Carlos André Ferreira Dias

A Privacidade na era da Internet das Coisas

Direitos de Personalidade e Proteção de Dados

Mestrado em Direito: Ciências jurídico-Civilísticas

Trabalho realizado sob a orientação de

Prof. Doutora Maria Raquel Guimarães

Outubro/2019

Esta tese foi elaborada no âmbito do projecto “It’s a wonderful (digital) world: O direito numa sociedade digital e tecnológica”, do CIJE — Centro de Investigação Jurídico-Económica, da Faculdade de Direito da Universidade do Porto

À minha orientadora.

Aos que me acompanham.

Ao Dr. Armindo, em especial.

"Ou bem que a história não tem sentido e futuro,

ou o seu sentido e futuro são os do Homem e seu progresso"

Orlando de Carvalho

"The Internet of Things has the potential to change the world,

just as the Internet did. Maybe even more so."

Kevin Ashton

RESUMO

A Internet evoluiu de uma rede que interligava computadores, para um novo conceito chamado Internet das Coisas, um sistema que interliga todo o tipo de objetos do nosso quotidiano permitindo que comuniquem entre si. Um dos principais desafios trazidos pela Internet das Coisas diz respeito à privacidade dos seus utilizadores. De facto, onde está a privacidade, numa nova era em que milhares de milhões de sensores incorporados nestes objetos são capazes de recolher, tratar e transferir, a todo o momento, todo o tipo de dados sobre os seus utilizadores?

O presente trabalho visa, assim, posicionar a privacidade no direito civil português num mundo que se encontra cada vez mais conectado. Para tal, partindo dos fundamentos da nossa Constituição, analisamos a proteção da personalidade levada a cabo pelo nosso Código Civil, para perceber se este está preparado para fazer face às novas ameaças à privacidade decorrentes das novas tecnologias e, em particular, da Internet das Coisas. Neste sentido, decidimos apresentar, com a pormenorização necessária, o conceito da Internet das Coisas, levantando de seguida as suas implicações em matéria de privacidade e proteção de dados.

Dada a grande proximidade destas questões com o Regulamento Geral de Proteção de Dados que recentemente entrou em vigor, pareceu-nos inevitável enquadrar aquelas implicações no caminho que a União Europeia parece querer seguir com este novo regime, atestando a compatibilidade de um fenómeno tecnológico tão invasivo, com um quadro regulatório, em princípio, apertado.

Por fim, numa época em que os dados pessoais possuem um valor incalculável e em que o controlo sobre eles está do lado das instituições, procuramos sugerir um modelo de mercado que, indo ao encontro deste panorama normativo, transfira para os titulares o papel ativo no controlo e na exploração – quiçá, monetária – dos seus dados pessoais.

Palavras-chave: Privacidade, Direitos de Personalidade, Proteção de Dados, Internet das Coisas, *IoT*, Regulamento Geral de Proteção de Dados, RGPD, *Descentralização Monetizada*

ABSTRACT

The Internet has evolved from a network that interconnected computers to a new concept called the Internet of Things, a system that interconnects all kinds of objects present in our daily lives, allowing them to communicate with each other. One of the main challenges brought by the Internet of Things has to do with the privacy of its users. In fact, where is privacy, in a new era where billions of sensors embedded in these objects are able to collect, process and transfer all kinds of data about their users, at all times?

The present work aims to place privacy in Portuguese civil law in a world that is increasingly connected. In this sense, starting from the foundations of our Constitution, we analyzed the protection of personality carried out by our Civil Code to see if it is prepared to face the new threats to privacy arising from new technologies and, in particular, from the Internet of Things. To this end, we decided to present, with the necessary detail, the concept of the Internet of Things, raising then the implications concerning privacy and data protection.

Given the proximity of these issues with the General Data Protection Regulation, which has recently come into force, it seemed inevitable to us to frame those implications on the path that the European Union seems to want to follow with this new regime, attesting to the compatibility of such an invasive technological phenomenon with a regulatory framework, which is, in theory, strict.

Finally, at a time when personal data is invaluable and where control over them is on the side of the institutions, we seek to suggest a market model that, in line with the legal landscape, transfers to the holders the active role in the control and exploitation – perhaps, monetary – of their personal data.

Keywords: Privacy, Personality Rights, Data Protection, Internet of Things, *IoT*, General Data Protection Regulation, GDPR, *Monetized Decentralization*

SUMÁRIO

1. Introdução 8
2. A proteção constitucional da privacidade 9
3. A proteção civil da privacidade 13
3.1 Pessoa e direitos de personalidade 13
3.2 O direito geral e os direitos especiais de personalidade 15
3.3 A privacidade como direito de personalidade 17
3.4 A limitação voluntária do direito à reserva sobre a intimidade da vida privada 21
4. A Internet das Coisas 24
4.1 Aproximação ao conceito 24
4.2 Casa e entretenimento 25
4.3 Saúde e *Fitness* 27
4.4 Cidades e mobilidade 28
4.5 Brinquedos inteligentes 30
4.6 A emergência de uma privacidade inteligente 31
5. A Internet das Coisas e o Regulamento Geral de Proteção de Dados 35
5.1 Controlo e Transparência 36
5.2 Consentimento 39
5.3 Limitação da finalidade e minimização dos dados 44
5.4 Categorias especiais 46
5.5 Decisões individuais automatizadas e definição de perfis 48
6. Proposta de Superação 50
6.1 A admissibilidade de uma *descentralização monetizada* 50
7. Conclusão 54
BIBLIOGRAFIA 55

SIGLAS E ABREVIATURAS

al.	alínea
art./arts.	artigo/artigos
BFD	Boletim da Faculdade de Direito
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CEJ	Centro de Estudos Judiciários
cit.	citado(a)
DPD	Diretiva 95/46/CE
FTC	Federal Trade Comission
GPS	Sistema de Posicionamento Global (do inglês, "*global positioning system"*)
GT29	Grupo de Trabalho do Artigo 29.º para a Proteção de Dados
IdC	Internet das Coisas
IoT	Internet das Coisas (do inglês "*Internet of Things*")
pág./págs.	página/páginas
Código *QR*	Código de Resposta Rápida (do inglês, "*Quick Response Code*")
RGPD	Regulamento Geral de Proteção de Dados
ROA	Revista da Ordem dos Advogados
SMS	Serviço de Mensagens Curtas (do inglês, *Short Message Service*)
ss.	seguintes
TFUE	Tratado sobre o Funcionamento da União Europeia
TJUE	Tribunal de Justiça da União Europeia
Trad.	Tradução
Vol.	Volume

1. Introdução

A tecnologia tem vindo a invadir o quotidiano das pessoas ao longo da história, colocando desafios novos ao direito. Foi assim, primeiramente, com a invenção da máquina a vapor (Indústria 1.0), depois com a eletricidade (Indústria 2.0), mais tarde com a automatização e a digitalização (Indústria 3.0) e, agora, com a integração de sistemas ciberfísicos e de inteligência artificial, e com a utilização do *big data*, da computação em nuvem e da internet das coisas (Indústria 4.0). Ora, a privacidade é, indubitavelmente, um dos domínios em que a força motriz da tecnologia mais se tem feito sentir ao longo dos séculos, sendo, de resto, indesmentível, a influência principal desta última na proteção que o direito vai conferindo àquela. É por isso que faz sentido, em plena revolução digital, dedicar um estudo à privacidade, neste caso, à sua relação com um dos pilares dessa revolução tecnológica: a Internet das Coisas (do inglês, *Internet of Things – IoT*).

Numa tese de mestrado em Ciências-jurídico-Civilísticas, abordaremos, claro está, a proteção da privacidade levada a cabo pelo nosso Código Civil. Nesse sentido, partimos do enquadramento jusfundamental da privacidade na Constituição, para chegar à centralidade da pessoa no direito civil e ao elenco de direitos de personalidade responsável pela tutela da privacidade. Aqui chegados, analisamos a possibilidade de limitação voluntária dos direitos de personalidade, em particular, do direito à reserva sobre a intimidade da vida privada. Concretamente, na senda da presente revolução tecnológica, em que se esbatem as fronteiras entre um mundo físico e um mundo virtual, quisemos perceber se podemos continuar a assumir a privacidade como uma projeção una e intransmissível da pessoa e da sua dignidade, ou se, por outro lado, os novos tempos toleram uma gradual disponibilidade e patrimonialização da intimidade de cada um.

De seguida, dedicamos uma atenção detalhada ao conceito da Internet das Coisas, para tentar perceber quais as suas potenciais implicações em matéria de privacidade e proteção de dados. Trata-se, de facto, de um conceito complexo, pelo enorme volume e variedade de dados pessoais recolhidos e pela complexidade dos tratamentos a que são sujeitos após a recolha, por parte, de resto, de outras tecnologias emergentes como a Inteligência Artificial, a *machine learning* e o *Big Data*. Por isso, importa esclarecer, por um lado, que, sem prejuízo da proteção da privacidade em legislação especial, o presente trabalho se debruça apenas sobre o estudo da privacidade, em sentido estrito, do Código Civil. Depois, não obstante algum

enquadramento oportuno sobre outro fenómeno tecnológico conexo, o foco incidirá sobretudo sobre a Internet das Coisas e as aplicações desta que diretamente se reflitam na privacidade do indivíduo. Domínios como a indústria, a agricultura, a aviação, ou questões relacionadas com o indivíduo-trabalhador, estão, assim, à partida, fora do nosso intento, num trabalho que se pretende direto, incisivo e pouco descritivo.

Porque um trabalho que aborda a relação da privacidade com a tecnologia nos leva inevitavelmente à proteção de dados, pareceu-nos imperioso, pelo menos, aproveitar a atualidade regulatória nesta matéria para perceber quais os principais desafios colocados pelo Regulamento Geral de Proteção de Dados ao desenvolvimento da Internet das Coisas. Há, de facto, uma grande expetativa quanto à questão de saber da compatibilidade de um quadro normativo, por natureza, protecionista, com uma inovação tecnológica vista como disruptiva em todos os quadrantes.

Finalmente, quisemos propor uma solução de mercado que fosse ao encontro desta conjuntura, tentando harmonizar o direito e a informática num desenlace amigável, numa altura em que estas áreas do saber parecem continuar, preocupantemente, cada vez mais apartadas.

2. A proteção constitucional da privacidade

A Constituição da República portuguesa – tal como veremos acontecer com o Código Civil em matéria de direitos de personalidade – ocupa um lugar de destaque no panorama internacional ao nível da proteção da privacidade. Com efeito, não obstante o berço comum da proteção jusfundamental das constituições modernas, estabelecido nas revoluções liberais, é possível encontrar entre elas diferenças significativas sobretudo no que toca ao reconhecimento dos direitos do individuo face à informática[1]. Na verdade, há neste âmbito uma evidente resistência por parte do legislador constitucional dada a "natureza fortemente instável do objeto de regulamentação"[2], que se encontra em permanente evolução, como de resto testemunha a acuidade do tema que serve de mote a este trabalho. De facto, o nosso

[1] Para um estudo comparado das Constituições europeias quanto à consagração de um preceito especial em matéria de proteção de dados pessoais, v. C. SARMENTO E CASTRO, *Direito da informática, privacidade e dados pessoais*, Coimbra, Almedina, 2005, pág. 32, nota 33.
[2] JORGE MIRANDA e RUI DE MEDEIROS, *Constituição Portuguesa Anotada*, Tomo I, Coimbra, Coimbra Editora, 2010, pág. 783.

ordenamento jurídico-constitucional consagra uma "dicotomia protecional"[3] da privacidade, através, simultaneamente, dos arts. 26.º e 35.º.

Poderíamos caracterizar a conceção do art. 26.º de igualmente dicotómica: por um lado, ao reunir em si mesmo sete direitos distintos pretende, sem prejuízo da sua diversidade, equipará-los num objectivo comum de "proteção de uma esfera nuclear das pessoas e da sua vida", correspondente aos direitos de personalidade do Código Civil. Por outro, sob a epígrafe "outros direitos pessoais", parece querer inserir-se na mesma categoria dos direitos à vida e à integridade física dos arts. 24.º e 25.º, imediatamente anteriores[4].

De um ponto de vista material, a previsão constitucional do direito à reserva da intimidade da vida privada e familiar (26.º n.º 1 *in fine* e n.º 2) radica naquele que é "a pedra angular do ordenamento jurídico (e social e ético) português"[5], o princípio da dignidade humana, que a Constituição consagra logo no seu art. 1.º como "valor básico logicamente anterior à própria ideia do Estado de Direito democrático e que constitui a referência primeira em matéria de direitos fundamentais"[6]. Neste contexto, e como veremos adiante, trata-se de um direito que se pode desdobrar em dois direitos menores: um direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e outro a impedir que essas informações sejam divulgadas[7].

O art. 26.º constitui também a "sede fundamental do direito geral de personalidade"[8], tipificando, ainda, uma série de direitos especiais de personalidade. O legislador consagra ainda neste artigo, desde 1997, um direito ao desenvolvimento da personalidade – considerado um "reflexo constitucional"[9] ou uma "projeção dinâmica"[10] do direito à reserva sobre a intimidade da vida privada –, inspirado na Lei Fundamental Alemã, o qual comporta

[3] C. SARMENTO E CASTRO, "40 anos de "utilização da informática" – o artigo 35.º da Constituição da República Portuguesa", *Revista e-Pública*, Vol. 3, N.º 3, 2016, pág. 50.
[4] J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa – Anotada*, Vol. I, Coimbra, Coimbra Editora, 2007, pág. 461.
[5] LUÍSA NETO, *Código Civil Anotado*, Coimbra, Almedina, 2017, pág. 121.
[6] JORGE MIRANDA e RUI DE MEDEIROS, cit., pág. 607.
[7] J. GOMES CANOTILHO e VITAL MOREIRA, v. pág. 467. Os autores indicam ainda o direito à inviolabilidade do domicílio e da correspondência (art. 34.º), como garantia deste. Também JORGE MIRANDA e RUI DE MEDEIROS entendem o referido artigo "um regime especial de tutela do direito à reserva da intimidade da vida privada", cit., pág. 756. Refiram-se, ainda, os arts. 32.º n.º 8 e 268.º n.º 2.
[8] JORGE MIRANDA e RUI DE MEDEIROS, "a consagração deste direito postula a tutela abrangente de todas as formas de lesão de bens de personalidade independentemente de estarem ou não tipicamente consagrados", cit., pág. 607.
[9] C. SARMENTO E CASTRO, *Direito da informática…*, 2005, pág. 22.
[10] LUÍSA NETO, *Código Civil Anotado*, pág. 118.

duas dimensões: o direito geral de personalidade e a liberdade geral de acção[11]. O art. 26.º n.º 2 estabelece ainda uma imposição legiferante que obriga o Estado, não só a respeitar, como a estabelecer garantias contra a obtenção e utilização abusivas de informações, seja por entidades públicas ou privadas.

Já o art. 35.º amplia a proteção constitucional da privacidade do individuo, mas, desta vez, face às ameaças susceptíveis de advir do tratamento informatizado dos seus dados, elencando uma série de direitos que consubstanciam o "moderno" direito à autodeterminação informacional[12]. De facto, desde 1976 que a Constituição protege a privacidade da "ameaça tecnológica", num preceito que fez dela pioneira e, para J. BACELAR GOUVEIA, "o documento constitucional mais aperfeiçoado na proteção conferida à pessoa relativamente à informática"[13]. E a verdade é que, mais de 40 anos depois, a tutela do indivíduo relativamente ao uso da informática nunca se mostrou tão necessária, tendo em conta, na esteira de JORGE MIRANDA e RUI DE MEDEIROS, "o alargamento das possibilidades de recolha e de armazenamento de dados relativos ao cidadão individual por parte de entidades privadas e poderes públicos, e a facilidade e a velocidade de acesso e de cruzamento de todos esses dados", situação agora extremada na senda de uma nova revolução digital, e tornando, como nunca antes, "justificado o receio da construção de um *Big Brother* no mais puro sentido *orwelliano*"[14]. São, de resto, esses progressos tecnológicos sucessivos que fazem do art. 35.º "um preceito em devir", referido a "uma realidade em cada momento tecnologicamente datada" e carente de uma "necessidade de adaptação evolutiva"[15], tendo, por isso, sido alvo de diversas revisões constitucionais até à sua formulação atual[16].

Este direito à autodeterminação informacional é, antes de mais, um direito ao controlo por parte do indivíduo sobre os seus dados pessoais, permitindo-lhe, se assim o entender, dispor

[11] Sobre as diferenças entre a previsão alemã e a portuguesa, *vide* JORGE MIRANDA e RUI DE MEDEIROS, págs. 612 e ss. Também GOMES CANOTILHO e VITAL MOREIRA tentam densificar o direito ao desenvolvimento da personalidade, v. págs. 463 e ss. Para um estudo mais aprofundado, v. P. MOTA PINTO, "O direito ao livre desenvolvimento da personalidade", *Direitos de Personalidade e Direitos Fundamentais – Estudos*, Gestlegal, 2018, págs. 7-122.

[12] JORGE MIRANDA e RUI DE MEDEIROS definem-no como o "direito de cada indivíduo dispor livremente dos respetivos dados e informações pessoais e, assim, determinar os termos de acesso e utilização por terceiros desses mesmos dados e informações", cit., pág. 620.

[13] J. BACELAR GOUVEIA, "Os direitos fundamentais à proteção dos dados pessoais informatizados", *ROA*, N.º 3, Lisboa, 1991, pág. 706, nota 22.

[14] JORGE MIRANDA e RUI DE MEDEIROS, cit., pág. 788.

[15] C. SARMENTO E CASTRO, "40 anos de…", págs. 64 e 65.

[16] O art. 35.º foi alterado nas revisões constitucionais de 1982, 1989 e 1997. Sobre as revisões constitucionais que introduziram alterações ao art. 35.º, *vide* C. SARMENTO E CASTRO, "40 anos de…", págs. 46 e ss.

deles e definir em que condições[17]. Trata-se de um direito que se desdobra principalmente em três direitos: um *direito de acesso* aos registos informáticos para conhecimento dos dados pessoais (n.º 1), um *direito ao não tratamento de dados sensíveis*[18] (n.º 3) e ainda um *direito ao sigilo dos dados* em relação a terceiros e um *direito à não interconexão* de ficheiros com dados da mesma natureza (n.º 4). O n.º 1 prevê, ainda, uma série de outros direitos: o *direito ao conhecimento da identidade dos responsáveis e ao esclarecimento* sobre a finalidade do tratamento dos dados; o *direito de contestação*, ou seja, à retificação dos dados e sobre a identidade e o endereço do responsável; o *direito de atualização* dos dados; e ainda o *direito à eliminação* dos dados cujo registo é proibido[19].

Neste sentido, o art. 35.º é, simultaneamente, um "direito de defesa e um direito de liberdade com um conteúdo negativo", na medida em que o indivíduo pode recusar o tratamento de certas informações, mas assume também uma "dimensão positiva", enquanto conjunto de poderes e faculdades de controlo sobre os dados pessoais que, "prevenindo e corrigindo lesões da liberdade individual", dão corpo àquilo que se tem chamado de *Habeas Data*, a "garantia de uma liberdade de natureza fundamental dos tempos modernos"[20].

Realçariamos, afinal e como veremos, a proibição da interconexão dos dados como, possivelmente, a garantia mais relevante na era da Internet das Coisas, contra o chamado "perigo da concentração"[21], susceptível, como defendem JORGE MIRANDA e RUI DE MEDEIROS a propósito do n.º 5[22], de gerar "uma imagem completa da pessoa capaz de identificar todos os seus movimentos, os seus bens, as suas doenças, as suas crenças, em suma, todos os espaços mais recônditos da sua vida privada e pessoal"[23].

[17] Como escrevem JORGE MIRANDA e RUI DE MEDEIROS, "abrange todos os poderes e faculdades que permitem garantir que a pessoa não é usada como fonte de informação para terceiros contra a sua vontade, podendo além disso controlar a informação que é fornecida e os termos e abrangência em que ela é tratada", cit., pág. 786.

[18] JORGE MIRANDA e RUI DE MEDEIROS definem dados sensíveis como "elementos de informação cujo tratamento informático além de poder contender com a privacidade do seu titular, pode dar origem a tratamentos desiguais ou discriminatórios", cit., pág. 797.

[19] Seguimos aqui o elenco apresentado por J. GOMES CANOTILHO e VITAL MOREIRA, pág. 551.

[20] JORGE MIRANDA e RUI DE MEDEIROS, cit., pág. 789.

[21] GOMES CANOTILHO e VITAL MOREIRA, cit., pág. 555.

[22] O art. 35.º n.º 5 proíbe, desde 1976, a atribuição de um número nacional único aos cidadãos, tal como se chegou a projetar no passado em Portugal. Para mais detalhes sobre este tema, v. C. SARMENTO E CASTRO, "40 anos…", págs. 56 e ss.

[23] JORGE MIRANDA e RUI DE MEDEIROS, cit., págs. 788 e 789.

3. A proteção civil da privacidade

3.1 Pessoa e direitos de personalidade

Nunca será demais relembrar a ideia segundo a qual um qualquer direito civil parte da *Pessoa*. Efetivamente, e como estatui a capital doutrina de ORLANDO DE CARVALHO sobre esta matéria, "é inconcebível um direito civil sem *cives*, isto é, sem homens cuja energia moral – a que compete a cada homem como homem – é fonte e a razão de efeitos jurídicos autênticos"[24]. A pessoa, como bem a define este autor, "é o ser humano vivo que, pela sua estrutura físico-psíquica e pela sua capacidade de conhecimento e de amor, é o único verdadeiro centro de decisão e de imputação, de liberdade e de responsabilidade, na natureza e na história, assumindo-se como um projeto autónomo e transformante de si mesmo e do mundo"[25]. É o reconhecimento, pelo direito, desta *Pessoa*, que é humana e já não burguesa, e do seu progresso, que legitima uma ordem jurídica e sem a qual "não só o direito civil é acéfalo como qualquer Direito ou Ramo de Direito é uma violência monstruosa"[26]. É por isso que, desde a Grande Revolução, os Direitos do Homem passaram a figurar em quase todas as Constituições europeias e, não obstante a ensombrada suspensão que sofreram até ao final da Segunda Guerra, ressurgiram em defesa de uma "consciência de classe" numa sociedade capitalista e de consumo enquanto "direitos da pessoa concreta e socialmente *engagée*" continuando a atuar, hoje, como "um autêntico germe de inconformismo indestrutível"[27].

---

[24] ORLANDO DE CARVALHO, "Os Direitos do Homem no Direito Civil Português", *Teoria Geral do Direito Civil*, Coimbra Editora, Coimbra, 2012, cit., pág. 227. Como escreve C. A. MOTA PINTO, "o reconhecimento pelo direito civil – ou por qualquer outro – da ideia de pessoa ou de personalidade começa por ser, para além de um princípio normativo, a aceitação de uma estrutura lógica sem a qual a própria ideia de Direito não é possível", *Teoria Geral do Direito Civil*, Coimbra, Coimbra Editora, 4ª edição, 2ª reimpressão, 2012, cit., pág. 98. Ou, nas palavras de R. CAPELO DE SOUSA, "a pessoa humana – toda e qualquer pessoa humana – é o bem supremo da nossa ordem jurídica, o seu fundamento e o seu fim", *O Direito Geral de Personalidade*, Coimbra, Coimbra Editora, 1995, cit., pág. 97.

[25] ORLANDO DE CARVALHO, "Para uma Teoria da Pessoa Humana (Reflexões para uma desmitificação necessária)", *Teoria Geral do Direito Civil*, Coimbra, Coimbra Editora, 2012, cit., págs. 255 e 256. Para D. COSTA GONÇALVES, "Pessoa é aquele ente que, em virtude da especial intensidade do seu acto de ser, autopossui a sua própria realidade ontológica, em abertura relacional constitutiva e dimensão relacional unitiva", *Pessoa e Direitos de Personalidade: Fundamentação ontológica da tutela*, Almedina, 2008, cit., pág. 64. Sobre a origem e evolução do conceito de "pessoa" e dos seus direitos, v. D. LEITE CAMPOS, "Lições de Direitos da Personalidade", 2ª edição, reimpressão, *Separata do Vol. LXVI (1990) do BFD*, Coimbra, 1995, págs. 9 e ss. Também, LUÍSA NETO, *O Direito fundamental à disposição sobre o próprio corpo*, Coimbra Editora, 2004, págs. 183 e ss.

[26] ORLANDO DE CARVALHO, "Para uma Teoria…", cit., pág 267.

[27] ORLANDO DE CARVALHO, "Os Direitos do Homem…", págs. 226 e 227.

Mas, não é só a *Pessoa* que "pré-existe"[28] ao Direito, também a personalidade humana[29] é "um *prius*" da personalidade jurídica e o seu "alicerce"[30]. Na verdade, é a personalidade humana que faz "grandes reivindicações" à ordem jurídica quanto ao reconhecimento da personalidade jurídica: desde logo, exige a sua *essencialidade*, porque a personalidade jurídica é essencial e pressupõe a personalidade humana; a *indissolubilidade*, pois a personalidade jurídica é indissolúvel da personalidade humana; e a *ilimitabilidade*, dado que ambas são ilimitadas na mesma medida[31]. É esta ilimitabilidade que reclama ao direito um conjunto de condições para que o indivíduo possa ser pessoa, "o «minimum» necessário e imprescindível"[32] ao conteúdo da personalidade, a que damos o nome de direitos de personalidade.

Ao contrário da opção assumida no Código de Seabra no que toca aos "direitos originários", o atual Código Civil não prevê uma noção de direitos de personalidade[33]. Porém, não obstante a compreensível resistência inicial relativamente à existência privatística dos direitos de personalidade e as críticas quanto ao seu conceito[34], os direitos de personalidade são hoje aceites como direitos que "incidem sobre a própria pessoa ou sobre alguns fundamentais modos de ser, físicos ou morais, dessa personalidade, e que inerem, portanto, à pessoa humana"[35]. Entre as suas características destacarimos a sua *absolutidade*, porque são oponíveis *erga omnes* – mas aos quais não se contrapõe um mero dever de abstenção, mas um

[28] ORLANDO DE CARVALHO, "Para uma Teoria…", pág. 255.

[29] Para R. CAPELO DE SOUSA, personalidade é "o real e o potencial físico e espiritual de cada homem em concreto, ou seja, o conjunto autónomo, unificado, dinâmico e evolutivo dos bens integrantes da sua materialidade física e do seu espirito reflexivo, sócio-ambientalmente integrados", cit., pág. 117. D. COSTA GONÇALVES define-a como "o conjunto das qualidades e relações que determinam a pessoa em si mesma e em função da participação na ordem do ser", cit., pág. 68.

[30] ORLANDO DE CARVALHO, "Os Direitos do Homem…", págs. 228 e 229. Como escreve o autor, "a personalidade humana é, pois, o *cur*, o *quando* e o *quantum* da personalidade jurídica".

[31] Neste ponto, v. ORLANDO DE CARVALHO, "Os Direitos do Homem…", págs. 230 e ss.

[32] ADRIANO DE CUPIS, *Direitos da Personalidade*, Lisboa, Livraria Morais Editora, Trad., 1961. Para o autor, estes direitos são "a medula da personalidade" e "se não exitissem, a pessoa não existiria enquanto tal", cit., págs. 17 e 18.

[33] O Código Civil de Seabra, de 1867, definia os então "direitos originários", no art. 359.º, como "*os que resultam da própria natureza do homem, e que a lei civil reconhece, e protege como fonte e origem de todos os outros*". Preceituava, depois, o art. 368.º, as características destes direitos: "*os direitos originários são inalienáveis e só podem ser limitados por lei formal e expressa. A violação deles produz a obrigação de reparar a coisa*". Para um estudo mais aprofundado em torno do reconhecimento legislativo e jurisprudencial dos direitos de personalidade no direito civil português, v. A. MENEZES CORDEIRO, "Os Direitos de Personalidade na Civilística Portuguesa", *ROA*, 2001, págs. 1229-1256. Também A. F. MORAIS ANTUNES, *Comentário aos Artigos 70.º a 81.º do Código Civil (Direitos de personalidade)*, Lisboa, Universidade Católica Editora, 2012, págs. 17 e ss., P. PAIS DE VASCONCELOS, *Direito de Personalidade*, Coimbra, Almedina, 2017, págs. 11 e ss. e D. COSTA GONÇALVES, págs. 70 e ss.

[34] Sobre este assunto, v. P. MOTA PINTO, "O Direito à Reserva sobre a Intimidade da Vida Privada*"*, *BFD*, Vol. LXIX, Coimbra, 1993, págs. 484 e ss.

[35] P. MOTA PINTO, cit., pág. 482.

dever geral de respeito –, a sua *pessoalidade*, não só no sentido da sua não patrimonialidade mas sobretudo pela sua ligação incindível à pessoa do seu titular, e ainda a sua *relativa indisponibilidade*, na medida em que, embora não sejam transmissíveis (*inter vivos* ou *mortis causa*) nem renunciáveis, o seu titular pode consentir na sua limitação, nos termos do disposto no art. 81.º[36].

De facto, o reconhecimento de um sólido regime de tutela da pessoa nunca se mostrou tão necessário, tendo em conta, como veremos, a proliferação e, sobretudo, a sofisticação das ameaças colocadas ao indivíduo do século XXI, em particular, pela tecnologia, que tem vindo, ao longo dos tempos, a deixar o homem "transformado em máquina ou quase devorado pelo poder da cibernética"[37]. Como defende M. RAQUEL GUIMARÃES, "só uma disciplina civilística verdadeiramente «humanista», consciente do papel fundacional da pessoa humana no seu seio, que se assuma como um Direito que nasce e vive ao serviço da pessoa humana, poderá acompanhar o «admirável mundo novo» em que vivemos"[38].

3.2 O direito geral e os direitos especiais de personalidade

Queremos admitir a existência de um direito geral de personalidade no Código Civil português. Também aqui o nosso regime acolheu a solução apresentada pelo sistema alemão, no qual coexiste um direito geral de personalidade com vários direitos especiais de personalidade[39]. Desde logo, é nesse sentido que vai o art. 70.º n.º 1, que, sob a epígrafe, "tutela geral da personalidade", estatui que "a lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral". Segundo R. CAPELO DE SOUSA, seu principal defensor e estudioso, este direito geral de personalidade é "o direito de cada homem ao respeito e à promoção da globalidade dos elementos, potencialidades e expressões da sua personalidade humana bem como da unidade psico-fisico-sócio-ambiental dessa mesma personalidade humana"[40].

[36] Este é um tema que aprofundaremos mais à frente no ponto 3.4.
[37] ORLANDO DE CARVALHO, "Os Direitos do Homem…", cit., pág. 235.
[38] M. RAQUEL GUIMARÃES, "A tutela da pessoa e da sua personalidade como fundamento e objeto da disciplina civilística. Questões atuais", *La famiglia nella società contemporânea*, Roma, Aracne editrice, 2016, cit., pág. 192.
[39] Sobre o reconhecimento do direito geral de personalidade noutros ordenamentos, v. P. MOTA PINTO, págs. 492 e ss.
[40] R. CAPELO DE SOUSA, cit., pág. 93.

De facto, o reconhecimento de uma construção normativa desta natureza é reclamado, antes de mais, pela própria personalidade humana – ou, se quisermos, pela ilimitabilidade da personalidade jurídica[41] – enquanto estrutura complexa, relacional e dinâmica, que impõe à ordem jurídica a criação de um meio capaz de a proteger em todas as suas "manifestações previsíveis e imprevisíveis", um direito à "pessoa-ser em devir", um "*jus in se ipsum* radical", reflexo de um direito ao livre desenvolvimento da personalidade[42]. Isto porque, claro está, essa tutela não pode ser conferida absolutamente pela – sóbria e, inevitavelmente, desatualizada – previsão normativa dos direitos especiais de personalidade. Como muito bem realçam M. REGINA REDINHA e M. RAQUEL GUIMARÃES, "a complexidade da personalidade humana e a constante evolução social e técnica não são compatíveis com um elenco taxativo de direitos de personalidade, com uma enumeração exaustiva de todos os aspetos da personalidade merecedores de proteção"[43]. Efetivamente, a par da complexidade da personalidade humana, existe uma correspondente realidade social igualmente complexa e metamórfica, cuja evolução tem sido fortemente dominada pelos avanços tecnológicos que se têm feito sentir em todos os domínios da nossa sociedade. Assim, como "não é possível nem desejável"[44] alcançar um elenco de direitos de personalidade susceptível de abarcar todas as dimensões da personalidade humana, devemos aceitar a necessidade de reconhecer um direito

[41] Neste sentido, M. REGINA REDINHA e M. RAQUEL GUIMARÃES, "O uso do correio eletrónico no local de trabalho: algumas reflexões", *Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria*, Coimbra Editora, 2003, pág. 653. Também P. MOTA PINTO, pág. 495.

[42] ORLANDO DE CARVALHO, "Teoria Geral do Direito Civil", *Teoria Geral do Direito Civil*, Coimbra, Coimbra Editora, 2012, pág. 203. Aproveitamos a definição de "homem" apresentada por R. CAPELO DE SOUSA: "um ser eminentemente dinâmico, evolutivo, com um ciclo próprio de vida animal, com uma trajetória particular de existência moral e integrado num processo humano comunitário, em que proprio género humano evolui", cit., pág. 117.

[43] Como referem M. REGINA REDINHA e M. RAQUEL GUIMARÃES, "as possíveis agressões à personalidade multiplicam-se e diversificam-se ao mesmo ritmo que se desdobram os meios tecnológicos à disposição do consumidor (…) Já anteriormente a industrialização, o desenvolvimento urbano e a proteção do ambiente tinham desencadeado a aplicação dos direitos de personalidade em situações novas e levaram os tribunais a reconhecer um direito à saúde, ao sono, ao repouso, à qualidade de vida e a um ambiente de vida humano e sadio, não tipificados na lei (…)", cit., pág. 652. Também R. CAPELO DE SOUSA alertava para esta realidade: "a complexidade da vida moderna, a crescente especialização dos trabalhos e das atividades, as sinuosidades dos mecanismos de troca e de redistribuição de bens e serviços, a competição e o "stress", a inelutável intervenção do Estado na vida socio-económica, a informatização, o crescimento e o refinamento das tecnologias interferentes na vida privada, familiar e profissional dos indivíduos. Tudo o que implica uma tutela horizontal e vertical da personalidade, respetivamente, a mais ampla e a mais funda possível, e dotada do máximo possível de unidade e de coerência", cit., pág. 115.

[44] R. CAPELO DE SOUSA, cit., pág. 202.

geral de personalidade para impedir que a tutela juscivilistica da pessoa se torne lacunosa numa realidade em permanente mudança[45].

Um direito geral de personalidade concebido nestes termos, aproximar-se-á, para ORLANDO DE CARVALHO de um "direito-matriz ou fundante"[46], ou, como prefere R. CAPELO DE SOUSA, de um "direito-mãe, ou direito-fonte" que, "tendo como objeto a personalidade humana no seu todo, fundamenta, enforma e serve de princípio geral mesmo aos próprios direitos especiais de personalidade"[47]. Este direito geral de personalidade não é, assim, "um mero suprimento da escassez dos direitos de personalidade especiais, nem uma súmula desses direitos"[48], mas antes, a raiz onde esses direitos vão entroncar, enquanto "formas descentralizadas" e "projeções do objeto verdadeiro desta tutela jurídica, que é a personalidade no seu todo"[49].

3.3 A privacidade como direito de personalidade

A tutela juscivilística da privacidade decorre, já sabemos, da dignidade de cada pessoa, a qual, na esteira de R. CAPELO DE SOUSA, lhe confere autonomia física e moral "na condução da

[45] Como entende ORLANDO DE CARVALHO, "só um tal direito ilimitado e ilimitável permite uma tutela suficiente do homem ante os riscos de violação que lhe oferece a sociedade contemporânea", "Teoria Geral…", cit., pág. 203. M. RAQUEL GUIMARÃES lembra que "o legislador que esteve na base da elaboração do Código Civil nunca poderia ter antecipado as exigências que a tutela da personalidade humana iria fazer ao direito, à época nem sequer equacionáveis remotamente como ficção científica", cit., pág. 192. Neste sentido, também P. PAIS VASCONCELOS, pág. 62. Mais em jeito de crítica ao regime do Código Civil, LUÍSA NETO, afirma que "[se] protegem no Código Civil direitos como cartas missivas confidenciais e/ou pseudónimo e minimizam-se (ou remetem-se para o direito geral da personalidade) aspetos muito mais relevantes dessa mesma personalidade". A autora explica: "Basta atentar em que, dos dez preceitos atinentes a particulares objetos de tutela (72.º a 81.º), quatro referem-se a cartas e outros escritos. Há-de convir-se que, num juízo actual, este âmbito normativo de proteção incide sobre uma dimensão da personalidade em progressiva perda de significado pessoal e social, não se justificando este detalhe regulador", "Direitos (fundamentais) de personalidade?", *in Pessoa, Direito e Direitos*, DHCII/EDUM, 2016, cit., págs. 275 e 276. No mesmo sentido, J. SOUSA RIBEIRO, entende que "a enumeração que o Código Civil contém dos concretos modos de ser em que a personalidade se projeta é parca e algo desatualizada", acrescentando que, "são silenciadas dimensões hoje expostas a riscos sérios de ação lesiva, como, por exemplo, em toda a área de utilização de meios informáticos e das tecnologias de informação e comunicação", "Os Direitos de Personalidade como Direitos Fundamentais", *in Pessoa, Direito e Direitos*, DHCII/EDUM, 2016, cit., pág. 259.

[46] ORLANDO DE CARVALHO, "Teoria Geral…", cit., pág. 206.

[47] R. CAPELO DE SOUSA, cit., pág. 559. Também M. RAQUEL GUIMARÃES fala de um "direito progenitor", v. pág. 179.

[48] ORLANDO DE CARVALHO, "Para uma Teoria…", cit., pág. 263.

[49] ORLANDO DE CARVALHO, "Teoria Geral…", cit., pág. 206. Sobre a tipicidade dos direitos de personalidade, v. P. PAIS VASCONCELOS, págs. 64 e ss. Num sentido crítico ao reconhecimento de um direito geral de personalidade, defendendo um elenco de direitos especiais de personalidade em regime de *numerus apertus*, v. J. DE OLIVEIRA ASCENSÃO, *Direito Civil - Teoria Geral*, Vol. I, Coimbra Editora, 2000, págs. 86 e ss. e A. F. MORAIS ANTUNES, pág. 62.

sua vida, na auto-atribuição de fins a si mesmo, na eleição, criação e assunção da sua escala de valores, na prática dos seus atos, na reavaliação dos mesmos e na recondução do seu comportamento". É esta autonomia, conjugada com a complexidade da realidade em que vivemos – a mesma que impõe o reconhecimento de um direito geral de personalidade nos moldes tratados anteriormente – que leva a que o direito proteja um ambiente íntimo onde cada um "possa recolher-se, pensar-se a si mesmo, avaliar a sua conduta, retemperar as suas forças e superar as suas fraquezas"[50]. De resto, é daquele direito geral de personalidade que ORLANDO CARVALHO retira um direito à inviolabilidade pessoal, do qual, o direito à privacidade é uma projeção vital[51].

A privacidade é protegida de uma realidade complexa, em que a principal ameaça é, e sempre foi, a tecnologia. Na verdade, como refere M. JANUÁRIO GOMES, a propósito do advento do computador, "o nascimento da necessidade de tutelar juridicamente a existência duma zona íntima ou privada nasceu duma particular evolução da técnica"[52], a qual vai impondo uma necessidade de atualização contínua ao direito, em particular, à proteção conferida à pessoa e à sua personalidade, vulnerabilizadas a cada inovação concebida. Foi assim inicialmente com o microfone, com as primeiras técnicas de impressão e fotografia, depois com o telégrafo e o telefone, mais tarde com o computador e a internet, como será agora, numa nova revolução digital marcada pela ubiquidade e incomensurabilidade das informações pessoais[53]. Serão,

[50] Neste ponto, R. CAPELO DE SOUSA, cit., pág. 317.
[51] ORLANDO DE CARVALHO, "Para uma Teoria…", págs. 255 e 256, nota 69.
[52] O autor explica que "a intimidade só mereceu a atenção dos homens do Direito quando, nos fins do século passado, começou, muito timidamente a princípio, aquilo a que alguém chamou a revolução da informação", M. JANUÁRIO GOMES, "O problema da salvaguarda da privacidade antes e depois do computador", *Separata do "Boletim do Ministério da Justiça"* (319), Lisboa, 1982, cit., pág. 8. Também R. AMARAL CABRAL repara, neste sentido, que "confinada até há bem pouco tempo a uma tutela indirecta decorrente da proteção legal do nome, da imagem, da honra e da liberdade e segurança individuais, a defesa autónoma da vida privada surgiu, na época contemporânea, associada a alguns dos caracteres específicos da denominada civilização industrial (…) o desenvolvimento das técnicas de informação (…) enfim, a criação de condições de vida inconciliáveis com qualquer possibilidade de isolamento foram alguns dos fatores que determinaram um vasto movimento internacional conducente à prodigalização, pelas múltiplas ordens jurídicas internas, de vigorosa proteção legal à intimidade da vida privada", "O Direito à intimidade da vida privada", *Estudos em memória do Professor Doutor Paulo Cunha*, Lisboa, 1989, pág. 385. Também GUILHERME DRAY, *Direitos de Personalidade - Anotações ao Código Civil e ao Código do Trabalho*, Almedina, 2006, pág. 54.
[53] Sobre o surgimento do computador escreve M. JANUÁRIO GOMES: "salto técnico espetacular que determinará a necessidade de repensar o direito à intimidade da vida privada como ponto vulnerável da moderna sociedade técnica e, mais latamente, todos os direitos de personalidade", cit., pág. 10. A este propósito, R. AMARAL CABRAL, sobre a influência da técnica na tutela da vida privada, refere que a doutrina americana distingue três fases na evolução legislativa: a era pré-tecnológica (1780-1880); a era do primeiro desafio tecnológico (1880-1950), referente à invenção do microfone, da fotografia, do telefone e da gravação de sons; e a era do segundo desafio tecnológico (1950 até à atualidade), marcada pelos procedimentos eletrónicos de deteção, reprodução e informatização, v. pág. 389.

certamente, novos tempos de "*assault on privacy*" cujo impacto no conceito de privacidade merece ser estudado[54].

Já a recondução da proteção da privacidade à tutela da personalidade, também merece aqui especial destaque porque nem sempre foi assim. Com efeito, a privacidade começou por ser uma prerrogativa classista, regalia de um grupo social específico, a burguesia, e inicialmente ligado à proteção da propriedade privada[55]. A migração do direito à privacidade para o domínio dos direitos fundamentais, só aconteceu no final do século XIX, muito graças a uma publicação assinada pelos americanos S. WARREN e L. BRANDEIS, que defendia a preservação de um "espaço vital" que defendesse o indivíduo da intromissão alheia[56]. Publicação que, por sua vez, desencadeou um movimento democratizador do direito à intimidade que redundaria, mais tarde, na *misery of privacy,* uma gradual perda de significado do conceito, que, "por tudo abranger, acaba por não ter conteúdo"[57].

Embora com uma abrangência mais restrita que o anglo-saxónico "*right to be let alone*", o nosso Código Civil, consagrou, no art. 80.º, um direito especial de personalidade à reserva sobre a intimidade da vida privada. Na verdade, o reconhecimento da personalidade e da privacidade no direito civil sempre andaram ligados e se influenciaram mutuamente, como referem M. REGINA REDINHA e M. RAQUEL GUIMARÃES, "toda a evolução da questão do reconhecimento de verdadeiros direitos subjetivos incidentes sobre as várias manifestações da personalidade humana foi sempre fortemente condicionada pelas tomadas de posição em sede de privacidade"[58]. Este direito à reserva sobre a intimidade da vida privada atribui à

[54] Como escreve LUÍSA NETO, "o âmbito de proteção do direito à reserva da vida privada exige hoje, no mundo atual, uma configuração obviamente distinta daquela a que se referia Brandeis no final do século XIX. Não nos iludamos: a questão hoje em dia deslocou-se da discussão sobre «o que cabe no âmbito de proteção» para a necessidade de tutela face a novos meios de violação", *Código Civil Anotado*, cit., págs 120 e 121.

[55] Neste sentido, M. JANUÁRIO GOMES, "a intimidade é, portanto, um privilégio duma classe, é um índice dum certo "status" social, merecendo então, de facto, uma visualização nos moldes do direito de propriedade", cit., pág. 8.

[56] SAMUEL D. WARREN, e LOUIS D. BRANDEIS, "The right to privacy", *Harvard Law Review*, Vol. IV, N.º 5, págs. 193-220, 1890. Numa estudo mais alargado sobre o histórico artigo, A. SOUSA PINHEIRO, *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015, págs. 267 e ss.

[57] P. MOTA PINTO, págs. 504 e 505.

[58] M. REGINA REDINHA e M. RAQUEL GUIMARÃES, cit., pág. 650. Neste sentido, também P. MOTA PINTO escreve que "o direito à reserva sobre a intimidade da vida privada andou estreitamente ligado a toda a problemática dos direitos de personalidade – a orientação adotada em geral quanto a estes influiu sobre o reconhecimento daquele direito, tal como muitas vezes os problemas da proteção da privacidade levaram a reformular os instrumentos de tutela da personalidade", cit., pág. 481. Também R. CAPELO DE SOUSA, "com efeito, e para além da amplitude com que é consagrado no art. 80.º um direito de guardar reserva quanto à intimidade da vida privada de outrem, aquele âmbito geral decorre direta e mais extensamente da natureza da personalidade moral do homem geralmente tutelada no art. 70.º n.º 1", cit., pág. 318.

privacidade um estatuto principal na disciplina personalista prosseguida pela nossa lei civil. Com efeito, o art. 80.º reconhece à intimidade uma zona autonomizada de projeção da personalidade humana merecedora de uma tutela individualizada. Estatui o referido artigo no seu n.º 1 que "todos devem guardar reserva quanto à intimidade da vida privada de outrem", acrescentando o n.º 2 que "a extensão da reserva é definida conforme a natureza do caso e a condição das pessoas"[59].

Procuraremos preencher o conteúdo do art. 80.º a partir da formulação sugerida pela sua epígrafe, "reserva sobre a intimidade da vida privada"[60]. A "vida privada" refere-se à vida pessoal do indivíduo e surge por oposição à vida pública, que integra a vida social daquele[61]. Podem aqui incluir-se aspetos como a identidade e outros dados pessoais, o estado de saúde, a vida conjugal, amorosa e afetiva, a vida do lar (também protegida pela inviolabilidade do domicilio[62]) e outros locais privados como um automóvel, a correspondência e outras formas de comunicação, o passado do indivíduo (enquanto "direito ao esquecimento"), o património e a situação financeira e determinados eventos e hábitos da sua rotina[63]. A imagem e a voz também podem fazer parte da vida privada quando o interesse em causa for a privacidade. Relativamente à expressão "intimidade da vida privada", a palavra "intimidade" parece querer circunscrever a proteção da vida privada apenas aos seus aspetos mais íntimos, a um âmbito mais pessoal que "normalmente se exclui de todo o conhecimento alheio"[64]. Neste sentido,

[59] Importa sublinhar que a privacidade é protegida, além de, como vimos, constitucionalmente, nos arts. 26.º n.º 1 e 2, 34.º e 35.º, também no Código Penal, nos arts. 190.º a 198.º e no Código do Trabalho, nos arts. 16.º a 22.º.

[60] Seguiremos neste parágrafo o método preferido por P. MOTA PINTO, v. págs. 524 e ss.

[61] Como escreve M. JANUÁRIO GOMES, "a vida privada é a vida que não é pública", cit., pág. 14. Já P. MOTA PINTO serve-se de dois critérios para fazer esta distinção: um critério espacial, de acordo com o qual a vida pública é aquela que ocorre em público ou em lugares públicos e a vida privada é aquela que ocorre em privado ou em locais privados; e um critério pessoal ou volitivo, que coloca na disposição do sujeito a determinação do âmbito da sua vida privada (o qual deve ser harmonizado com um critério mais objetivo relativo às valorações sociais), v. págs. 525 e ss.

[62] R. AMARAL CABRAL reconhece mesmo o domicílio como "indiscutivelmente o principal baluarte da intimidade da vida privada", cit., pág. 399. Mas a proteção estende-se, claro está, também aos locais públicos. Como lembra D. LEITE CAMPOS, "a pessoa não é só privada, íntima, reservada, quando passa a porta da sua morada, corre as cortinas. Na rua, nos edifícios públicos, nos jardins, a pessoa continua envolta numa esfera privada: veste-se, manifesta-se, como entender, sem que os outros possam invadir essa esfera (salvo ofensa dos seus direitos)", "Lições…", cit., pág. 97. Ainda sobre a hegemonia deste direito face ao direito à informação, escreve que "o direito à privacidade, direito da pessoa, é anterior e superior a qualquer outro direito de carácter "público" como, por exemplo, o direito à informação. Este cessa na fronteira da esfera privada", cit., pág. 99.

[63] Num sentido idêntico, acrescentando a "reserva sobre a individualidade privada do homem no seu ser para si mesmo", v. R. CAPELO DE SOUSA, págs. 318 e ss.

[64] P. MOTA PINTO, cit., pág. 531. Num sentido idêntico, ADRIANO DE CUPIS fala de um direito de "*riservatezza*": "o modo de ser da pessoa que consiste na exclusão do conhecimento pelos outros daquilo que se refere a ela só", cit., pág. 129.

não caberão aqui aspetos ligados à vida profissional[65], afinal, aqueles que normalmente o indivíduo não partilha com mais ninguém[66]. Quanto à "reserva", traduz desde logo uma dupla proteção, na medida em que abrange quer a tomada de conhecimento, quer a divulgação das informações pessoais[67]. Além disso, a *exceptio veritatis* não é admitida, ou seja, a reserva estende-se quer aos factos verdadeiros, quer aos falsos[68].

Foram também a constante evolução e complexidade da realidade social e da personalidade humana a fazer com que o legislador preferisse entregar à doutrina e à jusrisprudência o preenchimento casuístico do objeto deste direito, com recurso a dois critérios previstos no art. 80.º n.º 2: a natureza do caso (critério objetivo), que manda olhar para a situação concreta, e a condição das pessoas (critério subjetivo), que se baseia na posição ou no circunstancialismo social do indivíduo[69].

3.4 A limitação voluntária do direito à reserva sobre a intimidade da vida privada

A intransmissibilidade e a irrenunciabilidade dos direitos de personalidade não prejudicam a possibilidade de os seus titulares os restringirem, nomeadamente, pela via negocial. É nesse sentido que vai o art. 81.º n.º 1 quando admite a possibilidade de "limitação voluntária" dos direitos de personalidade, desde que conforme aos princípios da ordem pública[70]. Acrescenta

[65] Neste sentido, D. LEITE CAMPOS, "a proteção da privacidade esbate-se algo no domínio da vida profissional", "Lições…", cit., pág. 99.

[66] No sentido de graduar as ofensas à privacidade, vulgarizou-se na doutrina a chamada "teoria das três esferas". ORLANDO DE CARVALHO distinguia uma *esfera privada*, uma *esfera pessoal* e uma *esfera de segredo*. A primeira, que envolve aspetos que não são pessoais mas que também ainda não são públicos, a segunda, que envolve informações que a pessoa só partilha com um grupo restrito de pessoas, tais como, os seus gostos e preferências, e a terceira, que envolve apenas informações secretas (naturalmente secretas ou por determinação do titular), "Para uma Teoria…", pág. 265, nota 69 e M. REGINA REDINHA e M. RAQUEL GUIMARÃES, pág. 655. Na doutrina portuguesa vários autores adotam esta teoria, por vezes com formulações diferentes, R. CAPELO DE SOUSA fala antes em "círculos concêntricos de reserva", v. págs. 326 e ss. Num sentido crítico à teoria das três esferas, v. P. PAIS VASCONCELOS, págs. 80 e ss.

[67] Neste sentido, ADRIANO DE CUPIS, admite, inclusivamente, um direito ao segredo, enquanto "aspeto particular" do direito de "*riservatezza*", v. pág. 147. Também neste sentido, P. MOTA PINTO, págs. 533 e ss.

[68] P. MOTA PINTO, pág. 532 e ss. No mesmo sentido, P. PAIS VASCONCELOS, v. pág. 82.

[69] Para R. CAPELO DE SOUSA, a natureza do caso, passa pela "justa identificação, avaliação e ponderação do conjunto dos bens ou interesses juridicamente relevantes na concreta situação ou relação jurídica de personalidade", enquanto a condição das pessoas é "a veste ou o circunstancialismo sócio-individual objetivo em que as pessoas agem", cit., pág. 326, nota 824. É neste último âmbito que se debate a proteção da privacidade das chamadas *figuras públicas*, assumindo aqui alguns autores um "custo da notoriedade" ou mesmo um "direito à curiosidade", v. M. JANUÁRIO GOMES, pág. 16. Em sentido contrário, P. PAIS VASCONCELOS, pág. 82. Também sobre este assunto, R. AMARAL CABRAL, págs. 393 e ss.

[70] A ordem pública aqui em causa é a ordem pública interna (e não a ordem pública internacional) do Estado português e é definida por C. A. MOTA PINTO como "o conjunto dos princípios fundamentais, subjacentes ao

o n.º 2 que as limitações são sempre revogáveis "ainda que com obrigação de indemnizar os prejuízos causados às legítimas expetativas da outra parte".

Não obstante a natureza pessoal dos bens de personalidade, tem-se assistido a um crescente reconhecimento de uma dimensão patrimonial a alguns direitos de personalidade, em particular, ao direito à reserva sobre a intimidade da vida privada, que confere ao titular a possibilidade de explorar economicamente as suas informações pessoais. Como entende P. MOTA PINTO, "quando o direito assegura ao titular, pelo seu conteúdo, o controlo sobre determinadas informações, uma das formas de o exercer é ainda através da sua "comercialização", isto é, pela sua limitação voluntária com contrapartidas económicas"[71]. O nosso ordenamento segue, assim, um modelo monista que reconhece, dentro daquele direito de personalidade, um conjunto de poderes ou faculdades que admitem a sua mobilização económica[72]. Por oposição, claro está, a um modelo dualista, seguido, nomeadamente, no direito americano, em que se entendem os direitos de personalidade como direitos com um conteúdo exclusivamente pessoal e se distingue, por um lado, um *right to privacy* exclusivamente pessoal, e por outro, um *right to publicity* objeto de aproveitamento económico[73].

Esta disposição a título oneroso de informações sobre a vida privada parece-nos perfeitamente admissível e compatível com a ordem pública e os bons costumes. De resto, a liberdade, que inclui a liberdade negocial, é também um importante direito de personalidade e só deve ceder quando confrontada com outros direitos de personalidade que devam considerar-se superiores, nomeadamente, os que protejam a vida e a integridade física[74]. Não queremos, assim, cair na

---

sistema jurídico, que o Estado e a sociedade estão substancialmente interessados em que prevaleçam e que têm uma acuidade tão forte que devem prevalecer sobre as convenções privadas", cit., págs. 557 e 558.

[71] P. MOTA PINTO, "A Limitação Voluntária do Direito à Reserva sobre a intimidade da Vida Privada", *Estudos em Homenagem a Cunha Rodrigues*, Vol. II, Coimbra Editora, Coimbra, 2001, cit., pág. 551.

[72] Neste sentido, ELSA DIAS OLIVEIRA, *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional*, Almedina, 2012, pág. 118.

[73] Assim, quanto ao *right to publicity*, já não estamos, claro está, no âmbito da limitação voluntária aos direitos de personalidade, mas da exploração de meras coisas materiais, que se desentranharam da personalidade para serem objeto de direitos de propriedade, v. R. CAPELO DE SOUSA, págs. 410 e 411. Para uma análise sedimentada deste *right to publicity*, v. ELSA DIAS OLIVEIRA, págs. 105 e ss. *Vide* também D. DE OLIVEIRA FESTAS, *Do contudo patrimonial do direito à imagem – Contributo para um Estudo do seu Aproveitamento Consentido Inter Vivos*, Coimbra Editora, 2009, págs. 154 e ss. Também sobre este tema, P. PAIS VASCONCELOS, págs. 156 e ss.

[74] Sobre este assunto, v. R. CAPELO DE SOUSA, cit. págs. 448 e 449. Neste sentido, os arts. 280.º, 335.º e 340.º do Código Civil. Neste sentido, também, D. LEITE CAMPOS, "qualquer limitação aos direitos de personalidade é nula se não visar o (livre) desenvolvimento desta personalidade segundo valores éticos", "A relação da pessoa consigo mesma", *Nós – Estudo sobre o direito das pessoas*, Coimbra, Almedina, 2004, cit., pág. 92.

chamada "tirania da dignidade" que pudesse sufocar qualquer liberdade de exercício da autonomia privada – também ela, afinal, concretizadora das aspirações da personalidade humana – pelo que reconhecemos, neste âmbito, o direito de o titular dispor, em grande medida, ainda que sempre de forma revogável, do seu direito à reserva sobre a vida privada[75].

O consentimento do ofendido, na terminologia de ORLANDO DE CARVALHO, pode assumir a forma de consentimento tolerante, ou seja, a mera tolerância do lesado em relação à lesão que funciona como causa de justificação daquela, nos termos do art. 340.º. Pode ser um consentimento autorizante que constitui "um compromisso jurídico *sui generis"*, em que o titular atribui ao autorizado um verdadeiro poder de agressão, nos termos do art. 81.º n.º 2. O consentimento pode ser, ainda, vinculante, originando, neste caso, um "compromisso jurídico autêntico", nomeadamente, um contrato, que cria um verdadeiro direito para a outra parte e uma obrigação para o titular que deve ser cumprida, sob pena de incorrer em incumprimento contratual[76]. Esta tendência no sentido do aproveitamento patrimonial dos direitos de personalidade faz com que o consentimento para a limitação voluntária no âmbito da utilização de dispositivos inteligentes, como perceberemos de seguida, seja, muitas vezes, um consentimento vinculante, o qual, deverá ser sempre anterior à limitação, livre e esclarecido, expresso ou tácito, determinado, e livremente revogável[77] [78].

---

[75] Assim, apenas em casos extremos o princípio da dignidade da pessoa humana deve obstar a este poder de dispor dos direitos de personalidade. Sobre este assunto, BENEDITA M. CRORIE explica que "justificar a defesa da pessoa contra si própria invocando o principio da dignidade corresponderia a aplicar este princípio contra a finalidade da sua consagração, pois a dignidade traduz-se precisamente na possibilidade de o indivíduo escolher em liberdade o rumo que pretende seguir na sua vida", "A (ir)renunciabilidade dos direitos de personalidade", *in Pessoa, Direito e Direitos*, DHCII/EDUM, 2016, cit., pág. 271.

[76] Seguimos aqui a classificação feita por ORLANDO DE CARVALHO, "Teoria Geral…", pág. 205. Esta classificação tripartida não é unânime na doutrina, também aqui P. PAIS VASCONCELOS deixa algumas críticas dizendo que se trata de uma "falsa tricotomia" que consente "uma tendência reprovável para a comercialização da personalidade ou de alguns dos seus bens", deixando claro que "a dignidade humana e os seus bens de personalidade não são comercializáveis", v. pág. 155.

[77] Como escreve HEINRICH E. HÖRSTER, "para ser válido, o consentimento que implica a limitação voluntária, além de legal, deve ser consciente, isto é, resultante de uma vontade esclarecida, devidamente ponderado e concreto, tendo efectivamente em vista situações determinadas". O autor acrescenta ainda que, não obstante a possibilidade de o consentimento ser prestado tacitamente, "por via de regra, será prestado de maneira expressa e não pode ser deduzido de um comportamento anteriormente observado", *A Parte Geral do Código Civil Português – Teoria Geral do Direito Civil*, Coimbra, Almedina, 1992, pág. 269.

[78] Outra questão relevante a este propósito tem a ver com o consentimento dos menores para a limitação voluntária do direito à reserva. Nestes casos, em princípio, o menor pode consentir se tiver o "discernimento necessário" para perceber as consequências da limitação voluntária para o seu direito de personalidade. No entanto, quando estiver em causa uma "atuação negocial", o acordo do menor deve sempre ser acompanhado do consentimento do representante legal. Já os "proventos" dessa limitação pertencerão sempre ao incapaz. Neste sentido, P. MOTA PINTO, "A Limitação…", págs. 542 e ss.

4. A Internet das Coisas

4.1 Aproximação ao conceito

A Internet das Coisas ou *Internet of Things* (doravante, *IoT*) representa a fase mais recente da história da Internet. Como é sabido, a Internet surgiu nos anos sessenta como um meio de interligação de computadores através da troca de mensagens entre si, tendo evoluído, no final do século XX, para uma enorme rede de informação, a *World Wide Web*. Já no início do presente século, a internet passou a interligar outros dispositivos (como os *smartphones* e os *tablets*) e a possibilitar a transmissão de voz e de vídeos entre eles, tornando-se uma "plataforma de comunicação universal"[79]. Nos dias que correm, estima-se que a internet possa ligar todo o tipo de objetos, marcando, assim, o início de uma nova revolução na história da internet conhecida como Internet das Coisas[80].

Existem várias definições para a Internet das coisas[81], mas podemos defini-la, simplesmente, como um sistema que interliga todo o tipo de objetos via internet, permitindo que

[79] "Advancing the Internet of Things in Europe", *Comission Staff Working Document*, Bruxelas, 2016, pág. 5.

[80] Convém ressalvar que, embora só nos últimos anos se tenha começado a falar mais "seriamente" deste fenómeno, a expressão "Internet das Coisas" data do ano de 1999 e é atribuída a Kevin Ashton, um empresário com trabalhos na área dos sensores e da *Radio-Frequency IDentification* (*RFID*). Sobre a *RFID* e a sua relação com a *IoT*, *vide* A. SOUSA PINHEIRO, págs. 209 e ss.

[81] Entre as várias definições destacamos, em Portugal, J. MORAIS CARVALHO, "a *Internet of Things* consiste na ligação das coisas, como roupa e acessórios, eletrodomésticos ou meios de transporte, entre muitos outros, à Internet, garantindo uma gestão inteligente (*smart*) dessas coisas", "Desafios do mercado digital para o Direito do Consumo", *in Direito do Consumo 2015-2017*, Coleção Formação Contínua – Jurisdição Civil, CEJ, 2018, pág. 113. Mais tecnicamente, HÉLDER FRIAS fala de uma "rede ou sistema de equipamentos que servem uma finalidade específica, sendo dotados de sensores eletrónicos/informáticos interrelacionados, que possuem um identificador único, e que podem comunicar com humanos (*man to machine* ou *M2H*) e/ou entre equipamentos (*machine to machine* ou *M2M*) através da rede, mediante a transmissão de informação", "A Internet das Coisas (*IoT*) e o mercado segurador", *in* A. MENEZES CORDEIRO, A. PERESTRELO DE OLIVEIRA, D. PEREIRA DUARTE (Coord.), *Fintech – Desafios da Tecnologia Financeira*, 2ª edição, Almedina, 2019. V. também a definição apresentada por PEDRO COELHO, *Internet das Coisas – Introdução Prática*, FCA, 2017, pág. 2. Indicamos também a definição apresentada pelo *European Research Cluster on IoT* (*IERC*): "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*", disponível em http://www.internet-of-things-research.eu/about_iot.htm, e pela americana *Federal Trade Comission (FTC)*: "*an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people*", "Internet of Things – Privacy & Security in a Connected World", *FTC Staff Report*, 2015, cit., pág. 1. Em Espanha, "*El internet de las cosas consiste, essencialmente, en colocar ordenadores y sensores a todo tipo de bienes, de modo que pueden recoger información de su uso y del ambiente que les rodea para transmitirla a otros bienes, también computerizados, e interactuar com ellos*", C. GÓRRIZ LÓPEZ, "Tecnología blockchain y contratos inteligentes", *in* S. NAVAS NAVARRO (Dir.), *Inteligencia artificial: Tecnología-Derecho*, cit., págs. 182 e 183. Em Itália, "*Con Internet of Things si intende l'insieme di connessioni internet operate da oggetti e da luoghi, senza l'intervento di operatori umani. In questo contesto gli oggetti possono collegarsi alla rete, comunicare il proprio status e dati sul proprio operato, come statistiche ed*

comuniquem entre si. A tendência no sentido da ligação de cada vez mais dispositivos em rede, com funções cada vez mais diversas – de monitorização, sensorização, aviso, interação ou mesmo distribuição do processamento – tem levado alguns especialistas a preferir o conceito de *Internet of Everything* (*IoE*), uma noção muito mais vasta que, além de coisas, abrange pessoas, processos e dados, interligados nesta rede[82]. Tal sistema depende, pelo menos, de três componentes essenciais: de um dispositivo remoto (como os sensores), de conectividade de rede (sem fios, normalmente) e da capacidade de computação (nesses dispositivos remotos e/ou no sistema central)[83]. Revelamos, de seguida, algumas das aplicações deste conceito.

4.2 Casa e entretenimento

O ambiente doméstico é considerado o melhor para desenvolver aplicações *IoT*. Trata-se, efetivamente, de um espaço onde, normalmente, existe uma boa cobertura de rede elétrica e de internet e em que as possibilidades de implementação de projetos são maiores e vão desde o conforto e da monitorização, à segurança das habitações[84].

Um dos dispositivos mais conhecidos para uso doméstico é o termóstato *Nest*. Como qualquer outro termóstato, o *Nest* controla a temperatura da habitação, mas, permite também que seja o consumidor a regular a temperatura da sua casa através de uma aplicação instalada no seu *smartphone*. Além disso, possui sensores que detetam, não só a temperatura, mas também a luminosidade, a humidade e até as movimentações das pessoas em cada divisão. A partir da memorização dos hábitos e das configurações dos utilizadores, graças à tecnologia *machine learning*[85], o *Nest* pode passar a controlar autonomamente a temperatura da casa. Assim, o aparelho pode regular o calor da casa "lembrando-se" da temperatura que o utilizador definiu

---

altro, ed accedere ad informazioni utili per il proprio funzionamento, in modo del tutto automático", F. IPPOLITO e M. NICOTRA, *Diritto della Blockchain, Intelligenza Artificiale e IoT*, Ipsoa, 2018, cit., pág. 281.

[82] PEDRO COELHO, pág. 13. Como refere PAULA R. ALVES, "a internet deixa de estar só nos computadores e, depois, nos telefones e passa a estar em *chips* integrados em potencialmente tudo, em todo o lado", "Os desafios digitais no mercado segurador", *in Fintech – Desafios*…, cit., pág. 41.

[83] PEDRO COELHO, pág. 20.

[84] Como refere PEDRO COELHO, "tudo o que se pode ligar em casa a uma tomada de energia pode potencialmente ser alvo de automação, pelo que as possibilidades são infinitas", cit., pág. 58.

[85] A *machine learning* (aprendizagem automática) é "um campo da Inteligência Artificial que lida com sistemas que "aprendem" com os dados", cit., PEDRO COELHO, pág. 34.

imediatamente antes de se deitar e depois de se levantar pela manhã, do mesmo modo que pode desligar o aquecimento quando este sai de casa[86].

No domínio do conforto, destacaríamos ainda dois exemplos clássicos: as máquinas de café inteligentes, como a *Firebox*, que pode ser controlada a partir do *smartphone* do utilizador e permite, entre outras coisas, servir um café automaticamente quando o tempo arrefece, ou mediante a localização que o *GPS* oferece do utilizador, e ainda os frigoríficos inteligentes como o *Samsung Smart Hub*, que, também via *smartphone*, informa o usuário dos produtos que precisa de trazer do supermercado, reproduz músicas e ainda acede aos calendários dos restantes elementos da família[87].

De resto, quanto ao entretenimento, é inevitável dedicar atenção às *smart TV's* e aos *smart speakers*. Preferindo uma noção mais técnica, as televisões inteligentes, em termos gerais, designam serviços baseados em televisão que podem ser implementados quando a televisão está ligada à rede e incluem não só a obtenção de conteúdos, mas também a interação com serviços que estão na rede[88]. Permitem aceder a informação interativa durante as emissões, visionar conteúdos a pedido (em vez de ser em direto), e utilizar diversas aplicações (de jogos, redes sociais, de áudio e vídeo, entre outras). Possibilitam ainda o controlo dos hábitos de visualização, das crianças, em particular, alertando-as no caso de estarem muito próximas do ecrã[89]. Quanto aos *smart speakers*, o mais conhecido é certamente a *Alexa* da *Amazon*, um assistente virtual inteligente capaz de comunicar com os utilizadores, informando-os sobre a meteorologia, as notícias do dia ou reproduzindo músicas, podendo inclusivamente ser usada para controlar outros dispositivos domésticos inteligentes. Além disso, a *Alexa* foi também concebida para ajudar o utilizador a fazer as compras sem sair de casa. Perante um pedido de encomenda do consumidor, a assistente virtual apresenta várias opções de compra daquele produto – de acordo com o preço ou a cotação que possuem no *site*, por exemplo – e divulga, finalmente, todas as informações sobre a entrega e o valor total da encomenda[90].

---

[86] SWAROOP POUDEL, "Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security", *Berkeley Technology Law Journal*, 2016, pág. 998.

[87] HILLARY BRILL e SCOTT JONES, "Little things and big challenges: information privacy and the Internet of Things", *American University Law Review*, 2017, v. pág. 1193.

[88] PEDRO COELHO, pág. 68.

[89] HILLARY BRILL e SCOTT JONES, pág. 1193.

[90] *Vide* ainda o caso do *Amazon Dash*, um dispositivo que permite a compra instantânea de um determinado produto através de um mero clique num botão que lhe está associado, HILLARY BRILL e SCOTT JONES, pág. 1194.

4.3 Saúde e *Fitness*

A similitude do tipo de sensores utilizados nas áreas da saúde e do *fitness* justificam a união dos dois temas neste único ponto. Podemos, assim, distinguir pelo menos cinco tipos de sensores *IoT* usados nestes domínios: os dispositivos terminais, os sensores vestíveis (*wearable*), os sensores de contacto íntimo, os sensores ingeríveis e os sensores implantáveis[91]. Na primeira categoria, inserem-se uma série de dispositivos externos concebidos para monitorizar ocasionalmente certos aspetos relacionados com a saúde ou a atividade física do utilizador, desde balanças, a todo o tipo de medidores (de pressão arterial, da temperatura corporal, do nível de oxigénio no sangue, entre outros). Quanto aos sensores *wearable*, são incorporados em roupa e acessórios usados para fins de desporto ou de controlo médico (relógios, pulseiras, t-shirts, e muitos outros). Os sensores de contacto íntimo assemelham-se aos dispositivos vestíveis mas estão mais em contacto com a pele e são sobretudo usados para fins médicos (autocolantes, curativos, ligaduras ou mesmo tatuagens). Finalmente, os sensores ingeríveis e implantáveis são a tecnologia de ponta da *IoT*, desenvolvidos para monitorizar a saúde do individuo a partir do interior do organismo.

Entre os dispositivos mais conhecidos estão certamente as pulseiras de *fitness*, como a *Fitbit*, capazes de monitorizar o ritmo cardíaco, os passos e distâncias percorridas e mesmo os padrões de sono do usuário. A pulseira está associada a uma conta de utilizador à qual pode igualmente ser interligada a *Aria*, uma balança conectada à rede que apura o peso, a percentagem de gordura e o índice de massa corporal do indivíduo. Além disso, ambos os dispositivos podem ser combinados numa aplicação para *smartphone* como a *SmartPlate*, que informa o utilizador sobre o valor nutricional dos produtos que consome e o incita a complementar a atividade física com um plano alimentar adequado[92].

A IoT será particularmente revolucionária no sector da saúde, onde já se fala da *Internet of Health Things* (*IoHT*), um conceito que resulta da combinação das tecnologias de saúde pessoais com a *IoT* e que apresenta *"expanded abilities to exchange useful data,*

[91] Acolhemos, assim, a classificação proposta por SCOTT R. PEPPET, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent", *Texas Law Review*, 2014, págs. 98 e 99.

[92] HILLARY BRILL e SCOTT JONES, pág. 1191 e SCOTT PEPPET, pág. 99.

improvements in context awareness, and the ability to initiate actions based on data that are collected and analyzed"[93]. A principal vantagem inovadora da *IoT* no âmbito da saúde tem a ver, sem dúvida, com a possibilidade de comunicação entre os vários sensores. Em jeito de exemplo, os dispositivos pessoais de um indivíduo asmático serão capazes de receber um alerta sobre os níveis elevados de poluição do ar num determinado local, e redirecioná-lo automaticamente para uma atividade ao ar livre, ou, até, de aumentar a capacidade de filtração do ar da sua casa ou do seu automóvel. De igual modo, uma bomba de insulina não só transmitirá uma mensagem de erro em caso de falha, como notificará o cuidador de saúde da necessidade de proceder à sua reposição. No mesmo sentido, o profissional de saúde poderá ser informado quando a temperatura da casa de um paciente idoso desceu a um certo nível, ou, quando o mesmo paciente não tomou a medicação[94]. Efetivamente, adianta NICOLAS P. TERRY, esta possibilidade de interconexão dos dados recolhidos pelos vários sensores pode solucionar o problema da fragmentação dos dados de saúde sentido até aqui com o uso das tecnologias da informação convencionais[95].

4.4 Cidades e mobilidade

A entrada dos dispositivos inteligentes nos espaços públicos das cidades dará origem a uma nova conceção de cidade, a *smart city*, uma cidade inteligente. Como entende JESS W. WOO, *"a smart city is one that integrates information and communication technologies (ICTs) and the Internet of Things (IoT) to manage the city's assets and delivery of services"*[96].

Também aqui as aplicações são infinitas e vão desde a gestão eficiente do trânsito e da iluminação pública, ao auxílio na mitigação de problemas sociais comuns nos meios urbanos

[93] NICOLAS P. TERRY, "Will the Internet of Things Transform Healthcare?", *Vanderbilt Journal of Entertainment & Technology Law*, pág. 329, 2016.
[94] NICOLAS P. TERRY, págs. 349 e 350.
[95] Como explica o autor, as informações de saúde *"are themselves fragmented and lack standards that make data "liquid", which makes it difficult to control and mold them to change the healthcare industry"*, mas, com a chegada da *IoHT*, *"sophisticated yet inexpensive monitoring of and coaching for chronic conditions may address some of healthcare's fragmentation problems by better coordinating care when patients are handed off between providers"*, NICOLAS P. TERRY, cit., págs. 330 e 331.
[96] JESS W. WOO, "Smart Cities Pose Privacy Risks and Other Problems, but That Doesn't Mean We Shouldn't Build Them", *UMKC Law Review*, 2017, cit., pág. 955. Para JANINE S. HILLER e JORDAN M. BLANKE, "*Smart Cities are designed to ubiquitously collect information about people, places, and activities and to use that data to provide more efficient services and to build resilience against disasters",* "Smart Cities, Big Data, and the Resilience of Privacy", *Hastings Law Journal*, 2017, cit., pág. 309. Já PEDRO COELHO entende que "consiste numa visão de integração entre muitas tecnologias de informação com o objectivo de gerir os ativos das cidades da forma mais inteligente possível", cit., pág. 70.

como a criminalidade e o consumo de drogas[97]. Só em jeito de exemplo, a empresa *Awesense*, voltada para a criação das chamadas *smart grids*, utiliza sensores para medir os gastos de eletricidade e identificar problemas de instalação ou eventuais fugas de energia. Já a tecnologia *Echelon* permite adaptar a iluminação pública de acordo com a hora do dia, as condições do tempo e a estação do ano, ao passo que o *Big Belly Trash*, um caixote do lixo inteligente, pode desencadear a recolha automaticamente, logo que necessário[98]. Estima-se que a *smart city*, em particular, conduza a uma vigilância permanente e sem precedentes dos indivíduos com prejuízos sérios para os seus direitos, nomeadamente, para a sua liberdade de ação. Como escrevem JANINE S. HILLER e JORDAN M. BLANKE, "*living in a panopticon*[99]*, where private lives become public – or at least perceived as public – is harmful to the very essence of privacy and the necessary freedoms that are important for autonomy and even democracy*"[100].

No plano das cidades inteligentes, as soluções de mobilidade têm chegado também aos automóveis, pelo que se tem falado de *smart cars*[101], automóveis capazes de transferir e receber dados através da sua ligação à internet[102]. Para tal, os veículos dispõem de, pelo menos, três tipos de sensores[103]: os *Event Data Recorders* (EDR's), sensores que revelam o estado do automóvel no momento de um acidente (a velocidade, o estado dos travões, o uso do cinto de segurança, o desenvolvimento do *airbag*, entre outros); os sensores de consumo automóvel, que permitem que o condutor aceda a informações sobre o veículo via *smartphone*, desde alertas para manutenção, informações sobre o consumo de combustível e até indicações para evitar o trânsito; e ainda os dispositivos de seguro automóvel, que são

[97] Neste sentido, v. JANINE S. HILLER e JORDAN M. BLANKE, pág. 315.
[98] Entre outros exemplos, HILLARY BRILL e SCOTT JONES, pág. 1196.
[99] Referência ao *Panóptico de Bentham*, "um modelo de prisão ou de torre de observação, idealizado para que os vigilantes possam facilmente observar todas as partes do edifício ou recinto, sem serem observados" (noção retirada do Dicionário Priberam da Língua Portuguesa). Sobre este assunto, *vide* A. SOUSA PINHEIRO, págs. 186 e ss.
[100] JANINE S. HILLER e JORDAN M. BLANKE, cit., pág. 325.
[101] A Sociedade de Engenharia Automóvel americana (*SAE International*), define seis níveis de automação automóvel, que vão desde uma condução totalmente humanizada (nível 0), até uma condução sem qualquer intervenção humana, os chamados veículos sem condutor (nível 5). Para mais desenvolvimentos sobre a escala, *vide* PETER J. PIZZI, pág. 3.
[102] Como explica PETER J. PIZZI, "*a «connected car» generally refers to a vehicle equipped with technologies and services that transmit and receive data via wireless internet*", "Connected Cars and Automated Driving: Privacy Challenges on Wheels", *Defense Counsel Journal*, 2017, cit., pág. 2. Segundo a *FTC*, "*some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013*", cit., pág. 1.
[103] Seguiremos também aqui a categorização adotada por SCOTT R. PEPPET, págs. 104 e ss.

fornecidos pelas próprias seguradoras aos condutores para calcularem o valor do prémio em função do seu comportamento ao volante[104].

4.5 Brinquedos inteligentes

O aparecimento dos brinquedos inteligentes marca a entrada da *IoT* no mundo das crianças. Os brinquedos conectados estão a revolucionar o mercado e há cada vez mais pais a preferirem os *smart toys* para fornecerem um entretenimento e, sobretudo, uma aprendizagem interativa aos seus filhos[105].

Um dos *smart toys* mais famosos – se não mesmo o mais famoso – é a *Hello Barbie*. A *Hello Barbie* não é mais do que o resultado da incorporação das tecnologias mais avançadas na boneca mais conhecida do mundo, a *Barbie*. Efetivamente, esta boneca inteligente utiliza a conectividade à Internet, a Inteligência Artificial[106] e outras tecnologias como o reconhecimento por voz para interagir ativamente com a criança, como se fosse a sua melhor amiga. Como explica CORINNE MOINI, *"these features allow Barbie to engage in a two-way conversation, play games, and even tell jokes"*[107]. Praticamente, a criança carrega no botão localizado no cinto da boneca para que a sua voz seja gravada e, posteriormente, enviada para uma *cloud* que armazena e processa essa mensagem, devolvendo, por fim, uma resposta apropriada. Para tal, a empresa que desenvolveu a boneca, a *Mattel*, colabora com a *ToyTalk*, uma outra empresa voltada para as tecnologias no entretenimento, que apetrecha a

[104] De facto, o montante do prémio do seguro deixou de se basear na quantidade de quilómetros percorridos (*Pay As You Drive – PAYD*) e passou a ser determinado pela qualidade da condução (*Pay How You Drive – PHYD*). Neste sentido, v. PAULA R. ALVES, págs. 41 e 42. Sobre a emergência de novos tipos de seguros na revolução digital, v. págs. 47 e ss. A autora entende mesmo a *IoT* "como a base do próximo grande desenvolvimento no sector segurador, que passa por uma diferente conceção do seguro", cit., pág. 67. Sobre este assunto, também escreveu HÉLDER FRIAS, v. págs. 240 e ss. A tendência é a mesma no âmbito dos seguros de saúde, como entende o GT29, as companhias "podem querer oferecer pedómetros aos clientes para controlar a frequência com que fazem exercício e adaptar os prémios do seguro de acordo com esses valores", "Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas", *Grupo de Trabalho do Artigo 29.º para a Proteção de Dados*, 2014, cit., pág. 14.

[105] HILLARY BRILL e SCOTT JONES, cit., pág. 1200. Como referem os autores, *"technology inherent in the IoT can be used for interactive learning and could revolutionize our education industry"*, cit., pág. 1203.

[106] Reproduzimos aqui a definição, elementar, de Inteligência Artificial apresentada por S. NAVAS NAVARRO: "*Se trata de emular las diversas capacidades del cérebro humano para presentar comportamentos inteligentes sintetizando y automatizando tareas intelectuales*", "Derecho e inteligencia artificial desde el diseño. Aproximaciones", in S. NAVAS NAVARRO (Dir.), *Inteligencia artificial: Tecnología-Derecho*, cit., pág. 24. Também CORINE MOINNI apresenta uma noção, distinguindo "*weak AI*" e "*strong AI*", "Protecting Privacy in the Era of Smart Toys: Does Hello Barbie have a Duty to Report?", *The Catholic University Journal of Law & Technology*, 2017, v. págs. 291 e 292.

[107] CORINNE MOINI, cit., pág. 281.

Hello Barbie com uma base de dados de oito mil linhas de diálogo e gere os servidores onde todos estes dados são armazenados, ajudando a boneca a "lembrar-se" de todas as conversações mantidas até aí com a criança[108].

Obedecendo a uma lógica tecnicamente idêntica, mas com funcionalidades diversas, existem outros brinquedos conectados: a título de exemplo, o *Urso Fisher Price* e a *mesa de atividades VTech*, mais voltados para a aprendizagem e o desenvolvimento cognitivo das crianças, ou o *smartwatch hereO*, um relógio *GPS* especialmente concebido para crianças e que permite que os pais acompanhem a sua localização através de uma aplicação móvel[109].

4.6 A emergência de uma privacidade inteligente

Como já tivemos oportunidade de perceber, a privacidade e a tecnologia andaram sempre "de mãos dadas" ao longo da história e tudo indica que na era da *IoT* não será diferente. O número de sensores tem crescido exponencialmente e estima-se que em 2020 estarão ligados à rede pelo menos cinquenta mil milhões de dispositivos inteligentes[110]. Num mundo em que tudo estará conectado não é difícil de antever mais uma profunda mudança nos paradigmas da privacidade que vigoraram até aqui[111]. Com efeito, onde fica a privacidade quando uma infraestrutura de milhares de milhões de sensores integrados em dispositivos do quotidiano de qualquer pessoa são capazes de registar, tratar, armazenar e transferir dados a todo o momento e de forma contínua?[112] Ou, como problematiza SONA R. MAKKER, "*how can we preserve and manage privacy in a world of pervasive sensing and ubiquitous computing?"*[113].

---

[108] CORINNE MOINI, pág. 282.
[109] HILLARY BRILL e SCOTT JONES, págs. 1200 e ss.
[110] Não há um consenso sobre o número, a consultora *Gartner* estima que sejam 26 mil milhões, a empresa *Cisco* aponta para 50 mil milhões, mas a *Intel* arrisca mesmo 200 mil milhões dispositivos conectados em 2020, v. MICHAEL MILLER, *The Internet Of Things - How Smart Tvs, Smart Cars, Smart Homes, and Smart Cities are changing the world*, Pearson Education, Indianapolis, 2015, pág. 27 (versão *e-book*).
[111] Neste sentido, LUÍS F. ANTUNES, quando afirma que "os avanços tecnológicos já ultrapassaram os quadros legais existentes criando uma tensão entre inovação e privacidade, sempre que as leis não refletem os novos contextos sociais e não garantem os direitos dos cidadãos", "A Privacidade no mundo conectado da Internet das coisas", *in Revista Fórum de Proteção de Dados*, N.º 2, 2016, pág. 55. Também CORINE MOINNI reforça esta ideia: "*it's widely accepted that the development of privacy laws lag behind the speed of technological innovation*", cit., pág. 299.
[112] Só em jeito de exemplo, refira-se que a *FTC* descobriu que, por exemplo, menos de 10 mil casas podem gerar mais de 150 milhões de dados por dia, v. pág. 14.
[113] SONA R. MAKKER, "Overcoming "foggy" notions of privacy: How data minimization will enable privacy in the Internet of Things", *UMKC Law Review*, 2017, pág. 895.

Assumiríamos como principal ameaça da *IoT* à privacidade, aquela que, como vimos, é simultaneamente a sua principal vantagem, e que tem a ver com a real possibilidade de combinação dos dados recolhidos pelos vários sensores. É que, na verdade, nesta tarefa a *IoT* não está sozinha, pois, beneficia igualmente de outras tecnologias emergentes como o *Machine Learning* e o *Big Data*[114], vistos como um "novo paradigma" no tratamento de dados pessoais[115]. Num quadro destes, em que às possibilidades de recolha maciça de dados brutos, se juntam capacidades avançadas de tratamento e análise da informação, será possível extrair informações sensíveis a partir de dados "aparentemente inócuos"[116]. A possibilidade de combinação dos dados já era conhecida no mundo da informática a partir de um fenómeno chamado "fusão de sensores" (*sensor fusion*), um conceito que "consiste em combinar dados de sensores ou dados provenientes de fontes diferentes a fim de obter informação melhor e mais precisa do que a que seria possível obter no caso de estas fontes estarem a funcionar isoladamente"[117], pelo que estas ameaças não são uma novidade completa. De qualquer modo, é caso para aceitarmos a premissa segundo a qual estamos mesmo prestes a entrar numa realidade conectada em que *"everything may reveal everything"*[118].

O primeiro corolário que podemos retirar daqui é, assim, que há uma grande dificuldade prática (para não dizer impossibilidade) de garantir a anonimização dos utilizadores dos dispositivos *IoT*[119]. Como vimos, ainda que os dados sejam à partida anonimizados, é possível

---

[114] O termo *Big Data* nasceu nos anos 2000 e designa, literalmente, um "grande volume de dados". Refere-se, basicamente, às práticas de criação e análise de enormes conjuntos de dados, v. PEDRO COELHO, pág. 180 e ss. O *Big Data* costuma ser caracterizado pelos "cinco V's": Volume, Variedade, Velocidade, Veracidade e Valor (sendo este último, entre nós, o mais importante, embora nem sempre assumido), v. TAL Z. ZARSKY, "Incompatible: The GDPR in the age of big data", *Seton Hall Law Review*, 2017, págs. 998 e 999. Também PAULA R. ALVES se refere a estas características, acrescentando mais duas que entretanto se autonomizaram: a Variabilidade e a Visualização. Também a autora refere que "a internet das coisas é, atualmente, uma das principais fontes de *big data*", *in Fintech – Desafios…*, págs. 43 e 67, respetivamente. Também A. ALVES LEAL se debruça sobre o tema, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *in Fintech – Desafios*…, págs. 93 e ss.

[115] Como escreve TAL Z. ZARSKY, o *Big Data* representa "*a tectonic change in the way data is collected, analyzed and applied in the digital era*", cit., pág 998.

[116] Neste sentido, SCOTT R. PEPPET: *"sensor data tend to combine in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources"*, cit., pág. 120. Também A. ALVES LEAL chama a atenção para esta realidade, v. págs. 126 e 127.

[117] GT29, "Parecer 8/2014", cit., pág. 9.

[118] SCOTT R. PEPPET, pág. 120. Como explica este autor, *"sensor data are so rich, accurate, and fine-graned that data from any given sensor context may be valuable in a variety of – and perhaps all – other information contexts".* Merece ainda destaque a referência à alegoria da "visão estereoscópica" para exemplificar o fenómeno da fusão de sensores, v. pág. 121.

[119] A anonimização é um "tratamento posterior de dados pessoais" que visa "evitar irreversivelmente a identificação", "Parecer 05/2014 sobre técnicas de anonimização", *Grupo de Trabalho do Artigo 29.º para a Proteção de Dados*, cit., pág. 3. As principais técnicas de anonimização são a *aleatorização* – que consiste na

não só re-identificar um individuo, como retirar grandes inferências sobre a sua vida[120]. Como explica SCOTT R. PEPPET, "*sensor data capture such a rich picture of an individual, with so many related activities, that each individual in a sensor-based dataset is reasonably unique*"[121]. Por exemplo, a pulseira *Fitbit*, ao registar o percurso do utilizador, regista igualmente o ritmo da sua marcha, pelo que é perfeitamente possível identificar o individuo a partir do seu modo de andar. No caso dos sensores de saúde, ao recolherem todos os movimentos do usuário ao longo do dia, permitem perceber quais os meios de transporte por ele utilizados, o que, conjugado com pequenas informações sobre as rotinas de um utilizador, o permite identificar com alguma facilidade. Alguns *smartphones*, além de estarem equipados com um *GPS*, contêm também um acelerómetro, o qual, a partir de outros telemóveis que emitam movimentações semelhantes, permite perceber se essas pessoas se encontram no mesmo local[122].

A possibilidade de conhecer, pormenorizadamente, os hábitos e comportamentos das pessoas tornou-se o negócio mais rentável da atualidade, encontrando-se em ascensão um novo mundo voltado para a obtenção de conhecimento sobre os utilizadores. São, como refere JOÃO FACHANA, *novos* tempos em que *novos* anglicanismos, associados ao *novo* mundo da exploração de dados pessoais, começam a entrar no nosso vocabulário: *data mining*, *data analytics*, *data brockerage*[123], *data science*, entre outros[124]. Na verdade, mais do que conhecer

---

alteração da veracidade dos dados no sentido de eliminar a ligação com a pessoa – e a *generalização*, que passa pela alteração da escala ou ordem de grandeza dos atributos dos titulares dos dados. Para uma análise mais detalhada, v. págs. 13 e ss.

[120] Neste sentido, MANUEL D. MASSENO fala da possibilidade de detetar "microtendências", dada a circunstância de as "analíticas" usadas "terem por objeto todos os dados e não apenas amostragens, o que multiplica exponencialmente as correlações que passam a ser possíveis de inferir", "Protegendo os cidadãos-consumidores em tempos de Big Data: uma perspetiva desde o Direito da União Europeia", *Revista Portuguesa de Direito do Consumo*, n.º 89, 2017, cit., pág. 46.

[121] SCOTT R. PEPPET, cit., pág. 130.

[122] SCOTT R. PEPPET, v. pág. 131. Ou então, como escreve o autor, "*So long as one phone (with a known location) has travelled the same roads as the previously "hidden" phone (with unknown location), the latter can be located*".

[123] Os *databrokers* (ou corretores de dados) "compram dados das empresas para criar listas de indivíduos pertencentes a uma mesma categoria ou grupo", GT29, "Parecer 8/2014", cit., pág. 12, nota 13. M. PERESTRELO DE OLIVEIRA chama-lhes "empresas de comércio de dados" que "recolhem informação de diferentes fontes, em nome dos seus clientes ou por conta própria, compilam a informação para desenvolver perfis de pessoas, que são, posteriormente, colocados em segmentos. Os perfis já segmentados são vendidos a empresas que queiram melhorar o direcionamento dos seus produtos e serviços", "Definição de perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados", *in* A. MENEZES CORDEIRO, A. PERESTRELO DE OLIVEIRA, D. PEREIRA DUARTE (Coord.), *Fintech – Novos estudos sobre tecnologia financeira*, Almedina, 2019, cit., pág. 71. *Vide*, por exemplo, o caso paradigmático da empresa *ONZO*, NIKOLE DAVENPORT, "Smart washers may clean your clothes, but hacks can clean out your privacy, and underdeveloped regulations could leave you hanging on a line", *The John Marshall Journal of Information Technology & Privacy Law*, 2016, págs. 268 e 269.

as preferências dos consumidores tendo em vista, por exemplo, o *marketing* direcionado, têm-se pretendido, inclusivamente, com recurso a áreas científicas como a psicologia cognitiva, formatar o seu comportamento e as suas escolhas, orientando-os no sentido dos interesses das empresas, ou, de um modo mais preocupante, de determinadas vertentes políticas[125].

Outros problemas podem conduzir às violações de privacidade, ou resultar delas, como é o caso, respetivamente, dos relacionados com a segurança e a discriminação. Quanto aos problemas de segurança, de facto, os dispositivos *IoT* apresentam fragilidades que os deixam vulneráveis a *hackers.* A opinião unânime é a de que, na verdade, os fabricantes não revelam grandes preocupações com a segurança dos dispositivos desde a sua conceção[126]. Além disso, existem ainda limitações técnicas, tendo em conta que, nomeadamente, o reduzido tamanho destes dispositivos não os apetrecha com bateria e capacidade de processamento suficientes para suportar medidas de segurança adequadas[127]. Quanto à discriminação, existe, sobretudo, um enorme risco de segregação económica, que se poderá fazer sentir no acesso ao emprego e a bens e serviços – como a um empréstimo bancário, ou a um seguro de saúde[128].

---

[124] JOÃO FACHANA, "Que papel para o consentimento na sociedade em rede?", *Direito e Informação na Sociedade em Rede: Atas*, FDUP/FLUP, 2016, pág. 103.

[125] Esta formatação do comportamento humano tem o nome de *Nudge*. Para M. PERESTRELO DE OLIVEIRA, "é qualquer aspeto do processo de escolha que altera o comportamento das pessoas de forma previsível e sem proibir qualquer das opções ou alterar significativamente os seus incentivos económicos", cit., pág. 72. Sobre a "manipulação em massa", v. págs. 64 e ss.

[126] Como refere SCOTT R. PEPPET a propósito da *Fitbit*, "*the device simply was not engineered with data security in mind*", apresentando uma possível explicação: "*these products are often manufactured by traditional consumer-goods makers rather than computer hardware or software firms. The engineers involved may therefore be relatively inexperienced with data-security issues, and the firms involved may place insufficient priority on security concerns*", cit., pág. 135. Também neste sentido, STEVEN I. FRIEDLAND: "*security was treated more as an externality, not as an essential component of the core part of the IoT system*", "Drinking from the fire hose: how massive self-surveillance from the internet of things is changing the face of privacy", *West Virginia Law Review*, 2017, cit., pág. 905.

[127] Neste sentido, SCOTT R. PEPPET, pág. 135. Sobre as vulnerabilidades de segurança nos *smart toys* referidos, v. HILLARY BRILL e SCOTT JONES, págs. 1201 e ss.

[128] Sobre a discriminação no acesso aos seguros, em particular, no seguro automóvel por parte dos "maus condutores", v. PAULA R. ALVES, págs. 46 e 47. Também nos seguros de saúde: "*insurers could use Fitbit data to charge higher premiums to people with higher preceived health risks*", SWAROOP POUDEL, cit., pág. 1013. Sobre este assunto, também se debruçou M. PERESTRELO DE OLIVEIRA, págs. 62 e ss. Sobre a discriminação nas *Smart Cities*, entre vários exemplos, escreve JESSE W. WOO, "*for example, transportation schemes that rely solely on smartphone hailed ride sharing services could exclude elderly or homeless populations without access to that technology*", cit., pág. 956. Num sentido oposto, há também quem encare a *IoT* como um fenómeno capaz de promover a inclusão e a igualdade sociais, v. JULES POLONETSKY e STACEY GRAY, "The Internet of Things as a Tool for Inclusion and Equality", *Federal Communications Law Journal*, 2017, págs. 103-118.

5. A Internet das Coisas e o Regulamento Geral de Proteção de Dados

Em Maio de 2018 passou a ser aplicável o Regulamento Geral de Proteção de Dados[129] (doravante, RGPD), que veio revogar a Diretiva 95/46/CE (em diante, DPD). Sem dúvida que as razões subjacentes à necessidade de criação de um novo regime sobre esta matéria se prendem essencialmente com as inovações tecnológicas desenvolvidas nos últimos anos, que, tornando a anterior diretiva desatualizada, deixaram desprotegidos os direitos das pessoas face às novas ameaças[130]. Neste sentido, como veremos de seguida, o RGPD veio, na linha da DPD, reforçar a proteção dos titulares dos dados pessoais, atribuindo-lhes mais direitos e "apertar o cerco" às organizações, impondo-lhes obrigações acrescidas no tratamento dos dados pessoais[131].

Porém, têm-se questionado até que ponto uma política regulatória mais rígida para as empresas, não poderá constituir um entrave excessivo no seio da revolução tecnológica em curso. No caso específico da *IoT*, sabemos de antemão a importância de um nível de proteção elevado para a confiança dos utilizadores dos dispositivos inteligentes, mas será uma questão de balancear vantagens e desvantagens de uma tal orientação normativa no sentido de perceber a sua viabilidade[132]. É o que tentaremos perceber de seguida, apresentando, com o merecido detalhe, os traços do RGPD que nos parecem, à partida, potencialmente mais comprometedores para a *IoT*[133].

---

[129] Regulamento (UE) 2016/679 do Parlamento 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. Nos termos do art. 99.º, entrou em vigor "no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*", ou seja, no dia 4 de Maio de 2016, mas, acrescenta o n.º 2, apenas foi aplicável "a partir de 25 de Maio de 2018".

[130] Como prescreve o Considerando 6, "*a rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais*", acrescentando o Considerando 7 que "*esta evolução exige um quadro de proteção de dados sólido e mais coerente na União (...)*". Mais ao encontro do propósito deste trabalho, adianta MANUEL D. MASSENO, que "a respetiva Proposta [do RGPD] teve, entre outros, o objectivo de dar uma resposta cabal às questões suscitadas por tecnologias novas, como as subjacentes à *Big Data* ou à *Internet das Coisas*", cit., pág. 52. De resto, como escreve TAL Z. ZARSKY, "*among the challenges data protection law faces in the digital age, the emergence of Big Data is perhaps the greatest*", cit., pág. 996.

[131] Obrigações cujo incumprimento pode resultar em coimas – com valores, diga-se, nunca vistos em matéria de violação de legislação de proteção de dados pessoais – que podem chegar aos 20 milhões de euros, ou a 4% do volume de negócios anual a nível mundial de uma empresa, v. art. 83.º n.ºs 5 e 6 e o Considerando 150. Para mais desenvolvimentos, v. MARCO A. SAIAS, "Reforço da responsabilização dos responsáveis pelo tratamento de dados", Revista Portuguesa de Direito do Consumo, n.º 89, 2017, págs. 67-86.

[132] *Vide*, neste sentido, o estudo da Comissão Europeia, "Advancing the Internet of Things in Europe", *Comission Staff Working Document*, Bruxelas, 2016.

[133] Têm-se distinguido dois modelos regulatórios aplicáveis, nomeadamente, ao tratamento dos grandes volumes de dados (*big data*): por um lado, uma abordagem baseada no risco (*risk based approach*) e, por outro, uma abordagem de auto-defesa (*self-defence approach*), M. EDUARDA GONÇALVES, "The EU data protection

5.1 Controlo e Transparência

Como já dissemos, o RGPD veio reconhecer aos titulares um maior controlo sobre os seus dados pessoais, reforçando os seus direitos e criando novos deveres para os responsáveis pelo tratamento. Entre esses direitos encontra-se, desde logo, o direito de acesso do titular aos seus dados pessoais (art. 15.º). De acordo com este direito, os indivíduos têm o direito de saber se os seus dados estão a ser objeto de tratamento e, em caso afirmativo, podem aceder aos seus dados pessoais, "com facilidade e a intervalos razoáveis"[134]. Nesse sentido, o responsável pelo tratamento deve fornecer uma cópia dos dados pessoais em fase de tratamento, nos termos do art. 15.º n.º 3[135]. Ainda que os dados brutos possam ser incompreensíveis para os utilizadores – mais interessados, claro está, nos dados interpretados – o direito de acesso permite que possam optar por um serviço que não o proposto pelo fabricante do dispositivo, transferindo os seus dados para outro responsável pelo tratamento[136]. Ademais, o direito de acesso é uma manifestação evidente do princípio da transparência porque pressupõe igualmente o acesso às informações elencadas no art. 15.º n.º 1[137]. Ainda num reflexo do princípio da transparência, o Regulamento reconhece também um direito de retificação (art. 16.º), segundo o qual, o titular pode retificar os dados pessoais inexatos ou completar os dados pessoais incompletos[138]. É ainda reconhecido um direito ao apagamento dos dados

---

reform and the challenges of big data: remaining uncertainties and ways forward", *Information & Communications Technology Law*, 2017, págs. 99 e ss. Também A. ALVES LEAL, págs. 129 e ss.

[134] Nos termos do Considerando 63, "*Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude".*

[135] Estamos aqui perante uma manifestação evidente do direito à portabilidade (art. 20.º), "uma variante do direito de acesso", GT29, "Parecer 8/2014", v. pág. 22. Sobre o direito à portabilidade, v. D. PEREIRA DUARTE e ALEXANDRA GUSEINOV, "O direito de portabilidade de dados pessoais", *in Fintech – Novos estudos…*, págs. 105 e ss. Num sentido crítico, M. LEONOR TEIXEIRA, entende que este direito "não cuida de proteger o responsável pelo tratamento de potenciais abusos na utilização de dados que recolheu, tratou e organizou", "A União Europeia e a Proteção de Dados Pessoais – «Uma visão futurista»?", *Revista do Ministério Público*, n.º 135, Ano 34, 2013, cit., pág. 98.

[136] Como explica o GT29, na falta de um direito de acesso, "essas pessoas não têm outra possibilidade para além de interromper a utilização dos seus dispositivos", pelo que se pretende também "desbloquear os impedimentos à concorrência e ajudar novos intervenientes a inovar neste mercado", GT29, "Parecer 8/2014", v. págs. 22 e 23.

[137] Nos termos do Considerando 63, "*cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências*".

[138] Este direito é particularmente relevante no âmbito da definição de perfis, v. "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679", *Grupo de*

(também conhecido por "direito ao esquecimento" ou "direito a ser esquecido"[139]), que confere ao titular o direito de obter do responsável pelo tratamento, sem demora injustificada, o apagamento dos seus dados pessoais, mediante a verificação dos motivos elencados no art. 17.º n.º 1.

De facto, a transparência é há muito um valor importante consagrado no direito da União Europeia. Mas, em matéria de proteção de dados pessoais, o RGPD vem reforçar fortemente esta ideia, tendo em conta que a DPD não lhe fazia qualquer referência explícita[140]. Com efeito, para além da exigência de que os dados sejam "*objeto de um tratamento lícito e leal*", o art. 5.º n.º 1 al. a) do RGPD acrescenta agora que esse tratamento deve também ser "*transparente em relação ao titular dos dados*". O GT29 afirma a transparência como um corolário do princípio da lealdade que passa por "criar confiança nos processos que afetam os cidadãos fazendo com que estes compreendam e, se necessário, se oponham a esses processos"[141]. Ora, na *IoT*, parece inconciliável, por um lado, querer garantir que os utilizadores saibam da recolha e do tratamento dos seus dados pessoais quando, por outro lado, "os sensores são concebidos para serem discretos, ou seja, para serem o mais invisíveis possível"[142].

Os requisitos em matéria de informação estão presentes nos arts. 12.º a 14.º e são aplicáveis ao longo de todo o tratamento e independentemente do seu fundamento jurídico. O art. 12.º define as regras gerais aplicáveis ao fornecimento de informações ao titular (13.º e 14.º), às comunicações relativas ao exercício dos seus direitos (15.º a 22.º) e ainda nos casos de

---

Trabalho do Artigo 29.º para a Proteção de Dados, 2018, pág. 19. Num sentido crítico à dificuldade de exercício deste direito por parte do titular, SANDRA WACHTER escreve que *"unfortunately,these rights also do not require data controllers to indicate precisely which data was (most) relevant to a particular decision or effect of identification or profiling. As a result, individuals may have to comb through thousands of entries to identify potentially inaccurate, incomplete, or misleading data"*, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR", *Computer Law & Security Review*, N.º 34, 2018, cit., pág. 445.

[139] Sobre o direito ao esquecimento, *vide* A. PERESTRELO DE OLIVEIRA, "Direito ao apagamento dos dados ou «direito a ser esquecido»", *in Fintech – Novos estudos*…, págs. 89 e ss. *Vide* ainda a crítica de FILIPA U. CALVÃO à denominação deste direito: "não se pretende, pois, um apagar da história" pelo que a designação não é "a mais apropriada", "A proteção de dados pessoais na internet: desenvolvimentos recentes", *Revista de Direito Intelectual*, n.º 2, 2015, pág. 79. Também M. LEONOR TEIXEIRA defende que este direito e o direito à portabilidade sofrem de uma necessidade de desenvolvimento, v. pág. 106.

[140] Apenas no Considerando 38 da DPD estipulava que *"a pessoa em causa deve poder ter conhecimento da existência dos tratamentos e obter, no momento em que os dados lhe são pedidos, uma informação rigorosa e completa das circunstâncias dessa recolha"*.

[141] "Orientações relativas à transparência na aceção do Regulamento 2016/679", *Grupo de Trabalho do Artigo 29.º para a Proteção de Dados*, 2018, pág. 5.

[142] GT29, "Parecer 8/2014", pág. 18.

violações de dados pessoais (34.º)[143]. Quanto à forma de apresentação destas informações, o art. 12.º n.º 1 prescreve que essas informações devem ser prestadas "*de forma conscisa, transparente, intelegível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças*"[144]. O artigo estipula ainda que as informações devem ser "*prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos*", havendo ainda a possibilidade de "*ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios*". O art. 12.º n.º 5 acrescenta que todas estas informações devem ser "*fornecidas a título gratuito*"[145].

Como perceberemos melhor, o cumprimento dos deveres de informação será um verdadeiro desafio na *IoT*, tendo em conta que os dispositivos que recolhem os dados pessoais geralmente assumem um tamanho reduzido, não possuem um ecrã nem um mecanismo de *input* (como um teclado ou um ecrã táctil) que permita a exibição das políticas de privacidade[146]. Assim, devem ser procurados meios alternativos de revelação dessas informações, tais como, ícones, códigos QR, alertas de voz, indicações escritas em papel, vídeos, mensagens enviadas por *SMS* ou por correio eletrónico, entre outros[147]. Já no Parecer 8/2014, o GT29 sugeria que se imprimissem códigos *QR* ou um *flashcode* nos dispositivos, que, mediante leitura, informassem o titular sobre o tipo de sensores, as informações

[143] É de referir igualmente o importante papel das Avaliações de Impacto no sentido de reforçar a confiança dos utilizadores, razão pela qual o GT29 recomenda a sua publicação: "os responsáveis pelo tratamento devem considerar, pelo menos, a publicação parcial da AIPD, por exemplo, um resumo ou uma conclusão", "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679", *Grupo de Trabalho do Artigo 29.º para a Proteção de Dados*, 2017, cit., pág. 21. A *IoT* é, de resto, neste âmbito, alvo de particular preocupação por parte do GT29: "algumas aplicações da «Internet das Coisas» podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD", cit., pág. 12. Sobre as avaliações de impacto, *vide* JOANA MOTA, "Proteção de dados desde a conceção e por defeito. Avaliação de impacto e segurança" *in Fintech – Novos Estudos…*, págs. 141 e ss.

[144] Neste sentido, o considerando 39 dispõe que "*o princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples*". Como entende o GT29, "a qualidade, a acessibilidade e a compreensIbilidade das informações são tão importantes como o conteúdo", "Orientações relativas à transparência…", cit., pág. 6.

[145] O art. 5.º n.º 2 atribui ao responsável pelo tratamento a responsabilidade de assegurar a transparência e o poder de comprovar que os dados foram tratados de forma transparente. Também neste sentido, o art. 24.º n.º 1.

[146] SCOTT R. PEPPET, pág. 140.

[147] GT29, "Orientações relativas à transparência…", v. pág. 25. De resto, o RGPD sugere no art. 12.º n.º 7 que as informações sejam "*dadas em combinação com ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e claramente legível, uma perspetiva geral significativa do tratamento previsto*", acrescentando que "*se forem apresentados por via eletrónica, os ícones devem ser de leitura automática*".

recolhidas e as finalidades dessa recolha[148]. Como veremos, a transparência é um valor transversal a todo o regulamento, com implicações, desde logo, nas informações prestadas ao titular dos dados tendo em vista a prestação do seu consentimento para o tratamento.

5.2 Consentimento

O art. 4.º n.º 11 do RGPD define consentimento como *"uma manifestação de vontade, livre, específica, informada e explicita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".* Tal como na anterior Diretiva[149], o consentimento continua a ser um dos fundamentos de licitude do tratamento de dados pessoais, nos termos do artigo 6.º[150]. Porém, o RGPD vem aumentar a exigência na obtenção de um consentimento válido, ao clarificar mais detalhadamente os seus requisitos necessários.

Elegeriamos o consentimento como o grande *calcanhar de Aquiles* no uso de dispositivos inteligentes. Na verdade, todo modo de funcionamento e estruturação da *IoT* entrará em ruptura com os modelos atuais de prestação de consentimento. Como defende o Parecer 8/2014 do GT29, muito frequentemente, o utilizador não chega sequer a ter conhecimento do tratamento de dados efectuado pelos sensores. Como se lê no documento, "a comunicação entre objetos pode ser desencadeada automaticamente, bem como por predefinição, sem o conhecimento do indivíduo". Além disso, alguns dispositivos, os vestíveis em particular, como os *smart watches*, não são facilmente detetáveis. Com efeito, é difícil distinguir um

[148] GT29, "Parecer 8/2014", v. pág. 20.

[149] Em jeito de comparação, na Diretiva 95/46/CE o consentimento era definido, no artigo 2.º al. h), como "*qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento*", exigindo o artigo 7.º al. a) que esse consentimento fosse "*dado de forma inequívoca*".
A importância do consentimento é realçada nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (em diante, CDFUE), onde se pode ler, no artigo 8.º n.º 2, que os dados pessoais "*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*".

[150] Não obstante, curiosamente, o mesmo não sucedia com a legislação transposta da referida Diretiva. Na verdade, ao contrário do que acontecia na Lei 67/98, no RGPD o consentimento é colocado "em pé de igualdade" com as restantes condições de licitude, v. MAFALDA M. BARBOSA, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil", *Estudos de Direito do consumidor*, N.º 12, Coimbra, Centro de Direito Do Consumo/FDUC, 2017, pág. 91.

relógio normal de um relógio inteligente, quando, "este último pode incorporar câmaras, microfones e sensores de movimento capazes de registar e transferir dados"[151].

Para o consentimento ser válido deve ser "*livre*", ou seja, deve implicar uma verdadeira escolha e controlo, sem coação, por parte do titular dos dados[152]. Destacamos, com especial relevância para o presente trabalho, a previsão do art. 7.º n.º 4 que estabelece que a execução de um contrato ou a prestação de um serviço, não pode estar dependente do consentimento que não é necessário para esse fim[153]. De facto, como explica o GT29, muitas vezes, "a possibilidade de renunciar a determinados serviços ou funcionalidades de um dispositivo IdC é mais um conceito teórico do que uma alternativa real"[154]. A liberdade do consentimento depende ainda da verificação do requisito da *granularidade*, o qual impõe que o consentimento seja dado separadamente, para cada finalidade, e não em conjunto[155].

O requisito da granularidade é exigido também para que o consentimento possa ser "*específico*"[156]. Além disso, o elemento da especificidade exige a especificação em função da finalidade contra o chamado *desvirtuamento da função* – isto é, "o alargamento ou a diluição progressiva das finalidades para as quais os dados são processados" – e ainda a separação clara entre as informações relacionadas com a obtenção do consentimento e as informações sobre outras questões[157].

---

[151] GT29, "Parecer 8/2014", cit., pág. 8.

[152] O GT29 chama uma atenção particular para os casos em que há um desequilíbrio de poder entre o titular dos dados e o responsável pelo tratamento, nomeadamente quando este último é uma autoridade pública ou um empregador, "Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679", *Grupo de Trabalho do Artigo 29.º para a Proteção de Dados*, 2018, v. págs. 6 e ss. Neste sentido, o Considerando 43, "*a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública (…)"*.

[153] Como entende o GT29, "o RGPD assegura que o tratamento dos dados pessoais relativamente ao qual se solicita o consentimento não pode ser direta ou indiretamente uma contrapartida da execução de um contrato", "Orientações relativas ao consentimento…", cit., pág. 8. Também neste sentido, a parte final do Considerando 43.

[154] GT29, "Parecer 8/2014", pág. 8.

[155] Segundo o GT29, "se o responsável pelo tratamento interligar várias finalidades de tratamento sem tentar procurar separar o consentimento para cada finalidade, estamos perante falta de liberdade", "Orientações relativas ao consentimento…", v. pág. 11. Neste sentido, o Considerando 43: "*presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico".*

[156] O art. 6.º n.º 1 al. a) estabelece que o consentimento deve ser dado "*para uma ou mais finalidades específicas*". No mesmo sentido, dispõe o Considerando 32, que "*o consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins*".

[157] GT29, "Orientações relativas ao consentimento…", v. pág. 13. A. MENEZES CORDEIRO acrescenta ainda uma quarta dimensão: a "especificação dos dados a tratar", "O consentimento do titular dos dados no RGPD", *in Fintech – Novos estudos…*, v. pág. 50.

Quanto ao consentimento "*informado*", obriga a que se forneçam informações aos titulares dos dados para que estes tomem decisões esclarecidas. Nomeadamente, entende o GT29, são necessárias, pelo menos, informações sobre a identidade do responsável pelo tratamento, a finalidade de cada uma das operações de tratamento[158], o tipo de dados recolhidos, a existência do direito de retirar o consentimento, a utilização dos dados para decisões automatizadas e ainda informações sobre os riscos das transferências de dados para países terceiros devido à inexistência de uma decisão de adequação ou de garantias adequadas, nos termos do art. 46.º[159]. Diriamos que a prestação de um consentimento informado na *IoT* é comprometida, sobretudo, por duas dificuldades: a imprevisibilidade e a interpretabilidade. Por um lado, parece impossível que, quer o titular, quer o responsável pelo tratamento possam antever as utilizações a que os dados serão sujeitos após a recolha. Por outro, a excessiva complexidade técnica dos métodos analíticos usados no tratamento obsta a que possam ser "traduzidos" numa linguagem acessível ao titular[160].

Quanto à exigência de um consentimento "*inequívoco*", impõe que o consentimento seja dado por meio de uma ação positiva ou declaração[161]. Trata-se, como vimos, de uma exigência desenvolvida no RGPD, mas que a DPD não previa. Por "*ato positivo inequívoco*" deve entender-se que o titular "deve agir deliberadamente para consentir o tratamento em causa"[162]. Destacariamos, neste particular, a rejeição do silêncio e das chamadas opções pré-assinaladas, bem como da aceitação do contrato e das condições gerais, como formas de obtenção de um consentimento inequívoco[163].

---

[158] Neste sentido, o Considerando 42 indica: "*para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina*".

[159] GT29, "Orientações relativas ao consentimento…", págs. 14 e 15. Opondo-se a esta limitação do direito à informação e propondo um conjunto mais amplo de informações devidas aos titulares, v. A. MENEZES CORDEIRO, pág. 52.

[160] Neste sentido, TAL Z. ZARSKY: "*quite often, analyzing Big Data involves methods and usage patterns which neither the entity collecting the data nor the data subject considered or even imagined at the time of collection*", cit., págs. 1005 e 1006 e SANDRA WACHTER: "*long and complicated privacy notices have proven to be ineffective, as users often do not read them*", cit., pág. 446.

[161] O considerando 32 preenche este conceito indicando que o consentimento pode ser dado, "*por exemplo, mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral (...) validando uma opção ao visitar um sítio web na Internet (...) ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais*".

[162] GT29, "Orientações relativas ao consentimento…", pág. 17.

[163] Como dispõe o Considerando 32, "*o silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento"*. Quanto ao silêncio, no entanto, como lembra A. MENEZES CORDEIRO, as partes poderão atribuir-lhe um conteúdo positivo, pág. 54. Além disso, caem assim por terra, em princípio, as propostas de pré-consentimento baseadas nas preferências de privacidade dos utilizadores, sugeridas por alguns autores, em particular, na literatura americana, a passagem do *Notice & Choice* para o

Como vimos, os dispositivos inteligentes não dispõem de características físicas que lhes permitam exibir avisos de privacidade, razão pela qual essas informações costumam ser publicadas na embalagem do aparelho, na aplicação móvel que lhe está associada, ou, sobretudo, nos *sites* dos fabricantes. Porém, estudos têm alertado para várias deficiências nestas políticas, que vão desde ambiguidades nos termos usados, a omissões de informações importantes sobre o tratamento subjacente[164]. Têm vindo, no entanto, a ser apresentadas outras soluções especialmente concebidas para a *IoT* e que vão ao encontro destas exigências regulatórias, nomeadamente, a utilização de *sticky policies* ou de *proxies* para privacidade[165]. De resto, a este propósito, embora o RGPD não preveja expressamente que o consentimento deva ser dado antes da atividade de tratamento, essa anterioridade retira-se implicitamente, nomeadamente, da redação do art. 6.º n.º 1 al. a) e do Considerando 40[166].

Choice & Notice, v. M. LETA JONES, "Privacy without screens & the internet of other people's things", *Idawo Law Review*, 2015, págs. 653 e ss.
Ainda assim, o RGPD continua sem responder a todas as questões. Como questiona JOÃO FACHANA, a propósito da *IoT*, "o facto do titular dos dados ter adquirido o objeto é suficiente para concluir pela sua concordância no processamento dos dados (…)? E se estivermos a falar de um titular de dados estranho a esse objeto? (…) por exemplo, um grupo de amigos que se reúne em casa de um deles, equipada por uma *smart TV*", cit. págs. 101 e 102. Ou, como afirma A. MENEZES CORDEIRO, "o simples facto de um titular entrar num espaço que se encontra sujeito a vigilância vídeo não significa que consinta no tratamento de dados pessoais aí recolhidos", cit., pág. 55. Também neste aspeto se detem MAFALDA M. BARBOSA, defendendo que não obstante a rejeição expressa da relevância do silêncio como declaração de vontade, "persistem dúvidas acerca do comportamento concludente como via de manifestação de vontade do sujeito", cit., pág. 94.

[164] *Vide* o estudo de SCOTT R. PEPPET, págs. 140 e ss. Como conclui o autor, *"in short, this policies seem to have been shaped by the needs and expectations relevant to the normal Internet, not the Internet of Things".* Neste sentido, também o GT29: "a prática revela, no entanto, que frequentemente os pedidos de autorização feitos por criadores de aplicações de terceiros não apresentam informações suficientes para que o consentimento do utilizador possa ser considerado específico e suficientemente informado", "Parecer 8/2014", cit., pág. 13.

[165] GT29, "Parecer 8/2014", pág. 23, notas 29 e 30. Por exemplo, SANDRA WACHTER refere-se à modalidade de *consentimento dinâmico* e refere o exemplo do "privacy coach": *"an RFID reader embedded in a mobile phone that scans an object and downloads its privacy policy, then compares it to the user's privacy preferences and provides a recommendation about whether the device meets the user's requirements, and thus whether it should be used*", v. pág. 445. Sublinhe-se que o que está aqui em causa é uma recomendação com base nas preferências de privacidade pré-definidas pelo utilizador e não um pré-consentimento prestado unilateralmente pelo dispositivo. Trata-se, por assim dizer, de um meio "facilitador" do consentimento face à complexidade das políticas de privacidade, mas que jamais poderá substituir a vontade de consentir do usuário. *Vide* também as sugestões apresentadas por A. MENEZES CORDEIRO de "atos inequívocos menos clássicos", pág. 55.

[166] O referido artigo prescreve "*tiver dado*", o que parece impor que o consentimento seja sempre dado por via de *opt in* (i.e., antes do início do tratamento). Também neste sentido, o Considerando 40 dispõe que "*para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento do titular dos dados em causa ou noutro fundamento legítimo*". Também neste sentido, S. NAVAS NAVARRO, "Derecho e inteligencia…", pág. 67. Como refere JOÃO FACHANA, "esta nova formulação implicará a ilegitimidade do processamento de dados automática em que o titular, para impedir o tratamento, tenha de clicar num determinado botão a declarar que não dá o seu consentimento (*opt out*), assim como limitará as possibilidades da existência de consentimento implícito", pág. 106.

O RGPD confere também ao titular o direito de retirar o consentimento a qualquer momento[167]. As condições aplicáveis ao consentimento figuram no art. 7.º. Desde logo, o n.º 1 estipula a obrigação de o responsável pelo tratamento demonstrar que o titular dos dados deu o seu consentimento[168]. Além disso, de acordo com o artigo 7.º n.º 3, "*o consentimento deve ser tão fácil de dar quanto de retirar*", pelo que, em princípio, o consentimento deve poder ser retirado do mesmo modo com que foi dado[169]. Suponhamos, se o consentimento foi dado a partir de um relógio inteligente, esse mesmo dispositivo deve possibilitar a retirada do mesmo[170].

Há situações que envolvem um risco acrescido para a proteção de dados e para as quais o RGPD exige um *consentimento explícito*[171]. Segundo o GT29, o termo "*explícito*", "significa que o titular dos dados deve manifestar expressamente o consentimento", sugerindo várias formas de proceder nesse sentido. Desde logo, através de uma declaração escrita (que pode ser assinada pelo titular), ou por uma declaração oral (uma chamada telefónica, por exemplo). Em contexto digital, pode ser preenchido um formulário eletrónico, pode ser enviada uma mensagem de correio eletrónico, pode recorrer-se à assinatura eletrónica ou pode ser digitalizado um documento com a assinatura do titular[172].

---

[167] Esta é mais uma novidade do RGPD face à DPD, embora, nesta última, já se reconhecesse implicitamente um direito de revogação, v. A. MENEZES CORDEIRO, pág. 57. Já no "Parecer 15/2011 sobre a definição de consentimento", o GT29 apoiava o reconhecimento expresso do direito de revogação do consentimento, v. pág. 41.

[168] Como determina o Considerando 42, "*sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados*".

[169] Poderá, claro está, ser retirado de um modo ainda mais fácil, como refere A. MENEZES CORDEIRO, "a lei estabelece um máximo – quanto à forma e formalidades – mas já não um mínimo", v. pág. 59. Além disso, também aqui releva a obrigação de transparência do responsável pelo tratamento, na medida em que o titular dos dados deve ser informado deste direito bem como do modo como poderá exercê-lo.

A retirada de consentimento não se aplica retroativamente, pelo que, em princípio, as operações de tratamento de dados baseadas no consentimento retirado permanecem lícitas. Porém, salvo a existência de outro fundamento legal que justifique a conservação, os dados devem ser apagados, nos termos do art. 17.º n.º 1 al. b) e n.º 3.

É por isso que o responsável pelo tratamento deve, antes da recolha dos dados, ser claro quanto às finalidades e ao fundamento legal do tratamento, sob pena de não poder "migrar silenciosamente" para outro fundamento e ter de, claro está, voltar a notificar o titular nesse sentido, em conformidade com os deveres de informação, v. GT29, "Orientações relativas ao consentimento", págs. 25 e 26. Também neste sentido, o Considerando 65.

[170] O GT29 refere-se diretamente aos dispositivos *IoT*, explicando que "mudar para outra interface unicamente para efeitos de retirada do consentimento exigiria um esforço indevido", acrescentando ainda que esta possibilidade deve ser dada "de forma gratuita ou sem baixar os níveis do serviço", v. "Orientações relativas ao consentimento…", págs. 24 e 25.

[171] É o que acontece no âmbito do artigo 9.º a propósito do tratamento de categorias especiais de dados, no artigo 49.º, relativamente às transferências de dados para países terceiros ou organizações internacionais na ausência de uma decisão de adequação ou de garantias adequadas e ainda no art. 22.º, sobre as decisões individuais automatizadas incluindo definição de perfis.

[172] GT29, "Orientações relativas ao consentimento…", págs. 21 e 22.

O RGPD confere ainda uma proteção reforçada aos dados pessoais das crianças, relevante, desde logo, neste estudo, no âmbito da utilização dos *smart toys*. Nos termos do artigo 8.º n.º1, quando o fundamento de licitude for o consentimento, no que respeita à oferta direta de bens e serviços da sociedade da informação às crianças, o tratamento é lícito se elas tiverem pelo menos 16 anos[173]. Se a criança tiver menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares da responsabilidade parental (podendo os estados-membros definir um limite diferente, desde que não seja inferior a 13 anos[174]). Ademais, o responsável pelo tratamento deve encetar esforços no sentido de fornecer às crianças um "consentimento informado", simplificando as informações que lhes são transmitidas[175].

5.3 Limitação da finalidade e minimização dos dados

Tal como o consentimento, o princípio da limitação das finalidades também decorre do artigo 8.º n.º2 da CDFUE e segue igualmente as orientações da DPD. Este princípio está previsto no artigo 5.º n.º1 al. b) do RGPD, nos termos do qual "*os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades*"[176]. Assim, as finalidades da recolha dos dados devem ser "*determinadas, explícitas e legítimas*". Seguindo as orientações do GT29[177], com a expressão "*determinadas*", o legislador quer dizer que o responsável pelo tratamento se deve abster de recolher dados que não sejam necessários, adequados ou relevantes para a

[173] Neste sentido, dispõe o Considerando 38 que "*as crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças*". Para mais detalhes, consultar GT29, "Orientações relativas ao consentimento…", págs. 28 e ss.

[174] Num tom crítico a esta possibilidade de conformação dos estados-membros, v. M. LEONOR TEIXEIRA, pág. 93. Entretanto, já sabemos que a lei que executa o Regulamento em Portugal, preferiu o limite mínimo de 13 anos de idade.

[175] Como prescreve o Considerando 58, "*uma vez que as crianças merecem proteção específica, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá estar redigida numa linguagem clara e simples que a criança compreenda facilmente*".

[176] O art. 6.º n.º 1, al. b) da anterior Diretiva, numa redacção praticamente igual à do RGPD, impunha aos estados-membros que garantissem que os dados são "*recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades*".

[177] Seguimos, neste ponto, a "Opinion 03/2013 on purpose limitation" do GT29.

finalidade pretendida[178]. Não é possível, deste modo, contornar este princípio delimitando amplamente as finalidades do tratamento. As finalidades devem também ser "*explícitas*", isto é, devem ser "reveladas, explicadas e expressas de um modo inteligível" e sem ambiguidades, igualmente, antes do momento da recolha dos dados[179]. Por fim, as finalidades devem ser "*legítimas*", ou seja, devem estar em conformidade com a lei, entendida aqui num sentido amplo.

O artigo admite, no entanto, que os tratamentos realizados após a recolha dos dados se baseiem, quer na finalidade inicial, quer noutra, desde que compatível com aquela[180]. Acrescenta, por fim que "*o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º n.º1*". De facto, esta exceção relativa aos *fins estatísticos* poderia constituir uma *válvula de escape* que abrisse caminho às práticas do *Big Data*, a partir, nomeadamente, dos dados dos utilizadores de dispositivos *IoT*, mas, repare-se, a este propósito, que o Considerando 162 alerta para que *"esses resultados ou os dados pessoais não sejam utilizados para justificar medidas ou decisões tomadas a respeito de uma pessoa singular*"[181].

O princípio da "minimização dos dados" (*Data Minimization*), está intimamente ligado ao princípio da limitação das finalidades[182], e encontra-se presente no art. 5.º n.º1 al. c), o qual estabelece que os dados devem ser *"adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados"*[183]. Assim, como refere o GT29, "os

[178] Além disso, esta especificação das finalidades deve ser feita antes da recolha dos dados, de modo a que seja possível estabelecer as medidas de proteção de dados adequadas e perceber se o tratamento de dados é feito de acordo com a lei, v. GT29, "Opinion 03/2013", págs. 15 e ss.

[179] Trata-se, este, de um imperativo decorrente dos princípios da transparência e da previsibilidade que visa oferecer a todos os intervenientes – não apenas ao titular dos dados, mas também ao responsável pelo tratamento, subcontratantes, autoridades de proteção de dados e outras partes interessadas – um entendimento comum sobre o uso posterior dos dados pessoais, v. GT29, "Opinion 03/2013", pág. 17.

[180] Esta compatibilidade deve ser aferida em concreto nos termos definidos pelo art. 6.º n.º 4, nomeadamente, tendo em conta a ligação entre a finalidade inicial e a finalidade do tratamento posterior, o contexto em que os dados foram recolhidos, a natureza dos dados pessoais, as consequências do tratamento posterior e ainda a existência de salvaguardas adequadas. Para mais desenvolvimentos, v. GT29, págs. 23 e ss.

[181] Neste sentido, e alargando a crítica ao art. 6.º n.º 4, v. TAL Z. ZARSKY, págs. 1007 e 1008.

[182] "O princípio da limitação da finalidade está intrinsecamente ligado ao princípio da minimização dos dados", "Parecer 2/2013 sobre as aplicações em dispositivos inteligentes", *Grupo de Trabalho do Artigo 29.º para a Proteção de Dados*, 2013, cit., pág. 18. Porém, ao contrário daquele, este princípio não está especificamente previsto na CDFUE, uma omissão que oferece às autoridades europeias uma maior discricionaridade na definição dos seus limites, v. TAL Z. ZARSKY, pág. 1009.

[183] Na DPD este princípio já estava presente no art. 6.º n.º 1 al. c), o qual previa que os dados pessoais devem ser "*adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente*".

dados que sejam desnecessários para esse fim não devem ser recolhidos e armazenados *para qualquer eventualidade* ou porque *podem vir a ser úteis*" e devem ser apagados logo que cumpram a sua finalidade[184]. Este princípio tem várias dimensões: desde logo, refere-se ao âmbito e categorias dos dados inicialmente recolhidos, à duração limitada durante a qual os dados pessoais podem ser retidos e à exigência de que esses dados sejam apagados após o uso pretendido[185].

O respeito pela minimização dos dados exige, sobretudo neste âmbito, a prossecução dos princípios da privacidade por defeito (*privacy by default*) – que obriga que o tratamento se limite ao estritamente necessário para as finalidades pretendidas – e da privacidade desde a conceção (*privacy by design*) – que impõe que o respeito pela privacidade do utilizador seja pensado preventivamente, isto é, desde a fase de desenvolvimento do dispositivo[186]. Neste último caso, como prevê o art. 25.º, podem ser usadas técnicas como a pseudonimização[187], não obstante o prejuízo para a qualidade dos dados. O grande receio de um princípio assim concebido, prende-se com a possibilidade evidente de a limitação da recolha aos dados estritamente necessários, venha a constituir um "obstáculo à inovação"[188], dado o grande interesse (e dependência) por parte das tecnologias emergentes, do máximo de conhecimento acerca dos utilizadores.

5.4 Categorias especiais

À semelhança do que acontecia na Diretiva, o RGPD também confere uma proteção especial a certos tipos de dados pessoais relacionados com informações mais íntimas. Assim, nos termos do art. 9.º, *"é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica,*

[184] Mediante notificação prévia ao utilizador, v. GT29, "Parecer 8/2014", págs. 18 e 19.
[185] Como se lê no art. 25.º n.º 2, esta "*obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade*". De resto, este art. 25.º obriga o responsável pelo tratamento a adotar "*medidas técnicas e organizativas 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 este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados*".
[186] Sobre estes conceitos, v. JOANA MOTA, págs. 129 e ss. Também neste sentido, o Considerando 78.
[187] Pseudonimização é "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados especifico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular indentificada ou identificável", F. MATIAS MAGALHÃES e M. LEITÃO PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático*, 2ªedição revista e ampliada, pág. 11 (versão *e-book*).
[188] Neste sentido, v. GT29, "Parecer 8/2014", pág. 18.

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[189] *ou dados relativos à vida sexual ou orientação sexual de uma pessoa*". Porém, o RGPD veio alargar o leque de categorias especiais apresentado pelo regime anterior, passando a integrar também o tratamento de dados genéticos e biométricos para a identificação inequívoca de uma pessoa, bem como os dados relativos à orientação sexual[190]. O processamento dessa informação é ainda possível sujeito a um *consentimento explícito* ou em situações em que se apliquem as exceções específicas previstas no n.º2.

Porém, na era da *IoT*, em que se antevêem as já relatadas práticas maciças de análise e tratamento de grandes volumes de dados, questiona-se, se continuará a fazer sentido atribuir a um conjunto específico de dados pessoais um estatuto especial como este, tendo em conta que, como vimos, será possível inferir informações sensíveis a partir de dados aparentemente insignificantes. Esta é uma questão que também já foi levantada pelo GT29: segundo orientações adotadas em 2017, "a definição de perfis pode criar dados de categorias especiais por inferência a partir de dados que não sejam dados de categorias especiais *per se*, mas que passem a sê-lo quando combinados com outros dados"[191]. Assim, estaremos perto de admitir que as categorizações deste tipo que visam proteger especialmente certos dados considerados mais sensíveis, assumirão um valor meramente simbólico na senda desta nova revolução tecnológica[192].

---

[189] *Vide* a noção ampla de dados relativos à saúde definida pelo Considerando 35: "*Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro (...)*".

[190] Nos termos do art. 8.º n.º 1 da Diretiva, "*Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual".*

[191] Por exemplo, "existe a possibilidade de inferir o estado de saúde de uma pessoa a partir de registos das suas compras de produtos alimentares, em combinação com dados relativos à qualidade e ao valor energético dos alimentos". Nestes casos, o GT29 recomenda que o responsável pelo tratamento assegure a compatibilidade do referido tratamento com a finalidade inicial, encontre um fundamento lícito para o tratamento de dados das categorias especiais e informe o titular sobre o referido tratamento, v. "Orientações sobre as decisões…", págs. 16 e 17.

[192] Como questiona TAL Z. ZARSKY, "*if nearly all forms of data categories and data sets can produce special data, why even bother with this distinction, which is rendered almost artificial?*", cit., pág. 1013. Também neste sentido, problematiza SCOTT R. PEPPET, sobre se continuará a fazer sentido distinguir, na legislação americana, "*Personally Identifiable Information (PII)*", apresentando algumas soluções já estudadas, v. págs. 132 e 133.

5.5 Decisões individuais automatizadas e definição de perfis

O art. 22.º atribui ao titular dos dados *"o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar"*[193]. Este artigo estabelece uma proibição geral, ou seja, aplica-se independentemente de ser invocado pelo titular dos dados[194]. A decisão em causa deve ser "*tomada exclusivamente com base no tratamento automatizado*", ou seja, não pode haver qualquer intervenção humana no processo decisório. É pertinente reparar, neste aspeto, na ressalva feita pelo GT29, em que estabelece que esta intervenção humana não pode ser um "mero gesto simbólico" mas sim algo relevante e feito por alguém "com autoridade e competência para alterar a decisão"[195], tentando impedir, assim, que o responsável pelo tratamento ficcione uma insignificante intervenção humana com o único intuito de escapar à proibição do artigo[196]. Além disso, o RGPD não indica o que se deve entender por "*efeitos na sua esfera jurídica ou que o afete significativamente de forma similar*" mas depreende-se que estejam em causa apenas as decisões que causem "impactos graves"[197].

---

[193] Já o art. 15.º da DPD dispunha que *"os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento".*

[194] Como entende o GT29, esta interpretação do art. 22.º como uma proibição e não como um direito "significa que as pessoas estão automaticamente protegidas dos possíveis efeitos deste tipo de tratamento", "Orientações sobre as decisões…", cit., pág. 21. Em sentido diferente, concebendo o art. 22.º como um "direito de *opt out*", *vide* M. PERESTRELO DE OLIVEIRA, págs. 80 e ss.

É importante distinguir "*decisões individuais automatizadas*" de "*definição de perfis*". Segundo o GT29, as primeiras "correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana", enquanto a segunda surge expressamente definida no art. 4.º n.º 4 do RGPD como "*qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações*". Fundamentalmente, a definição de perfis implica a avaliação de uma pessoa no sentido de inferir algo sobre ela, enquanto as decisões automatizadas implicam uma tomada de decisão que pode (ou não) resultar daquela definição de perfis. Para mais detalhes, v. GT29, "Orientações sobre as decisões…", págs. 6 e ss. M. PERESTRELO DE OLIVEIRA, evidencia que apenas nas decisões automatizadas o processo é "totalmente automatizado", v. págs. 68 e ss.

[195] GT29, "Orientações sobre as decisões…", v. pág. 23.

[196] Deixam de fazer sentido, assim, em princípio, as críticas apontadas por alguns autores sobre a facilidade com que os responsáveis pelo tratamento poderiam contornar este artigo, v. TAL Z. ZARSKY, págs. 1016 e 1018. Também neste sentido, M. PERESTRELO DE OLIVEIRA, pág. 75. A autora acrescenta que o referido direito "não existe se o tratamento de dados for anonimizado ou pseudonimizado", v. nota 38.

[197] Para uma densificação destas expressões, v. GT29, págs. 23 e ss. *Vide* também o Considerando 71. Também M. PERESTRELO DE OLIVEIRA, págs. 76 e ss. Em jeito de crítica à indeterminação deste preceito, v. SANDRA WACHTER, pág. 443.

Este artigo pode ser visto como um verdadeiro entrave à revolução digital em curso. É que, ao incentivar, deste modo, a "humanização" do tratamento dos dados pessoais, o RGPD contraria as estruturas de base de tecnologias como a *IoT*, as técnicas de *machine learning* e o *Big Data*, voltadas para o tratamento de dados exclusivamente automatizado[198]. O Regulamento parece duvidar do sentido de justiça das máquinas, encarando a intervenção humana como uma garantia da equidade das decisões, mas, como entendem alguns autores, "em breve, as máquinas poderão ultrapassar algumas limitações humanas e tomar decisões comprovadamente mais justas"[199].

A definição de perfis adquiriu um papel central no RGPD face à Diretiva anterior. Na origem da preocupação regulatória crescente sobre esta matéria está, em particular, a *IoT*. Como defende o GT29, "a disponibilidade generalizada de dados pessoais na Internet e a partir de dispositivos da Internet das Coisas, bem como a capacidade para encontrar correlações e criar relações, podem tornar possível determinar, analisar e prever aspetos que digam respeito à personalidade ou ao comportamento, aos interesses e aos hábitos de uma pessoa"[200]. De facto, como vimos, as possibilidades de obtenção de conhecimento e de formatação do comportamento dos utilizadores através da *IoT*, tem levado a uma corrida às informações pessoais por parte das empresas, com prejuízos sérios, como vimos, para a privacidade dos indivíduos, para a justiça social e, enfim, para a sua liberdade de ação[201]. A invisibilidade associada à atividade de definição de perfis e a falta de precisão das decisões individuais automatizadas ajudam a perceber que as obrigações de transparência dos responsáveis pelo tratamento assumam um papel importante neste tópico. Nos termos dos arts. 13.º n.º2 al. f), 14.º n.º2 al. g) e 15.º n.º1 al. h), deve ser comunicada ao titular a existência de decisões

[198] Como afirma TAL Z. ZARSKY, "*article 22 is perhaps the most salient example of the GDPR's rejection of the Big Data revolution*", antevendo que as empresas serão obrigadas a mudar as suas arquiteturas tecnológicas de tratamento de dados para conseguirem respeitar esta regra, v. pág. 1017.

[199] M. PERESTRELO DE OLIVEIRA, cit., pág. 86. Outra questão é a de saber qual o impacto deste tratamento exclusivamente automatizado das informações pessoais na restrição à privacidade dos indivíduos. Como questionam HILLARY BRILLS e SCOTT JONES, "*Are individuals more confortable with a computer knowing their sensitive information than another person?*", cit. pág. 1200.

[200] GT29, "Orientações sobre as decisões…", cit., pág. 5.

[201] Como problematiza o GT29, "o individuo será pressionado a evitar comportamentos não habituais, a fim de prevenir a deteção de tudo o que possa ser entendido como uma anomalia", cit., "Parecer 8/2014", pág. 10. Também nas "Orientações sobre as decisões…", o GT29 alegava que a definição de perfis pode "amarrar as pessoas a uma categoria específica e limitá-las às respetivas preferências sugeridas, pondo assim em causa a sua liberdade para escolher, por exemplo, determinados produtos ou serviços", cit., pág. 6.

automatizadas, incluindo a definição de perfis, bem como informações sobre a lógica subsequente e sobre a importância e as consequências desse tratamento para o titular[202].

O art. 21.º confere ainda ao titular um direito de oposição ao tratamento de dados que lhe digam respeito, particularmente, para efeitos de comercialização direta, incluindo a definição de perfis, a qualquer momento. Em caso de exercício do direito de oposição, o responsável pelo tratamento deve interromper o processamento (18.º n.º1 al. d)) e apagar os dados pessoais em causa (17.º n.º1 al. c)). Para lá do problema crónico e transversal a todo o Regulamento relativo à ambiguidade dos seus preceitos[203], a operacionalização destes direitos, na prática, sofre de muitas dificuldades técnicas[204]. No caso deste direito de oposição, por exemplo, os aparelhos, muitas vezes, ou não têm como parar o tratamento, ou então, não foram concebidos para funcionar com um acesso limitado aos dados pessoais dos utilizadores[205].

6. Proposta de Superação

6.1 A admissibilidade de uma *descentralização monetizada*

Já percebemos que os dados pessoais possuem hoje um valor incalculável, são considerados o novo petróleo[206]. Neste contexto, em que a valiosa privacidade das pessoas é trocada pela

[202] O considerando 60 sublinha a importância do fornecimento destas informações "*para assegurar um tratamento equitativo e transparente*". Já o Considerando 63, relembramos, dispõe que "*cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente (...) da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências*". Ainda o Considerando 58, preceitua que a transparência *"é especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos (...)*". Finalmente, o considerando 71 fala mesmo de um direito do titular a obter uma "*explicação sobre a decisão tomada*". Em jeito de crítica a este último direito, em particular, no âmbito da *machine learning*, sobre as dificuldades em informar "de forma que seja compreensível para o utilizador médio", v. M. PERESTRELO DE OLIVEIRA, págs. 85 e ss.

[203] Em jeito de crítica à indeterminação dos preceitos, v. SANDRA WACHTER, pág. 443. Também, M. LEONOR TEIXEIRA, pág. 99.

[204] Por exemplo, quanto aos meios de auto-defesa conferidos pelo art. 22.º, M. PERESTRELO DE OLIVEIRA entende que são de "difícil efetivação pelos particulares afectados" e "não funcionam em situações igualmente problemáticas, mas que apenas afetam grupos e não pessoas individuais", v. pág. 87.

[205] Prevendo que os utilizadores serão confrontados com uma escolha de "pegar ou largar", v. SANDRA WACHTER, pág. 443. Daí a preocupação do GT29: "os utilizadores não devem ser penalizados economicamente nem ter um acesso de pior qualidade às capacidades dos seus dispositivos se decidirem que não pretendem utilizar o dispositivo ou um serviço específico", cit., "Parecer 8/2014", pág. 27.

[206] Sobre o crescente valor patrimonial dos dados pessoais, escreve A. PERESTRELO DE OLIVEIRA que "a informação pessoal é, cada vez mais, vista como uma nova categoria de ativo", cit., pág. 71. Também M. LEONOR TEIXEIRA, fala de um "mercado livre, economicista, concorrencial e em que quase tudo pode ser

utilização, em princípio, gratuita, dos dipositivos *IoT*, é essencial definir a quem, afinal, pertencem os dados pessoais. Não obstante o tão proclamado chavão de que "os dados não são das empresas", vivemos numa realidade em que a propriedade sobre os dados pessoais não é dos seus utilizadores. De facto, as empresas têm assumido não apenas o controlo, como sobretudo, a exploração patrimonial das informações pessoais. Como explica LUÍS F. ANTUNES, "há uma cadeia de valor, invisível para o utilizador comum, construída em torno da informação gerada na *IoT*, existindo mesmo uma indústria de recolha e agregação de dados pessoais"[207]. Num quadro destes, em que aparentemente o mercado dos dados pessoais se auto-regula, entendemos que pelo menos uma parte desse valor deve reverter a favor dos titulares dos dados pessoais, em consonância, de resto, com a orientação já admitida no sentido do aproveitamento económico dos bens de personalidade[208].

É neste enquadramento que nos parece interessante apresentar aqui, embora sem grande aprofundamento técnico num trabalho que é jurídico, um modelo de computação descentralizado ou distribuído designado "computação em nevoeiro" (em inglês, *fog computing* também conhecido por *edge computing*[209]). Tradicionalmente, o processamento da informação é feito a partir de um modelo de "computação em nuvem" (*cloud computing*), segundo o qual, os dados, após serem recolhidos, são enviados para uma base centralizada (a chamada nuvem ou *cloud*) onde são objeto de tratamento. Ora, assumindo, nestes termos, um modelo de computação distribuído, os dados, em vez de serem transferidos para a referida *cloud* centralizada, seriam armazenados e processados no próprio dispositivo. Aqui chegados, entendem alguns especialistas que, esta descentralização na análise da informação reforçaria a privacidade dos utilizadores da *IoT*, ao evitar, desde logo, o perigo potencial já referido,

---

reconduzido a cifras monetárias sendo os dados pessoais um "património" valioso (…)", cit., pág. 98. Muito antes da revolução digital, já M. REGINA REDINHA e M. RAQUEL GUIMARÃES reparavam: "o domínio dos mercados centra-se agora mais no controlo dos sistemas de comunicação do que na produção de equipamentos e a informação tende, inclusive, a ser tratada como um bem apropriável", cit., pág. 648. Sobre a valoração dos dados pessoais, v. S. NAVAS NAVARRO, "Datos personales y mercado", in S. NAVAS NAVARRO (Dir.), *Inteligencia artificial: Tecnología-Derecho*, págs. 270 e ss.

[207] Também neste sentido, S. NAVAS NAVARRO escreve que "*existe un valor oculto en ellos con enorme potencial en todos los órdenes, sobre todo, en el económico*", "Datos personales y mercado – Conclusiones", cit., pág. 290.

[208] Rejeitamos, assim, desde já, as propostas que vão no sentido inverso ao referido, defendendo que devem ser os consumidores a pagar pela sua própria privacidade, v. STEVEN I. FRIEDLAND, "Drinking from the fire hose: how massive self-surveillance from the internet of things is changing the face of privacy", *West Virginia Law Review*, 2017, pág. 912.

[209] A designação "*fog computing*" foi atribuída pela empresa *CISCO*, pelo que preferimos a designação "*edge computing*".

relativo à combinação dos dados entre os vários dispositivos[210]. Na senda de um paradigma assim concebido, que sustém os dados nos dispositivos que os recolhem impedindo que estes cheguem à esfera das empresas (e do Estado), chegamos a um ponto em que os utilizadores parecem recuperar o domínio sobre os seus dados pessoais e, consequentemente, o ónus de os explorarem patrimonialmente. É assim que a descentralização se pode tornar monetizada, se for essa, como parece ser, a vontade dos utilizadores[211].

A tecnologia que promete revolucionar este processamento descentralizado da informação é a *blockchain*[212], uma base de dados distribuída inicialmente concebida para a moeda virtual *bitcoin*, mas cujas aplicabilidades já extravasaram o mundo financeiro, e se estima que cheguem inclusivamente ao mundo conectado da *IoT*. Neste domínio, e para o nosso interesse, a *blockchain* poderá ser usada para oferecer ao utilizador um controlo efetivo sobre a divulgação das suas informações pessoais, pois "*permite a cada usuario definir el grado de conectividad y privacidad que desea, sin necesidad de depositar la confianza en una autoridad central*"[213].

Paralelamente, a *blockchain* têm vindo a assumir um papel importante no que toca à criação de valor económico. Em jeito de exemplo, no domínio da robótica, poderá permitir que os *robots* respondam pelos seus próprios danos, materializando-lhes um *"ius patrimonii"*, "*un pequeño patrimonio con el que responder de sus responsabilidades civiles*"[214]. Num sentido idêntico, na *IoT*, contribuindo para uma progressiva autonomia dos dispositivos inteligentes,

---

[210] Como explica SONA R. MAKKER, "*an application developer can direct the device to process the data on the edge, and avoid sending information to the cloud where the dataset might then be cross-referenced with other kinds of data*", cit., pág. 903.

[211] De acordo com LUÍS F. ANTUNES, "os consumidores exigem "monetizar" os seus dados, isto é, ter um retorno monetário do uso dos seus dados pessoais", cit., pág. 54.

[212] A *blockchain* pode ser definida como uma base de dados distribuída que permite eliminar a presença de um terceiro confiável (responsável por validar a transação), estabelecendo um mecanismo alternativo de confiança e introduzindo o conceito de escassez digital, o qual, possibilita a criação de valor tornando os ativos registados nesta rede intercambiáveis e susceptíveis de avaliação económica, v. F. IPPOLITO e M. NICOTRA, pág. 18. *Vide* também a definição apresentada por A. PERESTRELO DE OLIVEIRA, pág. 103. Também C. GÓRRIZ LÓPEZ discorre sobre o conceito e sobre a dificuldade em defini-lo, v. págs. 151 e ss. PAULA R. ALVES afirma, inclusive, que a *blockchain* "poderá ter um impacto tão significativo como teve e tem a internet", cit., pág. 68.

[213] Para C. GÓRRIZ LÓPEZ, a *IoT* é, inclusivamente, "*uno de los ámbitos en que el binómio blockchain y propiedad puede tener más éxito*", cit., pág. 183. Já no Documento de Trabalho "*Advancing the Internet of Things in Europe*", de 2016, a Comissão Europeia apelava à exploração das potencialidades das redes *blockchain* no âmbito da *IoT*, v. pág. 21. Mas a *blockchain* terá também outras aplicações, mesmo no quadro da revolução digital, *vide* o conceito de *Inteligência Artificial Descentralizada*, F. IPPOLITO e M. NICOTRA, págs. 119 e ss.

[214] J. ERCILLA GARCÍA, cit., págs. 43 e 44. O autor entende mesmo que, *"en definitiva la tecnologia criptográfica y de la cadena de bloques, se erige como esencial para la patrimonialización de las personas ciber-físicas"*, cit., págs. 50 e 51. Sobre a utilização da *blockchain* para a criação de uma propriedade inteligente, v. C. GÓRRIZ LÓPEZ, págs. 180 e ss.

entraremos numa realidade conectada em que "*cada bien tendrá un patrimonio que generará a través de sus servicios y que gastará en su mantenimiento, reparación, etc.*"[215].

Na verdade, terão sido as redes sociais as pioneiras nesta monetização, em particular, dos dados pessoais dos utilizadores, nomeadamente, através de publicidade personalizada que posteriormente lhes é paga pelas entidades promovidas. Porém, "essa monetização, que ascende a vários milhões de euros anualmente, é captada integralmente pelas redes sociais, não havendo geralmente lugar à partilha com os utilizadores que são quem está na génese da criação desse valor"[216]. Foi precisamente a superação desta dificuldade que fez com que a *blockchain* chegasse ao mundo das redes sociais[217] e que nos leva a questionar porque não extendê-la também, por razões semelhantes, ao mundo da *IoT*. Entretanto, encontra-se aberta a discussão em torno do reconhecimento de um valor económico aos dados pessoais, vistos como um novo "bem intangível", bem como em torno da sua quantificação e titularidade[218].

Porém, os modelos distribuídos como a *blockchain*, parecem esbarrar com as exigências regulatórias vigentes, máxime, com o RGPD e, desde logo, com o seu direito ao esquecimento. De facto, a característica da imutabilidade associada a estas redes descentralizadas impede que os dados, uma vez inseridos, jamais possam ser apagados[219]. Na verdade, mais do que poder obstar ao desenvolvimento dos modelos distribuídos como a *blockchain*, o Regulamento parece não ter sido sequer concebido para ser aplicado ao tratamento descentralizado dos dados pessoais[220], razão pela qual alguns autores chegam a

---

[215] C. GÓRRIZ LÓPEZ, pág. 184.

[216] PEDRO MARTINS, *Introdução à Blockchain*, FCA, 2018, pág. 132.

[217] Referimo-nos, neste caso, à *Steemit*, uma rede social com uma popularidade crescente suportada por uma rede *blockchain*, que remunera os seus utilizadores pela sua interação com a plataforma, v. PEDRO MARTINS, págs. 132 e 133.

[218] No entender de S. NAVAS NAVARRO, *"la compensación económica por los datos debería tener en cuenta las muchas formas distintas en que podrán ser explotados, en un futuro"*. Além disso, acrescenta, este "bem intangível" sobre a informação pessoal tanto pode pertencer ao responsável pelo tratamento, quando *"la ceden a terceros a cambio de una contraprestación o la tratan ellos mismos para obtener "datos-conocimiento"*, como ao titular dos dados, enquanto prestação económica que pode assumir a forma de *"datos-conocimiento", como pueden ser perfiles, patrones, correlaciones, etc…"*, "Datos personales y mercado – Conclusiones", cit., págs. 289 e 290.

[219] De facto, além do direito ao esquecimento, a imutabilidade compromete também o direito de retificação. Em ambos os casos acresce ainda a dificuldade de os dados estarem registados em todos os nós da *blockchain*, pelo que a sua alteração ou supressão teria de ser feita em toda a rede. Têm-se defendido a possibilidade de inserir uma "declaração adicional" que altere ou suprima os dados em causa, na impossibilidade de os excluir. Também o direito de acesso parece ficar em risco tendo em conta que o armazenamento dos dados pode ser feito sob a forma criptografada e pseudonimizada, v. F. IPPOLITO e M. NICOTRA, págs. 84 e ss. Outras soluções têm sido estudadas, como a *blockchain* editável e os códigos de ocultação, v. A. PERESTRELO DE OLIVEIRA, págs. 103 e 104.

[220] Veja-se, desde logo, a dificuldade em qualificar os participantes da rede (saber *quem é quem*, agravada pelas especificidades de a *blockchain* poder ser aberta ou fechada). A ubiquidade da rede gera igualmente dificuldades

questionar "se o regulamento não surgiu já desatualizado"[221]. Além disso, a assumida natureza humanista do RGPD e do direito à proteção de dados na União Europeia também parece colidir com esta possibilidade de monetização dos dados[222], embora uma tendência no sentido da coisificação das informações pessoais tenha vindo a ser acolhida noutros atos de direito derivado da União[223].

7. Conclusão

A nossa Constituição confere uma proteção completa à privacidade, através, em primeiro lugar, do art. 26.º e, depois, especificamente face à informática, no art. 35.º, uma tutela que nunca se mostrou tão adequada na senda da nova revolução digital em curso. No mesmo sentido, no Código Civil, a privacidade emana de um direito geral de personalidade e mereceu uma consagração individualizada num direito especial de personalidade. Nunca como antes se mostrou tão necessário reconhecer um direito geral de personalidade, dada a complexidade e o dinamismo, quer da personalidade humana, quer da própria realidade social, cujas mutações acontecem a um ritmo impossível de acompanhar pelo direito e vão tornando o regime de tutela da pessoa inevitavelmente desatualizado ao longo do tempo.

A Internet das Coisas invadiu as nossas vidas e veio para ficar. Não há, praticamente, esfera da intimidade que fique preservada da recém-chegada "ditadura dos sensores". Em casa, na rua, da saúde ao lazer, a técnica vai compondo e impondo uma realidade global na qual o indivíduo vai entrando, por curiosidade, comodismo, ou, simplesmente, para não cair no isolamento. Cabe ao direito a grande responsabilidade de garantir que o homem não se torna

---

ao nível da aplicação territorial do Regulamento, bem como ao regime das transferências de dados, v. F. IPPOLITO e M. NICOTRA, págs. 76 e ss.

[221] Neste sentido, e a propósito do direito ao esquecimento, A. PERESTRELO DE OLIVEIRA, pág. 89.

[222] Como refere S. NAVAS NAVARRO, "*la visión europea de los datos personales en clave de "derechos humanos" es incompatible com la visión de los datos personales en clave de "derechos de propriedad*". Mas, como acaba por entender a autora, ao reconhecermos um valor económico aos dados a partir do qual derivem direitos para o titular, estamos também a proteger a sua dignidade e o seu direito à privacidade. De resto, acrescenta, o direito de propriedade é igualmente reconhecido na CDFUE e no TFUE, v. "Datos personales y mercado", pág. 265. Em sentido diferente, opondo-se ao que chama de "reificação da dignidade do ser humano", v. FILIPA U. CALVÃO, pág. 78.

[223] Referimo-nos, em particular, à Diretiva sobre certos aspetos relativos aos contratos de fornecimento de conteúdos digitais, na qual se admite que o consumidor aceda a conteúdos digitais em troca dos seus dados pessoais. Para uma análise mais detalhada, v. S. NAVAS NAVARRO, "Datos personales y mercado", págs. 259 e ss. Também MANUEL D. MASSENO lhe faz referência, v. pág. 54. De resto, também o Comité Económico e Social Europeu se pronunciou neste sentido num Parecer de 2018: "os consumidores devem dispor de informação sobre o valor económico dos seus dados e reservar-se o direito de os partilhar", v. *Confiança, privacidade e segurança para os consumidores e as empresas na Internet das coisas (IdC)* – INT/846, 2018.

refém das suas próprias criações, com o progressivo desvanecimento do seu direito à privacidade, sob a desculpa de que "não tem nada a esconder". O direito à reserva sobre a intimidade da vida privada protege as informações pessoais do acesso e, sobretudo, da divulgação indevida por terceiros. De facto, nunca o interesse nos dados dos utilizadores foi tão grande, razão pela qual entendemos que deve ser o próprio a decidir ou não dispor deles, beneficiando do valor económico que um emergente e lucrativo mercado de dados pessoais lhes vai atribuindo. E que esta autolimitação ao direito à privacidade tendo em vista uma contraprestação de natureza patrimonial nem por isso despreza a assumida natureza pessoal daquele direito.

É, também, parece-nos, nesse sentido, que vai o Regulamento Geral de Proteção de Dados que confirma a transparência como a nova face da privacidade, a arma possível num mundo digital opaco e em que as ameaças são invisíveis. Uma invisibilidade que é só dos dispositivos e do tratamento dos dados, já que o indivíduo, esse, nunca foi tão observável e, por causa disso, tão manipulável e objetificável. E o RGPD pode ser um contributo, até demasiado ambicioso, para quebrar esta corrente de desumanização pela técnica, com a ajuda, claro está, das instituições europeias, nomeadamente, o TJUE, na densificação e operacionalização dos seus preceitos, dos informáticos no respeito pelos conceitos de *privacy by design* e *by default* no desenvolvimento dos dispositivos, ou, porque não, do próprio utilizador, enquanto, também ele, vinculado a um dever de vigilância e de auto-informação.

Em suma, como alguém já escreveu: *Esperemos que nuestro pensamiento jurídico, actual y futuro, junto a los ingenieros, físicos, matemáticos y demás científicos, sea capaz de encontrar fórmulas para disciplinar las fuerzas tecnológicas y sus rendimentos, sin entorpecer su avance pero garantizando al miesmo tiempo la pervivencia de los derechos de las personas (humanas: valga aquí el pleonasmo)*[224].

[224] A. MOZO SEOANE, "La revolución tecnológica y sus retos: medios de control, falos de los sistemas y ciberdelincuencia", *in Los robots y el derecho*, Colección Jurídica General – Jornadas, Editorial Reus, Madrid, 2018, pág. 98.

BIBLIOGRAFIA

ALVES, Paula R., "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", in *Fintech – Desafios da Tecnologia Financeira,* 2ª edição, Almedina, 2019, págs. 33-69

ANTUNES, Ana Filipa Morais, *Comentário aos Artigos 70º a 81º do Código Civil (Direitos de personalidade),* Lisboa, Universidade Católica Editora, 2012

ANTUNES, Luís F., "A Privacidade no mundo conectado da Internet das coisas", *in Revista Fórum de Proteção de Dados,* N.º 2, 2016, págs. 52-58

ASCENSÃO, José de Oliveira, *Direito Civil - Teoria Geral*, Vol. I, 2ª edição, Coimbra Editora, 2000

BARBOSA, Mafalda Miranda, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil", *Estudos de Direito do consumidor*, N.º 12, Coimbra, Centro de Direito do Consumo/FDUC, 2017, págs. 75-131

BRILL, Hillary e JONES, Scott, "Little things and big challenges: information privacy and the Internet of Things", *American University Law Review*, 2017, págs. 1183-1230

CABRAL, Rita Amaral, "O Direito à intimidade da vida privada", *Estudos em memória do Professor Doutor Paulo Cunha*, Lisboa, 1989, págs. 373-406

CALVÃO, Filipa Urbano, "A proteção de dados pessoais na internet: desenvolvimentos recentes", *Revista de Direito Intelectual*, N.º 2, Almedina, 2015, págs. 67-84

CAMPOS, Diogo Leite,

- "Lições de Direitos da Personalidade", *Separata do Vol. LXVI (1990) do BFD*, 2ª edição, reimpressão, Coimbra, 1995

- "A relação da pessoa consigo mesma", *Nós – Estudo sobre o direito das pessoas*, Coimbra, Almedina, 2004, págs. 85-92

CARVALHO, Jorge Morais, "Desafios do mercado digital para o Direito do Consumo", *in Direito do Consumo 2015-2017*, Coleção Formação Contínua – Jurisdição Civil, CEJ, 2018, págs. 111-123

CARVALHO, Orlando de

- "Os Direitos do Homem no Direito Civil Português", *Teoria Geral do Direito Civil,* Coimbra, Coimbra Editora, 2012, págs. 221-243

- "Para uma Teoria da Pessoa Humana (Reflexões para uma desmitificação necessária)", *Teoria Geral do Direito Civil*, Coimbra, Coimbra Editora, 2012, págs. 245-267

CASTRO, Catarina Sarmento e,

- "40 anos de "utilização da informática" – o artigo 35.º da Constituição da República Portuguesa", *e-Pública*, Vol. 3, N.º 3, 2016, págs. 43-66

- *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005

COELHO, Pedro, *Internet das Coisas - Introdução Prática*, Lisboa, FCA, 2017

COMISSÃO EUROPEIA, "Advancing the Internet of Things in Europe", *Comission Staff Working Document*, Bruxelas, 2016

COMITÉ ECONÓMICO E SOCIAL EUROPEU, "Confiança, privacidade e segurança para os consumidores e as empresas na Internet das coisas (IdC)", INT/846, 2018

CORDEIRO, A. Menezes, OLIVEIRA, A. Perestrelo de, DUARTE, D. Pereira (Coord.)

- *Fintech – Desafios da Tecnologia Financeira*, 2ª edição, Coimbra, Almedina, 2019

- *Fintech – Novos Estudos sobre Tecnologia Financeira*, Coimbra, Almedina, 2019

CORDEIRO, António de Menezes,

- "O consentimento do titular dos dados no RGPD", in *Fintech – Novos Estudos sobre Tecnologia Financeira*, Coimbra, Almedina, 2019, págs. 33-59

- "Os Direitos de Personalidade na Civilística Portuguesa", *ROA*, 2001, págs. 1229-1256

CRORIE, Benedita Mac, "A (ir)renunciabilidade dos direitos de personalidade", *Pessoa, Direito e Direitos*, DHCII/EDUM, 2016, pág. 263-274

CUPIS, Adriano de, *Os Direitos da personalidade* (Trad.), Lisboa, Livraria Morais Editora, 1961

DAVENPORT, Nikole, "Smart washers may clean your clothes, but hacks can clean out your privacy, and underdeveloped regulations could leave you hanging on a line", *The John Marshall Journal of Information Technology & Privacy Law*, 2016, págs. 259-297.

DRAY, Guilherme Machado, *Direitos de Personalidade - Anotações ao Código Civil e ao Código do Trabalho*, Almedina, 2006

DUARTE, D. Pereira e GUSEINOV, Alexandra, "O direito de portabilidade de dados pessoais", in *Fintech – Novos Estudos sobre Tecnologia Financeira*, Almedina, 2019

ERCILLA GARCÍA, Javier, *Normas de Derecho Civil y Robótica: Robots Inteligentes, Personalidad Jurídica, Responsabilidad Civil y Regulación*, Pamplona, Arazandi, 2018

FACHANA, João, "Que papel para o consentimento na sociedade em rede?", *Direito e Informação na Sociedade em Rede: Atas*, Porto, FDUP/FLUP, 2016, págs. 91-110

FAZENDEIRO, Ana, *Regulamento Geral de Proteção de Dados*, Almedina, 2ª Edição, 2018

FEDERAL TRADE COMMISSION, "Internet of Things: privacy & security in a connected world", *FTC Staff Report*, 2015

FESTAS, David de Oliveira, *Do contudo patrimonial do direito à imagem – Contributo para um Estudo do seu Aproveitamento Consentido Inter Vivos*, Coimbra Editora, 2009

FRIAS, Hélder, "A Internet das Coisas (*IoT*) e o mercado segurador", in *Fintech – Desafios da Tecnologia Financeira*, 2ª edição, Almedina, 2019, págs. 237-254

FRIEDLAND, Steven I., "Drinking from the fire hose: how massive self-surveillance from the internet of things is changing the face of privacy", *West Virginia Law Review*, 2017, págs. 891-914

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados

- "Opinion 03/2013 on purpose limitation", 2013
- "Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679", 2018
- "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679", 2018
- "Orientações relativas à transparência na aceção do Regulamento 2016/679", 2018
- "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679", 2017
- "Parecer 15/2011 sobre a definição de consentimento", 2011
- "Parecer 2/2013 sobre as aplicações em dispositivos inteligentes", 2013
- "Parecer 05/2014 sobre técnicas de anonimização", 2014
- "Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas", 2014

GOMES, Manuel Januário, "O problema da salvaguarda da privacidade antes e depois do computador", *Separata do "Boletim do Ministério da Justiça,* N.º 319, Lisboa, 1982

GONÇALVES, Diogo Costa, *Pessoa e Direitos de Personalidade: Fundamentação ontológica da tutela*, Almedina, 2008

GONÇALVES, Maria Eduarda, "The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward", *Information & Communications Technology Law*, 2017, págs. 90-115

GOUVEIA, Jorge Bacelar, "Os direitos fundamentais à proteção dos dados pessoais informatizados", *ROA*, N.º 3, Lisboa, 1991

GÓRRIZ LÓPEZ, Carlos, "Tecnología blockchain y contratos inteligentes", *in Inteligencia artificial: Tecnología-Derecho*, Valencia, Tirant lo Blanch, págs. 151 e ss.

GUIMARÃES, Maria Raquel, "A tutela da pessoa e da sua personalidade como fundamento e objeto da disciplina civilística. Questões actuais", in *La famiglia nella società contemporânea*, Roma, Aracne editrice, 2016, págs. 175-192

HILLER, Janine S. e BLANKE, Jordan M., "Smart Cities, Big Data, and the Resilience of Privacy", *Hastings Law Journal*, 2017, págs. 309-356

HÖRSTER, Heinrich Ewald, *A Parte Geral do Código Civil Português – Teoria Geral do Direito Civil*, Coimbra, Almedina, 1992

IPPOLITO, Fulvio e NICOTRA, Massimiliano, *Diritto della Blockchain, Intelligenza Artificiale e IoT*, Ipsoa, 2018

JONES, Meg Leta, "Privacy without screens & the internet of other people's things", *Idawo Law Review*, 2015, págs. 639-660

LEAL, Ana Alves, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", in *Fintech – Desafios da Tecnologia Financeira*, 2ª edição, Almedina, 2019, págs. 89-220

MAGALHÃES, Filipa Matias e PEREIRA, Maria Leitão, *Regulamento Geral de Proteção de Dados – Manual Prático*, 2ªedição revista e ampliada, 2018 (versão *e-book*)

MAKKER, Sona R., "Overcoming "foggy" notions of privacy: How data minimization will enable privacy in the Internet of Things", *UMKC Law Review*, 2017, págs. 895-914

MARTINS, Pedro, *Introdução à Blockchain*, FCA, 2018

MASSENO, Manuel D., "Protegendo os cidadãos-consumidores em tempos de Big Data: uma perspetiva desde o Direito da União Europeia", *Revista Portuguesa de Direito do Consumo*, n.º 89, 2017, págs. 43-66

MILLER, Michael, *The Internet Of Things - How Smart Tvs, Smart Cars, Smart Homes, and Smart Cities are changing the world*, Pearson Education, Indianapolis, 2015 (versão *e-book*)

MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Tomo I, Coimbra Editora, 2010

MOINNI, Corine, "Protecting Privacy in the Era of Smart Toys: Does Hello Barbie have a Duty to Report?", *The Catholic University Journal of Law &Technology*, 2017, págs. 281-318

MOREIRA, Vital e CANOTILHO, José J. G., *Constituição da República Portuguesa – Anotada*, Vol. I, Coimbra Editora, 2007

MOTA, Joana, "Proteção de dados desde a conceção e por defeito. Avaliação de impacto e segurança", *in Fintech – Novos Estudos sobre Tecnologia Financeira, Almedina, 2019*

MOZO SOANE, A., "La revolución tecnológica y sus retos: medios de control, falos de los sistemas y ciberdelincuencia", *in Los robots y el derecho*, Colección Jurídica General – Jornadas, Editorial Reus, Madrid, 2018, págs. 79 e ss.

NAVAS NAVARRO, Susana (Dir.), *Inteligencia artificial: Tecnología – Derecho*, Valencia, Tirant lo Blanch, 2017

- "Datos personales y mercado", in *Inteligencia artificial: Tecnología-Derecho*, Valencia, Tirant lo Blanch, 2017, págs. 259 e ss.

- "Derecho e inteligencia artificial desde el diseño. Aproximaciones", in *Inteligencia artificial: Tecnología-Derecho*, Valencia, Tirant lo Blanch, 2017, págs. 23 e ss.

NETO, Luísa

- *O Direito fundamental à disposição sobre o próprio corpo*, Coimbra Editora, 2004

- *Código Civil Anotado* (coord. Ana Prata), Vol. I, Coimbra, Almedina, 2017

OLIVEIRA, Ana Perestrelo de, "Direito ao apagamento dos dados ou «direito a ser esquecido»", in *Fintech – Novos Estudos sobre Tecnologia Financeira*, Almedina, 2019, págs. 89-104

OLIVEIRA, Elsa Dias, *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional*, Almedina, 2012

OLIVEIRA, Madalena Perestrelo de, "Definição de perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados", in *Fintech – Novos Estudos sobre Tecnologia Financeira*, Almedina, 2019, págs. 61-88

PEPPET, Scott R., "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent", *Texas Law Review*, 2014, págs. 85-178

PINHEIRO, Alexandre Sousa, *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL, 2015

PINTO, Carlos Alberto da Mota, *Teoria Geral do Direito Civil*, Coimbra, Coimbra Editora, 4ªedição, 2ª reimpressão, 2012

PINTO, Paulo Mota

- "O Direito à Reserva sobre a Intimidade da Vida Privada", *BFD*, vol. LXIX, Coimbra, 1993, 479-585

- "A Limitação Voluntária do Direito à Reserva sobre a intimidade da Vida Privada", *Estudos em Homenagem a Cunha Rodrigues*, Vol. II, Coimbra, Coimbra Editora, 2001, págs. 527-558

- "O direito ao livre desenvolvimento da personalidade", *Direitos de Personalidade e Direitos Fundamentais – Estudos*, Gestlegal, 2018, págs. 7-122

PIZZI, Peter J., "Connected Cars and Automated Driving: Privacy Challenges on Wheels", *Defense Counsel Journal*, 2017, págs. 1-14

POLONETSKY, Jules e GRAY, Stacey, "The Internet of Things as a Tool for Inclusion and Equality", *Federal Communications Law Journal*, 2017, págs. 103-118.

POUDEL, Swaroop, "Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security", *Berkeley Technology Law Journal*, 2016, págs. 997-1022

REDINHA, Maria Regina e GUIMARÃES, Maria Raquel, "O uso do correio eletrónico no local de trabalho: algumas reflexões", in *Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria*, Coimbra Editora, 2003, págs. 647-671

RIBEIRO, Joaquim de Sousa, "Os Direitos de Personalidade como Direitos Fundamentais", in *Pessoa, Direito e Direitos*, DHCII/EDUM, 2016, págs. 253-262

ROGEL VIDE, Carlos (Coord.), *Los robots y el derecho, Colección Jurídica General – Jornadas*, Editorial Reus, Madrid, 2018

SAIAS, Marco A., "Reforço da responsabilização dos responsáveis pelo tratamento de dados", *Revista Portuguesa de Direito do Consumo*, n.º 89, 2017, págs. 67-86

SOUSA, Rabindranath Capelo de, *O Direito Geral de Personalidade*, Coimbra, Coimbra Editora, 1995

TEIXEIRA, M. Leonor da Silva, "A União Europeia e a Proteção de Dados Pessoais – «Uma visão futurista»?", *Revista do Ministério Público*, n.º 135, Ano 34, 2013, págs. 65-106

TERRY, Nicolas P., "Will the Internet of Things Transform Healthcare?", *Vanderbilt Journal of Entertainment & Technology Law*, 2016, págs. 327-352

VASCONCELOS, Pedro Pais de, *Direito de Personalidade*, Almedina, Coimbra, 2017

WACHTER, Sandra, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR", *Computer Law & Security Review*, 2018, págs. 436-449

WARREN, Samuel D. e BRANDEIS, Louis D., "The right to privacy", *Harvard Law Review*, Vol. IV, N.º 5, 1890, págs. 193-220

WOO, Jesse W., "Smart Cities Pose Privacy Risks and Other Problems, but That Doesn't Mean We Shouldn't Build Them", *UMKC Law Review*, 2017, págs. 953-972

ZARSKY, Tal Z., "Incompatible: The GDPR in the age of big data", *Seton Hall Law Review*, 2017, págs. 995-1020