Robótica (Automation in Financial Advice)*, in *Fintech – Desafios da tecnologia financeira*, p. 223 e 224

¹⁹⁰ *Robot advisors e Responsabilidade Civil*, in *Revista de Direito Comercial*, disponível em: <https://www.revistadedireitocomercial.com/robot-advisers> e Pedro Maia, *A Robotização do mundo financeiro: reflexões introdutórias*, in *Direito e Robótica – Actas do Congresso*, n.º 16, 2020, p. 288

¹⁹¹ Embora, segundo refere António Barreto Menezes Cordeiro esta redução nos custos é empregue, na sua maioria, por empresas jovens em busca de um lugar sólido no mercado, p. 226 e 227

¹⁹² V. OCDE (2017), *Technology and innovation in the insurance sector* e António Barreto Menezes Cordeiro, ob. cit., p. 226

¹⁹³ Para mais desenvolvimento cfr. Menezes Cordeiro, ob. cit., p. 227

Por sua vez, em comparação com o aconselhamento robótico, a interação humana logra por fomentar a confiança e entendimento entre as partes. O que as empresas podem procurar colmatar recorrendo a *chat bot's*, instrumentos que fornecem assistência ao cliente *on-the-go*.

A *startup* francesa Minalea desenvolveu um *robot advisor* para a comercialização de seguros. O *Smart Sales Assistant* analisa em profundidade o conteúdo e os serviços dos produtos no mercado e pode ser usado tanto por redes de distribuição como bancos e seguradoras¹⁹⁴, como pode ser usado para contactar diretamente com os Clientes, através do “*chatbot Alfred*”¹⁹⁵. Através de algoritmos complexos e da IA este *robot* ajuda as seguradoras a aconselhar instantaneamente os seus clientes, mudando o foco do preço para os aspetos positivos do produto e do prestador de serviços, gerando um discurso de vendas adaptado ao Cliente, o que desenvolveu através da avaliação do perfil deste e do seu seguro atual.

À semelhança do que determinou o Código dos Valores Mobiliários, no seu art. 294.º/2 para a consultoria relativa aos produtos financeiros de investimento, a atividade de consultoria “requer a apresentação do conselho como adequado a um cliente em concreto, em função das suas circunstâncias individuais”. Nesta aceção, a consultoria não tem que consistir num atendimento efetivamente personalizado, *apenas* tem que ser percecionada como tal, algo que deve ser aferido em função da perspetiva do cliente.¹⁹⁶

5.1 Deveres de Informação do Segurador

Tal como o segurado, também o segurador está adstrito a deveres de informação.

Em primeiro lugar, devemos ter em conta que estes deveres são muito vastos. O art. 18.º do RJCS estatui que a seguradora está adstrita a um dever geral de esclarecimento e informação pré-contratual, no qual se incluem, entre outras, as informações relativas ao âmbito do risco que se propõe cobrir, às exclusões e limitações da cobertura e ao valor total do prémio, ou, não sendo possível, ao método de cálculo do mesmo. Na apólice, além dos elementos elencados no art. 18.º da do RJCS, o segurador deve incluir os elementos vertidos do art. 37.º/2 do mesmo diploma.

¹⁹⁴ Vide <https://www.minalea.com/assistant-commercial-intelligent-mi>

¹⁹⁵ Vide <https://www.minalea.com/alfred-le-chatbot>

¹⁹⁶ Pedro Maia, *A robotização do mundo financeiro...*, p. 277

Por imposição do art. 21.º, estas informações devem ser prestadas “de forma clara, por escrito e em língua portuguesa (...)” e “com a antecedência necessária para que, tendo em conta a importância do contrato e a extensão e complexidade das cláusulas, se torne possível o seu conhecimento completo e efetivo por quem use de comum diligência”, conforme dispõe o art 5.º/2 do DL n.º 446/85, de 25 de outubro, aplicável às cláusulas contratuais gerais. Relativamente à apólice e sempre que seja possível prescindir de meios técnicos, o legislador estabeleceu que devem ser usadas palavras e expressões do uso corrente. Para tal, o contrato deve ser comunicado individual e integralmente ao segurado.

Em determinadas situações, quando a complexidade da cobertura e o montante do prémio a pagar ou do capital seguro assim o justificarem, o segurador está sujeito a um dever especial de esclarecimento acerca de que modalidades de seguro, entre as que ofereça, são convenientes para a cobertura que o proponente procure (cfr. art. 22.º do RJCS). Neste ensejo, o segurador deve chamar a atenção para determinadas exclusões, períodos de carência, o regime da cessação do contrato por vontade do segurador, e ainda, nos casos de sucessão ou modificação de contratos, para os riscos de rutura de garantia, do montante do prémio e do meio de contratação usado. Ou seja, o segurador tem, não só, que responder a

A par disto, o segurador deve sempre disponibilizar-se para responder a todos os pedidos de esclarecimento feitos pelo tomador do seguro, como tem também que ter uma atitude proactiva no cumprimento do dever de esclarecimento aos Clientes (art. 22.º/2 do RJCS).

Também o DL n.º 95/2006, de 29 de maio que estabelece o regime jurídico aplicável aos contratos à distância relativos a serviços financeiros celebrados com consumidores (RCDSF), transpondo para a ordem jurídica nacional a Diretiva n.º 2002/65/CE, do Parlamento Europeu e do Conselho, de 23 de Setembro, relativa à comercialização à distância de serviços financeiros prestados a consumidores, nos seus arts. 11.º e 12.º, determina que a informação deve ser prestada em papel ou num outro suporte duradouro e deve ser prestada de modo inequívoco, claro e perceptível, de forma adaptada ao meio de comunicação à distância utilizado e com observância dos princípios da boa-fé.

Ademais, os contratos de seguro são geralmente celebrados com base em condições gerais de seguro que permitem ao fornecedor a elaboração de um contrato que lhe é mais favorável e que o proponente apenas aceita (ou não). Por isso mesmo, este encontra-se também sujeito à Lei das Cláusulas Contratuais Gerais (doravante LCCG). Resulta dos arts. 5.º e 6.º

da LCCG, os deveres de informação e de comunicação do segurador ao tomador do seguro ou segurado.

Não obstante, tem-se verificado, tendo em conta o complexo elenco de informação que o segurado, seja ele consumidor ou não, tem que ler, que muitas vezes o Cliente se inibe de analisar as informações que são prestadas pelo prestador de serviços. E embora deva ser-lhe exigido que esteja informado, mormente nos contratos que, como o de seguro, envolvem uma especial complexidade, verifica-se que a informação disponibilizada é maioritariamente composta por conceitos técnicos, não bastando uma simples leitura por parte do tomador/segurador.

Por sua vez, o art. 23.º da RJCS impõe a aplicação de sanções em caso de incumprimento dos deveres de informação e esclarecimentos pré-contratuais. Estatui o referido artigo que o incumprimento dos deveres acima referidos faz incorrer o segurador em responsabilidade civil, nos termos gerais, conferindo ao tomador do seguro, o direito de resolução do contrato, salvo quando o incumprimento não tenha razoavelmente afetado a decisão de contratar da contraparte ou haja sido acionada a cobertura por terceiro.

Finalmente, o art. 9.º do DL n.º 57/2008, que estabelece o regime aplicável às práticas comerciais desleais das empresas nas relações com os consumidores, ocorridas antes, durante ou após uma transação comercial relativa a um bem ou serviço¹⁹⁷, classifica a omissão dos deveres de informação impostos pelos diplomas acima referidos como prática comercial desleal, consagrando, várias sanções para esta infração.

Em função do exposto, a questão que se impõe é a de saber se a informação pode ser prestada pelo *chat bot*, ou *robot advisor* ou se este fornece “meros” conselhos? Por outro lado, cumpre questionar se os conselhos que o *robot* presta, se suficientemente completos, são o bastante para ver cumprida a obrigação de prestação de informações. E sendo-o, a informação pode considerar-se regularmente prestada “de forma clara” quando fornecida nesses trâmites? Ademais, preocupa o modo como a informação vai ser disponibilizada no *site* da seguradora.

¹⁹⁷ Este DL transpõe para a ordem jurídica interna a Diretiva n.º 2005/29/CE, do Parlamento Europeu e do Conselho, de 11 de Maio, relativa às práticas comerciais desleais das empresas nas relações com os consumidores no mercado interno.

Relativamente a esta última questão, parece ter-se como pacífico que a informação obrigatória tem que ser dirigida ao proponente, não bastando a simples disponibilização da mesma na Internet.

PAULA RIBEIRO ALVES estatui que a loja virtual da seguradora deve aproximar-se o mais possível a uma loja física. Sendo assim, da mesma maneira que uma seguradora não deixaria o segurado procurar as informações pela sua loja, entregando-a, ao invés, em mão, na loja virtual, a informação deve ser exposta ao cliente da forma mais evidente e direta possível.¹⁹⁸

Além do mais, quando a lei impõe que a informação seja transmitida de forma clara, deve entender-se que a informação deve ser prestada “sem sentidos dúbios, sem termos muito técnicos e demasiado complexos para um tomador de seguro médio normal e razoável compreender, sem recurso a técnicas que acabam por esvaziar ou alterar o sentido das cláusulas contratuais”.¹⁹⁹

No seguimento do exposto, compreende-se que as maiores dificuldades na prestação de deveres de informação por *robots* incidirão na necessidade de garantir que o Cliente fica esclarecido relativamente ao produto que adquire e todas as suas condições de aquisição, até porque o cumprimento cabal dos deveres de informação e esclarecimento depende da adequação da linguagem ao destinatário. A seguradora deve, sobretudo, ter em atenção que ao recorrer a sistemas automatizados, estas informações revestem importância acrescida. A meu ver, a aptidão destes instrumentos para satisfazerem os deveres de informação deve sempre ser aferida em concreto, não parecendo, contudo que deva ser imediatamente negada.²⁰⁰

5.2 Responsabilidade Civil dos *Robot-Advisors*

Em virtude das características dos *robots* que temos vindo a enunciar, pode surgir um número variado de riscos sobre interesses juridicamente protegidos. Designadamente, sempre que, como consequência de um determinado conselho no sentido da adesão a um determinado produto de investimento ou contratação de um seguro, o segurado sofra determinados danos, surgirá a dúvida sobre a viabilidade de articular um pedido de indemnização.

¹⁹⁸ Vide Paula Ribeiro Alves, *Contrato de seguro...* cit., p. 191

¹⁹⁹ Joana Galvão Teles, *Deveres de Informação das Partes*, p. 731

²⁰⁰ No mesmo sentido, v. A. Barreto Menezes Cordeiro, ob. cit. p. 234-236

À atuação destes *robots* aplicam-se as mesmas regras que impendem sobre a consultoria realizada com intervenção humana. No caso dos seguros, está regulada pela Lei n.º 147/2015, de 9 de setembro, o DL n.º 72/2008, de 16 de abril e o DL n.º 95/2006, de 29 de maio, que se aplica à contratação de serviços financeiros à distância.

Particularmente, quando a atuação por parte do prestador de serviços é feita sem a intervenção do ser humano, coloca-se a questão de saber quem deverá responder pelos danos que surjam para a outra parte de um conselho dado pela máquina. A principal questão reside na imputação das falhas perpetradas pelos *robots*.

Da análise feita por MAFALDA MIRANDA BARBOSA e ANTÓNIO PINTO MONTEIRO²⁰¹, constatamos que deve imputar-se a responsabilidade àquele que usa o *robot* para prestar o serviço. Eleva-se aqui o brocardo *ubi commodum, ibi incommodum*, segundo o qual aquele que tira benefícios da utilização de um *robot*, *in casu*, deve ser responsável pelos danos que decorrem dessa utilização.

Não nos parece que seja possível imputar, ao invés, a responsabilidade ao *robot*, atribuindo-lhe personalidade jurídica, com base na ideia de que estes são dotados de autonomia, têm capacidade de autoaprendizagem e de adaptação do seu comportamento ao meio ambiente. Neste sentido, os *robots* aproximar-se-iam dos seres humanos, i.e., ambos apresentam níveis de inteligência semelhantes.

Não obstante, estabelecer qualquer analogia ou comparação com os seres humanos “por maior que seja o grau de sofisticação dos *robots* e de outros mecanismos dotados de inteligência artificial – é desdignificante para o ser humano”. Tal como nota, e bem, MAFALDA MIRANDA BARBOSA, “a autonomia dos *robots* é uma autonomia tecnológica, fundada nas potencialidades da combinação algorítmica que é fornecida ao *software*. Está, portanto, longe do agir ético dos humanos, em que radica o ser pessoa”.

Note-se que, precisamente por esta razão, não será possível apurar a responsabilidade do intermediário financeiro ou do consultor nos termos do art. 500.º, que define os termos em que

²⁰¹ Vide Mafalda Miranda Barbosa, *Robot advisors e Responsabilidade Civil*, in *Revista de Direito Comercial* e António Pinto Monteiro, “*Qui Facit Per Alium, Facit Per Se*” - *Será ainda assim na Era da Robótica?*, in *Direito e Robótica, Actas do Congresso*, nº 16, 2020, Edição Especial.

o comitente responde pelos danos que o comissário causar, ou do art. 800.º relativo à responsabilidade contratual do devedor pelos atos dos representantes legais ou dos auxiliares que utilize no cumprimento da obrigação, ambos os artigos do CCiv. Neste caso, o *robot* seria apontado como “instrumento” de que o fornecedor ou prestador de serviços se serve para cumprir as suas obrigações. O que nos remete, em bom rigor, ao comportamento do próprio e não de terceiro.

De seguida, há que notar que o *robot* não consegue, ele mesmo, suportar os efeitos de lhe ser imputada a responsabilidade, pois não dispõe de meios para tal.

Dessarte, pode procurar responsabilizar-se o fornecedor ou prestador de serviços pelos atos dos *robots*, como se fossem seus “atos próprios” com base na má escolha dos meios que usou para fazer cumprir a sua prestação, numa vigilância deficiente da sua parte ou no fornecimento deficiente de instruções.

A solução poderá residir na aplicação do regime da responsabilidade civil do produtor, que consta no diploma que transpôs a Diretiva n.º 85/374/CEE, o DL n.º 383/89, desde logo porque o regime da responsabilidade do produtor “proporciona um nível de proteção que os regimes nacionais de responsabilidade culposa não são, por si só, capazes de garantir”²⁰² e que, complementarmente, na eventualidade de existirem vários produtores responsáveis, permite a responsabilização de todos eles, uma vez que, por força do art. 6.º do diploma, está em causa uma responsabilidade solidária²⁰³.

Para que caiba a aplicação do regime da responsabilidade objetiva do produtor, é necessário estarmos perante um produtor que, na acessão do art. 2º do diploma em análise pode ser produtor real ou efetivo (1.ª parte do n.º 2), aparente (2.ª parte do n.º1) ou presumido (alínea a) e b) do n.º 2). Neste sentido, o produtor pode ser o engenheiro robótico, o programador ou produtor de *software*, o produtor de hardware ou aquele que apenas tenha recebido

²⁰² *Relatório da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu - Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*, Bruxelas, 19.2.2020 COM (2020) 64 final

²⁰³ Filipe Albuquerque Matos, *Responsabilidade por danos causados a terceiros por robôs*, in *Direito e Robótica...* cit.

o *robot* de um fornecedor com o objetivo de o vender, alugar ou qualquer outra forma de distribuição.²⁰⁴

De seguida, cabe apurar se o *robot* pode ser entendido como um produto à luz do diploma. A distinção entre produto e serviço pode tornar-se mais ténue no seio digital. Na aceção do art. 3.º/1 do DL n.º 383/89, um produto “qualquer coisa móvel, ainda que incorporada noutra coisa móvel ou imóvel”, cabendo o *robot* no conceito de “coisa” que acolhemos - “bens (ou entes) de carácter estático, desprovidos de personalidade e não integradores do conceito necessário desta, suscetíveis de constituírem objeto de relações jurídicas, com existência autónoma ou separada, serem passíveis de apropriação exclusiva por alguém e estarem aptos a satisfazer interesses ou necessidades humanas”.²⁰⁵

Por fim, é de notar que a responsabilização do produtor se torna particularmente complexa se o *robot* for absolutamente autónomo, pois a lógica inerente à responsabilidade do produtor acaba defraudada.

A par disto, o regime que estudamos carece da verificação de outros requisitos, cujo preenchimento se verifica mais difícil. Em primeiro lugar, para ser assacada a responsabilidade ao produtor exige-se o defeito do produto. O que pode acontecer quando, por exemplo, se dê uma falha na construção ou programação do *robot*, ou ainda quando o produtor não inclui, com o produto, todas as suas instruções de utilização.²⁰⁶

Depois, os danos causados têm que resultar do defeito de conceção ou de fabrico, i.e., para que o lesado se possa fazer valer deste regime, tem que se verificar desconformidade entre o resultado final e o que era esperado pelo produtor (não raras vezes, os produtos defeituosos são comparados com outros fabricados nas outras linhas de produção onde não se verificaram irregularidades para averiguar a existência de um defeito de fabrico)²⁰⁷. Assim, na hipótese de os danos causados pelo *robot* serem despoletados pela sua atuação autónoma,

²⁰⁴ Juliana Campos, *A responsabilidade civil do produtor pelos danos causados por robôs inteligentes à luz do regime do Decreto-Lei n.º 383/89, de 6 de novembro*, disponível em: <https://revistadireitoresponsabilidade.pt/2019/a-responsabilidade-civil-do-produtor-pelos-danos-causados-por-robos-inteligentes-a-luz-do-regime-do-decreto-lei-n-o383-89-de-6-de-novembro-juliana-campos/>

²⁰⁵ Cfr Carlos Alberto Mota Pinto, *Teoria Geral do Direito Civil*, 4ª edição por A. Pinto Monteiro e Paulo Mota Pinto, Coimbra Editora, Coimbra, 2005, p. 341

²⁰⁶ V. Mafalda Miranda Barbosa, *Robot advisors* ob. cit.

²⁰⁷ Filipe Albuquerque Matos, *Responsabilidade por danos causados a terceiros por robôs*, in *Direito e Robótica...* cit.

não cabe a responsabilização do produtor. Não parece razoável alegar defeito do *robot* quando houve uma atuação conforme às características que lhe são intrínsecas.²⁰⁸

Ademais, o defeito tem que existir já no momento da entrada do produto em circulação. Ora, se momento da entrada em circulação, o estado da ciência e da técnica não permitiam saber como é que o *robot* se viria a desenvolver, aquilo que este viria a aprender, não se pode responsabilizar o produtor.

Mas o defeito poderá também incidir sobre a informação relativa à utilização do *robot*, quando as instruções foram fornecidas de forma insuficiente.

Do mesmo modo, se se apurar que houve “um comportamento culposo de quem tem a seu cargo a tarefa de coordenar ou fiscalizar o funcionamento dos robôs”, mesmo que esse seja um terceiro, o art. 7.º do DL n.º 383/89 dispõe que “a responsabilidade do produtor não se pode considerar diminuída com a intervenção de terceiro”.²⁰⁹

Por fim, o art. 8.º esclarece que são considerados apenas os danos que resultem de morte ou lesão pessoal e os que ocorram em coisa diversa do produto, desde que seja normalmente destinado ao uso ou consumo privado e o lesado lhe tenha dado principalmente este destino. Do exposto parece poder retirar-se que não são ressarcidos os danos puramente patrimoniais.

Concomitantemente, este regime não dá resposta à grande parte dos casos abrangidos no âmbito do nosso trabalho, em que o *robot* induz o segurado a optar por um produto que não é adequado a ele, levando-o, por exemplo, a pagar um prémio muito mais alto do que teria que pagar se se aconselhasse junto de uma pessoa física.

Por outro lado, tem-se colocado a hipótese de desencadear a responsabilidade contratual, segundo a qual o devedor deve ser responsável pelos danos causados pelos entes dotados de inteligência artificial que use no cumprimento dos seus deveres. Como não se lhes reconhece um estatuto pessoal, o *robot* deve ser compreendido como um instrumento, sendo esta uma responsabilidade com base no seu próprio comportamento, i.e., na medida em que não tenham sido cumpridos os deveres de cuidado a que está adstrito. Poderemos, a título de exemplo, estar a falar de deveres de vigilância relativamente ao *robot*. Havendo a possibilidade

²⁰⁸ Mafalda Miranda Barbosa, *Robot advisors* ob. cit.

²⁰⁹ Filipe Albuquerque Matos, *Responsabilidade...*

de o devedor afastar a presunção de culpa, é importante a previsão, a este nível, de uma hipótese de responsabilidade sem culpa²¹⁰.

Vale a pena referir o regime geral da responsabilidade extracontratual vertido no art. 483.º/1 do CCiv., sob o qual é responsável aquele que culposamente causar um dano a alguém. Desta sorte, poderão considerar-se também responsáveis pelos danos, os adquirentes destes produtos ou quem, com base numa relação jurídica de usufruto, locação, comodato, utilize estes bens no seu interesse próprio, o que se justifica pelo facto destes intervenientes assumirem uma posição de controlo relativamente aos *robots*.²¹¹ Neste caso, a principal dificuldade no inerente a este regime, recairá sobre o lesado. Este, por não ter cabimento nenhuma presunção legal de culpa do art. 493.º do CCiv., terá o ónus da prova da atuação culposa do *robot*.²¹²

Já ao abrigo deste último preceito, quem causar danos a outrem no exercício de uma atividade, perigosa por sua própria natureza ou pela natureza dos meios utilizados, é responsável por esses danos.²¹³

Também pode acontecer que o prestador de serviços, provando “que não houve culpa da sua parte, que os danos se teriam igualmente produzido se não houvesse culpa sua ou que, no caso do n.º 2, empregou todas as providências exigidas pelas circunstâncias com o fim de prevenir os danos”, consiga ilidir a presunção que sobre ele recaiu²¹⁴.

O Parlamento Europeu emitiu a 16 de fevereiro de 2017 uma Resolução com recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103 (INL)). Esta destaca que uma possível solução para a complexidade de atribuir responsabilidade pelos danos causados pelos *robots* cada vez mais autónomos pode ser a criação de fundos de compensação, conforme acontece já, por exemplo, com os automóveis. É diferente, contudo,

²¹⁰ Mafalda Miranda Barbosa, *Robots advisors* ...cit.

²¹¹ Em síntese, verificando-se o incumprimento de um dever de segurança ou prevenção, poderá haver lugar à responsabilidade extracontratual. Idem. V. também Juliana Campos Carvalho, ob. cit.,

²¹² *Ibidem*.

²¹³ Atente-se que, relativamente ao n.º 2 do art. 493.º do CCiv., será duvidoso conceber o recurso a um *robot*, nomeadamente aqueles que se englobam no contexto deste estudo, como a prática de uma atividade perigosa. Cfr. Filipe Albuquerque Matos, *Responsabilidade... e Juliana Campos Carvalho*, ...cit.

²¹⁴ Mafalda Miranda Barbosa, *Robots advisors e responsabilidade civil*, cit.

no facto de no regime de seguros para a circulação rodoviária, a cobertura incidir sobre os atos e as falhas humanas.²¹⁵

Em 2020, no Relatório da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu sobre as implicações em matéria de segurança e de responsabilidade decorrentes da Inteligência Artificial, da Internet das Coisas e da Robótica, a possibilidade de impor contratação de um seguro permanece em apreciação.²¹⁶

Prevendo a criação de um regime de responsabilidade objetiva, FILIPE ALBUQUERQUE MATOS entende que seria razoável, como acontece com o art. 503.º, relativamente aos veículos, limitar o elenco dos danos ressarcíveis aos riscos próprios da utilização do *robot*, cuja tarefa de delimitação caberá à doutrina e jurisprudência.

O Autor recomenda ainda a adoção de um regime semelhante ao do art. 505.º do CCiv., no sentido em que apenas se deve admitir o afastamento da responsabilidade daqueles quando houver contribuição causal para os danos de um facto do lesado, de terceiro ou de causa de força maior.

Depois, o Autor defende não ser conveniente a definição de limites indemnizatórios quando a utilização de *robots* é uma atividade à qual ainda está associada uma grande incerteza.²¹⁷

Sem prejuízo, no Relatório da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu sobre as implicações em matéria de segurança e de responsabilidade decorrentes da Inteligência Artificial, da Internet das Coisas e da Robótica²¹⁸, é avançada a hipótese de as legislações nacionais dos Estados Membros da UE sofrerem adaptações de modo a facilitar o ónus da prova do lesado no seio de uma atuação de uma tecnologia de IA.

²¹⁵ Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)), disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52017IP0051> Para uma análise sobre estes seguros, v. Aysegul Bugra, *Room for Compulsory Product Liability Insurance in the European Union for Smart Robots? Reflections on the Compelling Challenges*, in *InsurTech: A Legal and Regulatory View*, disponível em: https://doi.org/10.1007/978-3-030-27386-6_8

²¹⁶ Disponível em: <https://op.europa.eu/pt/publication-detail/-/publication/4ce205b8-53d2-11ea-aece-01aa75ed71a1/language-pt>.

²¹⁷ Filipe Albuquerque Matos, *Responsabilidade...*

²¹⁸ Cit. Vide também o relatório *Liability for Artificial Intelligence and other emerging technologies*, disponível em: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

6. Novos modelos de seguros

Como tivemos ocasião de assinalar, o recurso às tecnologias *IoT* permite que a seguradora adapte o produto ao segurado, designadamente que o prémio do seguro seja respaldado no perfil de risco do proponente.

Ora, com a introdução de dispositivos informáticos destinados à recolha de informação permitirá um modelo de avaliação do risco mais exato, permitindo, inclusive que estas traçam um esquema comportamental de cada proponente, as empresas de seguros podem ajustar o prémio em função, por exemplo, da utilização efetiva do veículo ou do estilo de condução do tomador de seguro ou beneficiário.

Mas não só na aferição do risco se verifica o impacto das novas tecnologias. Nesta concomitância, cumpre fazer referência aos vários novos modelos de seguro a que a inovação e uso da tecnologia fizeram dar origem.

6.1 Seguros Baseado no Uso

O seguro com base no uso é um tipo de seguro de automóvel que é alimentado pela recolha de dados e criação de perfis com vista a adaptar o prémio ao seu tomador.

Em primeiro lugar, encontramos os seguros *pay as you drive* (PAYD). Estes seguros surgem com o propósito de oferecer cobertura a bens cujo preço está ligado à quantidade de circulação, destinados a segurar o “segundo carro” ou o “carro de garagem. Automóveis que raramente circulam, mas que estão sujeitos a seguro obrigatório.

Nos seguros *pay how you drive* (PHYD), tem-se em conta não a quantidade de circulação, mas a qualidade da condução.

É o caso da *Drivit* que através do recurso aos dispositivos *IoT* colocados nos automóveis consegue uma aferição concreta e contínua do risco em relação a cada segurado.

A tarificação é baseada na quilometragem efetiva, no número de viagens realizadas e nos hábitos de condução do segurado, como a velocidade média, se faz muitas travagens bruscas e mesmo as zonas mais frequentadas, assim como os horários a que as frequenta. Esta adap-

tabilidade traduzir-se-á na premiação do segurado que demonstra ser um condutor responsável e diligente, mas também na penalização do condutor mais descuidado, através do aumento do prémio de seguro, ou mesmo a recusa de celebração do contrato. As empresas de seguros passam a descontar o prémio em função destes fatores e os seguradores sujeitam-se à Tarificação Instantânea do Seguro.

Este tipo de seguro passa também para os seguros de saúde, em que se verifica a adaptação do prémio do seguro ao estilo de vida levado a cabo pelo beneficiário do seguro, são os seguros *pay as you live* (PAYL). Através do recurso a dados registados e recolhidos pelas *apps* de *smartphone* como as associadas ao Fitness, hoje muito em voga, ou de controlo de ingestão de calorias ou mesmo de registo de níveis de glicémia, tensão arterial ou das horas e da qualidade de sonos, etc.

Estes dados vão ser utilizados para atribuir descontos no prémio em função do estilo de vida mais saudável. Além disto, permitirão reduzir, também nos seguros vida, a quantidade de sinistros, pois os segurados sentir-se-ão, pelo menos, mais motivados a adotar hábitos de vida mais saudáveis, pois sabem que estão a ser monitorizados pelos dispositivos móveis em tempo real.

Por fim, também nos seguros de habitação é possível implementar este modelo. Cada vez são mais comuns as *smart houses*. Como já referimos, existem aparelhos que possibilitam a deteção de tempestades e que podem avisar o proprietário e/ou o segurador para tomar precauções antecipadamente, ou sensores que denotem, por exemplo, a presença anormal de água no chão e enviem imediatamente alertas para o proprietário e/ou segurador de modo a poderem prevenir-se danos maiores e diminuir os prejuízos não só para o próprio, mas também para habitações contíguas e para o segurador.

Embora o objetivo seja, principalmente, o controlo do risco e a prevenção dos sinistros, o recurso a dispositivos deste género pode também servir como instrumentos para auxiliar na mensuração do risco, se estiverem instalados aparelhos que monitorizem o consumo de eletricidade ou se o proprietário/segurado tem o hábito portas destrancadas à mercê de intrusos, designadamente.

6.2 On-demand insurance

Os seguros a pedido ou *on demand insurance* são seguros que permitem ao titular do bem segurado acionar a cobertura do seguro apenas em determinadas ocasiões. Um exemplo prático é o da *startup* Trov que fornece um serviço de *app* para *smartphone* que contém um botão que deixa o consumidor “ligar ou desligar”, portanto ativar ou desativar a cobertura do seguro de “pequenos bens”, principalmente. A Trov oferece cobertura para objetos como equipamentos de desporto, instrumentos musicais ou aparelhos eletrónicos. Imagine-se contratar um seguro para uma máquina fotográfica de última geração e ter a possibilidade de ativar a respetiva apólice apenas quando se sai de casa, quando esta está sujeita a mais situações de risco. Dessarte, o cliente também só paga o seguro quando a cobertura está ativada.

A aplicação Trov, como é característico das empresas *Insurtech*, tem como objetivo a flexibilização de todo o processo de contratação, uma vez que basta o consumidor descrever o bem que pretende segurar, fazer o *upload* de uma ou mais fotografias do mesmo e de recibos correspondentes.

Outro exemplo no setor automóvel é promovido pela circulação de veículos autónomos. O “Programa InsureMyTesla” é um serviço fornecido pela empresa Tesla, responsável pela produção de veículos elétricos e automatizados, e que consiste num seguro customizado para o proprietário de um Tesla. Este permite inclusive contratar seguros para viagens específicas e determinadas, ao invés de um seguro automóvel de longa duração a que estamos acostumados.²¹⁹

Segundo PAULA RIBEIRO ALVES, este novo modo de contratar não se distancia muito do contrato de seguro em linha estandardizado em análise supra, composto por cláusulas contratuais gerais e ao qual não está associado o mínimo dos atos de negociação.²²⁰

6.3 Seguros colaborativos ou P2P

Por fim, devem referir-se, ainda que brevemente, os seguros colaborativos. A economia colaborativa tem-se desenvolvido a um ritmo acelerado, de tal forma que se fala mesmo numa quarta revolução industrial.

²¹⁹ Vide https://www.tesla.com/pt_PT/support/insuremytesla e Paula Ribeiro Alves, *Os desafios digitais...cit.*, p. 53 e 55.

²²⁰ Vide *Os Desafios Digitais no Mercado Segurador*, p. 53

Este movimento demarca a mudança da cultura do “eu” para a cultura do “nós”, evidenciando o sentimento de partilha e proximidade entre *peers* e desculpando a Internet pelo isolamento do ser humano. Este relacionamento viabiliza a redução dos custos de transação, a facilitação das trocas e aproveitamento sustentável através da partilha dos bens e serviços.

Embora ainda não se tenha chegado a um consenso relativamente à definição de economia colaborativa, sabe-se que esta envolve a divulgação de uma determinada atividade profissional, geralmente, através de uma plataforma *online*, que funciona como um mercado virtual que possibilita o contacto direto entre o fornecedor de um bem ou prestador de serviços e um consumidor daquele produto ou serviço.

Por sua vez, também o conceito de *peer* não reúne concordância, isto porque, o *peer* pode aparecer enquanto indivíduo que procura o serviço, mas pode, ocasionalmente, aparecer como alguém que tem um serviço para oferecer.²²¹

A característica essencial das relações P2P assenta na simetria dessa relação. Portanto, existe uma relação P2P sempre que dois *players* estiverem a agir no mesmo nível, independentemente de serem profissionais ou não profissionais.

Ora, também o setor dos seguros se conseguiu adaptar a esta nova realidade, dando origem a modelos de seguros colaborativos, que assentam nas ideias de partilha e otimização de recursos.

Estes modelos de seguro concretiza-se através da formação de pequenos grupos de segurados *online* dispostos a partilhar o risco. Isto significa que, através da criação de uma bolsa *online*, que pode ser suportada numa rede *Blockchain*, para a qual contribuem todos, e da qual uma parte flui para um fundo do grupo, e outra parte para uma companhia de seguros. Posteriormente, em caso de sinistro, pagam-se os danos menores ao segurado com fundos desse grupo. Para reclamações acima do limite estipulado, é responsável a seguradora.

²²¹ Para mais desenvolvimento sobre a Economia Colaborativa, cfr. Margarida Lima Rego e Joana Campos Carvalho, *Insurance in Today's Sharing Economy: New Challenges Ahead or a Return to the Origins of Insurance?*, in *InsurTech: A Legal and Regulatory View: AIDA Europe Research Series on Insurance Law and Regulation*, p. 27-47.

A ideia central dos seguros P2P é que um conjunto de pessoas com interesses semelhantes agrupe as suas apólices de seguro, introduzindo uma ideia de controlo, confiança e transparência enquanto ao mesmo tempo reduzindo custos.

Semelhantemente, nas suas primeiras formas, o seguro nasceu da cooperação e remonta aos mercadores dos portos que, em face das incertezas inerentes à atividade, arranjavam bolsas onde colocavam alguns valores para, na eventualidade de ocorrer alguma desgraça, estarem economicamente salvaguardados.²²²

Na generalidade, os modelos P2P não prescindem inteiramente do segurador, mas antes redefinem o seu papel.

Atualmente é possível distinguir entre três modelos de seguros P2P diferentes, a saber: (i) o modelo corretor; (ii) o modelo de transportadora; (iii) o modelo de auto-governo.

Na verdade, na maioria destes modelos, os *peers* não concluem contratos entre eles, apenas partilham o risco.

Em primeiro lugar, as empresas sob o modelo corretor atuam como intermediárias entre as seguradoras e seus clientes. Organizam os clientes em grupos, recolhem os prémios e entregam uma parte deles à companhia de seguros. O resto do dinheiro é guardado num fundo, que servirá para pagar as reivindicações apresentadas por membros do grupo. No final do período, algumas seguradoras devolvem o remanescente aos membros do grupo, outras doam a uma instituição de caridade designada. Na circunstância de o dinheiro do fundo ser insuficiente para cobrir todas as queixas, é ativado um seguro de contingência.

A *Friendsurance* é uma das plataformas mais conhecidas que fornece seguros P2P. Com parcerias com mais de 70 companhias de seguros, oferece uma vasta gama de produtos de seguro aos Clientes. Assentando na premissa da “amizade”, agrupa pessoas que tenham aderido ao mesmo tipo de seguros e, enquanto que parte do dinheiro é entregue diretamente à seguradora, o restante é usado para pagar as indemnizações devidas durante todo o ano. No fim do ano, o que restar no fundo é dividido entre os membros e usado para pagar uma parte dos prémios para o ano seguinte.

²²² Vide Margarida Lima Rego e Joana Campos Carvalho, *Insurance in Today's Sharing Economy...*, cit. 43 e ss.

No que toca às empresas com o modelo de transportadora, semelhantemente ao que se acabou de descrever, os segurados são também reunidos em grupos e uma parcela dos seus prémios é destinada a um fundo usado para as reivindicações apresentadas ao longo do ano. No entanto, neste modelo não existe intermediário. A companhia de seguros vende suas próprias apólices e também agrupa os segurados e gere os fundos.

Um exemplo é a Lemonade, que entrega os valores remanescentes a uma entidade não lucrativa escolhida, sendo este também o fator determinante no momento de agrupar os *peers*.

O modelo auto-governante, por sua vez parece ser o único modelo verdadeiramente P2P, no sentido em que não envolve nenhuma seguradora, resseguradora ou intermediário de seguros. Não são devidos prémios e o risco é compartilhado apenas entre os membros de um grupo, de acordo com os termos que eles definem. A plataforma representa, assim, um “mero” mercado virtual, através do qual qualquer pessoa pode comunicar, celebrar e executar contratos.

A *startup* Teambrella, que recorre a este modelo de seguros, organiza os seus clientes em grupos que são autorregulados. Isto implica que sejam os membros do grupo a avaliar o sinistro e decidir se a queixa da ocorrência deve ser aceite e se se deve realizar o pagamento da indemnização, assim como quanto deve ser pago ao segurado pelo dano sofrido tendo em conta as regras em vigor no grupo. Cada membro do grupo dispõe de uma carteira de *bitcoin* e as somas das carteiras são usadas para indemnizar o sinistrado.

Apesar de, na senda de MARGARIDA LIMA REGO e JOANA CAMPOS CARVALHO não se poder deixar de notar que não estamos, neste caso, perante um verdadeiro contrato de seguro, surpreende que se possa deixar escapar totalmente a aplicação da legislação do contrato de seguro a casos como os que estão aqui em apreço, isto porque, na essencialidade, a oferta destas empresas não é assim tão diferente daquela que é posta ao dispor por outras empresas de seguro às quais é efetivamente aplicado o regime.²²³

²²³ Para mais desenvolvimento, cfr. Margarida Lima Rego e Joana Campos Carvalho, ob.cit. p. 41-45.

Conclusão

Com a presente dissertação pretendemos explorar as inovações tecnológicas que se emergiram no setor segurador e que revolucionaram verdadeiramente a contratação do seguro.

Efetivamente pode dizer-se que o mercado dos seguros é um de entre os quais se verifica uma grande margem para desenvolvimento e inovação pelo uso da Internet e das novas tecnologias.

Em primeiro lugar, fazendo uma breve exposição do Estado da Arte em Portugal, concluímos que apesar de ainda não fazer parte do dia-a-dia das seguradoras, existem já, algumas iniciativas que são de louvar no que toca ao contributo que representam para o desenvolvimento tecnológico do ramo.

De seguida, tivemos oportunidade de analisar a possibilidade de celebração do contrato de seguros através sem intervenção humana. Embora tenhamos chegado à conclusão de que esta questão não parece relevante, uma vez que não há razão para supor que as partes não assinariam um contrato “tradicional”. Aliás, essa seria a situação ideal para que estas pudessem acordar os termos que regem a sua relação jurídica, como o âmbito da cobertura, definições, disposições gerais, exclusões da cobertura e entre outros elementos que se verifiquem relevantes. Neste sentido, a automatização do sistema de gestão de subscrições de sinistros resume-se à modalidade de execução desse contrato.

Ainda assim, foi possível observar que as seguradoras poderão especialmente beneficiar das novas tecnologias no momento de aferição do risco, no entanto, como decorre do estudo realizado, o recurso às novas tecnologias neste âmbito não se compagina com o Regime Jurídico do Contrato de Seguro atualmente em vigor que ainda concentra no preponente a responsabilidade de declarar com exatidão as circunstâncias que conhece e que sejam relevantes para a aferição do risco pelo segurador.

Não obstante, esta é uma realidade em crescimento, à qual as empresas seguradoras têm inevitavelmente que reagir, no sentido de adequarem o exercício da sua atividade.

Conseguimos, contudo, observar que o caminho que o mercado de seguros está a traçar aponta no sentido da simplificação do contrato. Introduzindo produtos mais simples e adaptados ao cliente, estes passam a ser reduzidos ao essencial.

Observa-se a transferência dos modelos de seguro baseados em resultados de eventos passados para uma interação mais pormenorizada entre o segurado e a empresa de seguros, passando estas a adotar uma atuação assente na proteção e prevenção.

Além disto, os mecanismos de avaliação de risco no contexto *Insurtech* têm permitido também ao segurador estabelecer preços equilibrados ou recusá-los imediatamente.

Concluimos ainda, a nível da proteção de dados, que a grande dificuldade das seguradoras se verificará relativamente ao tratamento dos dados de saúde do segurado é através do consentimento, porém, vimos ser um fundamento que não se revela apto a permitir o tratamento dos dados de saúde no âmbito da execução do contrato de seguro.

A par da criação de novos modelos de seguro, vimos que a revolução tecnológica deu origem a uma comunidade global colaborativa, de partilha.

Em conclusão, a complexidade de funcionamento de todos os instrumentos que esta disposição abarca resulta numa grande dificuldade em encontrar uma definição jurídica unívoca para cada um, sendo, igualmente difícil compreender a sua dimensão e impacto no mercado e até o seu funcionamento. Simultaneamente, a complexidade das tecnologias e a dificuldade em processar a rápida evolução tecnológica tem inibido a reflexão do legislador nesta matéria.

Por fim, é de reconhecer que se deixaram em aberto diversas questões. Com efeito, sob pena de nada concluir, cumpre arguir que se pretendeu sobretudo colocar questões que obrigassem a uma profunda e constante análise e investigação, em busca das melhores soluções face ao Estado da Arte e ao desenvolvimento do Direito no ramo.

Bibliografia

ABREU, J. M. Coutinho de, *Curso de Direito Comercial: Volume 1*, 12ª Edição, Coimbra: Almedina, 2019

_____, *Curso de Direito Comercial: Volume 2 – Das Sociedades*, 6ª Edição, Coimbra: Almedina, 2019

_____, *Empresas Virtuais (Esboços)*, in Estudos em homenagem ao Professor Doutor Inocêncio Galvão Telles, vol. IV, Coimbra: Almedina, 2003, p. 599-610.

ALVES, Francisco Luís, *A discriminação e a avaliação do risco nos seguros*, in *Revista de Direito e Estudos Sociais*, ano LII (XXV da 2ª série), julho/dezembro, ano de 2011, nº 3-4, p. 245-250

ALVES, Hugo Ramos, *Smart contracts: entre a tradição e a inovação*, in *Fintech II- Novos Desafios sobre a Tecnologia Financeira*/coord. António Menezes Cordeiro, a de Oliveira, Diogo Pereira Duarte – 2ª ed. Coimbra: Edições Almedina, 2019, p. 181-216.

ALVES, Paula Ribeiro, *Contrato de seguro à distância. O Contrato eletrónico*, p. 140-142

_____, *Os Desafios digitais no mercado segurador*, in *FinTech - Desafios da Tecnologia Financeira*/coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte – 2ª ed. Coimbra: Edições Almedina, 2019, p. 33-70

ASCENCIO, Pedro A. de Miguel, *Derecho Privado de Internet*, 3ª edição, Madrid: Civitas, 2002

ASCENSÃO, José de Oliveira, *Contratação Eletrónica*, in Sep de: *Direito da Informação*, Volume 4 (2003), Coimbra: Coimbra Editora, p.43-68.

AZAMBUJA, Luís Eduardo Meurer, *Direito Securitário e Boa-fé: o dever de informação nos contratos de seguros* - Dissertação de Mestrado em Ciências Jurídico – Civilísticas II, Coimbra: [s.n.], 2008.

BARBOSA, Mafalda Miranda, *Robot advisors e Responsabilidade Civil*, in *Revista de Direito Comercial*, disponível em: <https://www.revistadedireitocomercial.com/robot-advisers> (último acesso em 01/10/2020)

_____, *Diretiva de distribuição de seguros: os sujeitos*, in *Revista de Direito Comercial*, disponível em: <https://www.revistadedireitocomercial.com/diretiva-de-distribuicao-de-seguros-os-sujeitos> (último acesso em 01/10/2020)

BATALHA, Daniel Augusto de Senna Fernandes, *Criptocontratação – Uma nova forma de contratação automatizada*, Dissertação de Mestrado em Direito: Especialidade em Ciências Jurídico-Forenses apresentada à Faculdade de Direito, Coimbra: [s.n.], 2018, disponível em: <http://hdl.handle.net/10316/85817> (último acesso em 01/10/2020)

BIONI, Bruno Ricardo, *Proteção de Dados Pessoais: a função e os limites do consentimento*, Rio de Janeiro : Editora Forense, 2019

BLEMUS, Stéphane, *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*, in *Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review)* RTDF n°4, dezembro de 2017, disponível em: <https://ssrn.com/abstract=3080639> (último acesso em 01/10/2020)

BORSELLI, Angelo, *Smart Contracts in Insurance: A Law and Futurology Perspective*, in *InsurTech: A Legal and Regulatory View*, disponível em: https://link.springer.com/chapter/10.1007/978-3-030-27386-6_5#citeas (último acesso em 01/10/2020)

BUGRA, Aysegul, *Room for Compulsory Product Liability Insurance in the European Union for Smart Robots? Reflections on the Compelling Challenges*, in *InsurTech: A Legal and Regulatory View*, disponível em: https://doi.org/10.1007/978-3-030-27386-6_8 (último acesso em 01/10/2020)

CAMPOS, Juliana, *A responsabilidade civil do produtor pelos danos causados por robôs inteligentes à luz do regime do Decreto-Lei n° 383/89, de 6 de novembro*, in *Revista de Direito da Responsabilidade* disponível em: <https://revistadireitoresponsabilidade.pt/2019/a-responsabilidade-civil-do-produtor-pelos-danos-causados-por-robos-inteligentes-a-luz-do-regime-do-decreto-lei-n-o383-89-de-6-de-novembro-juliana-campos/> (último acesso em 01/10/2020)

CARIA, Riccardo de, *The Legal Meaning of Smartcontracts*, in *European Review of Private Law* 6-2019, p.731–752, disponível em: <https://core.ac.uk/download/pdf/302163043.pdf> (último acesso em 01/10/2020)

COELHO, Francisco Pereira, *Contratação Automatizada e Execução contratual automatizada: dos “software agentes” aos “smart contracts”*, in *Direito e Robótica, Actas do Congresso*, n°16 – 2020 – Edição Especial.

Comissão Europeia, *Liability for Artificial Intelligence and other emerging technologies*, disponível em: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199 (último acesso em 01/10/2020)

Comissão Europeia, *Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*, Bruxelas, 19.2.2020 COM(2020) 65 final, disponível em: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf (último acesso em 01/10/2020)

Comissão Europeia, *Relatório da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu - Relatório sobre as implicações em matéria de segurança e de responsabilidade decorrentes da inteligência artificial, da Internet das coisas e da robótica*, Bruxelas, 19.2.2020 COM (2020) 64 final

Comissão Nacional de Proteção de Dados, Deliberação nº 51/2001 da CNPD, disponível em: <https://www.cnpd.pt/home/orientacoes/DEL51-2001-ACESSO-DADOS-SAUDE.pdf> (último acesso em 01/10/2020)

_____, Parecer nº 20/2018 de 02/05/2018, disponível em: <http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d46446232317063334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true> (último acesso em 01/10/2020)

CORDEIRO, António Menezes, *Direito dos Seguros, 1ª ed. Janeiro, Coimbra: Edições Almedina, 2013.*

CORDEIRO, António Barreto Menezes, *Inteligência Artificial e consultoria Robótica (Automation in Financial Advice)*, in *Fintech – Desafios da Tecnologia Financeira* /coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte – 2ª ed. Coimbra: Edições Almedina, 2019, p. 221-236

CORREIA, Francisco Mendes, *A tecnologia descentralizada de registo de dados (Blockchain) no setor financeiro*, in *FinTech - Desafios da Tecnologia Financeira*/coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte – 2ª ed. Coimbra: Edições Almedina, 2019 p.83-88

CUNHA, Carolina, *Proteção de Dados e Aplicações Móveis na Área da Saúde: um diagnóstico sumário*, in *Revista Online Banca, Bolsa e Seguros*, nº 3 – 2018, p. 31 – 50, disponível em: https://www.fd.uc.pt/bbs/wp-content/uploads/2019/01/bbs3_final_2p.pdf (último acesso em 01/10/2020)

DIVINO, Sthéfano Bruno Santos, *Smart Contracts: Conceitos, Limitações, Aplicabilidade e Desafios*, in *Revista Jurídica Luso-Brasileira*, ano 4 (2018), nº 6, http://www.cidp.pt/revistas/rjlb/2018/6/2018_06_2771_2808.pdf (último acesso em 01/10/2020)

DUARTE, Diogo Pereira e ANDRADE, João Freire de, *Breves notas sobre o financiamento de startups e a sua regulação*, in *Fintech II – Novos Estudos sobre a Tecnologia Financeira*/coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte – 2ª ed. Coimbra: Edições Almedina, 2019, p. 217-248

DWORK, Cinthia, <http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf> (último acesso em 01/10/2020)

EU Blockchain Observatory and Forum, *Legal and Regulatory Framework of Blockchains*, disponível em: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf (último acesso em 01/10/2020)

FESTAS, David de Oliveira, *A contratação eletrónica automatizada*, in *Direito da Sociedade da Informação* (VI), p. 411-461

GolmanSachs, *Blockchain – The New technology of Trust*, disponível em <https://www.goldmansachs.com/insights/pages/blockchain/index.html> (último acesso em 01/10/2020)

GUARDEÑO, David Arroyo, Vico, Jesús Díaz e Encinas, Luis Hernández, *Blockchain*, CSIC, 2019

HEIRAN, Robert, *Regulating Blockchain: Critical Perspectives in Law and Technology*, New York, NY: Routledge, 2019

JIMÉNEZ, Javier Wenceslao Ibáñez, *Cuestiones jurídicas en torno a la cadena de bloques («blockchain») y a los contratos inteligentes («smart contracts»)*, in *Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, nº 101, 2017, disponível em: <https://revistas.comillas.edu/index.php/revistaicade/article/view/8407> (último acesso em 01/10/2020)

_____, *Blockchain: primeras cuestiones en el ordenamento español*, Madrid, 2018

LEAL, Ana Alves, *Aspetos jurídicos da análise de dados na Internet (big data analytics) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação*, in *Fintech - Desafios da Tecnologia Financeira*/coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte – 2ª ed. Coimbra: Edições Almedina, 2019, p. 89-220

LEÓN, Pedro J. Ponce de, *Blockchain, un nuevo patrón tecnológico*, in *Blockchain: aspectos tecnológicos, empresariales y legales*, Pastor Sempere Carmen, Vilarroig Moya Ramon, Thomson Reuters Aranzadi, p. 25 e 77

MAIA, Pedro, *A Robotização do mundo financeiro: reflexões introdutórias*, in *Direito e Robótica – Actas do Congresso*, nº 16, 2020, Edição Especial

MARTINS, Maria Inês de Oliveira, *Regime Jurídico do Contrato de Seguro em Portugal*, in *Actualidad Jurídica Iberoamericana*, ISSN 2386-4567, IDIBE, núm. 5 ter, dic. 2016, disponível em: <http://www.revista-aji.com/articulos/2016/num6-ter/199-231.pdf> (último acesso em 01/10/2020)

_____, *Contrato de Seguro e Conduta dos sujeitos ligados ao risco*, Tese de Doutoramento em Ciências Jurídico-Empresariais apresentada à Faculdade de Direito da Universidade de Coimbra, Coimbra : [s.n.], 2017, disponível em <http://hdl.handle.net/10316/29217> (último acesso em 01/10/2020)

MATOS, Filipe Albuquerque, *Regulamento de Proteção de Dados Pessoais [2016/679] no contexto dos desafios da actividade seguradora — o caso particular dos seguros de saúde*, in *Revista Online Banca, Bolsa e Seguros*, nº 3 - 2018, p. 31 – 50, disponível em: https://www.fd.uc.pt/bbs/wp-content/uploads/2019/01/bbs3_final_2p.pdf (último acesso em 01/10/2020)

_____, *Responsabilidade por danos causados a terceiros por robôs*, in *Direito e Robótica – Actas do Congresso*, nº 16, 2020, Edição Especial

MIK, Eliza, *Smart contracts: terminology, technical limitations and real world complexity*, in *Law, Innovation and Technology*, p. 269-300, disponível em: <https://doi.org/10.1080/17579961.2017.1378468> (último acesso em 01/10/2020)

MONTEIRO, António Pinto, “*Qui Facit Per Alium, Facit Per Se*” - *Será ainda assim na Era da Robótica?*, in *Direito e Robótica*, Actas do Congresso, nº 16, 2020, Edição Especial

NWOGUGU, Michael, *Corporate Governance, Financial Stability and evolving Insurtech: The Case of Insurance Australia Group (2011-2016)*, disponível em: <https://ssrn.com/abstract=2980133> (último acesso em 01/10/2020)

OCDE (2017), *Technology and innovation in the insurance sector*, disponível em: <https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf> (último acesso em 01/10/2020)

OLIVEIRA, Ana Perestrelo de, *O papel das startups na Fintech e o ciclo de financiamento de startups*, in *Fintech - Desafios da Tecnologia Financeira*/coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte – 2ª ed. Coimbra: Edições Almedina, 2019, p. 255-263

OLIVEIRA, Madalena Perestrelo de, *Definição de Perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados*, in *Fintech II*, / coord. Cordeiro, António Menezes, Oliveira, Ana Perestrelo de, Duarte, Diogo Pereira, Coimbra: Edições Almedina, 2019, p. 61-88

Orientações sobre os encarregados da proteção de dados (EPD) - Grupo do Artigo 29.º para a proteção de dados, disponível em: https://www.cnpd.pt/home/rgpd/docs/wp243rev01_pt.pdf (último acesso em 01/10/2020)

Parlamento Europeu, *Resolução de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL))*, disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52017IP0051> (último acesso em 01/10/2020)

_____, *Resolução de 3 de outubro de 2018, sobre tecnologias de cadeia de blocos e aplicações de cifragem progressiva: reforçar a confiança através da desintermediação (2017/2772(RSP))*, disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_PT.html (último acesso em 01/10/2020)

PEPPET, Scott R., *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, in *Texas Law Review*, 93, 2014, p. 85-179, disponível em: <http://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf> (último acesso em 01/10/2020)

PEREIRA, Alexandre Libório Dias, *Empresa, comércio eletrónico e propriedade intelectual*, in *Nos 20 anos do Código das Sociedades Comerciais, Homenagem aos Professores Doutores A. Ferrer Correia, Orlando de Carvalho e Vasco Lobo Xavier, Volume I - Congresso Empresas e Sociedades*, p. 450-453

_____, *O responsável pelo tratamento de dados segundo o Regulamento Geral de Proteção de Dados (RGPD)*, in *Boletim da Faculdade de Direito da Universidade de Coimbra*, vol. 95, no. 2, 2019, p. 1161-1188

PINTO, Carlos Alberto Mota, *Teoria Geral do Direito Civil*, 4ª edição por Monteiro, A. Pinto e Pinto, Paulo Mota, Coimbra: Coimbra Editora, 2005

POÇAS, Luís, *Aproximação económica à declaração do risco no contrato de seguro*, in *Revista de Direito e de Estudos Sociais*, 57 (2016), p. 279-325

_____, *O Dever de Declaração Inicial do Risco no contrato de Seguro*, Coimbra: Almedina, 2013

_____, *Problemas e Soluções de Direito dos Seguros*, Coimbra: Edições Almedina, 2019

REGO, Margarida Lima e CARVALHO, Campos, Joana, *Insurance in Today's Sharing Economy: New Challenges Ahead or a Return to the Origins of Insurance?*, in *InsurTech: A Legal and Regulatory View: AIDA Europe Research Series on Insurance Law and Regulation*, p. 27-47

SANTOS, João Vieira dos, *Aspetos jurídicos das startups*, in *Revista da Ordem dos Advogados*, Lisboa : O.A. - A. 77, n.º 1-2 (jan.-jun. 2017), p. 239-277

SANTOS, Maria Francisca Rodrigues, *Deveres de informação do tomador do seguro ou do segurado na fase pré-contratual. A informação na contratação eletrónica* - Dissertação de Mestrado em Direito, na Área de especialização de Direito Privado, Universidade Católica Portuguesa, Centro Regional do Porto, Escola de Direito, 2012

SAVICEVIC, Jovan, *Impact potential of the innovations*, disponível em: www.etd.ceu.edu

SCHREY, Joachim e Thalhofer, Thomas, *Rechtliche Aspekte der Blockchain*, in *Neue Juristische Wochenschrift*, vol. 70, n.º 20, 2017

SILVA, Paula Costa e, *A Contratação Automatizada*, in *Direito da Sociedade de Informação*, vol. IV, Coimbra: Coimbra Editora, 2003.

UNSWORTH, Rory, *Smart Contract This! An Assessment of the Contractual Landscape*, in *Legal Tech, Smart Contracts and Blockchain, and the Herculean Challenges it Currently Presents for “Self-executing” Contracts*, in *Legal Tech, Smart Contracts and Blockchain. Perspectives in Law, Business and Innovation*, (eds) Corrales M., Fenwick M., Haapio H., Springer, Singapore. https://doi.org/10.1007/978-981-13-6086-2_2 (último acesso em 01/10/2020)

TELES, Joana Galvão, *Deveres de Informação das partes*, in *Temas de Direito dos Seguros a propósito da Nova Lei do Contrato de Seguro*, Coimbra: Edições Almedina, 2012

VARELA, João de Matos Antunes, *Das Obrigações em Geral – Volume I*, 10ª ed., Coimbra: Almedina, 2018

VASQUES, José, *Contrato de Seguro (Notas para uma teoria geral)*, Coimbra: Coimbra Editora, 1999

Outros sites relevantes

ALLEN, Marshall, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, disponível em: <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates> (último acesso em 01/10/2020)

Dicionário Priberam da Língua Portuguesa, disponível em: <https://dicionario.priberam.org/>

Empresa Online, <https://eportugal.gov.pt/servicos/criar-uma-empresa-online>

Financial Times, *Blockchain believers hold fast to a utopian vision*, disponível em <https://www.ft.com/content/a12d7476-bc6a-11e6-8b45-b8b81dd5d080> (último acesso em 01/10/2020)

<https://afip.pt/en/>

<https://nakamotoinstitute.org/smart-contracts-glossary/>

<https://www.minalea.com/alfred-le-chatbot>

<https://www.minalea.com/assistant-commercial-intelligent-mi>

<https://www.portugalfintech.org/>

Programa InsureMyTesla, https://www.tesla.com/pt_PT/support/insuremytesla

Smart insurance Contracts: A discussion paper by Pinsent Masons and Applied Blockchain, disponível em: https://www.the-digital-insurer.com/wp-content/uploads/2017/10/980-FinTech_Smart_Insurance_Contracts_Flyer.pdf (último acesso em 01/10/2020)

Jurisprudência

Ac. do TRL de 22-05-2014, (relator: Ondina Alves), disponível em www.dgsi.pt (último acesso em 01/10/2020)

Acórdão do Tribunal de Justiça da União Europeia, de 1 de março de 2011 (Processo C-236/09, «Test-Achats»), disponível em: <http://curia.europa.eu/juris/document/document.jsf?jsessionid=B9024BDB1A0672FFD7D8652A8F72B385?text=&docid=80019&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=3354866> (último acesso em 01/10/2020)