



Universidade do Minho
Escola de Direito

Jorge Rúben Carvalho da Silva

Tecnologias Biométricas: Proteção de Dados em Contexto de Utilização de Próteses e Implantes

julho de 2018



Universidade do Minho

Escola de Direito

Jorge Rúben Carvalho da Silva

**Tecnologias Biométricas: Proteção de Dados
em Contexto de Utilização de Próteses
e Implantes**

Dissertação de Mestrado

Mestrado em Direito e Informática

Trabalho efetuado sob a orientação da

Professora Doutora Teresa Alexandra Coelho Moreira

e do

Professor Doutor Paulo Jorge Freitas de Oliveira Novais

julho de 2018

DECLARAÇÃO

Nome: *Jorge Rúben Carvalho da Silva*

Endereço eletrónico: *jr.csilva30@gmail.com*

Telefone: *910403398 / 253066630*

Número do Cartão de Cidadão: *14323448*

Título da Dissertação: *Tecnologias Biométricas: Proteção de Dados em Contexto de Utilização de Próteses e Implantes*

Orientadores: *Professora Doutora Teresa Alexandra Coelho Moreira,*

Professor Doutor Paulo Jorge Freitas de Oliveira Novais

Ano de conclusão: *2016-2018*

Designação do Mestrado: *Mestrado em Direito e Informática*

É AUTORIZADA A REPRODUÇÃO PARCIAL DESTA DISSERTAÇÃO, APENAS PARA EFEITOS DE INVESTIGAÇÃO, MEDIANTE DECLARAÇÃO ESCRITA DO INTERESSADO, QUE A TAL SE COMPROMETE.

Universidade do Minho, 31 / 07 / 2018

Assinatura: *Jorge Rúben Carvalho da Silva*

"The gods have not, of course, revealed all things to mortals from the beginning; but rather, seeking in the course of time, they discover what is better." – Xenófanés (570 a.C. - 475 a.C.): Stephen M. Trzaskoma, R. Scott Smith, Stephen Brunet, Thomas G. Palaima, Anthology of Classical Myth: Primary Sources in Translation.

Deixo o meu agradecimento a todos os que contribuíram para que este meu pequeno projeto se tornasse realidade.

Em especial, agradeço:

À Professora Doutora Teresa Alexandra Coelho Moreira, por toda a disponibilidade e interesse com que acompanhou o meu trabalho, pelos conselhos e sugestões, pela paciência, simpatia, e contributo indispensável para o desenvolvimento e completude desta Dissertação.

Ao Professor Doutor Paulo Jorge Freitas de Oliveira Novais, pelo valioso interesse desde sempre manifestado por este trabalho, pela simpatia e prontidão em apoiar, e pelas correções e conselhos desde a parte curricular.

À minha família e amigos, por todo o apoio, conselhos e paciência infindável para quando eu me ponho com ideias. A mais conversas pela noite dentro, séries de TV, barriga com tostas e sede de conhecimento.

Ao progresso da humanidade.

TECNOLOGIAS BIOMÉTRICAS: PROTEÇÃO DE DADOS EM CONTEXTO DE UTILIZAÇÃO DE PRÓTESES E IMPLANTES

Abstract:

Mais que tudo, este é um trabalho de pesquisa que procura analisar de forma o mais completa possível, as mais recentes alterações legislativas no que diz respeito ao acesso, armazenamento e tratamento de dados pessoais, particularmente os biométricos.

Servimo-nos, com esse propósito, do Regulamento Geral de Proteção de Dados, da Carta dos Direitos Fundamentais da União Europeia, da Convenção Europeia dos Direitos do Homem.

Ainda a jurisprudência do Tribunal Europeu dos Direitos do Homem e a do Tribunal de Justiça da União Europeia, para dar a compreender exemplos concretos de violações dos direitos e liberdades fundamentais do titular de dados.

Acrescenta-se à Constituição da República Portuguesa e às leis nacionais nº 12/2005, de 26 de janeiro e nº 5/2012, de 23 de janeiro, a análise que fazemos das normas do Código do Trabalho português, a respeito da proteção do trabalhador e dos seus dados pessoais, na sua relação laboral de subordinação para com o empregador.

Portugal, ao ser um Estado-Membro e parte interessada na UE, terá de ler estes seus diplomas à luz dos instrumentos europeus referidos anteriormente. Com a intenção de fazer o mesmo, servimo-nos das Opiniões do Grupo de Trabalho do artigo 29, para encontrar suporte doutrinal, nas ilações obtidas.

Ao mesmo tempo, damos a conhecer a evolução dos sistemas de informação, para que se compreenda não só, como se chegou às tecnologias biométricas atuais, mas ainda os perigos de um *homo conectus moderno*.

Fazemos ainda a ligação entre os temas das tecnologias biométricas e da inteligência artificial, ao explorar os métodos que, envolvendo agentes inteligentes e redes neuronais artificiais, permitem a otimização das primeiras.

Procuramos que a investigação e a elaboração da dissertação fiquem marcadas pela objetividade, clareza e rigor da análise científico-legalista. Sempre que se revele adequado e possível, fez-se um enquadramento doutrinal, técnico e jurisprudencial das questões tratadas.

BIOMETRIC TECHNOLOGIES: DATA PROTECTION IN THE USE OF PROSTHETICS AND IMPLANTS

Abstract:

More than anything, this is a research paper that seeks to analyze, in the most complete way possible, the most recent legislative updates, concerning the access, storage and treatment of personal data, particularly biometric data.

For that purpose, we take into consideration the General Data Protection Regulation, the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights.

Additionally, the decisions of the European Court of Human Rights and the Court of Justice of the European Union, to familiarize others with specific examples of the possible violations of the rights and freedoms of the data subject.

Complimenting the Constitution of the Portuguese Republic and the national laws no. 12/2005, of January 26 and no. 5/2012, of January 23, we analyze the Portuguese Labour Law, about the protections it stipulates, of the employee and his personal data, in his work relationship, one of subordination to the employer.

Portugal, by being a Member-State and an interested party in the EU, must hold its own laws to the standards of the European instruments referred previously. With that same intent, we consider the Opinions of the Working Party of the Article 29, to find doctrinal support in any conclusions we make.

Furthermore, we explore the evolution of the information systems, so that, with that knowledge, it becomes clear how we have the current biometric technologies, but also, the very real dangers of a modern homo conectus.

Finally, we connect the subjects of biometric technologies and artificial intelligence, by exploring the methods that, involving intelligent agents and neural networks, allow the optimization of the former.

It is the intent of the writer of the dissertation, that both the investigation and the writing process are guided by objectivity, clarity and rigor of the scientific and legal analysis. Whenever proper and possible, the topics were presented on a doctrinal, technical and jurisprudential framework.

ÍNDICE

A. I. Introdução – objeto, objetivos da análise, e respetiva temática.....	8
I. A Evolução Dos Sistemas De Informação	10
a. O zero e a sua importância para a Ciência Computacional	11
b. Noção de Software, Firmware e Hardware	12
c. Precusores da Máquina de Turing e sistema binário.....	13
d. Dispositivos Autómatos – o primeiro programa	14
e. Programação nos primeiros autómatos.....	16
f. Projetos de Leonardo da Vinci	18
g. Tabelas de multiplicação e réguas de cálculo.....	18
h. O fim da era da computação mecânica.....	19
i. Já o pai do computador, Charles Babbage e Ada Lovelace, a primeira programadora ...	20
j. Alan Turing e o seu contributo extraordinário para a computação	21
k. O conceito de memória única – o EDVAC.....	22
l. As várias gerações de computadores – uma breve análise	23
m. O Homo Conectus moderno e os seus perigos.....	25
II. Agentes De Software Inteligentes, Redes Neurais Artificiais E Inteligência Computacional.....	28
a. Aproximação à inteligência artificial por meio de uma inteligência computacional.....	28
b. Ainda a utilidade da Lógica no desenvolvimento de uma inteligência computacional ...	28
c. Os agentes de software	29
d. O debate da personalidade jurídica dos agentes inteligentes	31
e. Redes neuronais artificiais	34
f. Aprendizagem e otimização inteligente de sistemas	36
g. As tecnologias biométricas	39
h. Avanços tecnológicos no mercado dos implantes e próteses	43
III. Proteção Dos Dados Pessoais Do Utilizador	46
a. O Regulamento Geral de Proteção de Dados e o Grupo de Trabalho do Artigo 29	47
b. Coerência legislativa – os considerandos e as disposições finais do RGPD	58
c. A Carta dos Direitos Fundamentais da União Europeia.....	59
d. A Convenção Europeia dos Direitos do Homem	61

e. O Tribunal Europeu dos Direitos do Homem	62
f. O Tribunal de Justiça da União Europeia	66
g. A proteção de dados num contexto legislativo nacional.....	73
h. Uma relação de trabalho que respeite os direitos do trabalhador	75
i. A Constituição da República Portuguesa	80
 IV. Conclusão	 83
a. Que sentido fazer, de um mundo voltado para as tecnologias biométricas.....	83
 V. Bibliografia.....	 86

A.I. Introdução – objeto, objetivos da análise, e respetiva temática

Surge, no contexto tecnológico mas também legal atual, um jogo de forças entre novas técnicas e tecnologias que acedem, armazenam e fazem tratamento de dados pessoais, e legislação que pretende a proteção e a garantia, ou um equilíbrio com os riscos para os direitos e liberdades fundamentais dos titulares destes dados.

Pensamos ser pois, pertinente dar a conhecer os dois pontos de vista, e fazer perceber que para benefício de todos, é preferível que o avanço tecnológico ande de mãos dadas com o respeito dos direitos e liberdades do titular dos dados.

Com esse propósito, servimo-nos de instrumentos europeus legislativos na proteção e efetivação dos direitos e liberdades fundamentais, o Regulamento Geral de Proteção de Dados, a Carta dos Direitos Fundamentais da União Europeia, a Convenção Europeia dos Direitos do Homem.

Um dos mais elementares desses direitos é o respeito pela vida privada e familiar, e para fazer o compreender o porquê, pensamos que a análise deve passar por jurisprudência, casos concretos do Tribunal Europeu dos Direitos do Homem e do Tribunal de Justiça da União Europeia.

Em termos nacionais, à análise legal junta-se a Constituição da República Portuguesa, as leis nº 12/2005 de 26 de janeiro e nº 5/2012 de 23 de janeiro, e ainda, sublinha-se toda uma panóplia de circunstâncias onde o trabalhador, na sua relação laboral de subordinação com o empregador, vê felizmente no Código do Trabalho português, estabelecidas proteções legais dos seus dados pessoais.

Portugal, ao ser um Estado-Membro e parte interessada na UE, terá de ler estes seus diplomas à luz dos instrumentos europeus referidos anteriormente. Temos a intenção de fazer o mesmo, onde nos servimos das Opiniões do Grupo de Trabalho do artigo 29, para encontrar suporte doutrinal, nas ilações que se façam.

Ao mesmo tempo, queremos dar a conhecer a evolução dos sistemas de informação, para que se compreenda não só, como se chegou às tecnologias biométricas atuais, mas também os perigos de um *homo conectus moderno*.

Voltando à ideia inicial, das novas técnicas e tecnologias que surgem, em termos de avanços, estes tendem a seguir a via da computadorização.

Nos tempos que correm, fala-se muito da inteligência artificial, e como esta pode ser aplicada e beneficiar toda uma indústria.

Assim que, a respeito da nossa temática achamos ainda pertinente que se faça a ligação entre os temas das tecnologias biométricas e da inteligência artificial, ao explorar os métodos que, envolvendo agentes inteligentes e redes neuronais artificiais, permitem a otimização das primeiras.

Por fim, pela importância académica e jurídica deste estudo, conscientes das dificuldades com que nos debateremos, tudo faremos para que a investigação e elaboração da dissertação fiquem marcadas pela objetividade, clareza e rigor da análise científico-legalista.

I. A Evolução Dos Sistemas De Informação

É pertinente que se comece este estudo pela parte histórica da Informática, com a evolução dos sistemas de informação. Conforme introduzimos, e que será explicitado mais à frente, porque permite entender o seu contributo para o desenvolvimento das tecnologias biométricas, para que mais facilmente se possa ligar a tecnologia atual, à sua evolução tecnológica para o futuro.

Começemos pelo termo Informática, que caracteriza a área dos sistemas de informação computadorizados.

De definição atribuída em 1957, pelo cientista da computação alemão Karl Steinbuch, Informática designava um “processamento automático de informação”, estabelecendo-se como o termo alemão para a ciência da computação¹.

Trata-se de um galicismo nascido da fusão de “*Information*” e “*Automatique*”, significando um “tratamento automático da informação”. Esta “*estuda a estrutura e o tratamento da informação a partir dos dados nas suas diversas formas, nomeadamente, números, textos, gráficos, imagens, sons, fazendo o seu processamento, armazenamento, transmissão, recuperação e utilização*”².

Sendo certo que, nos dias de hoje, este vocábulo encontra-se especializado ao instrumento de qual se serve, significando a “ciência que estuda o processamento automático de informações por meio do computador”.

Como se sabe, o antecedente mais remoto do computador (e ainda em uso) é o ábaco, que surgiu na Ásia Menor, provavelmente pelas mãos dos babilónios, há cerca de 5.000 anos. Era habitualmente utilizado por mercadores, nas suas operações de cálculo de venda de produtos, e receção de pagamento, permitindo a realização de cálculos numéricos, através de um sistema de fileiras de contas, que deslizavam, presas numa grade. Aliás, só com o papel, permitindo o apontamento de contas e valores monetários, é que diminuiu a sua utilização.

Mas antes deste, crê-se que a 80.000 a.C., duas costelas esculpidas serviram como

¹ STEINBUCH, Karl, revista “*Informatik: Automatische Informationsverarbeitung*”, Standard Elektrik AG, Informatikwerk, SEG-Nachrichten, Heft 4, 1957.

² COELHO, Hélder, “*Sonho e Razão – Ao lado do artificial*”, Relógio d'Água, 1999.

instrumento de contagem. E que a 18.000 a.C., o osso de Ishango³, datado do Paleolítico Superior, serviria para o mesmo propósito, com os seus traços talhados, divididos em três colunas.

Entre o período da invenção do ábaco e a invenção da primeira calculadora mecânica houve cerca de 30 inovações tecnológicas com incidência na Matemática, cada uma mais complexa que a anterior, que nos permitiram a alfabetização tecnológica da sociedade moderna.

Em 1115 a.C., na Antiga China (Dinastia Shang, que durou de 1600 a 1046 a.C., período Yin) foi inventada a engrenagem diferencial, utilizada em conjunto com uma carroça-guia. Esta “指南車 (zhǐnán chē)” ou “carroça-aponta-o-sul”, de duas rodas, servia-se de uma bússola magnética e de uma engrenagem diferencial para que, independentemente da direção e do sentido da carroça, a figura externa (esculpida com o braço esticado) apontasse sempre o ponto cardeal Sul.

Esta engrenagem revelou-se indispensável em futuros computadores analógicos mecânicos, que por meio da integração da mesma, resolviam equações diferenciais.

I. a. O zero e a sua importância para a Ciência Computacional

A 500 a.C., encontramos registo do primeiro uso do zero (*śūnya*, do sânscrito शून्य), por matemáticos, na Antiga Índia⁴. É um número importante enquanto elemento neutro na álgebra matemática, mas também por ser um número racional e real, para além de algébrico e complexo.

No campo da Ciência Computacional ou da Informática, o zero é o menor número inteiro não atribuído, um dos mais fundamentais na programação e no design de hardware.

É assim geralmente, o mais utilizado na recursividade numérica, como caso base para a partir do mesmo, se definir as regras que formulem casos complexos. Sendo que na Matemática, a prova obtém-se através de um argumento dedutivo, o zero serve para este e outros raciocínios

³ Um longo osso castanho (a fíbula de um babuíno), com um pedaço de quartzo afiado incrustado na ponta. Descoberto pelo belga Jean de Heinzelin de Braucourt em 1960.

⁴ Em 2010, escreve Robert Logan no *The Poetry of Physics and the Physics of Poetry*: “The idea of sunya and place numbers was transmitted to the Arabs who translated sunya or “leave a space” into their language as sifr”.

lógicos na ciência computacional.

É ainda de realçar a importância do zero, na medida em que as instruções dadas a um computador são, na verdade, sequências numéricas binárias compostas por 0 e 1 (p. ex.: 01101100).

I. b. Noção de Software, Firmware e Hardware

Estas instruções compõem o software, cuja definição foi pela primeira vez proposta por Alan Turing e utilizada com este significado em 1957, por John W. Tukey⁵.

Assim, o software trata-se de uma sequência de instruções a executar, na realização, bloqueio, redireccionamento ou modificação de uma informação ou acontecimento⁶.

Insere-se especialmente num contexto tecnológico, devido ao seu uso em sistemas computadorizados, que compostos por diversas funções, bibliotecas e módulos, geram um programa executável que recebe dados (*data input*), processa-os segundo uma série de algoritmos pré-definidos⁷ e permite um resultado (*data output*) deste processamento.

Há ainda a acrescentar que, a respeito do *software de sistema*, especializado, e cujo objetivo é realizar detalhadamente a manutenção do sistema tecnológico em utilização, este conecta interfaces de alto nível às ferramentas, de modo a que tudo funcione como é suposto. Desde os sistemas operacionais, à interface gráfica que permite interagir com o sistema principal e os seus periféricos, a *drivers*⁸, a ferramentas de diagnóstico, a ferramentas de correção e otimização, a servidores.

⁵ Tukey (16 de junho de 1915 – 26 julho de 2000), matemático americano conhecido por inúmeras inovações, inventou o termo “bit” nos Laboratórios Bell, ao trabalhar no desenvolvimento de métodos estatísticos para computadores. De acrescentar que o Teste de Alcance de Tukey, a Distribuição de Lambda de Tukey, o Teste de Tukey da Aditividade e o Lema de Tukey carregam o seu nome.

⁶ Um software bem desenvolvido é normalmente criado pela área de engenharia de software e inclui não só o programa de computador em si, mas também manuais, especificações e configurações.

⁷ Ou pré-parametrizados.

⁸ Enquanto programas de computador que fornecem um interface de software a dispositivos de hardware, permitindo que sistemas operativos e outros programas de computador acessem às funções do hardware, sem que seja necessário estes saberem em detalhe o tipo de hardware em que estão a ser utilizados.

Neste conjunto inclui-se o *firmware*, que atua diretamente no *hardware* do sistema e define as operações básicas deste, a modos que, sem este, um dispositivo seria completamente não-funcional⁹.

Por fim temos o hardware, enquanto recursos físicos e equipamentos¹⁰ utilizados no processamento físico das instruções criadas em software.

I. c. Precusores da Máquina de Turing e sistema binário

Ainda em 500 a.C., Pāṇini, um gramático indiano nascido em Gandara¹¹ compôs a gramática do *Sânscrito*, altamente complexa e ainda assim, sistematizada em 3959 regras, conhecidas como *Ashtadhyayi*.

Os registos históricos disponíveis levam a que a comunidade científica lhe atribua a autoria da primeira gramática linguística na história da civilização humana¹².

O interesse deste trabalho é que Pāṇini usou meta-regras, transformações e recursões de tal modo sofisticadas, que a sua gramática tinha o poder computacional¹³ equivalente à máquina de

⁹ É com o propósito de facilitar a comunicação entre programador e hardware que existem as linguagens de programação. O programador escreve instruções numa linguagem de código programacional mais ou menos próxima da que as pessoas usam para comunicar entre si, e de seguida, um segundo programa traduz o que o programador escreveu para sequências compostas por 0 e 1 (*Compiladores*) ou interpreta as instruções dadas pelo programador e executa-as (*Interpretador*).

¹⁰ Desde microprocessadores, a discos rígidos, a memória RAM, a memória cache, a Placa-Mãe, Placa de Rede e outros, até mesmo periféricos – como uma impressora, um scanner, uma webcam.

¹¹ Em sânscrito पण्डित, um reino indiano antigo no norte do Paquistão e a leste do Afeganistão, que durou do século VI a.C. ao século XI d.C.

¹² Não é certo se Pāṇini redigiu o seu trabalho, mas dada a complexidade deste, em que sem anotações, a tarefa de organizar e compilar os conhecimentos seria penosa, crê-se que deve tê-la composto com a ajuda de um grupo de estudantes, cujas memórias lhe serviram como "blocos de notas". Isto baseia-se nas referências a palavras como "escrita" e "escriba" presentes na sua gramática.

¹³ I.e., o poder de processar cálculos complexos, com a mesma rapidez.

A respeito da máquina de Turing, inventada por Alan Turing em 1936, e cujo autor abordar-se-á posteriormente, é de dizer que a sua máquina provou a existência de limitações fundamentais no poder da computação mecânica. Embora possam expressar computações arbitrárias, o seu design minimalista torna-as inapropriadas para computar na prática, dada a inexistência de uma memória de armazenamento rápida, que armazene com frequência as instruções dos programas mais utilizados, de forma a aumentar a velocidade de processamento do sistema.

Turing.

Além disso, é precursor da teoria da linguagem formal moderna, e do seu uso na computação moderna.

Em 300 a.C., o músico, erudito e matemático indiano Pingala, famoso pela sua obra *Chandaḥśāstra* – um tratado sânscrito sobre prosódia¹⁴ –, apresentou nesta, a primeira descrição conhecida do sistema numérico binário¹⁵. Sistema esse que é atualmente utilizado no design de essencialmente, todo o equipamento computacional moderno.

I. d. Dispositivos Autômatos – o primeiro programa

A 200 a.C. deu-se a invenção do ábaco chinês, *Suanpan*. Embora não se tenha dada a sua expansão mundial, e atualmente só exista na cultura oriental de forma residual, o seu cálculo por meio de contas serviu para as operações matemáticas de multiplicação, divisão, adição, subtração, cálculo da raiz quadrada e ainda da raiz cúbica, a alta velocidade (e com rigor científico).

A 125 a.C. surgiu a *Máquina de Anticítera*, um mecanismo analógico semelhante a um relógio, hoje tido como o primeiro computador analógico na história da Humanidade, devido à sua complexidade e mesmo especialização e tamanho das suas peças¹⁶.

Já na transição de a.C. para d.C., ocorreram dois acontecimentos marcantes na história da computação.

Isto é, o que os computadores modernos possuem, conhecido como *Random-access memory*, ou memória RAM.

¹⁴ A prosódia, pertencente à Fonologia, é a área da linguística que estuda a entonação, o ritmo, e a acentuação (intensidade, altura, duração) da linguagem falada. Esta descreve todas as propriedades acústicas das palavras, para que se faça a correta acentuação tônica das mesmas.

¹⁵ Fê-lo ao longo da listagem das métricas védicas, relacionando a sua métrica com o que corresponde ao teorema binomial, por meio de sílabas e traços longos e curtos, com uma sílaba longa a equivaler (em comprimento) a duas sílabas curtas, escrevendo símbolos musicais num código semelhante ao Código Morse.

¹⁶ Composto por vinte e sete engrenagens de bronze, trabalhadas à mão, comparáveis às peças de um relógio feito no século XVIII, representa mecanicamente a órbita da Lua, de cada corpo celeste conhecido pelos gregos antigos: Mercúrio, Vênus, Marte, Júpiter e Saturno, e ainda do próprio Sol. É preciso no cálculo das órbitas de cada corpo celeste, ao que é capaz de prever eclipses lunares e solares, mesmo que ocorram muitos séculos depois.

Se a 100 a.C., há o primeiro uso por matemáticos chineses de números negativos¹⁷, já por volta de 60 d.C., *Heron da Alexandria* impulsionou a informática e a cibernética com a invenção do primeiro “programa” e a invenção de dispositivos autômatos que funcionavam a vapor.

Heron da Alexandria (10 a.C. a 70 d.C.), matemático grego e engenheiro considerado o maior experimentador da Antiguidade¹⁸, criou inúmeras invenções incluindo uma “Sequência de Controlo”, em que um operador programava uma máquina para que esta se deslocasse a grande velocidade, e esta obedecia, seguindo uma sequência de instruções, de uma forma pré-determinada.

Foi ainda pioneiro¹⁹ na invenção do moinho de vento como fonte de energia, capaz de movimentar uma máquina e outros dispositivos autômatos.

¹⁷ I.e., haver a aceitação e realização de cálculos com números reais menores que zero.

A respeito da importância do primeiro uso de números negativos ser em 100 a.C.: para a Informática, os números negativos são difíceis de expressar em binário, ao que, para que os computadores possam lidar com os mesmos, foram desenvolvidas 3 formas de representar valores negativos: o sinal e amplitude/magnitude (S+M), o complemento para 2, e ainda a notação em excesso (biased).

O primeiro caso envolve utilizar o bit mais à esquerda para representar o sinal, 0 para indicar um valor positivo e 1 para indicar um valor negativo.

Já no caso de representar os números em complemento para 2 (existe a possibilidade de representar em complemento para 1, mas este gera a equivalência, para zero (0), em que por exemplo, $010 = 000000002 = 111111112$, o que torna impossível de discernir um padrão de bit negativo de um padrão de bit positivo), para determinar o negativo de um número, negam-se todos os seus bits e soma-se uma unidade.

Ao que, de um modo exemplificativo, depois de inverter os bits, $100110112 + 1 = 100111002$.

O bit da esquerda (0 / 1) continua a indicar se é um número negativo ou positivo, o 0 passa a ter representação única – todos os bits a 0, e dado que o complemento é para dois, a gama de valores que é possível representar com n bits vai desde $-2^{n-1} \dots 2^{n-1} - 1$.

Por fim, a 3ª possibilidade é por notação em excesso, em que a vantagem face aos anteriores métodos é que a representação numérica tem sempre o mesmo comportamento: o valor em binário com todos os bits a 0, representa o menor valor inteiro, quer este tenha sinal ou não, e o mesmo se aplica ao maior valor em binário, a tender para os seus bits serem todos 1. Aqui, 000000012 equivalerá a -127 , e 111111102 a $+126$.

De qualquer modo, o importante a reter é que se trata de um marco importante para a história da computação, a primeira utilização de números negativos na história da humanidade.

¹⁸ Helicon Publishing, “*The Hutchinson dictionary of scientific biography*”, por Helicon Publishing (Abingdon, Oxon), Research Machines, 2004, p. 546.

¹⁹ Muito embora já 100 anos antes Vitruvius o tivesse feito, na sua compilação da teoria arquitetónica, “*De Architectura*”, em dez livros.

Quer moinhos de vento que funcionavam com um motor de propulsão a vapor²⁰, como a eolípila (ou *Máquina de Heron*).

Quer mesmo, por meio de fios atados, operando em redor de uma roda dentada cilíndrica, um teatro elegante, movível e programável, que automatizado, se mostrava capaz de atuar durante um máximo de 10 minutos²¹.

I. e. Programação nos primeiros autómatos

As inovações na Matemática e deste modo, na Ciência da Computação, no período da *Antiguidade* que se estende desde a invenção da escrita (de 4 000 a.C. a 3 500 a.C.) até a queda do Império Romano do Ocidente (a 476 d.C.), encerram-se com a invenção dos logaritmos, a 200 d.C. por matemáticos *Jain*, seguidores do Jainismo²².

De inúmeras aplicações para a Ciência da Computação, os logaritmos binários podem servir para calcular o número de bits necessários para codificar uma mensagem, ou contar o número de

²⁰ Composto por uma esfera oca que se movimenta ao estar ligada a turbos curvados (formando um eixo), que libertam o vapor formado numa bacia com água, debaixo, em constante aquecimento por meio de uma fogueira.

²¹ Conforme Noel Sharkey, para a revista online New Scientist edição 2611 in <https://www.newscientist.com/article/mg19526111-600-the-programmable-robot-of-ancient-greece/>: “The programmable robot of ancient Greece”:

«(...) Each loop of twine wrapped around the axle would propel the machine forward by one wheel revolution. But Hero had also found a way to make his robot move backwards. He stuck a peg into the center of the axle at right angles so he could wind the string in one direction, then wrap it around the peg and continue to wind around the axle in the opposite direction.

Hero's idea was so elegant that even as I read it, the hairs on the back of my neck stood on end. It also struck me that this mechanism provides the basis of a simple programming language. For example, winding the string around the axle 10 times in one direction, then passing it around the peg and winding it five times in the other can be represented as Forward (10), Backward (5).

It also turned out that Hero had devised a pause command for his robot that is a function of time. He simply pulled lengths of string off the axle and stuck them either to the axle or to the side of the robot using wax. When the weight pulled on the wax it would release the extra string, so the robot would pause while the slack was pulled in.

(...) Surprisingly, Hero used a much more explicit programming strategy than either da Vinci or Al-Jazari. His method of programming is unique in the history of robots. It relied on string.»

²² Sendo uma das religiões mais antigas da Índia (em conjunto com o hinduísmo e o budismo), estes matemáticos eram conhecidos como pandits ou “homem-culto”, treinados no idioma sânscrito e na literatura, na gramática (*vyākaraṇa*), exegese (*mīmāṃsā*) e ainda na lógica (*nyāya*).

passos necessários para uma pesquisa por meio de um algoritmo de busca. Mesmo na área da Bioinformática e da Fotografia, são uma mais-valia.

A 1206, *Al-Jazari*, engenheiro mecânico árabe, um artista, inventor, matemático e ainda erudito islâmico (1136-1206), compõe os primeiros planos de construção de autómatos, sendo estes operados por meio de moinhos d'água ou mesmo azenhas movimentadas por animais, por meio de eixos de manivelas/cambotas.

A importância da invenção destes autómatos, desde portões automáticos a humanoides programáveis²³ prende-se com a melhoria da qualidade de vida em sociedade, oferecendo proteção, entretenimento ou mesmo simples comodismos – como um autômato que permitia lavar as mãos, através de um mecanismo de autoclismo²⁴.

Já em 1300, *Raimundo Lúlio* ou *Lull* (1232-1315), conhecido como o mais importante escritor, filósofo, poeta, missionário e teólogo catalão, inventou o “*Círculo Luliano*”, uma “*máquina de noções*” que calculava a resposta a questões filosóficas²⁵ através da Lógica Combinacional.

Nesta máquina que assenta numa linguagem de programação simplificada²⁶, as combinações entre atributos/qualidades – presentes em dois (ou mais) discos de papel que podiam ser rodados individualmente – mostrariam todas as verdades possíveis acerca do tema escolhido²⁷.

Em 1674, 374 anos depois e já no século XVII, enquadrando a Lógica Combinacional de Lull na Ciência da Informação e Computação²⁸, Leibniz²⁹ deu à ideia de Lull o nome de *ars*

²³ Professor Noel Sharkey, *A 13th century programmable robot*, University of Sheffield, 2007, in <https://readtiger.com/https/web.archive.org/web/20070629182810/http://www.shef.ac.uk/marcoms/eview/articles58/robot.html>.

²⁴ Semelhante ao que utilizamos nos dias de hoje.

²⁵ Entenda-se filosófico-religiosas.

²⁶ Na verdade, pode-se pensar nesta máquina como “um computador, em abstrato”, diz Juha Sorva, no artigo “*Notional Machines and Introductory Programming Education*”, da coletânea “*ACM Transactions on Computing Education*”, Vol. 13, Nº 2, Artigo 8, Aalto University, junho de 2013.

²⁷ Pela noção de que existiriam um número limitado de verdades elementais (básicas e inegáveis) em todos os campos do conhecimento, e que, pelo estudo das várias combinações da sua máquina, estas poderiam ser alcançadas.

²⁸ Sendo um dos elementos fundamentais da mesma.

²⁹ Do qual falaremos posteriormente.

combinatoria, nome pela qual atualmente ainda se designa³⁰. Aliás, é entendimento de alguns cientistas, pelos factos anteriormente relatados, que Lull se trata de uma espécie de “pai fundador” da Ciência da Informação e Computação³¹.

I. f. Projetos de Leonardo da Vinci

Em 1492, Leonardo da Vinci³² (1452-1519) desenhou projetos para uma calculadora mecânica que por meio de rodas dentadas interligadas, era capaz de adição e subtração³³. Além disso, esboçou um projeto para a criação de um robot.

I. g. Tabelas de multiplicação e réguas de cálculo

Na procura de resolver o problema de mecanizar as 4 operações aritméticas (soma, subtração, multiplicação e divisão), o método que ao longo dos tempos se mostrou não só o mais eficiente mas o mais sofisticado, foi recorrendo a máquinas que combinassem alavancas e rodas dentadas, calculando fisicamente tabelas de multiplicação.

Aludimos assim a *John Napier* (1550-1617), matemático escocês, e ao seu sistema engenhoso de, por meio de tabelas de multiplicação gravadas em bastão, multiplicar e dividir de forma automática.

Estas tabelas, inventadas em 1617, ficaram conhecidas como *Ossos de Napier*.

³⁰ Ao tratar-se de um método que, apoiando-se na lógica combinacional, procurava obter conhecimento. Para Lull, o mais importante seria poder demonstrar que as doutrinas Cristãs eram indutíveis, artificialmente, de um conjunto fixo de ideias predefinidas. Por exemplo, uma das tabelas listava os atributos de Deus: Bondade, Grandiosidade, Eternidade, Poder, Sabedoria, Vontade, Virtude, Verdade e Glória. Lull sabia que todos os crentes em religiões monoteístas – quer fossem judeus, muçulmanos ou cristãos – concordariam com estes atributos, formando assim uma plataforma segura, com a qual argumentar.

³¹ Conforme informação presente no website: <http://www.historyofinformation.com/expanded.php?id=2335>.

³² O famosíssimo pintor da “Mona Lisa”, em 1503. Para além disso, enquanto ilustre homem renascentista, era cozinheiro, engenheiro, escultor, arquiteto, matemático, químico, botânico, geólogo, cartógrafo, físico, escritor, músico, etc. Um “homem dos mil ofícios”.

³³ Continua controverso se era, efetivamente, uma calculadora mecânica o que o Mestre da Vinci tinha em mente. Diga-se ainda, um modelo funcional deste dispositivo foi efetivamente construído em 1968.

Baseando-se nos logaritmos naturais desenvolvidos por Napier³⁴, a 1622, um matemático inglês de nome *William Oughtred* desenvolveu um computador mecânico analógico que, por meio do cruzamento de escalas de logaritmos, permitiu uma multiplicação e divisão de números mais rápida³⁵.

I. h. O fim da era da computação mecânica

Por volta de 1642, Blaise Pascal, matemático e filósofo francês, inventou uma calculadora mecânica, *Pascalina*, que se servia de discos móveis, para realizar somas e subtrações na casa das centenas de milhões³⁶.

Já em 1674, Gottfried Leibniz, matemático e filósofo alemão, melhorou a capacidade da *Pascalina*, permitindo que esta também realizasse multiplicações³⁷.

Restando assim a operação da divisão, entende-se que as quatro operações aritméticas só se tornaram completamente possíveis com Charles Colmar.

Charles Xavier Thomas de Colmar (1785-1870), inventor francês, colmatou essa falha com o “*Arithmomètre*”: em 1820, criando uma calculadora mecânica inovadora, que permitia selecionar a operação com o uso de alavancas. Internamente³⁸, a rotação de rodas dentadas selecionava a operação de soma/subtração ou multiplicação/divisão.

³⁴ Como foi referido antes, os logaritmos têm vastas e inúmeras aplicações para a Ciência da Computação, como por exemplo, os binários que podem servir para calcular o número de bits necessários para codificar uma mensagem. Ora, em 1588, Joost Bürgi (1552-1632), um relojoeiro e matemático suíço, descobriu os logaritmos naturais – 6 anos antes de John Napier.

Contudo, como não publicou nenhuma obra a fim de expor as suas ideias, perdeu a hipótese de reivindicar tratar-se do seu descobridor.

³⁵ I.e., desenvolveu réguas de cálculo que se baseiam na sobreposição de escalas logarítmicas.

³⁶ Quando a engrenagem virava à direita era feita a adição, virando a engrenagem à esquerda, era feita a subtração dos valores armazenados nos discos anteriores.

³⁷ Smith, David Eugene, *A Source Book in Mathematics* (1929): “[Em 1685] num artigo intitulado «*Machina arithmetica in qua non additio tantum et subtractio sed et multiplicatio nullo, diviso vero paene nullo animi labore peragantur*», Gottfried Leibniz descreveu uma máquina que, usando rodas com dentes móveis, que, acoplado a uma *Pascalina*, poderia realizar todas as quatro operações matemáticas”. Mas não há provas de que tal máquina tenha sido alguma vez construída por Leibniz.

³⁸ Como uma caixa-de-música.

Esta era de tal modo versátil, que o seu uso se estendeu até à 1ª Guerra Mundial, pondo cobro ao que se pode designar por *era da computação mecânica*³⁹.

I. i. Já o pai do computador, Charles Babbage e Ada Lovelace, a primeira programadora

Introduzimos agora Charles Babbage, cientista, matemático, filósofo, engenheiro mecânico e inventor inglês, hoje em dia considerado “o pai do computador”.

Em 1823, recebeu uma bolsa do Governo Britânico para projetar uma calculadora com capacidade até a vigésima casa decimal.

Até apresentar a sua “*Máquina Analítica*” em 1833, foi professor de matemática na Universidade de Cambridge (1828-1839), sendo a sua máquina considerada o ponto de partida para os modernos computadores eletrónicos⁴⁰.

³⁹ No mês de Janeiro de 1857, Edward Cave e John Nichols escrevem no The Gentleman's magazine, Volume 202, The monthly intelligencer: «*M. Thomas's arithmometer may be used without the least trouble or possibility of error, not only for addition, subtraction, multiplication, and division, but also for much more complex operations, such as the extraction of the square root, involution, the resolution of triangles, etc...*

A multiplication of eight figures by eight others is made in eighteen seconds; a division of sixteen figures by eight figures, in twenty four seconds; and in one minute and a quarter one can extract the square root of sixteen figures, and also prove the accuracy of the calculation...»

The working of this instrument is, however, most simple. To raise or lower a nut-screw, to turn a winch a few times, and, by means of a button, to slide off a metal plate from left to right, or from right to left, is the whole secret. Instead of simply reproducing the operations of man's intelligence, the arithmometer relieves that intelligence from the necessity of making the operations. Instead of repeating responses dictated to it, this instrument instantaneously dictates the proper answer to the man who asks it a question. It is not matter producing material effects, but matter which thinks, reflects, reasons, calculates, and executes all the most difficult and complicated arithmetical operations with a rapidity and infallibility which defies all the calculators in the world.

The arithmometer is, moreover, a simple instrument, of very little volume and easily portable. It is already used in many great financial establishments, where considerable economy is realized by its employment.

It will soon be considered as indispensable, and be as generally used as a clock, which was formerly only to be seen in palaces, and is now in every cottage».

⁴⁰ Garcia Marques e Lourenço Martins, Direito da Informática, 2006: «(...) *frustrado com a quantidade de erros que encontrou ao examinar os cálculos da Royal Astronomical Society, constatou que as máquinas podiam executar, ao serviço dos matemáticos, tarefas repetitivas de organização de tabelas, sem erros. A primeira tentativa ocorreu em 1822 com um modelo da “Difference Engine”, que executava equações diferenciais. Dotada de um programa, poderia fazer cálculos e imprimir automaticamente os resultados. Nela trabalhou mais de dez anos, com o apoio do Governo britânico, que acabou por se cansar de lhe abonar fundos*».

Em 1840, a máquina já operaria com números de até 40 dígitos, conteria uma *CPU* (Unidade Central de Processamento), dois acumuladores⁴¹ principais (e alguns auxiliares) e uma memória de armazenamento, com capacidade para pelo menos, 1000 números – de 50 dígitos cada.

Teria vários cartões, tanto para os programas como para os dados, que permitiam a alteração automática das sequências de operações.

Por fim, e quanto ao mais importante, esta era uma máquina que permitia a impressão dos resultados, após recorrer a um motor-a-vapor, como fonte de energia, para realizar somas em 3 segundos, e multiplicações ou divisões, em 2 a 4 minutos.

Se falamos de Charles Babbage será pois, mais do que justo, apresentar Ada Lovelace (1815-1852), sua assistente e conhecida como a primeira “programadora” da História⁴².

Trabalhando lado a lado com Babbage, ela desenvolveu os algoritmos que permitiriam à “Máquina Analítica” computar os valores de funções matemáticas, além de publicar uma coleção de revisões sobre os detalhes técnicos desta máquina.

Na prática, auxiliou não só à captação dos fundos do Governo Britânico, como concebeu as instruções para o público, para difundir a sua utilização em massa. Diga-se, no entanto, que a máquina não foi construída durante o tempo de vida da Condessa de Lovelace.

I. j. Alan Turing e o seu contributo extraordinário para a computação

Apenas a partir de 1936, através de Alan Turing (1912-1954), matemático, lógico, criptoanalista e cientista da computação britânico, é que se torna possível aceder aos desejos de Babbage: computar, seguindo regras lógicas, tarefas repetitivas de organização de tabelas sem erros.

⁴¹ O acumulador é um dos registradores da CPU, no qual se armazena os resultados de uma operação aritmética.

⁴² Tom Simonite, *Short Sharp Science: Celebrating Ada Lovelace: the 'world's first programmer*, <https://www.newscientist.com/blogs/shortsharpscience/2009/03/ada-lovelace-day.html>, New Scientist, a 24 de março de 2009.

Pai da Computação, o mais famoso feito de Turing foi, em 1943, ter conseguido decifrar as transmissões codificadas dos Alemães, num projeto secreto da 2ª Guerra Mundial – “*Projeto Enigma*” –, em que se serviu de um computador eletromecânico, o “*Colossus*”⁴³.

Contudo, o impacto deste projeto no desenvolvimento da indústria dos computadores não foi muito significativo, dado que esteve guardado em segredo durante décadas após a 2ª Guerra Mundial (com o intuito de prevenção, para a ocorrência de um evento semelhante).

I. k. O conceito de memória única – o EDVAC

Vimos que Babbage e Ada Lovelace criaram uma *unidade de controlo*, por meio de um programa que alterava automaticamente as sequências de operações.

Em 1945, na sequência desta ideia, John von Neumann (1903-1957), um matemático e prodígio húngaro, introduziu o conceito de *memória única* para os programas e dados.

Falamos assim de um projeto modelo, de um computador digital de programas pré-armazenados, que utiliza uma unidade central de processamento⁴⁴ (CPU). Essa unidade central de processamento permitia o controlo de todas as funções do computador a partir de uma única fonte, e ainda incluía uma memória de armazenamento para comportar instruções e dados.

Um computador possuidor desta *memória única*, como o caso do “*EDVAC*” (1944/1949), um dos primeiros computadores eletrónicos⁴⁵, podia parar a qualquer momento e recomeçar sem perdas, com uma versatilidade muito maior da programação.

Com isto, damos por encerrada a análise do que jaz na base da Informática moderna.

⁴³ Atribui-se a ele, e à sua equipa, o êxito sobre o afundamento do *Bismarck*, a destruição das linhas marítimas de abastecimento ao *Africa Korps*, de *Rommel*, e a decifração sistemática das mensagens para a frota de submarinos alemães no Atlântico Norte – in <http://www.cs.usfca.edu/www.AlanTuring>.

⁴⁴ Conhecida como a *Arquitetura de von Neumann*.

⁴⁵ O *Electronic Discrete Variable Automatic Computer* ou *Calculadora Eletrónica Automática de Variável Discreta (EDVAC)*.

I. I. As várias gerações de computadores – uma breve análise

Sendo um tema particularmente extenso, e na senda do que exploramos antes, procuramos aqui sintetizar as inovações que, dentro das várias gerações de computadores, têm relevância para a temática.

Como o caso da procura constante da miniaturização, em conjunto com a redução de recursos e aumento da capacidade computacional, enquanto télos da computação.

A primeira geração de computadores (1946-1954) é marcada pela utilização de válvulas, tubos de vidro que formavam um ambiente fechado a vácuo e que continham elétrodos. Conforme referido anteriormente, a programação era realizada diretamente na máquina, com o armazenamento dos dados em cartões perfurados (posteriormente, em fita magnética).

No período que vai do ano 1955 ao ano 1964, na segunda geração de computadores, surge o conceito de *multiprogramação*, isto é, a presença de vários programas em (aparente) execução simultânea, numa única máquina computacional.

Substituiu-se a válvula pelo transístor, o qual já não necessitava de pré-aquecimento, e assim, os computadores eram mais rápidos que nunca.

Relembramos que o conceito de CPU foi desenvolvido nesta altura, tal como o conceito de memória, linguagem de programação e entrada e saída.

Já a terceira geração (1964-1977) é marcada pelos circuitos integrados. Surge pois, em 1971, o *microprocessador*⁴⁶, com a possibilidade de integrar, em larga escala, centenas de milhares de transístores num único circuito, incluindo uma CPU.

E é aqui que surge o *PC*, ou *computador pessoal*, na fase final desta geração, pelas mãos de Steve Wozniak⁴⁷ e Steve Jobs⁴⁸: construído a partir de alguns circuitos integrados, colocados

⁴⁶ Com o passar do tempo, e ao contrário da sua finalidade inicial, o microprocessador passa a poder ser programável para rádios, aparelhos de televisão ou mesmo controlo de sistemas automóveis.

⁴⁷ Um inventor, engenheiro eletrónico, programador, empreendedor e filantropo americano, nascido em 1950, pioneiro da revolução dos computadores pessoais dos anos 70 e 80.

⁴⁸ Cofundador da Apple, em conjunto com Wozniak, Steven Paul Jobs foi um empreendedor e magnata dos negócios americano. Viveu entre 1955 a 2011.

num chip, e possuidor de um processador, memórias e controlos de entrada e saída de dados.

Podemos também acrescentar que, pelas mãos da IBM⁴⁹, passou a haver a separação da criação de hardware, da criação de software – que na altura, se limitava ao desenvolvimento do sistema operativo.

A quarta geração (1977-1991) é marcada pela venda dos computadores pessoais, pelo surgimento generalizado dos processadores e o uso dos discos rígidos como memória secundária, e ainda a construção dos sistemas operativos como o MS-DOS, UNIX e o Macintosh⁵⁰.

Por fim a quinta geração, surgida em 1991 e ainda presente atualmente, demarca-se das anteriores gerações, pela inteligência artificial e pelas possibilidades da conectividade.

Primeiro, é de referir que os processadores atuais contêm milhões de transístores. E em termos de memória, quer de armazenamento, quer de processamento, isto é, o desempenho das tecnologias atuais sustenta-se em arquiteturas de 64 bits, novos processadores, discos rígidos híbridos – SSD – com cada vez maior capacidade de armazenamento. De bytes a kilobytes. Kilobytes a megabytes, a gigabytes. E finalmente, terabytes.

E segundo, quanto à conectividade: inicialmente, a transmissão de dados fazia-se por ligação de cabos, física. Surgiu em 1993 a transmissão por Infravermelhos (IrDA), para depois, durante a primeira década de 2000, competir com a tecnologia emergente Bluetooth (inventada em 1994 por Jaap Haartsen, um engenheiro elétrico holandês). Ganhou a segunda, o mercado.

Surgimento a partir de 1997, ou melhor, ressurgimento da tecnologia NFC, baseada em identificação por radiofrequência (ou RFID), patenteada em 1983 por Charles Walton⁵¹. E só em 2003, pelas mãos da Sony e da Philips é que teve as suas especificações técnicas estabelecidas.

Esta tecnologia, enquanto conjunto de protocolos de comunicação, que permitem que dois dispositivos eletrónicos estabeleçam comunicação de dados entre si, é usada em sistemas de

⁴⁹ *International Business Machines* (IBM). É uma – senão a maior – das empresas norte-americanas especializadas em serviços das tecnologias de informação e comunicação, fundada em 1888.

⁵⁰ Desenvolveu-se ainda linguagens de programação orientadas a objeto, como C++ e o Smalltalk.

⁵¹ Engenheiro elétrico norte-americano, vivo entre 1921 a 2011, conhecido pelo primeiro a registar a patente da tecnologia RFID.

pagamento sem necessitar de contacto físico com os mesmos. Permite ainda a partilha de contactos, fotos, vídeos, ou mesmo ficheiros de todo o tipo.

Já a respeito da inteligência artificial, certamente um produto da ficção humana que veio e virá a fazer realmente parte do quotidiano da nossa sociedade, o seu interesse prende-se com as suas potencialidades nas tecnologias eletrónicas, nos sistemas computacionais. O poder desafiar a inteligência humana, e o conseguir melhorar a qualidade de vida do ser humano.

Mas não sem os seus perigos.

I. m. O *Homo Conectus* moderno e os seus perigos

O avanço tecnológico dos sistemas computacionais ao longo do século XX⁵² permitiu, finalmente, abrir as portas da discussão sobre a possibilidade de se construir uma *Inteligência Artificial*, não humana, superior para todos os efeitos. Este desejo, com origem na Antiguidade e de lendas e mitos de tradição oral na sua maioria, tem a sua base na vontade de forjar deuses.

O verdadeiro boom desta ciência, que é um ramo da Ciência da Computação dedicada a simular e progredir sobre a inteligência humana, está-se a dar sim no século XXI, com verdadeiros laboratórios de Inteligência Artificial, infraestruturas em *cloud* capazes de processar informações verdadeiramente complexas, distribuição de ferramentas de desenvolvimento de software, redes neuronais, entre outros.

Com efeitos que se repercutem em todo o género de tecnologias, para que as mesmas respondam mais eficazmente às necessidades da população⁵³, certo é que nos encontramos numa fase de transição, onde as respostas a dar pelas tecnologias requerem cada vez mais um acesso intrusivo aos dados dos utilizadores.

⁵² Comprovadamente, ao longo das várias gerações de computadores, com a invenção do primeiro computador digital programável na década de 1940; ao campo de pesquisa de IA a ser fundado na Universidade de Darmouth em 1956; a entre os anos 70s-80s, altos e baixos nos investimentos governamentais de capital na IA; à conferência científica de Inteligência Artificial e Neurociência Computacional – Sistemas de Processamento de Informações Neurais (NIPS) –, iniciada em 1987 e atualmente a maior conferência de Inteligência Artificial, etc.

⁵³ Como vimos antes, servindo de exemplo, os usos possíveis de um microprocessador não ficam limitados aos sistemas computacionais.

Muito por causa da finalidade de melhorar a qualidade de vida, com a obtenção de respostas a problemas cada vez mais complexos. Uma dessas respostas é a tecnologia⁵⁴ poder servir como sistema de suporte a falhas do organismo humano, recorrendo aos dados obtidos por meio de sensores. Dados estes, biométricos.

Com sistemas, técnicas e dispositivos que medem e analisam os atributos físicos e comportamentais das pessoas, como características faciais, padrões de voz, impressões digitais, leituras biométricas da palma da mão, padrões de veias e artérias, estrutura de órgãos, como o olho, íris ou retina, ou ainda mesmo a postura, a forma de andar, ou mesmo a forma de assinar⁵⁵.

Conforme nos faz lembrar Francisco Andrade⁵⁶: *“neste novo paradigma, alguns importantes princípios de direito relacionados com os direitos fundamentais à privacidade e à proteção de dados pessoais, parecem algo comprometidos. (...) Tomemos como exemplos o direito ao esquecimento e o direito a ser deixado só”*.

Falamos de dados biométricos digitalizados, e sujeitos a análise computacional. Falamos de dados que, sem o devido controlo legal por parte do legislador, sobre as tecnologias que tratam dos mesmos, levantam sérias dúvidas quanto aos riscos para a vida dos indivíduos.

Tanto pessoais como profissionais, afinal, a disseminação dos dados de saúde de alguém pode ter consequências sérias para um bom ambiente na relação de trabalho. Quebrar mesmo uma relação de confiança e respeito mútuo, se houver algum preconceito quanto à capacidade de trabalhar – por exemplo, no caso de uma mulher grávida, ou que pense engravidar eventualmente.

Daí haver barreiras legais e proibição de certas perguntas, principalmente para proteção do

⁵⁴ Máquinas de simples leitura dos dados de saúde, para máquinas que efetivamente colaboram num funcionamento normal do organismo humano, como pacemakers, banda gástrica, articulações, etc. Eventualmente, algo ainda mais sofisticado, mais capaz.

⁵⁵ Conforme ANDRADE, Francisco C. P., MOREIRA, Teresa, *Biometrics and Data Protection: These Data are Derived from an Individual*, in *Interdisciplinary Perspectives on Contemporary Conflict Resolution* (coord. Paulo Novais e Davide Carneiro), IGI Global, 2016 e ainda O'CONNOR, Sean, *Collected, tagged, and archived: legal issues in the burgeoning use of biometrics for personal identification*, Stanford Technology Law Review, 1998;

⁵⁶ ANDRADE, Francisco C. P., *Comunicações Eletrónicas e Direitos Humanos: O Perigo do “Homo Conectus”*, in *Direitos Humanos e Sua Efetivação na Era da Transnacionalidade*, Juruá Editora, Curitiba, 2012.

utilizador-trabalhador, na sua relação com o empregador⁵⁷.

Por serem dados sensíveis – podemos desde já dizer, conforme o artigo 9º do Regulamento Geral de Proteção de Dados⁵⁸, onde pelo nº1, *“é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa”*.

Com esta introdução, e ao mesmo tempo, conclusão da análise histórico-cultural das tecnologias computadorizadas; com ainda a advertência do perigo, que jaz numa sociedade que caminha a passos largos para um *homo conectus* permanente, 24 horas por dia; entendemos que ainda existe um outro ponto, final a considerar: desta evolução tecnológica generalizada, há a possibilidade que, à medida que surjam novas tecnologias para a finalidade de obtenção e tratamento dos dados biométricos, pelo facto de não haver um mercado tipo padrão dos mesmos⁵⁹ se promova uma concorrência desenfreada apelando à mais recente novidade, sem garantias de segurança no funcionamento dos produtos.

⁵⁷ Conforme o Código de Trabalho português, especificamente toda a subsecção II, quanto aos direitos de personalidade, artigos 14º a 22º. Principalmente o artigo 17º, proteção de dados pessoais, alíneas a) e b), e ainda o artigo 18º, dados biométricos, quanto ao tratamento dos dados do trabalhador por parte do empregador.

⁵⁸ REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

⁵⁹ Onde há efetivamente concorrência, e temos criadores e empresas testadas, certificadas, e confiáveis, em pelo menos a gama alta e média de preços (e qualidade de produtos), que se responsabilizam pelo produto e os usos feitos do mesmo.

II. Agentes De Software Inteligentes, Redes Neurais Artificiais E Inteligência Computacional

II. a. Aproximação à Inteligência Artificial por meio de uma Inteligência Computacional

Para se reconhecer Inteligência Computacional⁶⁰ num computador, este tem de ser capaz de aprender uma determinada tarefa a partir de dados ou observações experimentais.

Falamos portanto de um conjunto de metodologias computacionais, inspiradas na natureza, que por aproximação, tentam responder a problemas complexos, para os quais os modelos matemáticos tradicionais se tornam obsoletos (ou pelo menos, insuficientes).

Certo é, por cada resposta obtida, haverá outros tantos problemas demasiado complexos, com demasiadas incertezas, ou mesmo problemas orientados por processos estocásticos, definidos por um padrão de variáveis e distribuição aleatórias⁶¹.

Dito isto, a Inteligência Artificial e a Inteligência Computacional compartilham o objetivo, a longo prazo, de se obter uma *Inteligência Artificial Forte (AGI)*, capaz de realizar com sucesso, qualquer tarefa intelectual proposta por um ser humano à máquina.

II. b. Ainda a utilidade da Lógica no desenvolvimento de uma inteligência computacional

Mais que tudo, pretende-se uma inteligência orientada pela lógica.

Deste modo, apela-se a que as técnicas implementadas por programadores, na construção ontológica das propriedades e atributos do sistema computacional, se rejam por proposições, definições, semânticas, inferências, linguagens e metalinguagens, intenções e intensões, extensões, subclasses de fórmulas e modelos.

Já por exemplo, para o desenvolvimento do software, a sintaxe e a semântica, respetivamente, a forma e o conteúdo dos produtos desenvolvidos devem partir de um raciocínio lógico, de que é possível inferir e traduzir informação explícita, para algoritmos computacionais, numa linguagem que faça sentido e que produza resultados.

⁶⁰ E um *soft-computing* que se traduz em aproximação dos resultados.

⁶¹ Podem ser analisadas estatisticamente, mas não podem ser previstas de modo preciso.

Temos ainda que, a simples comunicação entre sistemas computacionais concorrentes, o facto de estes poderem transmitir conhecimento entre si, sem crasharem, deve-se precisamente à coerência lógica que está presente na construção de cada um dos sistemas.

II. c. Os agentes de software

Gerhard Weiss⁶², em 1999, diz-nos que *“um agente é um sistema computacional (de software, hardware ou misto) que, estando situado num determinado ambiente, atua sobre este através de ações autónomas tendo em vista atingir um dado objetivo”*.

Para Maria Ganzha, Marcin Paprzycki e Mohamed Essaaidi⁶³, os agentes de software representam uma das mais excitantes áreas de pesquisa na Ciência Computacional:

“With the development of powerful personal devices, the vision of a personal agent now seems increasingly appealing too. It can even be claimed that intelligent software agents will eventually become an essential part of Web 4.0.

Software agents are finding their way into areas such as environmental security, climate change, seismic safety, epidemic prevention, detection and response, computer emergency response and human and societal dynamics”.

Mas o que são agentes de software?

Respondem Francisco Andrade, Paulo Novais, José Machado e José Neves⁶⁴ que agentes *“são entidades computacionais com um componente rico em conhecimento, tendo propriedades sofisticadas como de planeamento, reatividade, aprendizagem, socialização, comunicação, e a possibilidade de argumentação”*.

Com as seguintes características:

⁶² Professor de Inteligência Artificial e Ciência Computacional e Diretor do Departamento de Ciência Computacional e Engenharia do Conhecimento (DKE) na Universidade de Maastricht.

⁶³ GANZHA, Maria, PAPRZYCKI, Marcin, e ESSAAIDI, Mohamed, *Software Agents, Agent Systems and Their Applications*, in NATO Science for Peace and Security Series (Vol. 32), IOS Press, 2012.

⁶⁴ ANDRADE, Francisco C. P., NOVAIS, Paulo, MACHADO, José Manuel, NEVES, José, *Software Agents and Virtual Organizations: Consent and Trust*, Inderscience Publishers, 2010

- *Autonomia*: os agentes operam sem intervenção humana ou outros agentes, têm capacidade de tomada de decisão e sobre o seu estado de conhecimento interno;
- *Reatividade*: os agentes têm percepção do que ocorre no seu universo de discurso e respondem adequada e atempadamente a mudanças ocorridas nesse ambiente;
- *Proatividade*: os agentes são capazes de se antecipar a metas futuras, conduzindo as suas próprias ações, segundo um comportamento que é orientado pela concretização de objetivos;
- *Sociabilidade*: os agentes interatuam com outros agentes, comunicando, competindo ou cooperando com estes na resolução de problemas que, entretanto, lhes tenham sido colocados.

No mínimo, para podermos considerar um programa de software⁶⁵, um *agente de software*, este terá de apresentar estas características. A isto chamamos de *agente de software fraco*.

Já um *agente de software* ou mesmo um *sistema multiagente* é considerado forte se esta entidade for eminentemente cognitiva, passível de desenvolver a sua própria consciência, adaptativa, com um raciocínio que conjugue conhecimentos, intenções, objetivos, crenças, princípios e ainda desejos, proactivamente.

Por conseguinte, deve possuir os seguintes traços:

- *Mobilidade*: um agente diz-se móvel quando se movimenta através da rede, executando as tarefas de que foi incumbido e cumprindo objetivos;
- *Intencionalidade*: capacidade de definição de objetivos, tal como estratégias para os atingir;
- *Aprendizagem*: capacidade para adquirir conhecimento. Qualquer atualização do conhecimento guia-se pelos padrões de comportamento e preferências específicas do próprio agente;

⁶⁵ Ou ainda uma combinação software/hardware.

- *Competência*: capacidade para conduzir, com sucesso e eficiência, as tarefas incumbidas de realizar⁶⁶;
- *Veracidade*: um agente não fornece, pelo menos propositadamente, informação falsa;
- *Racionalidade*: um agente racional não aceita tarefas avaliadas como impossíveis de executar, contraditórias com os seus princípios, ou quando, de um ponto de vista lógico, não compensa em termos de risco, custo e esforço envolvido;
- *Benevolência*: desde que não entre em conflito com os seus objetivos atuais, um agente irá adotar como seus, os objetivos de terceiros – e assim, a ser impelido a realizar toda e qualquer tarefa que lhe seja imputada;
- *Emotividade*: cada vez mais se crê que certas características comportamentais, identificadas tipicamente num ser humano, se estão a tornar parte constituinte destes sistemas computacionais.

Por último, um agente de software que seja inteligente, pode servir para bem mais do que ser uma ferramenta de auxílio para especialistas da computação; ser pois, parte atuante na dinâmica humana e na sociedade.

II. d. O debate da personalidade jurídica dos agentes inteligentes

Perante agentes de software inteligentes, sensíveis para os objetivos de terceiros, que não executam tarefas contrárias aos seus princípios, nem que tarefas que não compensam em termos de risco-recompensa, será que devemos considerar dar-lhes a possibilidade de realizar negócios com autonomia, por si e para si sós?

Por outras palavras, as do artigo “*O debate sobre personalidade jurídica para robôs – errar é*

⁶⁶ Habitualmente, esta encontra-se relacionada com a confiança depositada no agente, por terceiros.

*humano, mas o que fazer quando também for robótico?”*⁶⁷, legalmente falando, poder ser-lhes atribuída personalidade legal e com isso, terem capacidade negocial, serem considerados aptos para, de sua própria vontade, negociarem, conscientes dos riscos e efeitos dos negócios em que encentem⁶⁸.

Começando por uma análise europeia, estas tendem a focar-se mais na questão da personalidade ligada à responsabilidade e reparação por danos, do que propriamente uma capacidade negocial dos mesmos: *“(importa mais) a construção de um mecanismo de reparação à vítima de danos do que como resultado de uma discussão mais aprofundada sobre o que é um robô inteligente e seu estatuto jurídico de forma mais abrangente”*.

E para estes casos de responsabilidade e reparação por danos de um agente inteligente, “a resolução do Parlamento Europeu chega então a mencionar duas iniciativas relacionadas ao desenvolvimento de robôs inteligentes:

- (i) *a adoção de um registro obrigatório desses robôs; e*
- (ii) *a criação de um seguro que possa então fazer frente às hipóteses de danos causados pelos mesmos”*⁶⁹.

Quanto à Lei portuguesa, a personalidade jurídica para pessoas singulares é atribuída pelo artigo 66 nº1 do Código Civil, que nos diz que esta *“se adquire no momento do nascimento completo e com vida”*.

Uma entidade computacional não tem um nascimento completo e com vida, é programada para existir. Ao que, esta disposição e por conseguinte, a personalidade jurídica não pode ser atribuída a um agente de software.

⁶⁷ SOUZA, Carlos, “O debate sobre personalidade jurídica para robôs”, Revista Jota, 10 de outubro de 2017, in <https://jota.info/artigos/o-debate-sobre-personalidade-juridica-para-robos-10102017>.

⁶⁸ É de referir que este artigo levanta o ponto sensível da recente alteração legislativa, quanto à posição dos animais para o Direito Civil português, atualmente “seres vivos dotados de sensibilidade”, tanto no Código Civil, como no Código Penal, e como tal, em posição distinta do que ditam as disposições referentes às coisas: se os *“animais foram destacados da categoria de bens para ocupar uma nova posição, o mesmo raciocínio poderia ser aplicado aos robôs inteligentes?”*

⁶⁹ *European Civil Law Rules in Robotics, STUDY for the JURI Committee, 2016 in* http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU%282016%29571379_EN.pdf.

Diga-se que a respeito da capacidade jurídica, que depende da personalidade jurídica, esta encontra-se prevista no artigo 67, *“ser sujeito de quaisquer relações jurídicas, salvo disposição em contrário”*.

Ainda na linha deste raciocínio, se individualmente, a estes agentes não pode ser atribuída personalidade jurídica, como será se estivermos a falar de corporações de agentes inteligentes. Provavelmente, assemelhar-se-ão legalmente a pessoas coletivas.

Veremos o que diz o Código Civil português, desta vez, o artigo 33⁷⁰:

“1. A pessoa coletiva tem como lei pessoal a lei do Estado onde se encontra situada a sede principal e efetiva da sua administração;

2. À lei pessoal compete especialmente regular: a capacidade da pessoa coletiva; a constituição, funcionamento e competência dos seus órgãos; os modos de aquisição e perda da qualidade de associado e os correspondentes direitos e deveres; a responsabilidade da pessoa coletiva, bem como a dos respetivos órgãos e membros, perante terceiros; a transformação, dissolução e extinção da pessoa coletiva”.

Perante estes dois pontos, para a lei portuguesa não é possível atribuir personalidade jurídica coletiva a uma entidade que não tem uma sede principal e efetiva, não tem nem depende de uma declaração de vontade no momento da sua criação, não depende de um ato constitutivo a ser registado, descrevendo os fins para os quais foi criado.

O seu ato constitutivo, quando muito, é programacional, incorporando exatamente as características ditas anteriormente, de mobilidade, intencionalidade, aprendizagem, competência, veracidade, racionalidade, benevolência, emotividade.

Não é uma organização com associados com direitos e deveres.

Não tem património para que se possa responsabilizar, perante os respetivos órgãos e membros, e mesmo terceiros⁷¹.

⁷⁰ Também do Código Civil Português.

⁷¹ Património mínimo, para responder por eventuais obrigações fiscais.

E por último, a sua parte física, se consistir também em hardware, e a sua estrutura lógico-programacional não são agrupáveis, para serem administradas em grupo.

Mas ainda que estas dificuldades fossem ultrapassadas, valeria a pena atribuir-lhes uma personalidade jurídica e uma capacidade jurídica legal?⁷²

Embora como vimos, não é de resposta fácil, mas tudo aponta para que à data presente não, dado que a nível de mercado internacional, é mais fácil vê-los como instrumentos ao serviço de corporações, para realizarem entre si *e-commerce* ou comércio online⁷³.

De qualquer modo, relembra-se que os dados que sejam tratados por agentes inteligentes, estarão protegidos legalmente, com repercussões legais em caso de fuga ou utilização danosa, ou quando atentem contra a imagem de alguém – conforme sugere o estudo do Parlamento Europeu, “*European Civil Law Rules in Robotics*”.

II. e. Redes neuronais artificiais

Na senda de inteligência computacional cada vez mais capaz e autónoma, introduzimos agora as *redes neuronais artificiais*.

Definem-se como “*modelos de aprendizagem poderosos com uma performance excelente para a resolução de problemas de reconhecimento de voz ou visuais*”.

Para tal, trabalham numa computação expressa como arbitrária, tecendo um raciocínio

⁷² ANDRADE, Francisco C.P., NEVES, José, NOVAIS, Paulo, MACHADO, José Manuel, Software agents as legal persons, in Virtual Enterprises and Collaborative Networks, Kluwer Academic Publishers, 2004.

⁷³ “An easier and less risky way for the agent to make contracts... and to limit the liability of the user (at least, to some extent) is available. This consists in creating companies for on-line trading, which would use agents in doing their business.

Such agents would act in the name of a company, their will would count as the will of the company, their legally relevant location would be the company's domicile, and creditors could sue the company for obligations contracted by those agents. The counterparties of an agent could then be warranted by the capital of the company and by the legal remedies available towards defaulting commercial companies” (Sartor, 2002).

But under this point of view, software agents are still seen as mere objects, belonging to corporate bodies instead of natural persons. In this view, the software agent is seen as a mere object the corporate body uses.” - ANDRADE, Francisco C. P., NOVAIS, Paulo, MACHADO, José Manuel, NEVES, José, Software Agents and Virtual Organizations: Consent and Trust, Inderscience Publishers, 2010.

lógico sobre os vários fatores que ligam as suas coordenadas⁷⁴. Devem esta sua performance, à densa interconexão de elementos computacionais, sendo aliás em muito, baseadas na compreensão humana acerca dos sistemas nervosos biológicos.

Posto isto, qualquer resultado que produzam, é sempre de interpretação variável.

Mas é uma análise que se debruça sobre unidades individuais, ao explorar em simultâneo as muitas hipóteses em competição (recorrendo a redes massivas em paralelo, compostas de variados elementos computacionais, conectadas por links e com pesos variáveis)⁷⁵.

Podemos então dizer que uma rede neuronal consegue estabelecer, através de várias tentativas e compilação e remoção de dados, qual o caminho-ótimo para se obter o parâmetro que se quer encontrar⁷⁶.

Deste modo, permitem não só esclarecer *a-posteriori*, quaisquer decisões de classificação feitas por um modelo de análise, como ainda identificar os dados que, na computação, levaram à classificação correta de um dado impulso ou estímulo.

Para simplificar, as *redes neuronais artificiais* podem supervisionar e seleccionar dados de um conjunto que, à primeira vista, pareça ser aleatório. E ainda conectar itens às respetivas características ou propriedades, primeiro numa fase de pesquisa e depois, no agrupamento de um arquivo ou uma base de dados⁷⁷.

Pelo exposto, podemos dizer que as *redes neuronais artificiais* vão para além dos *agentes inteligentes*. Se os agentes precisam de mobilidade, intencionalidade, aprendizagem, competência, veracidade, racionalidade, benevolência e emotividade, já as redes neuronais partir destas

⁷⁴ Conforme SZEGEDY, Christian, ZAREMBA, Wojciech, SUTSKEVER, Ilya, BRUNA, Joan, ERHAN, Dumitru, GOODFELLOW, Ian, FERGUS, Rob, Intriguing properties of neural networks, International Conference on Learning Representations, 2014.

⁷⁵ Richard P. Lippman, "An Introduction to Computing With Neural Nets", IEEE Signal Processing Magazine, 4(2), 1987.

⁷⁶ O modelo computacional de qualquer rede neuronal está programado para que, na inspeção de unidades individuais, se faça a assunção que as unidades da última camada formam uma base distinta. Base esta que é tida como "particularmente útil" para a extração da informação semântica.

⁷⁷ Pelo que, a título de exemplo, certamente com utilidade para as forças policiais na deteção de algum carro roubado ou se existe alguma fotografia na base de dados policial, que corresponda à pessoa de interesse, o detentor de informações pertinentes para a investigação.

caraterísticas, para alcançar verdadeira reatividade, proatividade e mesmo autonomia no desempenho.

Autonomia esta, ligada à sua capacidade de aprendizagem e adaptação – essencial em áreas como o reconhecimento da fala, onde novos falantes, novas palavras, novos dialetos, novas frases e novos ambientes estão constantemente a ser explorados.

Primam pois, pela sua capacidade de otimizar sistemas, através dos dados que processam.

Ao que, conforme veremos, podemos e devemos, finalmente, falar de uma *computação avançada inteligente*, aplicando termos como *Machine Learning*, ou mesmo *Deep Learning*.

II. f. Aprendizagem e otimização inteligente de sistemas

Pondo de lado a temática anteriormente explorada, que conclui que, atualmente, não podemos autonomizar um agente inteligente para a realização de negócios jurídicos, dependendo pois de um agente humano, passemos agora à análise de como se concretiza esta *computação avançada inteligente*.

Alertamos para o facto de, se pretendemos que toda e qualquer análise se mantenha fiel às últimas inovações no mercado de sistemas computacionais, esta, em última instância, terá de se basear nos usos possíveis de agentes inteligentes e de redes neuronais artificiais, conforme anteriormente referido.

No uso de software para potenciar a aprendizagem de um sistema, enquanto subconjunto da *Inteligência Artificial*, o *Machine Learning* identifica a prática de utilizar algoritmos para obter dados e aprender com estes; relacionada com a estatística computacional, constrói modelos através dessas amostras de dados, que lhe ensinam como aprender a executar determinada tarefa.

Deste modo, ao invés de se ter de programar parâmetros, como as instruções específicas das tarefas a realizar, ou mesmo que ligações estabelecer; falamos de, numa forma dinâmica e inteligente, manipular uma quantidade grande de dados e com estes, compor modelos de algoritmos que permitem um sistema aprender, por si só: a fazer previsões ou a tomar decisões.

Conforme dissemos, as redes neuronais artificiais otimizam sistemas, por meio do

isolamento de algoritmos que permitam identificar o caminho-ótimo para o objetivo determinado.

Eis, pois que, com o tempo e o isolamento de algoritmos de aprendizagem certos, podemos recorrer a uma variedade de técnicas para implementar o *Machine Learning*, que encontram o seu suporte nas redes neuronais artificiais, nas suas camadas discretas, conexões e direções de propagação de dados: falamos de *Deep Learning*.

Nestas, procura-se imitar a capacidade de aprendizagem humana, tipicamente recorrendo a múltiplas camadas de redes neuronais, que traduzem conceitos abstratos altamente complexos, reconhecem padrões e compreendem conceitos⁷⁸. Veremos casos concretos, atuais.

Diz-nos Karla Lant, para a revista digital Futurism, que a máquina Google de *Machine Learning* aprendeu a auto-replicar-se⁷⁹.

Por definição, a auto-replicação identifica qualquer comportamento de um sistema dinâmico, que resulta na construção de uma cópia idêntica desse sistema.

Partindo do conceito de divisão celular, aplicada às redes neuronais artificiais, este projeto da Google, *Google AutoML*, pretende que uma rede neuronal “A” componha um modelo-protótipo de arquitetura, de uma rede neuronal “B”. Deste modelo resultará um feedback, que isola certos algoritmos, os que apontam o caminho-ótimo para o objetivo determinado.

Portanto, este novo modelo de arquitetura deverá passar por um processo de seleção, onde seja treinado e avaliado, quanto ao seu potencial para a realização de um objetivo⁸⁰.

Conforme as conclusões dessa avaliação, será extraído feedback: isolamento de algoritmos.

E de seguida, num processo que repete a ideia da primeira fase, mas parte da arquitetura “B”, serão geradas novas arquiteturas, desta vez para uma rede neuronal “C”.

⁷⁸ “Deep learning allows a program not only to recognize objects in real time but to understand speech. Current applications include medical diagnosis, robotics and engineering, automotive safety, and speech and text recognition, but has a lot of other potential uses.” - https://futurism.com/?post_type=glossary&p=53163?post_type=glossary&p=53163.

⁷⁹ LANT, Karla, “Google’s Machine Learning Software Has Learned to Replicate Itself”, Futurism, outubro 2017 in <https://futurism.com/googles-machine-learning-software-has-learned-to-replicate-itself/>.

⁸⁰ LE, Quoc, e ZOPH, Barret, “Using machine learning to explore”, Google Brain team, maio 2017 in <https://research.googleblog.com/2017/05/using-machine-learning-to-explore.html>.

Mais uma vez estas arquiteturas passarão por um processo de teste, onde no fim, cedem feedback para que o controlador extraia dados, e em si, algoritmos úteis. Repete-se o processo.

Falávamos de *Deep Learning*: o que este projeto provou, foi que esta é uma técnica que, na prática, derrota o elemento humano na construção de software de *Machine Learning*, pois é comprovadamente mais eficiente e mais poderoso que os sistemas construídos pelo ser humano.

E dois, mostrou que é uma técnica que alcança os objetivos traçados, o seu feedback não é aleatório.

Ao que lhe resta ser aperfeiçoada, ao ponto que o seu funcionamento seja acessível, porque facilitado, a programadores independentes, externos aos laboratórios de computação Google.

Vimos uma técnica de *Deep Learning* que recorre à auto-replicação de arquiteturas de redes neuronais. Nesta, uma das fases essenciais, é a de treino das redes.

É pois, algo que atualmente demora vários dias, que depende dos recursos computacionais dos centros de dados. Pelo que, um outro ponto de vista debruça-se sobre como acelerar, significativamente, o treino destas redes neuronais artificiais, por meio de processadores que consigam reduzir o tempo de computação.

Chamamos então à atenção para o estudo de Tayfun Gokmen e de Yurii Vlasov, quanto à aceleração do treino de redes neuronais artificiais, por meio de unidades de processamento resistentes⁸¹, vulgo *RPU*.

Tratam-se pois, de uns chips que combinam a *CPU* com uma memória não-volátil⁸², para que, conforme o estudo, as redes neuronais artificiais que corram nos mesmos, obtenham novos dados ao mesmo tempo que processam os já obtidos, assim diminuindo o tempo de processamento e identificação de algoritmos.

⁸¹ GOKMEN, Tayfun, e VLASOV, Yurii, “Acceleration of Deep Neural Network Training with Resistive Cross-Point Devices”, 2006. In <https://arxiv.org/ftp/arxiv/papers/1603/1603.07341.pdf>.

⁸² Isto é, incorporando memória RAM resistente, diretamente num CPU.

A respeito desta técnica, a Intel prepara-se para lançar no mercado um novo microprocessador, destinado a correr redes neuronais artificiais melhor que os chips atuais: o *Nervana*⁸³, “com alta performance”⁸⁴ e “revolucionando a Inteligência Artificial numa miríade de indústrias”⁸⁵, desde os cuidados de saúde, ao sector automóvel, meteorologia, redes sociais, entre outras.

Perante estas técnicas de *Deep Learning*, que concretizam a aprendizagem e otimização de sistemas computacionais, principalmente recorrendo às redes neuronais artificiais, pensamos que esta capacidade pode e deve ser aplicada às tecnologias biométricas de obtenção, tal como tratamento, dos dados dos utilizadores. Servindo para seleccionar os dados úteis que permitam uma otimização do software, e em alguns casos, hardware, das tecnologias biométricas.

Não esquecendo claro, o que dissemos antes quanto aos perigos do *homo conectus*, os perigos de criar e dar acesso a perfis de utilizador, indiscriminadamente.

II. g. As tecnologias biométricas

Conforme dissemos antes, e agora relembando, as tecnologias biométricas referem-se a sistemas, técnicas e dispositivos que medem e analisam os atributos físicos e comportamentais das pessoas, como características faciais, padrões de voz, impressões digitais, leituras biométricas da palma da mão, padrões de veias e artérias, estrutura de órgãos, como o olho, íris ou retina, ou ainda mesmo a postura, a forma de andar, ou mesmo a forma de assinar⁸⁶.

Destas, este trabalho debruça-se sobre a utilização de próteses e implantes, pelo que, seguindo essa linha de raciocínio, a melhor forma de introduzir estas tecnologias biométricas, será

⁸³ Projeto Nervana em <https://www.intelnervana.com/intel-nervana-neural-network-processors-nnp-redefine-ai-silicon/>.

⁸⁴ Conforme as especificações em <https://www.intelnervana.com/nervana-engine-delivers-deep-learning-at-ludicrous-speed/>.

⁸⁵ Transcrevendo as palavras do CEO da Intel, Brian Krzanich, a respeito do Nervana.

⁸⁶ Mais uma vez, conforme ANDRADE, Francisco C. P., MOREIRA, Teresa, *Biometrics and Data Protection: These Data are Derived from an Individual*, in *Interdisciplinary Perspectives on Contemporary Conflict Resolution* (ccord. Paulo Novais e Davide Carneiro), IGI Global, 2016, e ainda O'CONNOR, Sean, *Collected, tagged, and archived: legal issues in the burgeoning use of biometrics for personal identification*, Stanford Technology Law Review, 1998.

começando pela sua distinção.

Temos pois que, os implantes são dispositivos ou tecidos que se inserem quer na superfície, quer internamente, num organismo vivo, habitualmente um ser humano. Se no grupo maior dos implantes, a utilização a ser feita do mesmo, é a de substituição de um membro, passamos a identificar esse implante como prótese.

Assim, no conjunto das tecnologias biométricas, o grupo dos implantes entrega medicação, monitoriza funções corporais, ou suporta órgãos e tecidos – tipicamente, sendo este último, o propósito associado às próteses.

Destes três propósitos, pensamos que o mais importante a considerar, dada a temática de proteção de dados, será o de monitorização das funções corporais, onde haverá a obtenção, e se se criar condições de armazenamento, um possível tratamento de dados sensíveis dos utilizadores.

A respeito disto, utilizaremos as palavras de Isaac Perry Clements⁸⁷ para ilustrar os últimos avanços tecnológicos:

Primeiro, “uma forma mais avançada de controlar uma prótese é ouvindo os músculos restantes no membro residual que o paciente possa contrair. Porque os músculos geram pequenos sinais elétricos quando contraem, elétrodos posicionados na superfície da pele podem medir movimentos do músculo. Próteses que funcionem deste modo são chamadas mioelétricas”.

Segundo, “se os elétrodos podem sentir a eletricidade causada por contrações musculares, porque é que não podem aceder à própria fonte da informação, medir os sinais elétricos transportados pelos nervos, ou mesmo o cérebro? A resposta é que podem, mas medir a partir do cérebro e nervos é muito mais complicado por várias razões. Por exemplo, os sinais elétricos no cérebro e nos nervos são muito pequenos e difíceis de aceder”.

E terceiro, “como exemplo de uma tecnologia de interface neuronal, os cientistas podem implantar elétrodos de tamanho micrométrico no cérebro, para ouvirem a atividade cerebral. Quando o paciente tenta mentalmente mover o seu membro amputado, os microelétrodos podem

⁸⁷ Conforme escreve Isaac Perry Clements em <http://science.howstuffworks.com/prosthetic-limb4.htm> e em <http://science.howstuffworks.com/prosthetic-limb5.htm>.

interceptar sinais do comando motor gerados no cérebro, e esses sinais podem então ser utilizados para controlar uma prótese”.

Como vimos, o pensamento inovador a respeito dos implantes e próteses tende cada vez mais para a ideia de progresso suportado pela leitura de comandos/impulsos humanos⁸⁸, i.e., pela obtenção e tratamento dos dados de saúde de um paciente.

Leitura esta, realizada por microelétrodos ou mesmo outro tipo de sensores, que podem estar presentes nos respetivos implantes, ou como vimos, diretamente ligados ao cérebro do utilizador.

E um tratamento de dados que se baseie nas mais recentes tecnologias de análises de dados, como por exemplo, um *deep learning* por meio de redes neuronais artificiais.

Dando agora destaque aos sensores de implantes, à leitura de dados, na prática, que tipo de respostas pode a inteligência computacional dar a estas tecnologias?

Bem, o tratamento legal de dados de um utilizador pode levar ao melhoramento do *firmware* das tecnologias biométricas. Relembrando, o software funcional do sistema de uma tecnologia é o seu firmware. Este atua diretamente no *hardware*, e sem o qual o implante seria completamente não-funcional.

Podemos pois, falar numa espécie de mutualismo, ou talvez simbiose, se falarmos de tecnologias biométricas para os quais o seu funcionamento é indispensável para o bem-estar do utilizador. Como o caso de um pacemaker.

Pelo que, quanto maior for a fiabilidade dos dados lidos pelos sensores, a certeza de que se tratam, precisamente, dos valores dos impulsos e estímulos produzidos pelo corpo do utilizador, melhor desempenho poderão ter os implantes e nisto, as próteses ligadas ao corpo do utilizador.

Passando então à parte prática a respeito do tratamento de dados sensíveis do utilizador, e chamando para o que foi analisado até ao momento, poderíamos pegar nestes dados – primeiro recolhidos pelos sensores –, e de seguida, organizados metodicamente, por meio de *agentes de*

⁸⁸ Criados no cérebro e transmitidos por meio de sinapses, e de seguida, pelo sistema nervoso ao longo do corpo humano.

*software inteligentes*⁸⁹.

Depois, com o envio para laboratório destes, perante o tratamento destes dados obtidos e a comparação com análises independentes⁹⁰, poder-se-ia perceber o que é que, internamente, na forma como estava programado o *firmware* dos implantes, provocava essa discrepância entre valores⁹¹.

Isto é, poder-se-ia utilizar redes neuronais artificiais para perceber qual o caminho-ótimo a seguir, ao procurar-se obter uma equivalência, na leitura dos valores lidos. E usá-lo para programar o mais adequadamente possível, as tecnologias biométricas.

Contudo, conforme os últimos avanços tecnológicos que vimos antes, nas potencialidades das *RPU (Unidades de Processamento Resistente)*⁹² que se preparam para entrar no mercado, já deixa de fazer sentido uma otimização das tecnologias biométricas nestes moldes.

Mais que o novo microprocessador da Intel, *Nervana*, é capaz de “*correr redes neuronais artificiais melhor que os chips de computador atuais*”.

Assim, na verdade, podemos já pensar em incorporar as redes neuronais artificiais, num futuro próximo, nas próprias tecnologias biométricas, e pelos dados recolhidos e seus algoritmos, estas tratam de realizar a sua otimização, consoante os dados dos valores recolhidos do utilizador.

Pois que, recebendo programação comportamental e objetivos a cumprir, como o calcular um caminho dentro do implante que seja mais eficiente, por exemplo, reduzindo um atraso no comando dado, permitem melhorar o *firmware* que controle as tecnologias biométricas.

Definida uma atualização, esta deverá ser sempre monitorizada pela empresa produtora,

⁸⁹ Recorrendo a EDI ou Intercâmbio Electrónico de Dados, através de uma rede de dado qualquer. Conforme nos diz REED, Chris, EDI – contractual and liability issues, Computer Law and Practice (6), 1990.

⁹⁰ Cujos valores não provenham das tecnologias biométricas.

⁹¹ Como por exemplo, a existência de *delays* no tempo em que a ordem é dada no cérebro, transmitida, e recebida no ponto do sensor – e a intenção de diminuí-los.

⁹² Relembrando, chips que combinam CPU com uma memória não-volátil, para que consigam obter dados ao mesmo tempo que processam os já obtidos, assim diminuindo o tempo de processamento.

para evitar erros grosseiros⁹³.

Por fim, é de destacar o benefício para o utilizador, com a redução de custos, não necessitando de comprar modelos novos das tecnologias biométricas.

II. h. Avanços tecnológicos no mercado dos implantes e próteses

Conforme vimos anteriormente, deve fazer parte dos procedimentos de empresas de tecnologias especializadas, e que lidem com dados sensíveis, uma monitorização contínua, para que se previna fugas de dados, ou tratamentos de dados contrários não só a princípios ético-morais, como ao próprio consentimento dado pelo utilizador.

Quais as empresas de tecnologia que, lidando com as tecnologias biométricas, são pertinentes para o nosso trabalho: é o que veremos de seguida.

Primeiro que tudo, a noção da otimização das tecnologias biométricas ter como base a recolha e tratamento de dados, deriva dos resultados positivos, nos testes laboratoriais do Johns Hopkins University Applied Physics Laboratory (APL).

Neste laboratório, em 2014, um homem tornou-se o primeiro humano com ambos os braços amputados, a poder controlar por meio de implantes, dois dos membros prostéticos modulares do laboratório.

Comprovada a ideia, foi lançado em 2006, o programa autónomo da *Agência de Projetos de Pesquisa Avançada de Defesa* norte-americana⁹⁴, “*Revolutionizing Prosthetics*” (MPL)⁹⁵.

O que, desde então e até ao presente, o programa desenvolveu implantes e próteses cada vez mais complexas, incluído uns protótipos antropomórficos, avançados, modulares de próteses

⁹³ Tudo o que vimos antes confirma que a nível de cálculo e exploração do potencial de uma tecnologia, as redes neuronais artificiais são vastamente mais eficientes e eficazes que um ser humano.

⁹⁴ Defense Advanced Research Projects Agency ou D.A.R.P.A., trata-se de uma agência que pertence ao Departamento de Defesa norte-americano.

⁹⁵ Conforme informações constantes no artigo informacional presente em <http://www.darpa.mil/program/revolutionizing-prosthetics>.

de braços⁹⁶.

Posto isto, temos a mão biônica multiarticulada e mioelétrica da empresa *Bebionic*⁹⁷ que lidera o mercado de próteses.

É ainda de referir, também pelo seu peso substancial no mercado das próteses, e pela sua missão, enquanto organização não lucrativa, dedicada a disponibilizar a crianças que deles necessitem, próteses imprimidas a 3D, a preços acessíveis, a Limbitless Solutions⁹⁸.

Num conjunto extenso de vários programas e start-ups, uma das start-ups mais interessantes é sem dúvida, a *Open Bionics*, fundada em 2014 no Reino Unido, procurando também desenvolver próteses a baixo custo, operando a partir do Laboratório de Robótica de Bristol⁹⁹.

Dizemos interessante, porque além do mais já recebeu vários prémios na área da Engenharia e Inovação, reconhecendo não só a sua qualidade, mas também dedicação ao fim.

Pois que vários dos seus protótipos têm uma licença de utilização aberta¹⁰⁰, sendo política desta start-up, o encorajar outros engenheiros e desenvolvedores a contribuir para o desenvolvimento das próteses, juntando-se em comunidade.

Além destes programas, a título individual, um jovem inventor de nome Easton LaChappelle tem trabalhado incansavelmente para poder disponibilizar próteses acessíveis e de alta qualidade¹⁰¹ a quem precise das mesmas.

Falamos de impressão a 3D de dedos, palmas, antebraços, cotovelos, bíceps, ombros, a

⁹⁶ Incluindo fazer ligação da prótese ao ombro, da mesma forma que naturalmente a cabeça do úmero se liga à escápula (denominado socket no artigo).

⁹⁷ Uma mão mioelétrica que usa sinais elétricos para contrair, voluntariamente, os músculos residuais na superfície da pele onde assenta a prótese. Em http://bebionic.com/the_hand.

⁹⁸ O website principal desta empresa encontra-se disponível para consulta em <https://limbitless-solutions.org/>.

⁹⁹ O maior laboratório na Europa, de pesquisa na área da Robótica.

¹⁰⁰ O firmware de utilização está disponível, sem qualquer restrição monetária ou legal, para acesso livre, em <https://github.com/Open-Bionics>. Para explicação da importância de uma licença de utilização aberta, remetemos para S. Sonnenburg, et al., *The Need for Open Source Software in Machine Learning*, in *Journal of Machine Learning Research*, 2007.

¹⁰¹ O website principal desta empresa encontra-se disponível para consulta em <http://www.unlimitedtomorrow.com/>.

mesmo o próprio pulso e articulações, permitindo criar um braço robótico completo de 2 kg¹⁰².

Quanto a outros exemplos, para melhor compreensão, relembremos que um pacemaker faz parte das tecnologias biométricas, do mesmo modo que, a título de exemplo, um implante que sirva para medir a glucose de diabéticos.

Assim, a respeito de um implante desta natureza, este trata-se de um CGM, ou um monitorizador de glucose contínua, um dispositivo subcutâneo normalmente recomendado a diabéticos tipo 1 e 2, que permite testar os níveis de glucose (a quantidade de açúcar) no sangue e enviar os resultados em tempo real, através do website da empresa produtora do CGM¹⁰³.

Podemos ainda dar o exemplo de uma luva, semelhante a um exoesqueleto, que dá uma resposta a quem sofra de paralisia nas mãos, permitindo essa pessoa agarrar e apertar objetos.

E nisto, referimo-nos a um projeto sul-coreano, *Exo-Glove Poly*, uma luva robótica de três dedos¹⁰⁴ feita de polímeros, flexível, elástica, e com excelente durabilidade, cujo motor funciona controlado por um interruptor, que puxa as ligações internas para abrirem ou fecharem a luva¹⁰⁵.

Concluimos pois que, todas as tecnologias biométricas que surjam acabam por beneficiar, se as otimizações e atualizações que recebam, a respeito do seu software funcional, permitam uma maior precisão na receção de estímulos ou monitorização dos valores do utilizador-paciente.

Pelo que, sem mais demoras, passamos ao tema da proteção dos dados pessoais do utilizador, para que a utilização responsável das tecnologias biométricas, não dependa da boa vontade das equipas e laboratórios que as projetam.

¹⁰² Os componentes deste braço mecânico encontram-se descritos, detalhadamente e com instruções de montagem no seguinte website <http://theroboarm.com/overview.html>. Do seu uso prático, depende da atribuição do devido crédito/referência ao criador, em termos razoáveis. O material não pode ser utilizado para fins comerciais, de modo a que não se subverta o objetivo do projeto – uma comunidade aberta que permite um impacto positivo a qualquer um; qualquer um com o direito de utilizar as capacidades desta tecnologia.

¹⁰³ ROBINSON, Melia, “*San Francisco biohackers are wearing implants made for diabetes in the pursuit of ‘human enhancement’*”, Tech Insider, janeiro de 2017, in <http://www.businessinsider.com/san-francisco-biohacking-continuous-glucose-monitors-2017-1>.

¹⁰⁴ Polegar, indicador e médio.

¹⁰⁵ Desenvolvido pelo *SNU Biorobotics Lab*, conforme projeto descrito no website <https://atlasofthefuture.org/project/exo-glove-poly/>.

III. Proteção Dos Dados Pessoais Do Utilizador

“Hoje em dia, o uso generalizado da Internet e dos telemóveis levou a um alastramento das aplicações biométricas, e a pesquisa sobre os dados biométricos tem sido drasticamente expandida para novos domínios.

As tendências de pesquisa nas tecnologias biométricas podem ser categorizadas em três direções. A primeira direção é a Internet mais generalizada e as aplicações portáteis. Isto arrasta consigo um número de novos tópicos nos quais utilizar dados biométricos, como aplicações bancárias, serviços de saúde, arquivos médicos, ciber-segurança, e privacidade enquanto serviço, etc. Estas novas aplicações estão a criar um gigantesco mercado, de milhares de milhões de dólares, para as tecnologias biométricas e as necessidades da indústria redobram o esforço, para que se faça avançar a pesquisa ainda mais longe e vigorosamente.

A segunda direção leva-nos para o desenvolvimento algorítmico, que inclui a investigação de muitas novas técnicas de IA nas tecnologias biométricas, tais como a lógica difusa, MCS, e ainda o deep learning. Estas novas abordagens podem frequentemente melhorar a precisão do reconhecimento automatizado, levando à disponibilidade de muitas outras novas aplicações, para que entrem no mercado. Especialmente, com a vasta quantidade de dados provenientes de milhares de milhões de utilizadores ligados a serviços de Internet/aplicações portáteis, a biométrica torna-se um desafio da Big Data, com as partilhas em rede, o processamento, classificação e armazenamento de dados.

A terceira direção de pesquisa visa descobrir mais tipos de dados biométricos, para os mais variados usos. Para além da impressão digital e as assinaturas, por convencionais, falamos de outros tipos de dados biométricos (como a iris, o padrão das veias, a forma de andar, ou padrões de toque/teclado), a serem explorados nas mais recentes investigações biométricas. A sua combinação, enquanto Biométrica Multimodal¹⁰⁶, é uma outra forma, popular, de explorar e abusar

¹⁰⁶ Diz-nos o Grupo de Trabalho do artigo 29, na Opinião 3/2012, que Biométrica Multimodal “pode ser definida como a combinação de diferentes tecnologias biométricas, para melhorar a precisão ou a performance do sistema”.

destes tipos de dados biométricos, justificando-se com a investigação."¹⁰⁷

Com esta introdução, pretendemos sublinhar a ideia de que é premente que o avanço tecnológico acompanhe o legal, para que, conforme já várias vezes fizemos ver, não haja abuso dos dados do utilizador, dados esses sensíveis, no acesso, tratamento e utilizações maliciosas¹⁰⁸.

Devemos pois, ter em mente que o acesso não autorizado a dados pessoais pode vir de quem se lide com estes diariamente, seja em relações pessoais como profissionais, pelo acesso e leitura de comunicações pessoais.

Pois que, numa decisão do Tribunal Europeu dos Direitos do Homem, concluiu-se que o acesso não autorizado aos dados pessoais de um trabalhador, não constituía violação do seu direito à reserva da vida privada¹⁰⁹.

Referimo-nos portanto, ao processo de Bărbulescu contra a Roménia (Queixa n.º 61496/08), onde se concluiu que não houve falta de equilíbrio, entre o direito do trabalhador à reserva da vida privada e os interesses da entidade empregadora em monitorizar¹¹⁰.

III. a. O Regulamento Geral de Proteção de Dados e o Grupo de Trabalho do Artigo 29

Conforme referimos, de passagem, no subcapítulo a respeito do *homo conectus* moderno e os seus perigos, o Regulamento Geral de Proteção de Dados¹¹¹ é diretamente aplicável na ordem jurídica portuguesa¹¹², e é relativo à proteção das pessoas singulares no que diz respeito ao

¹⁰⁷ Conforme prefácio introdutório da obra de Richard Jiang, Somaya Al-maadeed, Ahmed Bouridane, Danny Crookes e Azeddine Beghdadi, *"Biometric Security and Privacy – Opportunities & Challenges In The Big Data Era"*, Springer, 2017.

¹⁰⁸ Exemplifica o Acórdão do STJ n.º 712/12.6TTPRT.P1.S1 de 03-12-2014, que consubstanciou assédio moral por impedimento de acesso a dados privados e que formavam prova.

¹⁰⁹ Artigo 8º da CEDH, Convenção Europeia dos Direitos do Homem.

¹¹⁰ É um acórdão que causa perplexidade entre nós, até porque é opinião e assim jurisprudência corrente nos tribunais portugueses, limitar ao máximo o controlo informático exercido pelo empregador sobre os seus trabalhadores – visto como uma ação ilegítima. Vide, a título exemplificativo, os Ac. da RL de 10/12/1991, Col. Jur., 1991, 5.º-151, e de 05/06/2008, Proc. n.º 2970/2008.4, www.dgsi.pt, e o Ac. do STJ de 05/07/2007, Proc. n.º 07S043, www.dgsi.pt.

¹¹¹ REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

¹¹² Tal como nos restantes Estados-Membros da União Europeia.

tratamento de dados pessoais e à livre circulação desses dados.

Conforme o seu artigo 99º, nº1 e nº2, entrou em vigor a partir de 25 de maio de 2019, 20 dias após a sua publicação no *Jornal Oficial da União Europeia*.

Assim que iremos, com base neste¹¹³, explicar em que termos, num contexto não só português mas europeu, se realiza a proteção de dados pessoais dos utilizadores.

Devemos ainda referir o Grupo de Proteção de Dados do artigo 29¹¹⁴, um grupo¹¹⁵ com carácter consultivo e independente, incumbido de, entre outras tarefas:

- dar parecer à Comissão sobre o nível de proteção na Comunidade e nos países terceiros;
- sobre os códigos de conduta elaborados a nível comunitário;
- e ainda, aconselhar a Comissão sobre quaisquer projetos de medidas adicionais ou específicas a tomar;
- para proteger os direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como sobre quaisquer outros projetos de medidas comunitárias com incidência sobre esses direitos e liberdades.

Num mundo cada vez mais voltado para a eletrónica, a proteção adequada dos dados biométricos é importantíssima.

Primeiro que tudo, o Regulamento Geral de Proteção de Dados diz-nos que dados pessoais são a *“informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente,*

¹¹³ E ainda, seguindo a orientação e abordagem a esta temática, do artigo de Pedro Freitas, Teresa Coelho Moreira e Francisco Andrade: *“Data Protection and Biometric Data: European Union Legislation”* in *Biometric Security and Privacy – Opportunities & Challenges In The Big Data Era*, Springer, 2017.

¹¹⁴ Criado pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

¹¹⁵ Composto por um representante da autoridade (ou autoridades de controlo) designadas por cada Estado-membro, por um representante da autoridade (ou autoridades) criadas para as instituições e organismos comunitários, bem como por um representante da Comissão – artigo 29º nº1 e 2.

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”.

E segundo, o RGPD define dados biométricos no seu artigo 4º nº14, *“dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais¹¹⁶ de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos”.*

Chamamos à atenção para o Considerando 51, *“merecem proteção específica os dados especiais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais”.*

E ainda, e novamente, o artigo 9º nº1, *“é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa”.*

Por conseguinte, entendemos que alguns dos dados biométricos inserem-se legalmente, e com a proteção que lhes está estipulada, na categoria de dados sensíveis.

Pois que esta visão se alinha precisamente com a do Grupo de Proteção de Dados do artigo 29, na sua Opinião de 3/2012¹¹⁷, quanto ao desenvolvimento de tecnologias biométricas, ponto 3.8., em que *“alguns dados biométricos poderão ser sensíveis nos termos do artigo 8 da Diretiva 95/46/CE e em particular, dados que revelem origens étnicas ou raciais, ou dados de saúde”.*

¹¹⁶ Acentuamos a ideia de que estes dados pessoais tanto se referem a dados biométricos fisiológicos, como quaisquer dados biométricos de personalidade. Como artigo de referência, MOREIRA, Teresa C., A proteção de dados pessoais dos trabalhadores e a utilização de tecnologias de identificação por radiofrequência, in *Memórias do XVI Congresso Ibero Americano de Derecho e Informática*, Quito, 2012.

¹¹⁷ E adotada a 27 de abril de 2013.

E pois que, novamente, conforme é opinião do Grupo de Proteção de Dados do artigo 29, define-se como sistemas biométricos, as *“aplicações que usam tecnologias biométricas, que permitem a identificação automática e/ou autenticação/verificação de uma pessoa (...), habitualmente usadas para as mais variadas tarefas, nas mais diferentes áreas, para diferentes propósitos e sob a responsabilidade alargada de diferentes entidades”*.

Voltando agora ao Regulamento Geral de Proteção de Dados, o que vimos antes implica que, de um modo geral, processar dados biométricos é proibido, se não seguir os termos do artigo 9º nº2, onde:

- em a), é dado o consentimento explícito para o tratamento desses dados, com finalidades específicas;
- em b), se o tratamento for necessário para cumprir obrigações, ou exercer direitos específicos do responsável pelo tratamento ou do titular dos dados, em matéria de legislação laboral, segurança social, ou proteção social;
- em c), se o utilizador estiver fisicamente ou legalmente impedido de dar o consentimento, e houver a necessidade para proteção dos seus interesses vitais;
- em d), falamos de dados que respeitem a membros de uma entidade legal, uma fundação, associação, ou outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e esses dados não podem ser partilhados fora do círculo dessa entidade;
- em e), se o tratamento incide sobre dados que sejam manifestamente públicos, pelas mãos do titular dos mesmos;
- em f), se os dados forem necessários para o exercício de um direito judicial;
- em g), se houver motivos de interesse público atendíveis;
- em h), se for com o propósito de medicina preventiva ou do trabalho, para que se avalie a capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou serviços e sistemas de ação social;

- em i), por motivos de saúde pública;
- por fim para j), para fins de interesse público no contexto de investigação científica ou histórica ou para fins estatísticos.

Excetuando estes casos restritos e específicos, não pode ser feito o tratamento de dados biométricos do utilizador.

Tratamento de dados esse, que está sujeito à autoridade de um *responsável pelo tratamento*, que nos termos do artigo 4º nº 7 do RGPD, é “a *pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais*”.

Sendo que o responsável pelo tratamento de dados tem de poder demonstrar que o titular de dados deu o consentimento para o tratamento destes.

Assim, quanto ao consentimento, o artigo 4º nº 11 do RGPD diz-nos que passa por “*uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*”.

Se o consentimento pede uma manifestação de vontade informada e explícita, que liga os dados, à finalidade do tratamento dos mesmos, este propósito também vincula o responsável pelo tratamento de dados. Pois que, no desempenho da sua função, tem de avaliar até da própria natureza dos dados recolhidos, e surgindo uma incompatibilidade entre os dados e o fim, tem de parar com o tratamento dos dados recolhidos.

Seguindo o artigo 24º do RGPD, que define a responsabilidade do responsável pelo tratamento de dados, nº1, “*tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas*

e atualizadas consoante as necessidades”.

E a isto também alude o ponto 3 do Grupo de Proteção de Dados do artigo 29, novamente na sua Opinião de 3/2012, onde é da opinião que, na análise legal, a respeito da proporcionalidade quanto ao uso feito dos dados biométricos, *“o responsável pelo tratamento, tem de se o processamento e os seus mecanismos, as categorias de dados a serem recolhidas e processadas e a transferência da informação contida na base de dados são necessários e indispensáveis. As medidas de segurança têm de ser adequadas e efetivas. O responsável pelo tratamento tem de considerar os direitos a serem concedidos aos indivíduos aos quais os dados pessoais se referem, e assegurar que um mecanismo adequado para o exercício desses direitos é incorporado nessa aplicação”.*

Perante isto, a proteção dos dados é desde a conceção e por defeito, conforme o artigo 25º do RGPD, nº1, *“tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares”.*

Sendo que estas medidas, aplicadas tanto no momento de definição dos meios de tratamento, como no momento do próprio tratamento, têm de ser *“adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que (...) proteja os direitos dos titulares de dados”.*

E a obrigação *“aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade”*, conforme o nº 2, do mesmo artigo 25º.

É de acrescentar que, atendendo às necessidades particulares das micro, pequenas e médias empresas¹¹⁸, o RGPD prevê no artigo 30º nº 5, uma derrogação das obrigações, mas não

¹¹⁸ Conforme sublinha o Considerando 13 do RGPD, incentiva-se mesmo as instituições e os órgãos da União, os Estados-Membros e as suas autoridades de controlo, a *“tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito de aplicação do presente regulamento”*. A noção a ter em conta *“deverá inspirar-*

das suas responsabilidades, enquanto responsáveis pelo tratamento de dados dos seus trabalhadores.

Assim, se pelo artigo 30º nº 1, “*cada responsável pelo tratamento, e, sendo caso disso, o seu representante, conservam um registo¹¹⁹ de todas as atividades de tratamento sob a sua responsabilidade*”, ou pelo nº 2, “*cada subcontratante, e, sendo caso disso, o representante deste, conservam um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento*”; já pelo nº 5, como dissemos antes, é derogada essa obrigação para as empresas ou organizações com menos de 250 trabalhadores.

Mas e novamente frisamos, não das responsabilidades, pois que, se o tratamento efetuado for “*suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados¹²⁰ a que se refere o artigo 9º, nº 1¹²¹*”, passam a ser obrigados (e responsabilizados se falharem) a conservar um registo de todas as atividades, ou todas as categorias de atividades de tratamento do artigo 30 nº 1 e nº 2.

Já em caso de violação de dados pessoais, diz-nos o artigo 33º nº1 do RGPD: “*o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso*”.

se no artigo 2º do anexo da Recomendação 2003/31/CE, de 6 de maio”, isto é, pelo nº 1, “*empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros*”.

¹¹⁹ Registo esse que, efetuado por escrito, incluindo em formato eletrónico, conforme o nº 3, é disponibilizado, a pedido, à autoridade de controlo, pelo nº 4.

¹²⁰ Relembrando, “*dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa*”.

¹²¹ Ou ainda dados pessoais relativos a condenações penais e infrações referido no artigo 10º.

Isto porque os próprios dados biométricos têm de ser precisos, conforme o que fizemos ver antes, sendo isto uma prioridade para os sensores das próprias tecnologias biométricas, ao que, uma prioridade para o próprio tratamento.

Por fim, e tom de resumo do que estivemos a analisar, chamamos a atenção para os princípios relativos ao tratamento de dados, onde, conforme o artigo 5º nº1, os dados pessoais são:

- a) *Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);*
- b) *Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades;*
- c) *Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);*
- d) *Exatos e atualizados sempre que necessário («exatidão»);*
- e) *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 («limitação da conservação»);*
- f) *Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»).*

E onde o responsável pelo tratamento, é responsável pelo cumprimento dos princípios do nº1, e tem de poder comprová-lo, conforme o princípio da responsabilidade presente no nº2, mesmo artigo.

Embora a Diretiva 95/46/CE contivesse os princípios de exatidão e limitação de conservação, artigo 6º nº1 alíneas d) e e), não os autonomizava, como estão presentes no Regulamento Geral de Proteção de Dados, artigo 5º nº1 alíneas d) e e).

E mais especificamente, os artigos 16º e 17º, que definem o direito de retificação e o direito

ao apagamento de dados¹²².

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

Já o artigo 17º, nº1, seguindo a matriz do considerando 65, diz-nos que “*o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais*¹²³, *sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada*¹²⁴, *quando se aplique*” um dos motivos presentes no nº2.

E estes motivos, referem-se a: desde os dados terem deixado de ser necessários para a finalidade (alínea a)); a o próprio titular ter retirado o consentimento – seja nos termos do artigo 6º nº1 a), ou o artigo 9 nº2 a) (alínea b)); a o titular opor-se ao tratamento, pois que não existem interesses legítimos prevalecentes que justifiquem o tratamento – artigo 21 (alínea c)); a ainda os dados pessoais terem sido tratados ilicitamente (alínea d)); a mesmo o apagamento ser para o cumprimento de obrigações jurídicas (alínea e)); a por fim, caso os dados pessoais tenham sido recolhidos no que respeita à oferta direta de serviços da sociedade da informação às crianças¹²⁵

¹²² Também conhecido como direito ao esquecimento, onde se consagra o direito de querer dados que sejam pessoais e estão na posse de outros (ou publicamente expostos, online), que não sejam mais processados, e mesmo apagados se não há uma razão legítima para esse terceiro os ter.

¹²³ Isto é um direito novo, como expõe a questão e motivação para a sua resolução, Teresa Moreira, em “*Estudos do Direito do Trabalho, Volume II*”: “*Na Internet não existe atualmente um direito ao esquecimento, o right to be forgotten ou o droit à l’oublié. E por isso, informações colocadas online podem perdurar no ciberespaço por muito tempo, correndo o risco de ficarem completamente desatualizadas e com a inerente descontextualização dos dados.*

Teoricamente, este direito ao esquecimento está ligado a um problema candente na era digital na medida em que se torna muito difícil escapar ao passado na Internet pois cada fotografia, atualização de estado ou tweet perdura para sempre na nuvem”, o chamado cloud computing.

¹²⁴ Relembremos aqui, o que foi dito quanto ao papel do responsável do tratamento de dados, nos termos do artigo 33º nº1.

¹²⁵ Que remete para o artigo 8º nº1, e este, para o artigo 6º nº1 a), quanto ao consentimento para o tratamento de certos dados, só ser lícito, se dado para uma finalidade específica – onde mesmo que o consentimento, porque a criança é menor de 16 anos, foi dado pelos titulares das responsabilidades parentais da criança, existe o direito do titular destes dados, ao apagamento dos mesmos, sem demora injustificada.

(alínea f)).

Ao que, pelo que vimos, o RGPD assenta em duas ideias essenciais: a desburocratização no tratamento dos dados pessoais e a devolução do controlo no acesso e tratamento dos dados pessoais, aos seus respetivos titulares.

Por fim, a respeito da temática deste trabalho, terminamos este subcapítulo com a análise de mais alguns pontos pertinentes, no conjunto de opiniões do Grupo de Trabalho do Artigo 29º.

Por exemplo, na introdução da opinião *“Working document on biometrics”*¹²⁶ faz-se uma chamada de atenção para o uso generalizado dos sistemas biométricos, a possível dessensibilização para os riscos e repercussões, de uma fraca proteção dos dados biométricos: *“antes, o uso das tecnologias biométricas estava confinado a áreas do ADN e à impressão digital.*

A coleção de impressões digitais era utilizada, em particular, para propósitos de aplicação das leis (por exemplo, investigação criminal).

Se a sociedade encoraja o desenvolvimento de bases de dados biométricas de impressões digitais ou de outro tipo, para mais aplicações rotineiras, isto pode aumentar a potencial reutilização por terceiros, como um elemento de comparação e pesquisa numa estrutura para os seus próprios propósitos, sem que tal objetivo tenha sido inicialmente procurado; onde estes terceiros podem incluir autoridades legais.

(...) O público pode ficar dessensibilizado, pelo uso generalizado destes dados, quanto aos efeitos que o seu processamento pode ter na vida diária. Por exemplo, o uso de tecnologias biométricas nas bibliotecas escolares pode leva a que as crianças tenham cada vez menos, a noção dos riscos da proteção de dados, que mais tarde podem ter impacto na sua vida futura”.

Pelo que, novamente dizemos, é incrivelmente importante a consagração do artigo 17 nº1 do RGPD, principalmente para os casos da alínea f), onde se estabelece o direito ao apagamento/esquecimento dos dados de crianças menores de idade – seja porque elas próprias deram o consentimento, ao ter mais de 16 anos, seja porque, ao ser menor de 16 anos, o consentimento para o tratamento foi dado pelos titulares das responsabilidades parentais – e não o

¹²⁶ Adotada a 1 de agosto de 2003.

titular dos dados.

Outro ponto, é o de que as atuais técnicas das tecnologias biométricas não são completamente infalíveis.

Para dar a entender o que se pretende dizer com isto, servimo-nos das palavras de Francisco Andrade e Teresa Moreira¹²⁷: *“uma óbvia vantagem das tecnologias biométricas, é que assegura um grande nível de confiança, relativamente à identificação de uma pessoa (Chinchilla, 2011¹²⁸). Pelo uso destes técnicas, podemos afirmar, com uma grau muito elevado de probabilidade (ou uma baixa margem de erro), que a pessoa por detrás de um terminal eletrónico é mesmo quem diz que é (O’Connor, 1998¹²⁹). E contudo, claro que estas técnicas não são infalíveis”*.

Novamente, a opinião 3/2012 do Grupo de Trabalho do artigo 29º, no seu ponto 2, e que remete para a opinião 4-2007 (WP136), diz-nos que os dados biométricos são definidos como *“propriedades biológicas, aspetos comportamentais, características fisiológicas, traços ou ações repetitivas, onde estes aspetos e/ou ações são ambos únicos para esse individuo ou mensuráveis, mesmo que os padrões usados na prática para fazer a medição técnica, possam envolver um certo grau de probabilidade”*.

E quando *“se usa sistemas biométricos, é difícil produzir resultados 100% livres de erros. Isto pode ser devido às diferenças no ambiente na altura da obtenção dos dados (iluminação, temperatura, etc.) e diferenças no equipamento utilizado (máquinas fotográficas, scanners, etc.)”*.

E a isto e ainda dentro da mesma opinião 3/2012, junta-se a necessidade de o sistema estar construído em termos de precisão e segurança, para que um *“processo de reentrada no sistema biométrico seja possível, para atualizar os dados biométricos registados”*.

¹²⁷ Em ANDRADE, Francisco C. P., MOREIRA, Teresa, *Biometrics and Data Protection: These Data are Derived from an Individual*, in *Interdisciplinary Perspectives on Contemporary Conflict Resolution* (coord. Paulo Novais e Davide Carneiro), IGI Global, 2016.

¹²⁸ Refere-se a Chinchilla, R. (2011). Ethical and Social consequences of Biometric Technologies. *Journal of Industrial Technology*, 27(1).

¹²⁹ Refere-se a O’Connor, S. (1998). Collected, Tagged, & Archived: The Burgeoning Use of Biometrics in Personal Identification. *Bender’s Immigr. Bull.* 1245.

Dado que existe “*o facto, inequívoco, de que as pessoas envelhecem e o seu corpo muda com o tempo*”, conforme nos lembram Francisco Andrade e Teresa Moreira¹³⁰.

Terminamos com a chamada de atenção para os princípios da transparência, licitude e lealdade, presentes na opinião 3/2012, ponto 3.4., onde “*os sujeitos à análise dos seus dados, têm de estar conscientes do armazenamento e/ou usos feitos dos seus dados biométricos*”, e “*qualquer sistema que faça o armazenamento de tais dados, sem o conhecimento dos titulares dos mesmos, tem de ser evitado*”.

No RGPD encontram-se consagrados no artigo 5º nº 1 a), onde os dados pessoais são “*objeto de um tratamento lícito, leal e transparente em relação ao titular de dados («licitude, lealdade e transparência»)*” e a responsabilidade de verificar o cumprimento destes, recai sobre o responsável pelo tratamento, conforme o nº 2¹³¹.

III. b. Coerência legislativa – os considerandos e as disposições finais do RGPD

Neste subcapítulo pretendemos dar a entender que o RGPD prima pela coerência das suas normas, com as de legislações anteriores, servindo-se de meios como a revogação ou ter os seus efeitos considerados *ex nunc*, portanto só afetando em alguns casos, contratos e acordos de dados, celebrados após a sua entrada em vigor.

A respeito da Diretiva 95/46/CE, pelo artigo 94º nº 1, esta é “*revogada com efeitos a partir de 25 de maio de 2018*”.

E dois, quanto ao grupo de trabalho do artigo 29º que vimos antes, diz-nos o mesmo artigo 94º nº2, que “*as remissões para a diretiva revogada são consideradas remissões para o presente regulamento*”, onde as referências deste grupo “*são consideradas referências ao Comité Europeu para a Proteção de Dados criado pelo presente regulamento*”.

Pelo que podemos afirmar, com toda a certeza, que as normas do RGPD fazem cumprir os

¹³⁰ Novamente ANDRADE, Francisco C. P., MOREIRA, Teresa, *Biometrics and Data Protection: These Data are Derived from an Individual*, in *Interdisciplinary Perspectives on Contemporary Conflict Resolution* (ccord. Paulo Novais e Davide Carneiro), IGI Global, 2016.

¹³¹ Que tem de poder comprová-lo (princípio da responsabilidade).

seus próprios considerandos, ou não fosse o considerando nº 71 dizer que:

“A Diretiva 95/46/CE deverá ser revogada pelo presente regulamento. Os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor”.

Já em relação à Diretiva 2002/58/CE, ainda em vigor, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, o artigo 95º diz-nos que o RGPD *“não impõe obrigações suplementares a pessoas singulares ou coletivas, no que respeita ao tratamento”.*

Em relação a acordos internacionais celebrados anteriormente, artigo 96º, *“os acordos internacionais celebrados pelos Estados-Membros antes de 24 de maio de 2016, que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais (...), permanecem em vigor até serem alterados, substituídos ou revogados”.*

Por fim e por último, se necessário, em revisão de outros atos jurídicos da União Europeia em matéria de proteção de dados, estabelece o artigo 98º que *“a Comissão apresenta propostas legislativas (...), a fim de assegurar uma proteção uniforme e coerente das pessoas singulares no que diz respeito ao tratamento”.*

III. c. A Carta dos Direitos Fundamentais da União Europeia

A Carta dos Direitos Fundamentais da União Europeia consagra, no direito da União Europeia, um conjunto de direitos pessoais, cívicos, políticos, económicos e sociais dos cidadãos e residentes na UE.

Perante esta, a União Europeia tem de atuar e legislar de modo consistente com a Carta.

E dois, o Tribunal de Justiça da União Europeia (TJUE) é o tribunal com jurisdição sobre as matérias de interpretação da legislação europeia, o que incluiu o respeito pelos direitos humanos.

Dito isto, passemos à análise dos princípios presentes na Carta, a respeito da proteção de dados dos utilizadores.

Primeiro, o artigo 7º define o *“direito ao respeito pela vida privada e familiar, pelo domicílio e*

pelas comunicações” de todas as pessoas. Este é um artigo que nos remete para o considerando 4 do RGPD, onde se diz que “o tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade”.

Pois que, avança ainda o RGPD, este *“respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais (...)”.*

Já no seu artigo 8º, a Carta estabelece a proteção de dados pessoais, onde:

- No ponto 1, *“todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito”;*
- No ponto 2, *“esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação”;*
- No ponto 3, *“o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”.*

Conforme vimos antes, estes três pontos são estabelecidos pelo direito da União Europeia, no RGPD, respetivamente, o ponto 1, pelo facto de se ter legislado o Regulamento Geral de Proteção de Dados, uniformizando a proteção concedida aos titulares dos dados, no que concerne ao seu tratamento no território da União Europeia.

Respetivamente, o ponto 2, que se refere aos princípios do artigo 5º do RGPD, mais propriamente o artigo 5º nº1 a), que consagra os princípios de licitude, lealdade e transparência no tratamento dos dados.

Respetivamente o ponto 3, que se refere à autoridade de controlo independente do artigo 51º do RGPD, que pelo nº 1, *“cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União”*.

III. d. A Convenção Europeia dos Direitos do Homem

Já quanto à Convenção Europeia dos Direitos do Homem, é um tratado internacional com o objetivo de proteger os direitos do homem e as liberdades políticas na Europa.

Nesta, todos os estados-membro do Conselho da Europa são parte da Convenção, e reconhecem um conjunto de direitos e liberdades a fazer respeitar no espaço europeu.

De modo a preservar estes direitos e liberdades, foi criado um órgão de jurisdição, ao qual os membros do Conselho da Europa se submetem, e são membros deste, o Tribunal Europeu dos Direitos do Homem (TEDH).

Posto isto, de novo tal como a Carta dos Direitos Fundamentais da União Europeia, o artigo importante é o que define o direito ao respeito pela vida privada e familiar.

Estabelece o artigo 8º nº 1, que *“qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”*.

E o nº 2, que *“não pode haver ingerência da autoridade pública no exercício deste direito, senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros”*.

E a estes pontos, alude o RGPD no artigo 89º, a respeito das garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos.

Diz pois, no nº 1, que *“o tratamento para fins de arquivo de interesse público, ou para fins de*

investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados.

Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo.

Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo”.

III. e. O Tribunal Europeu dos Direitos do Homem

Como vimos, de forma a proteger os direitos do homem e as liberdades políticas na Europa, e fazer respeitar a Convenção Europeia dos Direitos do Homem foi criado o TEDH, órgão de jurisdição, ao qual todos os membros do Conselho da Europa se submetem.

A nível de jurisprudência do Tribunal Europeu dos Direitos do Homem, sobre os dados pessoais, temos o acórdão “*S. e Marper c. Reino Unido*”, petição nº 30562/04 e nº 30566/04, de 4 de dezembro de 2008.

Este acórdão leva-nos para o cumprimento do artigo 5 nº 1 e) do RGPD, onde se define que os dados são “*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*”.

Concluiu pois, o TEDH que a retenção indefinida das impressões digitais, amostras de células e perfis de ADN dos dois requerentes, era desproporcional e desnecessária numa sociedade democrática, considerando que os procedimentos criminais contra ambos os requerentes tinham sido dados por terminados, com uma absolvição e desistência da ação.

E lembrou ainda que, se o armazenamento dos dados fosse para fins de interesse público, científico ou histórico, ou ainda para usos estatísticos, que poderia ser armazenado por períodos mais longos, conquanto os dados fossem utilizados para estes fins.

Existem outros acórdãos, que fazemos referência de seguida, embora a sua análise seja

mais sucinta, onde expomos o litígio e a decisão do TEDH.

No acórdão “*Biriuk c. Lituânia*” de 25 de novembro de 2008, petição n.º 23373/03, a requerente pedia a condenação de um jornal diário, ao pagamento de uma indemnização por ter publicado um artigo a revelar que esta é seropositiva.

Neste, o TEDH não considerou que o artigo tivesse contribuído para um debate de interesse geral, no sentido de que não havia interesse público importante, conforme estabelece o artigo 9º nº 2 d) do RGPD.

Assim, e reiterando a importância fundamental da proteção de dados pessoais, sobretudo os dados médicos, concluiu que o artigo 8º da Convenção Europeia dos Direitos do Homem, que estabelece para o caso, o direito ao respeito pela vida privada e familiar da requerente, tinha sido violado.

Quanto ao acórdão “*I. c. Finlândia*” de 17 de julho de 2008, petição n.º 20511/03: é um acórdão que sublinha a importância da confidencialidade no tratamento dos dados de saúde.

No caso em apreço, uma enfermeira seropositiva teve a sua condição médica de seropositiva, conhecida pelas colegas de trabalho: devido a um registo de pacientes do hospital completamente desadequado, em termos da proteção que conferia.

Em unanimidade, o TEDH pronunciou-se que este tratamento de dados é contra o artigo 24º nº 1 e artigo 25º nº 1 do RGPD, onde o responsável pelo tratamento não aplicou as medidas técnicas e organizativas adequadas, falhando na proteção de dados desde a conceção, e por defeito, isto é, desde no momento de definição dos meios de tratamento como no momento do próprio tratamento.

Sendo que a confidencialidade dos dados de saúde é crucial para a privacidade de um paciente, ademais ainda, na profissão médica e nos serviços de saúde, não esquecendo, claro, a sensibilidade da doença.

Pronunciou-se ainda, a respeito da clara violação do artigo 8º nº 1 da Convenção Europeia dos Direitos do Homem, quanto ao direito ao respeito pela vida privada e familiar de I.

Quanto ao acórdão “*L.L. c. França*” de 10 de outubro de 2006, petição n.º 7508/02, os

documentos médicos a respeito da condição de saúde de L.L. tinham sido apresentados em tribunal, sem a autorização do titular dos mesmos.

Como tal, pronunciou-se o TEDH quanto à uma intromissão injustificável na sua vida privada e familiar de L.L., violando pois, o artigo 8º nº 1 da Convenção Europeia dos Direitos do Homem.

A respeito do acórdão “*M.S. c. Suécia*” de 2 de julho de 2002, petição n.º 34209/96, falamos do artigo 18º do RGPD, quanto ao direito à limitação do tratamento, conjugado com o artigo 21º, direito de oposição.

O artigo 18º estabelece no nº 1, que “*o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento*”.

Já o artigo 21º estabelece que, nº 1 “*o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito (...). O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular de dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial*”.

O caso refere-se então a um requerente, M.S., que em sede de tribunal penal doméstico, estava a ser julgado por abuso sexual de menores. Por parte do Ministério Público, havia um testemunho do comportamento de M.S., por parte do professor de uma criança, e que poderia ser a prova derradeira, para o tribunal doméstico considerar o crime como provado.

Pois bem que, o requerente M.S., tentando fazer uso do direito a se opor ao tratamento dos seus dados, tentou evitar que o testemunho fosse considerado válido, por lhe dizer respeito, e ele a este não dar o seu consentimento.

Sobre isto, pronunciou-se o TEDH, não pode M.S. fazer valer o direito de oposição ao tratamento dos seus dados, pois que existem “*razões imperiosas e legítimas para esse tratamento*”, dado que estamos perante “*efeitos de declaração, exercício ou defesa de um direito num processo judicial*”.

Atualmente, encontramos isto disposto no artigo 21 nº 1 do RGPD.

Ainda que, a possível limitação ao tratamento, fazendo cumprir o artigo 18º nº 1 do RGPD, seria afastada, pois que estabelece o nº 2 do mesmo artigo: *“quando o tratamento tiver sido limitado nos termos do nº 1, os dados pessoais só podem (...) ser objeto de tratamento (...) para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro”*.

Por último, a respeito do acórdão *“Z. c. Finlândia”* de 25 de fevereiro de 1997, petição n.º 22009/93, o ex-marido de Z., requerente, tinha cometido uma série de crimes sexuais, tendo vindo a ser condenado pelo crime de homicídio não premeditado, por ter exposto deliberadamente as suas vítimas ao risco de infeção pelo VIH, ao ser seropositivo.

Nisto, o tribunal nacional queria que a versão integral do acórdão e dos autos se mantivessem confidenciais somente durante 10 anos, para fins de interesse público. Já por motivos de interesses privados, o respeito pela vida privada e familiar, a requerente queria que o tribunal decidisse por um período de confidencialidade mais longo.

O TEDH, fazendo referência ao artigo 8º nº 1 da Convenção Europeia dos Direitos do Homem, o direito ao respeito pela vida privada e familiar, entendeu que a proteção dos dados médicos reveste-se de importância fundamental para Z., especialmente quando estão em causa dados que indicam infeção pelo VIH.

E deste modo, que a concessão de acesso à identidade e ao estado de saúde da requerente, se fosse ao fim de apenas 10 anos, violaria o direito da mesma, na proteção dos seus dados de saúde.

A respeito deste último acórdão, chamamos só à atenção para o artigo 10º do RGPD, caso estivéssemos a falar do tratamento de dados pessoais do ex-marido de Z., portanto, alguém com uma condenação penal.

Diz o artigo 10º que *“o tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6º, nº 1, só é efetuado sob o controlo de uma autoridade pública ou se o tratamento for autorizado por*

disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas”.

III. f. O Tribunal de Justiça da União Europeia

Quanto ao TJUE, como vimos anteriormente, interpreta o direito europeu para garantir que este é aplicado da mesma forma em todos os países da União Europeia.

Vista a Carta, a Convenção Europeia dos Direitos do Homem e ainda o Tribunal Europeu dos Direitos do Homem, quanto à proteção das pessoas singulares, no que diz respeito ao tratamento dos seus dados pessoais (e a sua livre circulação), prosseguimos pois, este trabalho com as interpretações e pronúncias¹³² do Tribunal de Justiça da União Europeia (TJUE) em matéria de proteção de dados¹³³.

Comecemos pelos processos apensos C-446/12 a C-449/12W, P. Willems (C-446/12) contra Burgemeester van Nuth, e H. J. Kooistra (C-447/12) contra Burgemeester van Skarsterlân, e M. Roest (C-448/12) contra Burgemeester van Amsterdam, e L. J. A. van Luijk (C-449/12).

Este acórdão, conhecido como Willems, lida com dados biométricos obtidos para passaportes, seguindo o Regulamento nº 2252/2004, de 13 de dezembro de 2004, que estabelece as normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros¹³⁴.

E neste, o tribunal nacional em Willems tinha duas questões. Primeiro que tudo, se o regulamento se aplicava a alguns tipos de cartões de identificação, dado que estes podem, efetivamente, ser utilizados como passaportes ao viajar dentro da UE.

¹³² Como os acórdãos “essenciais” de 8 de abril de 2014, C-293/12 e C-594/12, *Digital RightsIreland*, de 13 de maio de 2014, C-131/12, *Google Spain*, de 6 de outubro de 2015, C-362/14, *Schrems*, e de 21 de dezembro de 2016, C-203/15, *Tele2 Sverige*, depois do *Tratado de Lisboa*, 2007/2009).

¹³³ Orientando-nos por ANDRADE, Francisco C. P., MOREIRA, Teresa, *Biometrics and Data Protection: These Data are Derived from an Individual*, in *Interdisciplinary Perspectives on Contemporary Conflict Resolution* (coord. Paulo Novais e Davide Carneiro), IGI Global, 2016.

¹³⁴ Regulamento esse, ainda em vigor.

E segundo, o tribunal nacional perguntou ao TJUE para interpretar as regras de proteção de dados aplicáveis aos usos posteriores dos dados biométricos, após ter sido obtido e armazenado, para os propósitos de funcionarem enquanto passaportes.

Isto pois que, como vimos, é uma preocupação legítima de um titular de dados, que os seus dados biométricos não sejam armazenados nem tratados de forma desadequada, não havendo condições técnicas de segurança. E no caso específico, os requerentes temiam pelo acesso a estes dados, sem que houvesse uma identificação claro de quem lhes tinha acedido.

Mais especificamente, quando falamos de interpretar as regras de proteção de dados aplicáveis aos usos posteriores dos dados biométricos, foi pedido, por parte do tribunal nacional, para que o TJUE dissesse se o artigo 4º nº 3 do Regulamento nº 2252/2004, à luz dos artigos 7º e 8º da Carta, artigo 8º nº 2 da Convenção Europeia dos Direitos do Homem, e o artigo 7º alínea f) da Diretiva 95/46/EC¹³⁵, lidos em conjugação com o artigo 6º nº 1 b) da mesma Diretiva, deveriam ser interpretados no sentido de que, para efeitos desse regulamento, os Estados-Membros estão obrigados a garantir, por lei, que os dados biométricos recolhidos e armazenados com base nesse regulamento, não poderão ser recolhidos, processados ou utilizados para outros fins que não sejam a emissão do passaporte (em causa).

Quanto à primeira questão, o TJUE olhou para o artigo 1º nº 3 do regulamento, que especifica que *“o presente regulamento é aplicável aos passaportes e documentos de viagem emitidos pelos Estados-Membros. Não se aplica aos bilhetes de identidade emitidos pelos Estados-Membros aos respetivos cidadãos nem aos passaportes e documentos de viagem temporários de validade igual ou inferior a 12 meses”*.

O TJUE decidiu que as palavras “validade igual ou inferior a 12 meses” só definem os “passaportes e os documentos de viagem temporários”, pelo que se tais documentos fossem válidos por mais de 12 meses, sim, aplicava-se o regulamento.

¹³⁵ Que lembramos, foi revogada pelo RGPD, artigo 94º nº 1, com efeitos a partir de 25 de maio de 2018, e em que pelo nº 2, *“as remissões para a diretiva revogada são consideradas remissões para o presente regulamento”*.

Já a respeito dos “bilhetes de identidade emitidos pelos Estados-Membros aos respetivos cidadãos”, entendeu que as palavras “validade igual ou inferior a 12 meses” não faziam parte nem se relacionavam com estes cartões de identificação. E assim, que as normas deste regulamento não se vão aplicar a qualquer bilhete de identidade, sejam ou não temporários e independentemente do seu prazo de validade.

Já quanto à segunda questão, o TJUE decidiu que o regulamento só trata da utilização dos dados biométricos, e que a utilização e o armazenamento dos dados não são regulados por este último. Qualquer outro uso dos dados, conforme especificado no preâmbulo seria para ser regulamentado por lei interna do estado.

Seguiu que o regulamento não aplicava uma limitação quanto aos usos que um Estado-Membro fizesse dos dados biométricos de um passaporte. E dado que o regulamento não se aplica a tais usos por Estados-Membros, a Carta não se aplica.

Apesar de que outros usos continuados dos dados poderão estar proibidos por leis nacionais ou pelo Tribunal Europeu dos Direitos do Homem, se for feito um *“eventual exame, por parte dos órgãos jurisdicionais nacionais, da compatibilidade de todas as medidas nacionais relacionadas com a utilização e o armazenamento dos dados biométricos com o seu direito nacional e, se for caso disso, com a Convenção Europeia de Proteção dos Direitos do Homem e das Liberdades Fundamentais”*.

Por último, e quanto à Diretiva, o TJUE declarou que o *“com as suas questões prejudiciais, o órgão jurisdicional de reenvio solicita a interpretação do Regulamento nº 2252/2004, e unicamente esse regulamento. Na medida em que resulte das considerações anteriores que o referido regulamento não é aplicável no caso em apreço, não há que examinar, de forma autónoma”*, se a Diretiva afeta o quadro jurídico nacional, as leis nacionais, no armazenamento e utilização contínua de dados biométricos, obtidos somente para propósitos do passaporte.

Por conseguinte, o *“Regulamento nº 2252/2004 deve ser interpretado no sentido de que o referido regulamento não é aplicável aos bilhetes de identidade emitidos por um Estado-Membro aos seus cidadãos, como os bilhetes de identidade neerlandeses, independentemente quer do seu*

prazo de validade quer da possibilidade de serem utilizados em viagens efetuadas fora desse Estado.”

E dois, *“o Regulamento nº 2252/2004 deve ser interpretado no sentido de que não obriga os Estados-Membros a garantirem, na sua legislação, que os dados biométricos recolhidos e armazenados em conformidade com o referido regulamento não serão recolhidos, tratados e utilizados para fins diferentes da emissão do passaporte ou do documento de viagem, uma vez que este aspeto não está abrangido pelo âmbito de aplicação do referido regulamento”*.

Veremos ainda o acórdão, de processos apensos, Volker und Markus Schecke GbR (C-92/09) e Hartmut Eifert contra Land Hessen (C-93/09), de 9 de novembro de 2010, pois que também lida com a proteção das pessoas singulares, no que diz respeito ao tratamento dos seus dados pessoais.

Mais precisamente, o artigo 8º nº 1 e nº 2 da Convenção Europeia dos Direitos do Homem, que estabelece o direito ao respeito pela vida privada e familiar.

E ainda, entretanto revogada pelo RGPD, a Diretiva 95/46/CE, quanto:

- ao seu artigo 1º nº 1, *“assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais”*¹³⁶;
- artigo 2º a), onde se consideram dados pessoais *“qualquer informação relativa a uma pessoa singular ou identificável”*¹³⁷;
- artigo 7º *“o tratamento de dados pessoais só poderá ser efetuado se”, a) “a pessoa em causa tiver dado de forma inequívoca o seu consentimento”*¹³⁸, c) *“o tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito”*¹³⁹, e) *“o tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é*

¹³⁶ Com correspondência no RGPD no artigo 1º nº 1 e nº 2.

¹³⁷ Com correspondência no RGPD no artigo 4º nº 1, embora com uma definição muito mais abrangente e precisa.

¹³⁸ Com correspondência no RGPD no artigo 6º nº 1 a).

¹³⁹ Com correspondência no RGPD no artigo 6º nº 1 c), onde obrigação legal é substituída por obrigação jurídica.

*investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados*¹⁴⁰;

- ainda o artigo 18º nº 1 em que *“o responsável pelo tratamento ou, eventualmente, o seu representante deve notificar a autoridade de controlo (...) antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente automatizados*¹⁴¹, e o nº 2, onde se estabelece a simplificação ou isenção da notificação em certos casos, quando os tratamentos não são suscetíveis de prejudicar os direitos e liberdades das pessoas em causa¹⁴²;
- ainda o artigo 19º nº 1, onde se especifica as informações que devem constar da notificação¹⁴³, desde a) *“o nome e o endereço do responsável pelo tratamento e, eventualmente, do seu representante”,* b) *“a ou as finalidades do tratamento”,* c) *“uma descrição da ou das categorias de pessoas em causa e dos dados ou categorias de dados que lhes respeitem”,* d) *“os destinatários ou categorias de destinatários a quem os dados poderão ser comunicados”,* e) *“as transferências de dados previstas para países terceiros”;*
- ainda o artigo 20º nº 1, *“os Estados-Membros especificarão os tratamentos que possam representar riscos específicos para os direitos e liberdades das pessoas em causa e zelarão por que sejam controlados antes da sua aplicação*¹⁴⁴ e nº 2, *“onde se estabelece o controlo prévio a ser efetuado pela autoridade de controlo, após a receção de uma notificação do responsável pelo tratamento ou pelo encarregado da*

¹⁴⁰ Com correspondência no RGPD no artigo 6º nº 1 e).

¹⁴¹ Com correspondência no RGPD no artigo 35º nº 1, nº 2 e nº 3, em que se faz uma avaliação de impacto sobre a proteção de dados, e o artigo 36º nº 1, em que se estabelece a consulta prévia do responsável pelo tratamento, à autoridade de controlo, se resulta que da avaliação de impacto do artigo 35º, o *“tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco”*.

¹⁴² Com correspondência no RGPD nos artigos 35º nº 3, *a contrario sensu*, pois este estabelece os casos em que a realização de uma avaliação de impacto sobre a proteção de dados do artigo 35º nº 1 é obrigatória.

¹⁴³ Com correspondência no RGPD no artigo 36º nº 1 e nº 3 alíneas a) a f).

¹⁴⁴ Com correspondência no RGPD no artigo 36º nº 4.

proteção de dados”¹⁴⁵;

- por fim, o artigo 28º, onde “*cada Estado-Membro designará uma ou mais autoridades públicas (a seguir «autoridade de controlo»)*”¹⁴⁶ *que ficarão incumbidas de, com toda a independência*¹⁴⁷, *fiscalizar a aplicação no seu território das disposições nacionais adotadas nos termos desta mesma diretiva*”¹⁴⁸.

O litígio, enquanto reenvio prejudicial, envolve uma empresa agrícola Land Hessen (processo C-92/09) e um agricultor a tempo inteiro residente no mesmo Land (processo C-93/09).

Para o exercício de 2008, os recorrentes apresentaram à autoridade local competente pedidos de fundos agrícolas, que foram deferidos.

No preenchimento do formulário do pedido, fazia-se saber que, nos termos do Regulamento nº 1290/2005/CE, artigo 44º a), impunha-se a “*publicação de informações sobre os beneficiários de fundos*” agrícolas, “*bem como sobre os montantes recebidos pelos beneficiários*”.

A isto, junta-se que o website da *Bundesanstalt*¹⁴⁹ coloca à disposição do público os nomes dos beneficiários dos apoios agrícolas, a localidade onde estão estabelecidos ou residem e o respetivo código postal, bem como os montantes anuais recebidos. Sendo que, por meio de um motor de busca interno, é possível pesquisar por estas informações.

É pois, desejo dos recorrentes, que “*seja ordenado ao Land Hessen que se abstenha ou se recuse a transmitir ou publicar*” os dados que lhes digam respeito, pois que entendem, não há interesses públicos que justifiquem a publicação dos montantes recebidos de apoio, e ainda as “*regras relativas ao Fundo Social Europeu não preveem que os beneficiários sejam nominalmente designados*”.

¹⁴⁵ Com correspondência no RGPD no artigo 36º nº 5.

¹⁴⁶ Com correspondência no RGPD nos artigos 53º e 54º.

¹⁴⁷ Com correspondência no RGPD no artigo 52º nº 1.

¹⁴⁸ Com correspondência no RGPD no artigo 51º nº 1.

¹⁴⁹ A Autoridade Federal de Supervisão Financeira alemã.

Em termos do referido Regulamento nº 1290/2005/CE, artigo 44º a), entendem pois que *“constitui uma violação injustificada do direito fundamental à proteção dos dados pessoais”*, ainda que esta publicação seja limitada à Internet, fazendo cumprir o Regulamento nº 259/2008/CE.

Levantado o problema e definidas as questões prejudiciais em 6 pontos:

1. Da validade dos artigos 42º nº 8 b) e 44º a) do Regulamento nº 1290/2005;
2. Da validade do Regulamento nº 259/2008, à luz da Diretiva 2006/24;
3. Se os anteriores forem válidos, o procedimento de publicação do Regulamento nº 259/2008 passa a ser substituído pelo que dita o artigo 18 nº 2 da Diretiva 95/46, quanto à simplificação e isenção de notificação da autoridade de controlo antes da realização do tratamento;
4. Se antes da publicação, nos termos do Regulamento 259/2008, terá de haver o controlo prévio pela autoridade de controlo do artigo 20º da Diretiva 95/46;
5. Em caso de ter de haver este controlo prévio, se o mesmo não contiver uma informação obrigatória, segundo o artigo 18 nº 2 da Diretiva 95/46, se se entende que o controlo prévio não foi eficaz;
6. Se o artigo 7º e) da Diretiva 95/46, o tratamento só poder ser efetuado quando *“necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados”*, se opõe então, à *“prática de armazenamento de endereços IP dos utilizadores de uma homepage, sem o seu consentimento expresso”*.

Perante estes pontos, o TJUE concluiu que, ao ser imposta uma obrigação de se publicar os dados pessoais, relacionados com cada pessoa individual, que fosse beneficiário de certos fundos agrícolas, sem ser estabelecida uma distinção baseada em critérios relevantes, como os períodos anuais nos quais essas pessoas recebiam tal apoio, a frequência deste apoio ou a natureza e quantidade do mesmo, o Conselho e a Comissão tinham excedido os limites impostos pelo

princípio da proporcionalidade, quanto aos Regulamentos nº 259/2008 e nº 1290/2005.

Considerou inválidos os artigos 42 nº 8 b) e 44º a) do Regulamento nº 1290/2005, e declarar o Regulamento nº 259/2008 como inválido.

E concluiu que o artigo 18º nº 2 da Diretiva 95/46/CE *“deve ser interpretado no sentido de que não sujeita o encarregado da proteção dos dados pessoais à obrigação de manter o registo previsto nessa disposição, antes da realização de um tratamento de dados pessoais”*.

E dois, que o artigo 20º da Diretiva 95/46/CE *“deve ser interpretado no sentido de que não obriga os Estados-Membros a sujeitar ao controlo prévio previsto nessa disposição, a publicação das informações”* quanto aos beneficiários de fundos agrícolas, imposta pelos artigos 42º nº 8 b) e artigo nº 44 a) do Regulamento nº 1290/2005.

III. g. A proteção de dados num contexto legislativo nacional

Por fim, e a nível de legislação nacional, que terá de estar conforme o Regulamento Geral de Proteção de Dados, sublinhamos a existência de duas leis avulsas.

Primeiro, a Lei n.º 12/2005, de 26 de janeiro, sobre a informação genética pessoal e informação de saúde, que conforme o seu artigo 1º, *“define o conceito de informação de saúde e de informação genética, a circulação de informação e a intervenção sobre o genoma humano no sistema de saúde, bem como as regras para a colheita e conservação de produtos biológicos para efeitos de testes genéticos ou de investigação”*.

Sendo que, pelo seu artigo 2º, informação de saúde *“abrange todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar”*.

Lembra o seu artigo 3º nº 1, que *“a informação de saúde, incluindo os dados clínicos registados, resultados de análises e outros exames subsidiários, intervenções e diagnósticos, é propriedade da pessoa, sendo as unidades do sistema de saúde os depositários da informação, a qual não pode ser utilizada para outros fins que não os da prestação de cuidados e a investigação em saúde (...)”*.

Por último, a respeito da proteção dos dados no tratamento, o artigo 4º define no seu conjunto, e no geral, pelo nº 1, que *“os responsáveis pelo tratamento da informação devem tomar as providências adequadas à proteção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais*¹⁵⁰.

E segundo, a Lei nº 5/2012 de 23 de janeiro, que conforme o seu artigo 1º, *“regula os requisitos de tratamento de dados pessoais para a constituição de ficheiros de âmbito nacional, contendo dados de saúde, com recurso a tecnologias de informação e no quadro do Serviço Nacional de Saúde (SNS)”*.

O seu princípio geral, estabelecido no artigo 2º, é o de que *“o sistema de tratamento de dados pessoais de saúde deve caracterizar-se pela simplicidade, flexibilidade, qualidade e estabilidade no estrito respeito pelos direitos, liberdades e garantias fundamentais, nomeadamente o direito à reserva da intimidade da vida privada”*.

Sublinha o artigo 3º que esta, é uma lei que prescreve um tratamento cuidadoso dos dados pessoais de saúde, não só para hospitais e serviços de saúde públicos, mas para todos os *“sujeitos jurídicos*¹⁵¹ *que, em razão das atribuições que prosseguem, do seu objeto social ou das atividades que exercem”*, fazem o tratamento de dados de saúde para a constituição de ficheiros de âmbito nacional.

Por último, fazendo cumprir o RGPD a respeito da responsabilidade pelo tratamento de dados¹⁵², dita o artigo 4º que *“a constituição de ficheiros para as finalidades previstas na presente lei é da responsabilidade da entidade que tenha a seu cargo o desenvolvimento, manutenção e*

¹⁵⁰ Indo neste esforço de educação dos deveres deontológicos, a todos os profissionais envolvidos, para além do estabelecido como necessário pelo RGPD.

¹⁵¹ Ainda que os atos sejam praticados em estabelecimentos de natureza privada ou social, conquanto impliquem encargos para o SNS.

¹⁵² Relembrando, do RGPD o artigo 5º nº 1 e nº 2, onde o princípio da responsabilidade, implica que o responsável pelo tratamento tem de fazer cumprir os princípios relativos ao tratamento de dados pessoais. O exercício de ponderação que faça, tem que obedecer ao artigo 24º nº 1 e nº 2, e ainda ao artigo 25º nº 1 e nº 2, isto é, uma proteção de dados desde a conceção e por defeito, e que tem em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares.

operação dos sistemas de informação das entidades do SNS e do Ministério da Saúde (...)”.

III. h. Uma relação de trabalho que respeite os direitos do trabalhador

Devemos ainda referir, a respeito do Direito do Trabalho, as regras que definem os usos possíveis dos dados biométricos numa relação laboral¹⁵³.

Pois que, entre um empregador e um trabalhador, torna-se imperativo que existam proteções específicas contra o abuso de poder do primeiro, face aos direitos do segundo.

Em tom introdutório, fazemos uso das palavras de Teresa Moreira para alertar para a necessidade desta proteção, num mundo cada vez mais voltado para o uso de tecnologias biométricas.

“As NTIC¹⁵⁴ tiveram e têm uma enorme repercussão no desenvolvimento do Direito do Trabalho, dando origem, mesmo, a um novo tipo de controlo, o controlo eletrónico do empregador¹⁵⁵”.

O uso destas novas tecnologias, principalmente a internet e o email, tornou o controlo do empregador cada vez mais presente e intrusivo, afetando em cada vez maior grau a privacidade

¹⁵³ Orientando-nos novamente por ANDRADE, Francisco C. P., MOREIRA, Teresa, *Biometrics and Data Protection: These Data are Derived from an Individual*, in *Interdisciplinary Perspectives on Contemporary Conflict Resolution* (ccord. Paulo Novais e Davide Carneiro), IGI Global, 2016.

¹⁵⁴ Novas tecnologias de informação e comunicação.

¹⁵⁵ Refira-se que o artigo 20 n.º 1 estabelece a proibição da utilização de meios de vigilância à distância, com a finalidade de controlar o desempenho profissional do trabalhador no artigo 20 n.º 1.

Fazendo uso das palavras de Catarina Sarmiento e Castro, em *“Direito da Informática, Privacidade e Dados Pessoais”*: *“note-se que a Organização Internacional do Trabalho (OIT) admite, no seu Código de Conduta para a proteção de dados dos trabalhadores de 1996, que apesar de considerar que os trabalhadores não devem ser continuamente vigiados, poderão sê-lo desde que tal se justifique por razões de segurança/saúde relativas ao tipo de atividade em causa [mais propriamente, no ponto 5.16: “workers should not be monitored on a continuous basis, unless this is specifically justified for safety reasons”].*

“Também nestes casos o trabalhador deve ser informado acerca da vigilância e respetiva metodologia. A OIT, aliás tal como a CNPD, defende que as imagens não podem ser utilizadas como fundamento para aplicação de quaisquer sanções aos trabalhadores”.

dos trabalhadores¹⁵⁶. Os empregadores podem, com a utilização das NTIC, reunir informação sobre os trabalhadores através da observação do que fizeram durante o tempo e no local de trabalho, descobrir os seus interesses e preferências, através da análise dos sites mais visitados, possibilitando a criação de perfis dos trabalhadores e a sua seleção baseada nestes dados¹⁵⁷.

Desta forma, as NTIC permitem, graças às suas capacidades praticamente ilimitadas de captar, armazenar, relacionar, e transmitir todo o tipo de dados, reunir de forma personalizada, a partir de vários tipos de informação, múltiplas facetas da vida dos trabalhadores e conhecer, de algum modo, a própria forma de pensar dos trabalhadores, efetuando conclusões de natureza preditiva sobre o próprio futuro da relação laboral¹⁵⁸.

A respeito destas conclusões de natureza preditiva, não só sobre o futuro da relação laboral, como do próprio trabalhador, devemos sublinhar a proteção conferida pelo legislador europeu para estes casos, o artigo 22 nº 1 do RGPD.

Pois que, em decisões individuais automatizadas, incluindo definições de perfis, o “titular dos dados tem 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”.

O que implica que, em termos legais, a existência de uma relação de trabalho não retira o direito do trabalhador, de ver a sua privacidade e dignidade respeitadas¹⁵⁹.

¹⁵⁶ Que como vimos, é um direito que está presente na mente e nos atos legislativos não só do legislador europeu, como nacional, fazendo respeitar tanto as provisões do RGPD, como especificamente, o “direito ao respeito pela vida privada e familiar” e o “direito à proteção de dados pessoais”, respetivamente o artigo 7º e o artigo 8º da Carta, como ainda o “direito ao respeito pela vida privada e familiar” presente no artigo 8º da Convenção Europeia dos Direitos do Homem.

¹⁵⁷ Chamamos à atenção para o que dispõe o RGPD a respeito da criação de perfis do utilizador, para que haja um tratamento equitativo e transparente, em que pelo artigo 14º nº 2 g), o responsável pelo tratamento, neste caso, falamos do empregador, fornece ao titular dos dados, o trabalhador, a informação de que existem decisões automatizadas, definindo perfis referidos no artigo 22º nº 1 e nº 4, e ainda as “informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados”.

¹⁵⁸ MOREIRA, Teresa C., Estudos de Direito do Trabalho, Almedina, 2011.

¹⁵⁹ O que vimos, é também opinião do Grupo de Trabalho do Artigo 29, onde se obriga à definição clara dos fins para os quais se efetua o armazenamento e tratamento dos dados biométricos, um pré-requisito com vista a garantir a proteção dos direitos e liberdades fundamentais.

Nesta monitorização e obtenção, armazenamento e tratamento dos dados pessoais dos trabalhadores, falamos de um controlo eletrónico que pode ser realizado à distância, secretamente, de forma oculta, contínua e intrusiva.

E este tipo de controlo eletrónico desrespeita claramente, a letra da lei, bem como a intenção do legislador europeu, ao estabelecer o artigo 24º nº 1 (e nº 2) e artigo 25 nº 1 e nº 2 do RGPD.

Pois que, e respetivamente primeiro, para poder avaliar da necessidade de obtenção destes dados do trabalhador, o empregador tem de ter em conta *“a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados bem como os riscos para os direitos e liberdades”* do trabalhador.

E segundo, já no artigo 25º nº 1, na aplicação das medidas técnicas e organizativas que forem adequadas, para assegurar e poder comprovar que o tratamento respeita os direitos e liberdades fundamentais do trabalhador, o empregador, desde a conceção deste sistema de controlo eletrónico, com armazenamento e tratamento de dados, tem de *“ter em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades”*.

Ao que, um controlo eletrónico que pode ser realizado à distância, secretamente, de forma oculta, contínua e intrusiva, vai contra as *“medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização”*, pois que não protege os direitos do trabalhador, enquanto titular de dados.

Isto é, tem de ser feito sempre um juízo de adequação, necessidade e proporcionalidade entre as medidas tomadas para o tratamento de dados, e os riscos para os direitos e liberdades fundamentais do trabalhador, titular de dados¹⁶⁰.

¹⁶⁰ Relembrando, a isto também alude o ponto 3 do Grupo de Proteção de Dados do artigo 29, Opinião de 3/2012, onde na análise legal, a respeito da proporcionalidade quanto ao uso feito dos dados biométricos, *“o responsável pelo tratamento, tem de se o processamento e os seus mecanismos, as categorias de dados a serem recolhidas e*

Por estes motivos, uma relação laboral honesta e de respeito mútuo suscita os seguintes artigos do Código do Trabalho.

Primeiro, o artigo 16º, quanto à “*reserva da intimidade da vida privada*”, diz no seu nº 1, que “*o empregador e o trabalhador devem respeitar os direitos de personalidade da contraparte, cabendo-lhes, designadamente, guardar reserva quanto à intimidade da vida privada*”.

E segundo, que pelo nº 2, este direito à reserva da intimidade da vida privada “*abrange quer o acesso, quer a divulgação de aspetos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afetiva e sexual, com o estado de saúde e com as convicções políticas e religiosas*”.

Pois que, o acesso ou conhecimento de uma informação de saúde do trabalhador, pelo empregador, ou do trabalhador, a respeito do empregador, não dá o direito nenhum dos dois, de fazer armazenamento ou tratamento dos dados, sem que haja conhecimento nem autorização por parte do titular dos mesmos.

Já a respeito do juízo de adequação, necessidade e proporcionalidade dos dados limitarem-se ao mínimo para os fins a prosseguir, diz o artigo 17º nº 1, quanto à “*proteção de dados pessoais*”, que o “*empregador não pode exigir a candidato a emprego ou a trabalhador que preste*”:

- Diz a alínea a), informações relativas à “*sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar a respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respetiva fundamentação*”;
- Diz a alínea b), informações relativas à “*sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da atividade profissional o justifiquem e seja fornecida por escrito a respetiva fundamentação*”.

processadas e a transferência da informação contida na base de dados são necessários e indispensáveis. As medidas de segurança têm de ser adequadas e efetivas. O responsável pelo tratamento tem de considerar os direitos a serem concedidos aos indivíduos aos quais os dados pessoais se referem, e assegurar que um mecanismo adequado para o exercício desses direitos é incorporado nessa aplicação”.

E para que não haja tentativa por parte do empregador, de violar gravemente o direito à vida privada e familiar do trabalhador, o legislador serve-se de medidas técnicas e organizativas adequadas para aplicar com eficácia os princípios da proteção de dados.

Nomeadamente, a minimização, ao pelo mesmo artigo 17º, já o nº 2, em que, a respeito das informações do trabalhador *“relativas à sua saúde ou estado de gravidez”*, estas *“são prestadas a médico, que só pode comunicar ao empregador se o trabalhador está ou não apto a desempenhar a atividade”*.

Isto é, os dados pessoais do trabalhador não são para conhecimento do empregador, do mesmo modo que os dados pessoais do empregador não são para conhecimento do trabalhador, senão quando sejam estritamente relevantes, num juízo que avalie a natureza, contexto e finalidades do tratamento dos dados. Um juízo de adequação, necessidade e proporcionalidade.

Dando como exemplo, se uma profissão exige grande resistência e força física, e o trabalhador é alguém que, devido à sua condição médica, não está ainda¹⁶¹ apto para realizar esse género de atividade, conforme o nº2 do artigo 17º, o empregador só deverá saber se o trabalhador está apto ou não para a desempenhar.

Em tom final de análise do Código do Trabalho, a respeito da proteção que este confere ao armazenamento e tratamento dos dados do trabalhador¹⁶², analisamos agora o artigo 18º, que se refere especificamente à temática deste trabalho, quanto à proteção concreta dos dados biométricos.

Assim, o nº 1 diz-nos que o *“empregador só pode tratar dados biométricos do trabalhador após notificação à Comissão Nacional de Proteção de Dados”*, onde pelo nº 4, *“deve ser acompanhada de parecer da comissão de trabalhadores ou, não estando este disponível 10 dias após a consulta, de comprovativo do pedido de parecer”*.

Dado que a monitorização e tratamento presume, *ab initio*, o respeito pelo princípio da transparência, na medida em que o trabalhador sabe da monitorização, armazenamento e

¹⁶¹ Por exemplo, perdeu os membros superiores e encontra-se a aguardar por próteses substitutivas desses membros.

¹⁶² Onde, como vimos, também inclui proteção dos dados do empregador.

tratamento de dados a que está a ser sujeito¹⁶³, é especialmente importante que o legislador português tenha definido que este tipo de monitorização precisa de ser notificado à Comissão Nacional de Proteção de Dados, e ainda à Comissão de Trabalhadores, que têm dez dias para se pronunciarem.

Por último, relembramos a ideia presente no nº 2, que o *“tratamento de dados biométricos só é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objetivos a atingir”*.

Assim que, diz o nº 3, cessando as finalidades a que se destinam, deixam de poder ser conservados *“devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho”*.

III. i. A Constituição da República Portuguesa

Ainda nos referimos à Constituição da República Portuguesa, nos termos em que se trata da Lei Fundamental da República Portuguesa, e que como tal, deverá espelhar os ideais a prosseguir, desde a dignidade da pessoa humana, a vontade popular, e a construção de uma sociedade livre, justa e solidária, conforme estabelece o seu artigo 1º.

Fazendo respeitar tanto o RGPD, como o artigo 7º e o artigo 8º da Carta, em conjunto com o artigo 8º da Convenção Europeia dos Direitos do Homem, o artigo 26º da CRP estabelece *“o direito à reserva da intimidade da vida privada e familiar”*, no seu nº 1, onde se reconhece o direito *“à proteção legal contra quaisquer formas de discriminação”*.

Proteção legal essa, que fica obrigada pelo nº 2, a *“estabelecer garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias”*.

¹⁶³ Fazemos, novamente, a chamada de atenção para os princípios da transparência, licitude e lealdade, presentes na opinião 3/2012 do Grupo de Trabalho do artigo 29, ponto 3.4., onde *“os sujeitos à análise dos seus dados, têm de estar conscientes do armazenamento e/ou usos feitos dos seus dados biométricos”*, e *“qualquer sistema que faça o armazenamento de tais dados, sem o conhecimento dos titulares dos mesmos, tem de ser evitado”*.

Isto é, o estabelecimento de garantias concretas, em termos de adequação, necessidade e proporcionalidade no juízo de valor entre os fins a prosseguir quando se pretende obter e utilizar, pelo que tanto armazenar como tratar, informações relativas a qualquer indivíduo.

Existe ainda o artigo 35º, onde se faz cumprir o princípio da transparência no acesso e conhecimento dos dados “informatizados” que digam respeito a alguém, fazendo cumprir o artigo 15º nº 1 do RGPD.

Não se limita a prescrever o direito ao acesso, mas também o direito a “*exigir a sua retificação e atualização*”, fazendo cumprir o artigo 16º do RGPD, “*o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos¹⁶⁴ que lhe digam respeito*”.

E por fim, ainda o “*direito de conhecer a finalidade a que se destinam*”, o que nos remete para o artigo 13º nº 1 c) do RGPD, onde se diz que o direito inclui não só “*as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento*”.

O artigo 35 nº 2 diz-nos que a “*lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado¹⁶⁵, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente*”¹⁶⁶.

Por último, o artigo 35 nº 3 leva-nos para o artigo 9º do RGPD, onde se proíbe o tratamento de dados sensíveis.

Enquanto que este nº 3, define a proibição para o “*tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem*

¹⁶⁴ Ou se incompletos, tornados completos, incluindo por meio de uma declaração adicional.

¹⁶⁵ Relembrando, artigos 21 nº 1 e artigo 22º nº 1 do RGPD, onde se define que, exercendo o seu direito de oposição, “*o titular dos dados tem 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*”.

¹⁶⁶ Entre nós, a Comissão Nacional de Proteção de Dados, com as suas competências atribuídas pela Lei nº 43/2004 de 18 de agosto de 2004, a Lei de funcionamento da CNPD, e ainda a Resolução da Assembleia da República nº 59/2004, o Quadro de Pessoal da CNPD.

étnica”, o RGPD vai mais longe, no seu artigo 9º nº 1, ao especificar o “tratamento de dados genéticos, dados biométricos para identificar uma pessoa inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa”.

Temos para nós que, muito embora se diga que caso não haja *“consentimento expresso do titular”,* ou *“para processamento de dados estatísticos não individualmente identificáveis”,* uma *“autorização prevista por lei com garantias de não discriminação”* não basta, para fazer a proteção, de modo inequívoco, dos dados biométricos, dados relativos à saúde, ou dados relativos à vida sexual ou orientação sexual de uma pessoa, como reclama ser direito do titular de dados, o RGPD.

Pelo que deverá haver uma alteração desta norma para incluir a proteção destes dados, principalmente se é intenção do legislador, fazer valer as garantias de não discriminação, não só do artigo 35º nº 3, como ainda, o princípio da igualdade estabelecido no artigo 13º, nº 1 e nº 2.

Pois que, artigo 13º nº 2, *“ninguém pode ser privilegiado, beneficiado, prejudicado, privado de qualquer direito ou isento de qualquer dever em razão de ascendência, sexo, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual”.*

No entretanto, relembra-se que o RGPD tem aplicação direta e uniformizada em todo o espaço europeu, desde o dia 25 de maio de 2018¹⁶⁷, em que os direitos e proteções que estabelece são os mínimos, para se fazer cumprir em qualquer um dos Estados-Membros.

¹⁶⁷ Artigo 99º nº 1 e nº 2 do RGPD.

IV. Conclusão

IV. a. Que sentido fazer, de um mundo voltado para as tecnologias biométricas

Começamos neste trabalho por introduzir o pensamento histórico inovador, por detrás dos atuais sistemas computadorizados, que fazem a ponte entre a inteligência artificial e a autenticação por meio dos dados biométricos dos utilizadores.

Há dez, vinte anos atrás, o mundo digital que tomamos por garantido não passava de ficção científica. Os documentos de identificação continham apenas uma fotografia e a impressão digital.

E comparar esta impressão com outras num conjunto, bem, estaríamos a falar de analisar um dossier, não fazer uma análise comparativa numa base de dados informática.

Do mesmo modo, o local de trabalho deixou de ser necessariamente aquele espaço físico para o qual nos deslocamos diariamente, para poder ser um espaço virtual, onde se armazena centenas de dados, introduzidos por meio de um teclado, um scanner, qualquer tecnologia de recolha de dados. Algumas ou talvez muitas das vezes, sem que tenhamos conhecimento disso.

Dados, que reúnem pensamentos, formas de teclar e falar, ideias políticas, preferências desportivas, leituras de retina que permitem recriar um molde a 3D dos nossos olhos, scanners de impressões digitais, mãos. O corpo e a mente, e certamente há inúmeros usos que se lhe pode dar.

Escolhas mais facilitadas pelo acesso à informação, bastante dela privada, independentemente de termos autorização para lhe aceder, armazenar e realizar o seu tratamento.

Como por exemplo, poder decidir da desadequação de alguém, para certa vaga num emprego, porque possui alguma característica menos “adequada”.

Dizíamos nós, há dez, vinte anos. Pois que o mundo era mais inocente, e não havia um acesso e partilha desenfreada da informação, incentivada pelo consumismo e, segundo os especialistas, as necessidades do mercado.

A tecnologia mudou e muda radicalmente a nossa forma de atuar, de comunicar com outros. O que certamente este trabalho mostra, é que a tecnologia não pode dar passos em falso, precisa do suporte de legislação adequada.

Consciente dos prós e contras, em cada permissão ou restrição que prescreve.

Pois que perdemos todos. Os nossos direitos e liberdades. O direito à nossa vida privada e intimidade. O que pensamos de nós próprios, se passamos a perder acesso a novas oportunidades, devido a registos criados sobre nós, e dos quais não temos conhecimento. O que pensamos de outros, para dar resposta a perfis automatizados que não são senão preconceitos informatizados.

O Regulamento Geral de Proteção de Dados entrou em vigor a 25 de maio de 2018.

E entrou para o melhor, ganha o utilizador e ganha a sociedade, principalmente a europeia.

Na emergência de novas tecnologias, terá de continuar a haver uma mente legislativa acutilante, energética mas decidida a proteger, como desde o início do pacto social que formou a sociedade como nós a conhecemos, sempre todos. Todos, mesmo os mais novos, que ainda não sabem dos seus direitos, deveres e liberdades fundamentais.

Deve-se pois, elogiar a atuação do legislador europeu, por ser por meio de um regulamento, com aplicação em todos os seus elementos e em todos os países da UE, que faz a salvaguarda dos interesses das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos.

Por fazer cumprir o artigo 5º nº 1 a) do RGPD com esta atuação, obrigando a um tratamento uniformemente lícito, leal e transparente em relação ao titular de dados, por todo o espaço europeu.

Por estabelecer princípios, onde pela violação destes se responsabiliza o responsável pelo tratamento. Pois que são várias as vezes, onde o responsável preferia não cumprir com os mesmos, não facultar ao titular de dados a informação de que está a proceder ao tratamento dos seus dados pessoais, não retificar ou apagar os dados, quando o titular dos mesmos exige.

Não ser, portanto, transparente.

E principalmente, poder escolher não fazer um juízo de proporcionalidade, acerca da adequação, necessidade e proporcionalidade, quando pondere proceder ao tratamento de dados.

Pois que num lado da balança há a natureza, o âmbito, o contexto e as finalidades do tratamento, e no outro, mede-se os riscos para os direitos e liberdades das pessoas singulares.

Assim que é importantíssimo o artigo 25º do RGPD, estabelecer-se que as medidas técnicas e organizativas, e ainda as garantias que se destinam a aplicar, com eficácia, os princípios da proteção de dados, são para ser aplicadas *“desde o momento de definição dos meios de tratamento, como no momento do próprio tratamento”*.

Espera-se que em 2030, todos tenhamos um assistente digital treinado para antecipar as nossas necessidades, planejar o nosso dia, combinar encontros, responder e intercetar comunicações, conduzir, cuidar da nossa saúde.

A inteligência artificial, por meio do cruzamento de dados e criação de perfis autonomizados individualizados, pela sua potencialidade na realização de otimizações e construção de modelos de aprendizagem, cada vez mais poderosos e precisos na resolução de problemas, irá infiltrar-se em quase todas, senão todas as áreas da nossa vida.

Uma inteligência artificial, ou mais propriamente dito, um agente inteligente ou uma rede neuronal artificial, não são preconceituosos por natureza. Não têm valores desse tipo. Vimos nós, buscam satisfazer objetivos estabelecidos por outros, conquanto não sejam avaliados como impossíveis de executar, contraditórios com os seus princípios, ou quando não justifica, de um ponto de vista lógico, em termos de risco, custo e esforço envolvido.

A sua aprendizagem conjuga racionalidade com benevolência. Se generalizarmos um modo de proceder em sociedade, composta por comportamentos que valorizam a ética e a moral, que respeitem os direitos e liberdades fundamentais de cada um, a inteligência artificial interiorizará, para si, esta forma de ser e agir.

Desenvolverá uma consciência, que muito embora adaptativa, não procura senão a satisfação dos objetivos que lhe sejam atribuídos, com correção na forma de proceder, por todo um conjunto de conhecimentos, intenções, objetivos, crenças, princípios e ainda desejos, que nos beneficiam. Não só individualmente, mas também enquanto espécie.

Que novos direitos poderão surgir? Que princípios lhes subjazem? Qual o seu impacto?

A nossa pequena comunidade, cada vez mais abarca uma toda sociedade em evolução.

V. Bibliografia

AMADO, João Leal, **Contrato de Trabalho**, 4.^a Edição, Coimbra Editora, 2014, pp. 227-233;

ANDRADE, Francisco C. P., **Comunicações Eletrónicas e Direitos Humanos: O Perigo do “Homo Conectus”**, in *Direitos Humanos e Sua Efetivação na Era da Transnacionalidade*, Juruá Editora, Curitiba, 2012;

ANDRADE, Francisco C. P., **Da Contratação Eletrónica – Em Particular Da Contratação Eletrónica Inter-Sistémica Inteligente**, 2008, 153-219, 230-255 pp.;

- ALLEN, Tom e WIDDISON, Robin, **Can Computers Make contracts?**, in “Harvard Journal of Law and Technology”, volume 9, number 1, 1996, pp. 35-43;
- ANDRADE, Francisco C. P., NOVAIS, Paulo, NEVES, José, **Issues on Intelligent Electronic Agents and Legal Relations**, in *The Law of Electronic Agents – Proceedings of the LEA 2004 Workshop*, Claudia Cevenini-Gedit edizioni, 2004;
- ANDRADE, Francisco C.P., NEVES, José, NOVAIS, Paulo, MACHADO, José Manuel, **Software agents as legal persons**, in *Virtual Enterprises and Collaborative Networks*, Kluwer Academic Publishers, 2004;
- ANDRADE, Francisco C. P., NOVAIS, Paulo, MACHADO, José Manuel, NEVES, José, **Intelligent Contracting: software agents, corporate bodies and virtual organizations**, Springer-Verlag, 2007, pp. 4-6;
- BARFIELD, Woodrow, **Issues of Law for Software Agents within Virtual Environments**, Presence, Vol. 14, Issue 6, The MIT Press, 2005, pp. 744-747;
- BOURCIER, Danièle, **De l’intelligence artificielle à la personne virtuelle: émergence d’une entité juridique?**, Droit et Société, Ed. juridiques associées 49, 2001, pp. 850-852;
- SARMENTO E CASTRO, Catarina, **Direito da Informática, Privacidade e Dados Pessoais**, Almedina, 2005;
- FELLIU, Silvia, **Intelligent Agents and Consumer Protection** in http://www.eclip.org/documents/elecagents/consumer_protection.pdf, Oxford University Press, 2001;

- **MARQUES**, Garcia, e **MARTINS**, Lourenço, *Direito da Informática*, Almedina, 2006;
- **O'CONNOR**, Sean, *Collected, tagged, and archived: legal issues in the burgeoning use of biometrics for personal identification* in http://stlr.stanford.edu/STLR/Working_Papers/98_O_Connor_1/index.htm, Stanford Technology Law Review, 1998;
- **REED**, Chris, *EDI – contractual and liability issues*, Computer Law and Practice (6), 1990;
- **RUSSEL**, S.J., e **NORVIG**, P., *Artificial Intelligence: a modern approach*, Prentice Hall, 1995, pp. 16-29, 34-36, 727-737;
- **STUURMANN**, K., e **WIJNANDS**, H., *Intelligent agents: a curse or a blessing? A survey on the legal aspects of the application of intelligent software systems*, Computer Law and Security Report, 2001, pp. 96-97;

ANDRADE, Francisco C. P., **MOREIRA**, Teresa, *Biometrics and Data Protection: These Data are Derived from an Individual*, in *Interdisciplinary Perspectives on Contemporary Conflict Resolution* (ccord. Paulo Novais e Davide Carneiro), IGI Global, 2016;

ANDRADE, Francisco C. P., **NOVAIS**, Paulo, **MACHADO**, José Manuel, **NEVES**, José, *Contracting Agents: legal personality and representation*, 2007, pp. 5-10;

ANDRADE, Francisco C. P., **NOVAIS**, Paulo, **MACHADO**, José Manuel, **NEVES**, José, *Software Agents and Virtual Organizations: Consent and Trust*, Inderscience Publishers, 2010;

ERHAN, Dumitru, **BENGIO**, Yoshua, **COURVILLE**, Aaron, **MANZAGOL**, Pierre-Antoine, **VINCENT**, Pascal, **BENGIO**, Samy, **BOTTOU**, Léon, *Why Does Unsupervised Pre-training Help Deep Learning?*, 2010, pp. 201-202;

FERREIRA, António Miguel, *Introdução Ao Cloud Computing*, 1.^a Edição, FCA, 2015, pp. 169-177;

FONTAINHAS, Emília da Conceição Golim, *Dos Testemunhos de Conexão no Quadro Legislativo Europeu da Proteção de Dados - Em particular do consentimento para a sua utilização*, 2013, 49-121 pp.;

FREITAS, Pedro Miguel, **MOREIRA**, Teresa Coelho, **ANDRADE**, Francisco C. P., *Data Protection and Biometric Data: European Union Legislation*, in *Biometric Security and Privacy – Opportunities & Challenges In The Big Data Era*, Springer, 2017;

GANZHA, Maria, **PAPRZYCKI**, Marcin, e **ESSAAIDI**, Mohamed, *Software Agents, Agent Systems and Their Applications*, in *NATO Science for Peace and Security Series (Vol. 32)*, IOS Press, 2012;

GOKMEN, Tayfun, e **VLASOV**, *Acceleration of Deep Neural Network Training with Resistive Cross-Point Devices*, 2006 in <https://arxiv.org/ftp/arxiv/papers/1603/1603.07341.pdf>;

GOODMAN, Bryce, *European Union regulations on algorithmic decision-making and a “right to explanation”*, Oxford Internet Institute, 2016;

HERT, Paul de, **GUTWIRTH**, Serge, **MOSCIBRODA**, Anna, **WRIGHT**, David e **GONZALEZ-FUSTER**, Gloria, *Legal Safeguards for Privacy and Data Protection in Ambient Intelligence*, Springer-Verlag London Limited, 2008, pp. 6-8;

IENCA, Marcello, e **ANDORNO**, Roberto, *Towards new human rights in the age of neuroscience and neurotechnology*, Life Sciences, Society and Policy, 2017, pp. 7-27;

LANT, Karla, *Google’s Machine Learning Software Has Learned to Replicate Itself*, Futurism, outubro 2017 in <https://futurism.com/googles-machine-learning-software-has-learned-to-replicate-itself/>;

LE, Quoc, e **ZOPH**, Barret, *Using machine learning to explore*, Google Brain team, maio 2017 in <https://research.googleblog.com/2017/05/using-machine-learning-to-explore.html>;

METZ, Cade, *Artificial Intelligence Is Setting Up the Internet for a Huge Clash With Europe*, in <http://www.wired.com/2016/07/artificial-intelligence-setting-internet-huge-clash-europe/>, 2016;

MOREIRA, Teresa C., *A privacidade dos trabalhadores e a utilização de tecnologias de identificação por radiofrequência*, in *Estudos em Homenagem ao Professor Doutor Heinrich Hörster*, Almedina, Coimbra, 2012;

MOREIRA, Teresa C., *A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação*, in *SHO2011: Colóquio Internacional de Segurança e Higiene Ocupacionais*, 7, Sociedade Portuguesa de Segurança e Higiene Ocupacionais, Guimarães, 2011, pp. 35-40;

MOREIRA, Teresa C., *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo eletrónico do empregador*, Almedina, Coimbra, 2010, 25-147, 195-244, 247-448 pp.;

MOREIRA, Teresa C., *Da esfera privada do trabalhador e o controlo do empregador*, Studia Iuridica, n.º 78, Coimbra Editora, Coimbra, 2004;

MOREIRA, Teresa C., e ANDRADE, Francisco C. P., *Электронный Контроль В Сфере Трудовых Отношений (Electronic Control in Labor Relations)*, in *Вестник Нижегородского университета им. Н.И. Лобачевского*, No. 3, 2015, pp. 158-172;

MOREIRA, Teresa C., *Esfera privada dos trabalhadores e novas tecnologias*, in *Minerva – Revista de Estudos Laborais*, No. 4, 2004;

MOREIRA, Teresa C., *Estudos de Direito do Trabalho*, Almedina, 2011;

MOREIRA, Teresa C., *Estudos de Direito do Trabalho – Volume II*, Almedina, 2016;

MOREIRA, Teresa C., *Every breath you take, every move you make: a privacidade dos trabalhadores e o controlo através de meios audiovisuais*, in *Prontuário de Direito do Trabalho*, No. 87, 2011;

MOREIRA, Teresa C., *Every breath you take, every move you make: cybersurveillance in the workplace and the worker's privacy*, in *Masaryk University Journal of Law and Technology*, vol. 7, No. 1, 2013, Heinonline and Scopus, pp. 75-85;

MOREIRA, Teresa C., *Igualdade e Não Discriminação – Estudos de Direito do Trabalho*, Almedina, Coimbra, 2013;

MOREIRA, Teresa C., *Interrogações sobre o poder de controlo do empregador e a esfera privada do trabalhador*, in *Minerva – Revista de Estudos Laborais*, No. 3, 2003;

MOREIRA, Teresa C., *Intimidade do trabalhador e tecnologia informática*, in VII Congresso Nacional de Direito do Trabalho – Memórias, Almedina, Coimbra, 2004, pp. 175-192;

MOREIRA, Teresa C., *O poder de controlo do empregador através de meios audiovisuais: análise do art. 20.º do Código do Trabalho*, in *Nos 20 anos do Código das Sociedades Comerciais – Homenagem aos Profs. Doutores A. Ferrer Correia, Orlando de Carvalho e Vasco Lobo Xavier*, Coimbra Editora, Coimbra, 2007;

MOREIRA, Teresa C., *The digital to be or not to be: privacy of employees and the use of online social networks in the recruitment process*, in *Journal of Law and Social Sciences*, vol. 2, No. 2, 2013 EBSCO, CrossRef, Proquest, Ulrich's, pp. 76-80;

MOREIRA, Teresa C., *The protection of workers' personal data and the surveillance by RFID in Portugal*, in *Journal of Law and Social Sciences*, vol. 3, No. 1, 2013, EBSCO, CrossRef, Proquest, Ulrich's, pp. 104-107;

MOREIRA, Teresa C., *The Worker's privacy and the electronic control*, in *Journal of Law and Social Sciences*, vol. 2, No. 1, 2012, EBSCO, CrossRef, Proquest, Ulrich's., pp. 8-11;

MOREIRA, Teresa C., *To Be or Not To Be Digital: o controlo das redes sociais online dos candidatos no processo de recrutamento*, in *Para Jorge Leite – Estudos Escritos Jurídico-Laborais*, Coimbra Editora, Coimbra, 2015, pp. 625-645;

MOREIRA, Teresa C., *Transparency and data protection in the workplace: the workers control by video surveillance*, in *Transparenz – Tagungsband des 17. Internationalen Rechtsinformatik Symposions – IRIS 2014*, (coord. Erich Schweigofer, Frank Kummer, Walter Hötzen-dorfer), Oesterreichische Computer Gesellschaft, Áustria, 2014, also published in www.jusletter-IT.eu, February 2014;

PASLUOSTA, C. F., CHIU, A. W. L., *Modulation of Grasping Force in Prosthetic Hands Using Neural Network-Based Predictive Control*, in CARTWRIGHT, Hugh, *Artificial Neural Networks, Methods in Molecular Biology*, vol. 1260, Springer, 2015;

RIOS, Billy, e BUTTS, Jonathan, ***Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies***, maio de 2017, in https://drive.google.com/file/d/0B_GspGER4QQTykJfaVIBeGVCSW8/view, pp. 1-7;

ROBINSON, Melia, ***San Francisco biohackers are wearing implants made for diabetes in the pursuit of 'human enhancement'***, Tech Insider, janeiro de 2017, in <http://www.businessinsider.com/san-francisco-biohacking-continuous-glucose-monitors-2017-1>;

ROUVROY, Antoinette, ***Privacy, Data Protection and the Unprecedented Challenges of Ambient Intelligence***, in "Studies in Ethics, Law and Technology", vol. 2, Issue 1, Article 3, 2008, pp. 8-13, 26-29, 39-46;

SHARKEY, Noel, ***A 13th century programmable robot***, University of Sheffield, 2007 in <https://readtiger.com/https/web.archive.org/web/20070629182810/http://www.shef.ac.uk/marcoms/eview/articles58/robot.html>;

SHARKEY, Noel, ***The programmable robot of ancient Greece***, New Scientist, 7 de julho de 2007, edição 2611 in <https://www.newscientist.com/article/mg19526111-600-the-programmable-robot-of-ancient-greece/>;

SIMONITE, Tom, ***Short Sharp Science: Celebrating Ada Lovelace: the 'world's first programmer'***, New Scientist, a 24 de março de 2009 in <https://www.newscientist.com/blogs/shortsharpscience/2009/03/ada-lovelace-day.html>;

SONNENBURG, S., BRAUN, Mikio L., ONG, Cheng Soon, BENGIO, Samy, BOTTOU, Léon, HOLMES, Geoffrey, LECUN, Yann, MÜLLER, Klaus-Robert, PEREIRA, Fernando, RASMUSSEN, Carl Edward, RÄTSCH, Gunnar, SCHÖLKOPF, Bernhard, SMOLA, Alexander, VINCENT, Pascal, WESTON, Jason, WILLIAMSON, Robert, ***The Need for Open Source Software in Machine Learning***, in *Journal of Machine Learning Research*, 2007, pp. 2449-2453;

SOUSA, Sérgio, ***Tecnologias de Informação – O Que São? Para Que Servem?***, 6.^a Edição, FCA, 2009;

SOUSA PINHEIRO, Alexandre, ***Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional***, AAFDL, Lisboa, 2015, pp. 639-663, 721-741;

SOUZA, Carlos, **O debate sobre personalidade jurídica para robôs**, Revista Jota, 10 de outubro de 2017, in <https://jota.info/artigos/o-debate-sobre-personalidade-juridica-para-robos-10102017>;

STEINBUCH, Karl, revista **Informatik: Automatische Informationsverarbeitung**, Standard Elektrik AG, Informatikwerk, SEG-Nachrichten, Heft 4, 1957;

SZEGEDY, Christian, **ZAREMBA**, Wojciech, **SUTSKEVER**, Ilya, **BRUNA**, Joan, **ERHAN**, Dumitru, **GOODFELLOW**, Ian, **FERGUS**, Rob, **Intriguing properties of neural networks**, International Conference on Learning Representations, 2014;

VALENTINO, Daniela, **Manuale di diritto dell'informatica**, 2ª Edição, Edizioni Scientifiche Italiane 2011, pp. 95-125.