Universidade do Minho
Escola de Direito

Aliaksandra Yelshyna

Segurança e Privacidade no Contexto de Ambientes Inteligentes

dezembro de 2014

Aliaksandra Yelshyna **Segurança e Privacidade no Contexto de Ambientes Inteligentes**
UMinho | 2014

Universidade do Minho
Escola de Direito

Aliaksandra Yelshyna

Segurança e Privacidade no Contexto de Ambientes Inteligentes

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho realizado sob a orientação do
Professor Doutor Francisco António Carneiro Pacheco de Andrade

e do
Professor Doutor Paulo Jorge Freitas de Oliveira Novais

dezembro de 2014

DECLARAÇÃO

Nome: Aliaksandra Yelshyna

Endereço eletrónico: yelshyna@gmail.com

Número do Bilhete de Identidade: 305437259zz2

Título dissertação: Segurança e Privacidade no Contexto de Ambientes Inteligentes

Orientadores: Professor Doutor Francisco António Carneiro Pacheco de Andrade e Professor Doutor Paulo Jorge Freitas de Oliveira Novais

Ano de conclusão: 2014

Designação do Mestrado: Mestrado em Direito e Informática

Universidade do Minho, ___/___/_____

Assinatura: _____

AGRADECIMENTOS

Agradeço ao Professor Doutor Francisco Pacheco Andrade e ao Professor Doutor Paulo Jorge Freitas de Oliveira Novais por terem aceitado orientar a presente dissertação, pela disponibilidade, pelo apoio e pelas críticas construtivas sempre manifestadas, essenciais à concretização deste trabalho.

Agradeço também a todos que me acompanharam neste caminho.

Este trabalho foi desenvolvido no contexto do projeto CAMCoF -Contextaware Multimodal Communication Framework financiado por Fundos FEDER através do Programa Operacional Fatores de Competitividade - COMPETE e por Fundos Nacionais através da FCT - Fundação para a Ciência e a Tecnologia no âmbito do projeto FCOMP-01-0124-FEDER-028980. Foi também desenvolvido em cooperação com o DHCII- Centro de Investigação Interdisciplinar em Direitos Humanos da Escola de Direito da Universidade do Minho.

RESUMO

Com a realização do presente estudo pretende-se levar a cabo uma análise de ambientes inteligentes e as suas repercussões na privacidade e na proteção de dados, bem como possíveis soluções legais e tecnológicas para os problemas que os mesmos levantam. Neste trabalho procurou-se, por um lado, esclarecer o conceito de ambientes inteligentes, bem como definir os seus campos da aplicação e as suas vantagens, e, por outro lado, expor as críticas mais comuns dirigidas às ameaças à privacidade e à proteção de dados. Para o efeito, a investigação focou-se na análise da relevância e adequação da legislação atual face aos desafios emergentes de ambientes inteligentes através de uma abordagem detalhada do regime legal da União Europeia relativa à privacidade e à proteção de dados pessoais, bem como da legislação nacional, em concreto do Decreto-Lei n.º 67/98, de 26 de outubro. Ao longo do presente estudo foi possível inferir que o paradigma de ambientes inteligentes introduz novos riscos à privacidade e proteção de dados pessoais, os quais obrigam a repensar questões relacionadas com segurança, autonomia, identidade e autodeterminação da pessoa humana.

ABSTRACT

This study intends to carry out an analysis of Ambient Intelligence and its impact on privacy and data protection; as well as possible legal and technological solutions to the problems that it raises. The aim is, on one hand, to clarify the concept of Ambient Intelligence, its advantages and application fields; and on the other hand, to expose common criticism regarding the threat that it poses to privacy and data protection. To this end, the main focus was to analyze the relevance and adequacy of current legislation towards Ambient Intelligence and the challenges that it faces; through a comprehensive breakdown of the European Union's legal regime, as well as national legislation, on the matter of privacy and personal data protection, namely the Decree-Law n.º 67/98, October the 26th

During this study it was possible to conclude that the paradigm of Ambient Intelligence introduces new and emerging concerns over privacy and personal data protection, which demand new thinking on issues related to security, autonomy, identity and self-determination of the individual.

ÍNDICE

LISTA DE SIGLAS E ABREVIATURAS

AAL - *Ambient Assisted Living* – Ambiente de Vida Assistida

AMI - Assistência Médica Internacional

RAL - *Alternative Dispute Resolution* - Resolução Alternativa de Litígios

AEPD - Autoridade Europeia para a Proteção de Dados

AI - Inteligência Artificial

AmI - Ambientes Inteligentes

CEDH - Convenção Europeia dos Direitos do Homem

CNPD - Comissão Nacional da Proteção de Dados

CRP - Constituição da república Portuguesa

DEI - Decisão Europeia de Investigação

ESHA - *Elizabeth Stewart Hands and Associates (Nutrient Database)*

EUA - Estados Unidos da América

GPS - *Global Positioning System* - Sistema de Posicionamento Global

ISTAG - *Information Society Technologies Advisory Group* - Grupo de Aconselhamento para as Tecnologias da Sociedade de Informação da Comissão Europeia

KDD - *Knowledge Discovery in Databases* - Descoberta de Conhecimentos em Bancos de Dados

LPDP - Lei de Proteção de Dados Pessoais

ONU - Organização das Nações Unidas

PC - Computador pessoal

PDA - Assistente Digital Pessoal

PET - *Privacy Enhancing Technology* - Tecnologias de Proteção da Privacidade

PNR - *Passenger Name Record* - Registo de Identificação de Passageiro

RFID - *Radio Frequency Identification* - Identificação por Rádio Frequência

RGPD - Regulamento Geral de Proteção de Dados

RLL - *Online Despute Resolution* - Resolução de Conflitos em Linha

RSSF - Rede de Sensores sem Fios

SWAMI - Safeguards in a World of Ambient Intelligence

TEDH - Tribunal Europeu dos Direitos do Homem

TET - *Transparency-Enhancing Technologies* - Tecnologias Indutoras de Transparência

TJUE - Tribunal de Justiça da União Europeia

TFUE - Tratado sobre o Funcionamento da União Europeia

TIC - Tecnologias de Informação e Comunicação

UE - União Europeia

INTRODUÇÃO

O conceito de ambiente inteligente ou AmI (do inglês *Ambient Intelligence*) apareceu no início dos anos 90. Os sistemas de AmI promovem ambientes em que os humanos se encontram rodeados de interfaces inteligentes e intuitivas, suportadas por computação e tecnologias de rede que estão incorporadas nos objetos do quotidiano, existindo dispositivos por detrás dessas interfaces sensíveis à presença, às necessidades do indivíduo, com capacidade de se adaptarem a requisitos pessoais.

O objetivo final dos ambientes inteligentes é facilitar e melhorar a vida das pessoas através da recolha de grandes quantidades de informação e a sua análise com vista a fornecer um ambiente personalizado, exclusivo e o mais adequado aos seus utilizadores. A tecnologia de AmI tem sido empregue em diversos campos de aplicação, alguns dos quais serão discutidos ao longo do presente trabalho.

Contudo, existe uma certa opacidade do funcionamento nos sistemas de vigilância emergentes que acarretam o risco de um processamento indevido e não solicitado de dados pessoais. No mundo atual pode-se esperar estar sob monitorização permanente, uma vez que a recolha de informação pessoal é constante e é efetuada em tempo real, sendo o seu posterior tratamento um pré-requisito para o funcionamento da tecnologia dos AmI.

Os sistemas de AmI vão apresentar uma capacidade mais abrangente e sofisticada de identificar, distinguir e classificar cada ser humano, graças às suas técnicas de criação de perfis, sensores embutidos e sofisticados agentes de *software* que prometem não só revolucionar o estilo de vida das pessoas e de interagir na sociedade, mas também vão afetar e mudar o sentido e a definição de identidade pessoal.

Por outro lado, o facto de os sistemas de AmI poderem operar de forma invisível, autónoma e impercetível pode levantar preocupações sobre o controlo do sistema, a perda de

confiança do indivíduo no ambiente tecnológico e o processamento indevido e não solicitado de dados pessoais.

Como muitas vezes acontece, a tecnologia está a evoluir mais rápido do que o processo de construção das políticas e da legislação adequadas que poderiam amenizar as preocupações dos cidadãos em relação aos ambientes inteligentes.

Inúmeras ameaças podem surgir como resultado das vulnerabilidades ainda não identificadas ou pouco conhecidas nos sistemas de AmI o que, por sua vez, pode levar à perda de controlo e de confiança no ambiente tecnológico que rodeia o utilizador.

O principal objetivo do trabalho desenvolvido consiste em abordar de forma multidisciplinar os desafios emergentes da tecnologia de AmI referentes à identidade, confiança, autonomia, mas, sobretudo, à privacidade, segurança e à proteção dos dados pessoais enquanto direitos fundamentais dos cidadãos na Sociedade da Informação. É certo que os AmI podem efetivamente colocar em risco a privacidade do indivíduo, faltando saber se o quadro legal existente é suficiente para proteger a privacidade e os dados pessoais no contexto desta nova realidade.

Para o efeito, nesta dissertação debruçar-nos-emos sobre a análise de ambientes inteligentes e as suas repercussões na privacidade e na segurança de proteção de dados, bem como possíveis soluções legais e tecnológicas para os desafios que os mesmos suscitam. Através do presente estudo propomo-nos retratar e responder às principais críticas e apreensões relacionadas com os AmI no sentido de mitigar os riscos e problemas decorrentes do uso destes sistemas ubíquos através de uma análise crítica da atual legislação atinente à privacidade e à proteção de dados, quer ao nível da União Europeia, quer ao nível nacional.

Assim, no Capítulo I desta dissertação iremos procurar abordar o conceito de sistemas de ambientes inteligentes através de um breve histórico, descrevendo as suas principais caraterísticas e o contexto tecnológico em que se inserem. Será ainda feita uma incursão na atual implementação destes sistemas através de uma análise detalhada dos campos de aplicação ligados à saúde, ao comércio eletrónico, à educação e, por fim, à resolução de conflitos em linha. Vamos focar a nossa atenção na perspetiva de uso dos AmI nos sistemas de

resolução de litígios em linha, nomeadamente na problemática de conciliação do seu uso com a proteção de dados pessoais.

No Capítulo II abordaremos de uma forma multidisciplinar as ameaças e os novos desafios à privacidade e à segurança de dados pessoais introduzidos pelo paradigma de ambientes inteligentes, sobretudo ligados à criação de perfis, monitorização, vigilância e à perda de confiança e de controlo dos utilizadores sobre os seus dados pessoais, por sua vez, conjugada com a infoexclusão e a falta de transparência dos sistemas de AmI. Será discutida a consequente necessidade de repensar questões relacionadas com segurança, confiança, autonomia, identidade e autodeterminação da pessoa humana. A seguir passaremos a uma breve abordagem da evolução do direito à privacidade ao direito à autodeterminação informativa, de forma a perceber como o desenvolvimento tecnológico teve um contributo indubitável neste processo. Ao mesmo tempo daremos conta do reforço de políticas de segurança dos Estados, acompanhado do desenvolvimento e da implementação dos novos tipos de tecnologias de deteção e vigilância em massa que podem pôr em risco os princípios protetores do tratamento de dados pessoais.

O Capítulo III destina-se à análise crítica do quadro legislativo europeu em matéria da proteção de dados pessoais vigente na União Europeia e ao nível nacional. Abordar-se-á a questão da relevância e adequação desse regime legal no contexto da nova realidade tecnológica, dando especial enfoque ao direito à privacidade e ao direito à proteção de dados pessoais enquanto direitos fundamentais de pessoas, sem deixar de referir os recentes desenvolvimentos na regulamentação da proteção de dados que se traduzem no novo quadro legal de proteção de dados pessoias na União Europeia.

De seguida, a nossa atenção focar-se-á no modo como os direitos à privacidade e à proteção de dados pessoais se encontram consagrados no ordenamento jurídico português, dando especial atenção ao artigo 35.º da Constituição da República Portuguesa, passando de seguida ao estudo detalhado das normas consagradas pela Lei n.º 67/98, de 26 de outubro, que transpôs para a ordem jurídica portuguesa a Diretiva 95/46/CE, realizando uma análise dos fundamentos legais do tratamento de dados pessoais, dos direitos dos titulares desses dados juntamente com as respetivas obrigações dos responsáveis pelo tratamento, bem como dos princípios fundamentais inerentes ao tratamento de dados pessoais.

Finalizando o Capítulo III tentaremos responder à questão de como é possível salvaguardar os direitos fundamentais à privacidade e à proteção de dados, face aos ambientes inteligentes, apresentando algumas reflexões sobre possíveis soluções legais e tecnológicas de reforço da segurança e do controlo sobre dados pessoais no contexto desta realidade emergente. Concluimos esta dissertação com algumas considerações decorrentes da necessidade vital de assegurar a proteção efetiva do utilizador e dos seus dados pessoais que fluem nos sistemas de AmI, de modo a que as pessoas possam beneficiar dos serviços disponibilizados sem deixar de estar, ao mesmo tempo, legalmente protegidas.

CAPÍTULO 1 – AMBIENTES INTELIGENTES

1.1. Conceito de Ambiente Inteligente

Em 1991, Mark Weiser, cientista do Centro de Investigação da Xerox em Palo Alto (PARC), nos Estados Unidos da América (Califórnia), publicou na revista *Scientific American* o artigo "O computador para o Século XXI", no qual apresentou a sua visão da terceira geração de sistemas de computação[1]. Essencialmente, esta nova visão descrevia a transição histórica das grandes *mainframes*[2] da década de 1960 e 1970 para o computador pessoal (PC) de 1980 e 1990 e, finalmente, para computação ubíqua. Weiser usou o termo "computação ubíqua" para descrever uma nova era de sistemas de computação, que marcaram o início de uma futura sociedade da informação.

Na Europa o termo "ambiente inteligente" - criado por Emile Aarts[3] e retomado posteriormente pelo Grupo de Aconselhamento para as Tecnologias da Sociedade da Informação da Comissão Europeia (*ISTAG)*[4], - tem muito em comum com a visão de computação ubíqua de Weiser, embora dê mais ênfase à "computação centrada no ser humano"[5], que se adapta aos interesses, necessidades e desejos das pessoas, auxiliando-as a executar tarefas do seu quotidiano, como o trabalho, o lazer ou o entretenimento[6]. Segundo Wright e Steventon, ambientes inteligentes são ambientes nos quais a computação é utilizada para melhorar impercetivelmente as atividades do dia a dia das pessoas. Uma das forças motrizes do interesse

---

[1] Weiser, M. (1999). The Computer for the 21st century. *ACM SIGMOBILE Mobile Computing and Communications Review*, *3* (3), 3-11.

[2] Até o final dos anos 70 predominavam os *mainframes*, isto é, computadores de grandes dimensões. Apenas grandes empresas e bancos podiam investir alguns milhões de dólares para tornar mais eficientes determinados processos internos e os fluxos de informações.

[3] Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E., Punie, Y. (Eds.). (2008). *Safeguards in a World of Ambient Intelligence.* Dordrecht: Springer, p. 54.

[4] ISTAG (*Information Society Technologies Advisory Group*) é o departamento que informa e aconselha a Comissão Europeia sobre assuntos de estratégia, conteúdo e direção do trabalho de investigação a ser realizado no âmbito do Programa de Tecnologia da Sociedade da Informação.Disponível em: http://cordis.europa.eu/fp7/ict/istag/about_en.html consultado a 17 de novembro de 2012.

[5] Punie, Y. (2005). The Future of Ambient Intelligence in Europe: The Need for More Everyday Life. *Communications and Strategies*, *57*(1), 141-165. Sevilha**:** Institute for Prospective Technological Studies (IPTS), pp.141, 153. Disponível em: http://www.idate.org/fic/revue_telech/410/CS57_PUNIE.pdf consultado a 2 de janeiro de 2013.

[6] Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J. C. (2001). (Eds.). *Scenarios for Ambient Intelligence in 2010*, *ISTAG Final Report*. Sevilha: Institute for Prospective Technological Studies (IPTS), p.11. Disponível em: http://www.ist.hu/doctar/fp5/istagscenarios2010.pdf consultado a 12 de março de 2014.

emergente nos ambientes altamente interativos prende-se com desejo de tornar os computadores não só amigáveis ao utilizador, mas também invisíveis para ele[7].

Esta nova abordagem coloca os seus utilizadores no centro de um ambiente digital que está ciente da sua presença e do meio envolvente em que se movimenta e presta serviços úteis de acordo com suas reais necessidades, hábitos, atitudes e emoções, tirando o máximo proveito da tecnologia disponível[8].

Pode-se, portanto, argumentar pela preferência do termo ambiente inteligente, uma vez que este decorre da convergência de três tecnologias-chave: computação ubíqua, comunicação ubíqua e interfaces adaptáveis ao utilizador, retratando uma visão da futura sociedade da informação, onde as pessoas estão rodeadas por interfaces inteligentes e intuitivas, incorporadas em todos os tipos de objetos e um ambiente com a capacidade de reconhecer e de responder à presença de diferentes indivíduos de forma discreta e muitas vezes invisível[9, 10].

A tecnologia dos AmI pode ser caraterizada como um ambiente digital que proativamente suporta o indivíduo no seu quotidiano[11]. O ambiente que rodeia o utilizador deve ser capaz de perceber os seus objetivos e as suas limitações, facilitando e auxiliando as suas atividades de forma não-intrusiva e pró-ativa[12]. Esta é a finalidade dos ambientes inteligentes. Esta visão dos AmI coloca o utilizador no centro do desenvolvimento futuro. Ao paradigma do utilizador se adaptar às tecnologias deverá suceder o paradigma das tecnologias se adaptarem ao utilizador.

---

[7] Steventon, A., & Wright, S. (Eds.) (2010). *Intelligent Spaces: The Application of Pervasive ICT*. Londres: Springer, p. 200.

[8] Novais, P., Costa, R., Carneiro, D., & Neves, J. (2010). Inter-Organization Cooperation for Ambient Assisted Living. *Journal of Ambient Intelligence and Smart Environments*, IOS Press, *2* (2), 179-195, 180-183. DOI: 10.3233/AIS-2010-0059.

[9] Friedewald, M., Vildjiounaite, E., Punie, Y., & Wright, D. (2006). The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues. In J.A. Clark, *et al.*. (Eds.), *Security in Pervasive Computing. Proceedings of the Third International Conference, SPC 2006, York, UK, April 18-21, 2006* (pp. 119-133). Berlim, Heidelberg, Nova Iorque: Springer, p. 119.

[10] Punie, Y. (2005), *op. cit.*, p. 142.

[11] Augusto J.C. Mccullagh, P. (2007). Ambient Intelligence: Concepts and Applications. *International Journal on Computer Science and Information Systems*, *4* (1), 1-28, p. 2. Disponível em: http://www.comsis.org/archive.php?show=pprnst-4604 consultado a 19 de janeiro de 2012.

[12] Cook, D. J., Augusto, J.C., Jakkula, V. R. (2009). Ambient Intelligence: Technologies, Applications, and Opportunities. *Pervasive and Mobile Computing*, *5* (4), 277-298, p. 280. DOI:10.1016/j.pmcj.2009.04.001.

1.1.1 Computação ubíqua

Como já foi referido anteriormente, o termo "computação ubíqua" foi criado e popularizado por Mark Weiser no seu artigo seminal "O computador para o Século XXI", referindo-se a computadores omnipresentes que estão ao serviço das pessoas no seu quotidiano, atuando de forma discreta em segundo plano e libertando as pessoas de tarefas rotineiras.

O ambiente criado pela convergência das tecnologias de radiotransmissão e difusão, pelo processamento informático de dados e pelos dispositivos móveis pessoais proporciona no ciberespaço a integração e a interação dos aparelhos ditos "inteligentes". O conceito da ubiquidade considera a ideia que algo existe ou está em qualquer lugar ao mesmo tempo a um nível constante, por exemplo, centenas de sensores colocados numa casa ou numa fábrica, onde um conjunto de agentes inteligentes na rede monitoriza a utilização dos eletrodomésticos, ferramentas, etc..

Nesta conceção, os sistemas de AmI possuem a capacidade de obter informação do espaço no qual se encontram inseridos e utilizá-la para construir modelos computacionais dinâmicos, ou seja, controlar, configurar e ajustar a aplicação para melhor servir às necessidades do utilizador. O ambiente também pode e deve ser capaz de detetar e interagir com outros dispositivos que venham a fazer parte dele.

A computação ubíqua pode abranger qualquer dispositivo computacional, que enquanto se movimenta com o utilizador é capaz de construir modelos dinâmicos dos vários ambientes, bem como definir serviços de acordo com esse mesmo ambiente. Os dispositivos podem ser capazes de se lembrar de ambientes anteriores em que foram utilizados, ou proativamente desenvolver novos serviços em novos ambientes, permitindo a interação entre pessoas e dispositivos e com o meio ambiente. Prevê-se que os sistemas de AmI estarão cientes das caraterísticas específicas da presença humana e personalidade, e serão capazes de atender às necessidades e responder de forma inteligente a uma vontade falada ou um gesto, podendo até se envolver em diálogos inteligentes com o utilizador[13].

[13] Punie, Y. (2003). A Social and Technological View of Ambient Intelligence in Everyday Life: What Bends the Trend? *Reports for European Media, Technology and Everyday Life Research Network (EMTEL2).* Key Deliverable Work Package 2, Joint Research Centre. Sevilha: Institute for

Segundo Weiser a computação ubíqua é o contrário da realidade virtual. A realidade virtual coloca as pessoas dentro de um mundo gerado por um computador, enquanto a computação ubíqua força o computador a viver no mundo com as pessoas[14].

1.1.2 Comunicação ubíqua

Atualmente, já existe um nível relativamente alto da computação ubíqua devido a inúmeros objetos equipados com capacidades computacionais no meio envolvente. No entanto, na maior parte dos casos, os computadores não funcionam no seu máximo potencial, uma vez que não são capazes de comunicar uns com os outros. A expansão da tecnologia de redes sem fios poderá promover a comunicação ubíqua permitindo interligar dispositivos de forma mais flexível[15]. A comunicação ubíqua é, assim, uma nova forma de obtenção de informação instantânea, rápida e eficiente através da Internet, telemóveis, isto é, através de uma rede de comunicação sem fios.

As tecnologias sem fios de curta distância surgiram para pemitir a interação entre dispositivos de uma forma transparente para o utilizador e que vai desde a ligação sem fios de um computador pessoal e seus periféricos até à conexão e comunicação entre dispositivos nos mais diversos ambientes (residência, escritório, sala de aula, lojas, hotéis, automóvel, etc.) para a realização das mais diversas tarefas.

Tecnologias de comunicação sem fios de curta e média distância, tais como o *Bluetooth*[16], *Wi-Fi*[17], juntamente com as redes de longa distância, compõem uma estrutura básica

---

Prospective Technological Studies (IPTS), p.8. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.4939&rep=rep1&type=pdf consultado a 16 de dezembro de 2012.

[14] Weiser, M. (1999), *op. cit.*, pp. 5-6

[15] Raisinghani, M. S. *et al.* (2006). Ambient Intelligence: Changing Forms of Human-computer Interaction and their Social Implications. *Journal of Digital Information*, *5* (4), p.2.Disponível em: http://journals.tdl.org/jodi/index.php/jodi/article/view/149/147 consultado a 9 de março de 2014.

[16] *Bluetooth* é uma tecnologia de comunicação sem fios que permite ligar e transferir dados entre equipamentos eletrónicos através de sinais de rádio. A ideia consiste em possibilitar que dispositivos se interliguem de maneira rápida e sem uso de cabos, bastando que um esteja próximo do outro. *Vide* mais em *Bluetooth Special Interest Group Member Website*. Disponível em: https://www.bluetooth.org/ consultado a 6 de dezembro de 2012.

[17] Palavra inglesa, redução de *wireless fidelity*, fidelidade sem fios, tecnologia de comunicação de informação sem uso de cabos, nomeadamente através de frequências de rádio, infravermelhos, via satélite, etc.. Cf. Al-Alawi, Adel Ismail. (2006). WiFi Technology: Future Market Challenges &

de suporte aos sistemas de AmI. Entretanto, com o aumento do potencial de processamento e armazenamento de dispositivos que estão cada vez mais baratos, a emergência de discos minúsculos, processadores milimétricos, dispositivos de energia em miniatura, telas pequenas com resolução cada vez melhor, além dos avanços no reconhecimento da fala e da escrita manual, do aumento de redes de comunicação sem fios, do surgimento de padrões abertos para conexão e interoperabilidade entre redes diferentes, a computação ubíqua não parece tão distante e certamente vai causar um enorme impacto na sociedade e no estilo de vida das pessoas.

Na medida em que a residência, o meio de transporte e o local de trabalho do utilizador se tornam cenários de aplicação da computação ubíqua, oferecendo serviços como segurança, comodidade, informação, entretenimento, etc., deverá existir um universo de dispositivos diferentes para suportar estes mesmos serviços. Alguns exemplos incluem: comandos, sensores para residências e automóveis, relógios, além de toda a linha de utensílios domésticos, televisões, telemóveis, PDAs[18], consolas de jogos e muito mais.

Em suma, o objetivo dos AmI consiste em alargar a interação entre os seres humanos e as tecnologias de informação digital a partir do uso de dispositivos de computação ubíqua.

1.1.3. Interfaces inteligentes

A tecnologia baseada nos ambientes inteligentes necessita que o processo de comunicação entre humanos e computadores seja o mais natural possível. Para tal, o desenvolvimento de interfaces naturais é uma peça fundamental. A visão de AmI assume que a interação física entre as pessoas e o mundo virtual será semelhante à forma de interação das pessoas no mundo real, daí o termo "interfaces naturais".

Opportunities. *Journal of Compute Science*, *2*, 13-18, p. 13. Disponível em: http://thescipub.com/PDF/jcssp.2006.13.18.pdf consultado a 9 de março de 2014.

[18] Aparelho portátil que combina as funcionalidades de um computador com as de um telefone, podendo funcionar em rede, e sendo também usado como agenda pessoal. Lextec-Léxico. *Técnico do Português do Instituto de Camões.* (2009). Disponível em: http://www.instituto-camoes.pt/lextec/por/domain_7/definition/19662.html consultado a 9 de dezembro de 2012.

Nos sistemas de AmI as interfaces estão centradas na pessoa humana, na medida em que são capazes de reconhecer não apenas a fala e a escrita, mas também os gestos, expressões e principalmente aliar todos estes dados ao contexto das operações, podendo inclusivamente captar alterações no meio envolvente e armazenar em memória experiências anteriores e até aprender com elas[19]. Muitos dispositivos e aparelhos podem estar distribuídos e escondidos no ambiente, tornando-se quase impossível reconhecê-los devido a um contínuo processo de miniaturização de componentes.

A incorporação da tecnologia de AmI no quotidiano das pessoas, nos objetos ou na infraestrutura de uma casa, escritório, hospital, escolas ou uma empresa cria uma rede de vigilância global, invisível e compreensiva, que cobre uma parte inédita da vida pública e privada. Neste contexto, aumenta a necessidade de estudo e implementação de interfaces inteligentes com o objetivo de adaptar o seu desempenho às necessidades e preferências do utilizador. A utilização de interfaces inteligentes é importante quando o objetivo consiste em apoiar grupos de utilizadores com diversas necessidades, habilidades e preferências, desde que facilitem uma eficiente e natural interação utilizador-computador, chegando mesmo a imitar a comunicação homem-homem[20].

As interfaces adaptáveis ao utilizador são uma parte integrante dos AmI que visam melhorar a interação humana com a tecnologia, tornando-a mais intuitiva, eficiente e segura. Através destas interfaces os sistemas computacionais têm capacidade de capturar mais dados do que as interfaces tradicionais, como, por exemplo, informação sobre o estado em que a pessoa se encontra, o tipo de espaço e os objetos relacionados, entre outros.

A interface inteligente é considerada aquela que entende e procura atingir os objetivos do utilizador, facilitando uma interação mais natural, com uma maior tolerância a eventuais erros e com formatos mais agradáveis[21].

Segundo Liebernan[22], o que torna uma interface inteligente é este poder de se adaptar às necessidades de diferentes utilizadores e aprender novos conceitos e técnicas, bem como a

---

[19] Quigley, Aaron J., Bodea, Florin. (2010). Face-to-Face Collaborative Interfaces. In A. Hamid, D. Ramón López-Cózar, J. C. Augusto (Eds.), *Human-Centric Interfaces for Ambient Intelligence* (pp.3-32). Amsterdão: Elsevier, pp. 10-15.

[20] Hammond, A. M. G. (2003). How Do You Write "Yes"?: A Study on the Effectiveness of Online Dispute Resolution. *Conflict Resolution Quarterly*, *20* (3), 261-286. DOI: 10.1002/crq.25.

[21] McTear, M. F. (2000). Intelligent Interface Technology: From Theory to Reality? *Interacting With Computers*, *12* (4), 323-336. DOI: 10.1016/S0953-5438(99)00002-8.

capacidade de antecipar as necessidades do utilizador, tomar iniciativas e, por conseguinte, oferecer sugestões e explicações das suas ações, criando um ambiente que compreende e responde ao utilizador em vez de um ambiente que fica à espera de uma interação por parte do utilizador.

A interface inteligente deverá ser fácil de usar e possuir capacidade de ser personalizada automaticamente, adaptável a padrões de comportamento de um utilizador em particular por meio de algoritmos inteligentes: o sistema analisa as ações e caraterísticas do utilizador e adapta-se automaticamente ao mesmo. Utilizando interfaces adaptativas, o sistema pode ser personalizado para estilos cognitivos individuais, personalidade, experiência, necessidades e tarefas de cada utilizador em particular. É importante ter uma interface expressiva, funcional e atrativa para que a interação entre o utilizador e o sistema possa ocorrer.

1.1.4. Agentes inteligentes de software

A tecnologia de AmI representa uma visão em que as pessoas estão rodeadas de interfaces inteligentes[23], que analisa o contexto e se adapta às necessidades e aos requisitos das pessoas que utilizam esses espaços. O contexto é definido como qualquer informação usada para caraterizar o estado de uma entidade, que pode ser uma pessoa, um espaço físico ou um objeto.[24]

A maior parte da informação do contexto pode ser recolhida por sensores incorporados no ambiente e até mesmo no próprio utilizador. Um sensor é um dispositivo capaz de detetar uma grandeza do mundo físico (temperatura, humidade, pressão, som, luminosidade, movimento, composição química, etc.) e transformá-la num sinal elétrico variável (analógico) que

---

[22] Lieberman, H. (1998). Integrating User Interface Agents With Conventional Applications. *Knowledge-Based Systems*, *11* (1), 15-23. Disponível em: http://web.media.mit.edu/~lieber/Lieberary/Integrating-UI-Agents/Integrating-UI-Agents.html consulatdo a 5 de março de 2013.

[23] Aarts, E., Roovers, R. (2003). Embedded System Design Issues in Ambient Intelligence. In T. Basten, M. Geilen, & H. De Groot (Eds.), *Ambient Intelligence: Impact on Embedded System Design*. Norwell, MA: Kluwer Academic Publishers, pp. 11-29. DOI: 10.1007/0-306-48706-3_2.

[24] Dey, A. K, Abowd, G. D. (2000). Towards a Better Understanding of Context and Context-Awareness. In *Workshop on the What, Who, Where, When, and How of Context-Awareness (CHI 2000)*. Haia, Países Baixos, p.1:"We define context as any information that can be used to characterize the situation of an entity, where an entity can be a person, place, or physical or computational object". Disponível em: https://smartech.gatech.edu/bitstream/handle/1853/3389/99-22.pdf;jsessionid=E9408D3271F7BA2980D7D8DD68E7A9E7.smart2?sequence=1 consultado a 2 de março de 2013.

representa a amplitude dessa grandeza[25]. As redes de sensores sem fios (RSSF)[26] são uma tecnologia cujo objetivo principal consiste na extração de informações do meio que a rodeia e que são inicialmente processadas e encaminhadas na maior parte das vezes por radiofrequência, sendo posteriormente disponibilizadas numa plataforma informática.

Redes de sensores sem fios são utilizadas para a recolha dos dados que são necessários para o funcionamento de ambientes inteligentes, seja em domótica, aplicações educacionais ou saúde. Alguns exemplos de possíveis tecnologias RSSF são de Identificação por Rádio Frequência (RFID), *ZigBee* ou *Bluetooth*.

A RFID[27] é uma tecnologia de comunicação sem fios que utiliza radiofrequência para capturar os dados, identificar e receber informações sobre os seres humanos, animais e objetos, sem contacto e sem a necessidade de um campo visual. Um sistema de RFID contém basicamente quatro componentes: etiquetas ou *tags*, leitores, antenas e *software*, permitindo que uma *tag* seja lida sem a necessidade de campo visual, através de barreiras e objetos tais como madeira, plástico, papel, etc..

A tecnologia *ZigBee* foi criada pela *ZigBee Alliance*[28] e descreve um protocolo de comunicações sem fios de baixo consumo, baixo custo, bidirecional e de curto alcance, com foco na padronização, que permite a interoperabilidade de produtos. O nome *ZigBee* surgiu em analogia à forma como as abelhas se movimentam entre as flores e trocam informação entre si sobre onde encontrar recursos[29].

Por sua vez, o *bluetooth* é um padrão global de comunicação sem fios e de baixo consumo de energia que permite a transmissão de dados que é feita por meio de radiofrequência entre dispositivos eletrónicos próximos entre si[30].

---

[25] Qi, H., Iyengar, S. S., Chakrabarty, K. (2001). Multiresolution Data Integration Using Mobile Agents in Distributed Sensor Networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 31*(3), 383-391, pp. 383-384. DOI:10.1109/5326.971666.

[26] Em inglês *Wireless Sensor Networks.*

[27] Em inglês *Radio Frequency Identification* – Identificação por Rádio Frequência.

[28] A *Zigbee Alliance* é um consórcio industrial que visa promover e desenvolver redes sem fios para fins de controlo e monitorização industrial, mas também para redes domésticas, aplicações em sensores médicos, jogos e outras áreas de aplicação onde são necessárias redes de baixo custo, baixa potência e interoperabilidade. Disponível em: http://www.zigbee.org/ consultado a 6 de novembro de 2012.

[29] Safaric, S., Malaric, K. (2006, junho). ZigBee Wireless Standard. In *Multimedia Signal Processing and Communications, 48th International Symposium ELMAR-2006* (pp. 259-262). Zadar, Croatia. DOI: 10.1109/ELMAR.2006.329562.

[30] McDermott-Wells, P. (2004). What is Bluetooth?. *Potentials, IEEE*, *23* (5), 33-35. DOI: 10.1109/MP.2005.1368913.

Contudo, não é suficiente reunir informações sobre o contexto. A informação deve ser processada por mecanismos dinâmicos, capazes de responder às alterações que ocorrem no meio ambiente. Assim, a informação obtida deve ser gerida por tecnologias inteligentes e auto-adaptáveis, com o objetivo de fornecer uma interação adequada entre os utilizadores e o seu ambiente. Os agentes de *software* e sistemas multi-agentes são uma dessas tecnologias[31].

Um agente de *software* pode ser definido como um sistema computacional situado num ambiente, com capacidade de actuar nele de forma autónoma a fim de atingir os seus objetivos[32]. De acordo com Stuart Russel e Peter Norvig um agente é tudo aquilo que pode perceber o ambiente em que se encontra inserido, através de sensores, e atuar sobre este ambiente por meio de atuadores e aprender com a experiência[33]. Deste modo, pode-se afirmar que agente é uma entidade cognitiva e autónoma, ou seja, dotada de um sistema interno de tomada de decisão, que atua sobre o meio envolvente e sobre os outros agentes que o rodeiam e possui capacidade de funcionar sem necessitar de algo ou de alguém para o guiar (possui mecanismos próprios de perceção do ambiente em que se encontra inserido).

Sistema multi-agentes é definido como qualquer sistema composto por múltiplos agentes autónomos, onde existe a coordenação das suas ações que lhes permite cooperar e trocar conhecimento para alcançar objetivos comuns[34]. Os agentes conseguem assim uma maior eficiência da sua ação, conseguindo solucionar problemas que, de outro modo, estariam fora do alcance das capacidades de cada agente, individualmente considerado[35].

Agentes de *software* podem ser distinguidos entre reativos e proativos em função da capacidade de reagir autonomamente aos impulsos e de acordo com as caraterísticas do meio envolvente. Nos sistemas reativos os agentes de *software* comportam-se como autómatos inseridos no ambiente que os rodeia, baseado numa lógica modal do conhecimento, não possuindo representação simbólica interna do mundo, nem raciocínio simbólico complexo para

---

[31] Russell S, Norvig P. (1995). *Artificial Intelligence: A Modern Approach.* Nova Jérsia: Prentice-Hall, Englewood Cliffs, p. 45.

[32] *Idem, ibidem.*

[33] *Idem,* pp. 45-46.

[34] "Num SMA (sistema multi-agente) para além da distribuição e da descentralização da execução por vários módulos ou entidades, aqui designados por agentes, o controlo é distribuído por esses agentes. Estes, além de selecionarem as suas próprias ações, socializam-se e cooperam". Cf. Novais, P. (2003). *Teoria dos processos de pré-negociação em ambientes de comércio eletrónico.* Dissertação de Doutoramento, Departamento de Informática, Universidade do Minho, Braga, Portugal, p. 6.

[35] Andrade, F. (2008). *Da contratação eletrónica: em particular da contratação eletrónica inter-sistémica inteligente.* Dissertação de Doutoramento, Universidade do Minho, Braga, Portugal, p. 194.

atingir os seus objetivos, e atuam num modo estímulo-resposta, isto é, o agente não tem memória da ação realizada no passado, nem qualquer previsão da ação a ser tomada no futuro[36]. O agente toma e realiza todas as suas decisões "em tempo real", geralmente com base num conjunto de informações provenientes de sensores e regras simples de situação/ação, apresentando um comportamento reativo.

Nos sistemas pró-ativos um agente não se limita a reagir a mudanças do seu ambiente, mas ele próprio toma iniciativa de acordo com as circunstâncias específicas. Os agentes pró-ativos possuem capacidade de planear a sua conduta de acordo com objetivos que pretendem alcançar[37]. São agentes chamados inteligentes. O agente pode ser dotado não apenas de capacidade de raciocínio, mas também de verdadeira capacidade de aprendizagem, ou seja, o agente pode não só adquirir conhecimento, mas também aprender os modos como melhor poderá ter acesso à informação e adquirir novos conhecimentos[38]. A partir dessa possibilidade de conhecimento o agente torna-se capaz de tomar decisões em ambientes complexos, em processo de constante mudança e escolher entre várias possíveis estratégias, ou seja, não se limita apenas a recolher e armazenar dados ou informação. O agente pode ainda aprender[39] quais são os hábitos e preferências do utilizador e agir e decidir em conformidade com esse conhecimento[40].

São as caraterísticas e propriedades básicas dos agentes de *software,* que determinam o seu grau de inteligência: autonomia[41] (um agente executa as suas tarefas com acessos a bases de conhecimento próprias sem intervenção direta do humano ou de outros agentes, tendo capacidade de tomar decisões e atuar sem ter que questionar constantemente o utilizador);

---

[36] *Idem,* p. 196.

[37] "Poderemos falar de agentes orientados por objetivos, os quais, para uma tomada de decisão, usam, para além do conhecimento que têm do mundo ou do universo de discurso, informação particular acerca dos problemas em equação (a qual é obtida mediante a invocação de procedimentos, de análise e/ou descoberta de conhecimento". Cf. Novais, P. (2003), *op. cit.*, p. 62.

[38] Andrade, F. (2008), *op. cit.,* p. 177.

[39] "A possibilidade de um sistema aprender a partir da observação e da experiência é uma das funcionalidades básicas de qualquer sistema inteligente; i.e., quaisquer entidades que atuem de um modo consciente, que têm opiniões sobre os objetos e os acontecimentos no seu espaço de perceção, dão corpo a um sistema inteligente. Esta faculdade de acumular conhecimento como ajuda à resolução de problemas, apresenta-se como uma das facetas mais marcantes da atividade humana. Facultar aos sistemas computacionais este talento é um dos objetivos em diferentes áreas do conhecimento que se abrigam sobre o guarda-chuva da Aprendizagem Automática". Cf. Novais, P. (2003), *op. cit.*, p. 44.

[40] Andrade, F. (2008), *op. cit., loc.cit.*

[41] Weitzenboeck, E. M. (2001). Electronic Agents and the Formation of Contracts. *International Journal of Law and Information Technology*, *9* (3), 204-234, pp. 207-208. Disponível em: http://folk.uio.no/emilyw/documents/EMILY%20%20Version%2019%20August%20&%20source.pdf consultado a 2 de fevereiro de 2013.

reatividade[42] (capacidade de perceção e reação às circunstâncias prevalecentes em ambientes dinâmicos e imprevisíveis, respondendo em tempo útil a alterações que neles ocorram[43]), pro-atividade[44] (o agente não atua apenas em resposta à observação do ambiente, mas possui objetivos e exibe comportamentos próprios, sendo capaz de tomar a iniciativa e decisões para se ajustar a novas variáveis ambientais e atingir as metas definidas); sociabilidade[45] e cooperação (o agente interage com outros agentes ou com o utilizador no sentido de finalizar a resolução de um problema ou ajudar os outros na sua atividade); comunicação[46] (capacidade do agente de se conectar e agir em conjunto com outros utilizadores e/ou agentes), capacidade de raciocínio[47], comportamento adaptativo e confiança[48]. Estes atributos de agentes de *software* proporcionam desenvolvimento de sistemas dinâmicos e distribuídos que possuam a capacidade de adaptação às caraterísticas do ambiente envolvente e seus utilizadores.

Um agente de *software* verdadeiramente autónomo possui capacidade de raciocínio adaptativo, sendo capaz de operar com sucesso numa ampla variedade de ambientes e de se adaptar às modificações que possam nele ocorrer[49]. Por sua vez, o grau de autonomia do agente está relacionado com a capacidade de decidir por si só e de relacionar as informações provenientes dos sensores com seus atuadores para atingir as suas metas e satisfazer as suas motivações[50].

Autonomia consiste na capacidade do agente de perseguir seus objetivos e cumprir as suas tarefas, sem qualquer intervenção humana, exercendo controlo[51] exclusivo sobre seus

---

[42] " (...) reactivity – agents perceive their environment, (which may be the physical world, a user via a graphical user interface, a collection of other agents, the internet, or perhaps all these combined), and responds in a timely fashion to changes that occur in it".Cf. Weitzenboeck, E. M. (2001), *op. cit.*, p. 207.

[43] Andrade, F. (2008), *op. cit.,* p. 166.

[44] "(...) pro-activeness – agents do not simply act in response to their environment, they are able to exhibit goal directed behavior by taking the initiative".Cf. Weitzenboeck, E. M. (2001), *op. cit.*, p. 208.

[45] "(...) social ability – agents interact with other agents (and possibly humans) via some kind of agent-communication language". *Idem, ibidem.*

[46] Andrade, F. (2008), *op. cit., loc.cit.*

[47] "O raciocínio é uma característica fundamental das entidades inteligentes. É a via segundo a qual é gerado novo conhecimento a partir de premissas ou axiomas. Um sistema em que a assimilação de novo conhecimento não altera as premissas do passado, designa-se por sistema monótono. Por outras palavras, num sistema monótono, a aquisição de novos dados nunca poderá invalidar ou alterar conclusões já transitadas em julgado".Cf. Novais, P. (2003), *op. cit.*, p. 30.

[48] Heilmann, K., Kihanya, D., Light, A., & Musembwa, P. (1995). *Intelligent Agents: A Technology and Business Application Analysis.* University of California: Berkeley, pp. 6-8.

[49] Andrade, F. (2008*), op. cit.,* p. 173.

[50] Russell S., Norvig P. (1995), *op. cit., loc.cit.*

[51] "(...) intelligent software agents must have "control" over their "internal state and behavior."- Cf. Heilmann *et al.* (1995), *op. cit.,* p. 6.

estados e comportamentos internos. A capacidade do próprio agente de tomar iniciativa e agir autonomamente requer que o agente tenha objetivos bem definidos, pois só assim faz sentido para um agente influenciar seu ambiente. O agente autónomo tem capacidade de escolha e de decisão, a partir de esquemas de racionalidade própria[52].

Os níveis de autonomia podem variar e, em muitos casos, apesar de o agente tomar decisões por si, sem intervenção humana, o utilizador poderá ter uma maior ou menor capacidade de controlo sobre os parâmetros que influenciam o comportamento do agente[53].

Embora o recurso aos AmI possa trazer as mais variadas vantagens, a tecnologia baseada nos agentes de *software* representa um sério potencial para retirar o controlo das mãos dos humanos. Poderão existir casos em que o agente, face à informação que dispõe, poderá - no interesse do utilizador - ultrapassar claramente aquilo que o próprio utilizador poderá ter previsto. Os riscos associados à perda de autonomia e do controlo do utilizador sobre a tecnologia serão discutidos mais adiante neste trabalho, no ponto 2.4.

1.2. Campos de aplicação de ambientes inteligentes

1.2.1. Saúde

A saúde e o bem-estar, bem como a possibilidade de permitir uma vida independente, principalmente aos mais idosos, são muito promissores na área dos AmI.

As aplicações mais recentes baseadas nos AmI incluem a utilização de casas inteligentes para proporcionar um ambiente mais seguro, onde as pessoas com necessidades especiais possam desfrutar de uma melhor qualidade de vida. Por exemplo, no caso de pessoas nas fases iniciais de demência (a situação mais frequente é a dos idosos que sofrem de doença de Alzheimer) o sistema pode ser adaptado para minimizar os riscos e garantir atendimento adequado nos momentos críticos graças à atividade de monitorização permanente, ao

[52] Andrade, F. (2008), *op. cit.,* p. 171.

[53] *Idem*, p. 174.

diagnóstico de situações de risco e à possibilidade de avisar o profissional de saúde quando a sua intervenção se torna necessária[54].

A saúde pode ser descentralizada e acessível em casa através de serviços de teleassistência e telessaúde que são comummente chamados de *Ambient Assisted Living* (AAL) - Ambiente de Vida Assistida[55] O conceito de Ambiente de Vida Assistida procura aliar à utilização de sistemas avançados de monitorização biomédica, outros dispositivos de domótica e monitorização ambiental, para fornecer a pessoas que vivam sozinhas e tenham necessidades de atenção especial, um ambiente de vida assistida[56]. Estes serviços baseados na tecnologia de AmI podem ser úteis na cura de doenças, que começa a partir de diagnóstico e continua como um tratamento a qualquer momento e em qualquer lugar. Trata-se de uma atividade de longo prazo voltada para o processo de recuperação dos pacientes e para o suporte das funções da vida quotidiana das pessoas que necessitam de atenção a longo prazo, tais como os idosos, deficientes ou doentes crónicos[57]. O funcionamento de AAL baseia-se na criação de perfis de paciente, partilha de informação entre os médicos e equipamentos médicos, e nos sistemas de AmI minúsculos capazes de administrar medicação (por exemplo dispositivos de insulina implantáveis para pacientes diabéticos). Os sistemas de AmI devem ser também capazes de efetuar diagnóstico automático de crise e dar a medicação necessária em tempo útil como, por exemplo, nos casos de problemas cardíacos ou epilepsia que exigem uma monitorização contínua.

Atualmente é possível observar o surgimento de empresas com iniciativas de trazer tecnologias inteligentes de assistência automatizada de atendimento aos idosos em casa[58], bem como o incremento da investigação[59] sobre o uso destas mesmas tecnologias com o intuito de melhorar a qualidade de vida das pessoas com limitações físicas ou cognitivas, permitindo-lhes

---

[54] Augusto J.C., Mccullagh, P. (2007), *op. cit.,* p. 7.

[55] Broek, G. Van den, Cavallo, F., Wehrmann, C. (Eds.). (2010). *AALIANCE Ambient Assisted Living Roadmap* (Vol. 6). Amsterdão: IOS Press, pp.7-8.

[56] *Idem ibidem.*

[57] O'Donoghue, J., Herbert, J. (2006). An Intelligent Data Management Reasoning Model Within a Pervasive Medical Environment. In J. C. Augusto, D. Shapiro (Eds.), *Proceedings of the 1st Workshop on Artificial Intelligence Techniques for Ambient Intelligence (AITAmI 2006)* (pp. 27-31). Riva del Garda, Itália. Disponível em: http://www.cs.ucc.ie/~herbert/pubs/AITAmI2006.pdf consultado a 19 de março de 2014.

[58] Intel Proactive Health. Disponível em: http://www.intel.com/content/www/us/en/healthcare-it/healthcare-overview.html consultado a 19 de novembro de 2012.

[59] Costa, Â., Castillo, J. C., Novais, P., Fernandéz-Caballero, A., Simoes, R. (2012). Sensor-Driven Agenda for Intelligent Home Care of the Elderly. *Expert Systems with Applications*, *39* (15), pp. 2192-12204. DOI: 10.1016/j.eswa.2012.04.058.

permanecer em suas habitações, e promover envelhecimento no local, mantendo os idosos independentes nas suas próprias casas[60, 61, 62] em vez de os mandar para lares de acolhimento ou outro tipo de instituições[63]. O desenvolvimento das tecnologias de cuidados de saúde no campo de domótica poderá ajudar na prevenção de doenças, que inclui a monitorização contínua da saúde e dos comportamentos relacionados com a saúde, por exemplo, exercícios de desporto; na promoção do estilo de vida saudável e aconselhamento; no alerta contra o consumo de produtos perigosos, por exemplo, aqueles que podem causar reações alérgicas[64].

Como um dos exemplos de aplicação dos ambientes inteligentes na assistência de saúde pode ser apontado o projeto "iGenda" que tem vindo a ser desenvolvido na Universidade do Minho em Portugal[65]. Trata-se de um projeto baseado em ambiente AAL e que integra uma agenda inteligente que automaticamente procede à marcação e calendarização de eventos e de atividades livres. Este desenvolvimento tem como principal objetivo a resolução de um problema de falhas de memória muito comum que afeta as pessoas idosas. Os eventos podem resultar da marcação por terceiros e o sistema processa a calendarização das tarefas e atividades na agenda do utilizador[66]. O "iGenda" opera em dois patamares distintos: por um lado, calendarização de eventos, por outro, gestão de tempos livres. A calendarização de eventos

---

[60] Pollack, M. E. (2005). Intelligent Technology for an Aging Population: The Use of AI to Assist Elders With Cognitive Impairment. *AI Magazine*, *26* (2), 9-24. Disponível em: http://www.aaai.org/ojs/index.php/aimagazine/article/view/1810/1708 consultado a 3 de abril de 2013.

[61] Saito, M. (2000, novembro). Expanding Welfare Concept and Assistive Technology. In *Proceedings of the IEEK Annual Fall Conference* (pp. 156-161). Ansan, Coreia do Sul. Disponível em: http://web.cecs.pdx.edu/~mperkows/Rehabilitation_Robots/Saito-paper.pdf consultado a 3 de abril de 2013.

[62] Stefanov, D. H., Bien, Z., Bang, W. C. (2004). The Smart House for Older Persons and Persons with Physical Disabilities: Structure, Technology Arrangements, and Perspectives.*IEEE Transactions on Neural Systems and Rehabilitation Engineering*, *12*(2), 228-250. Disponível em: http://www.schattauer.de/de/magazine/uebersicht/zeitschriften-a-z/imia-yearbook/imia-yearbook-2006/issue/special/manuscript/6806/download.html consultado a 5 de abril de 2013.

[63] Vitaliano, P. P., Echeverria, D., Yi, J., Phillips, E., Young, H., & Siegler, I. C. (2005). Psychophysiological Mediators of Caregiver Stress and Differential Cognitive Decline. *Psychology and Aging*, *20* (3), 402-411, pp. 402, 408. Disponível em: http://faculty.washington.edu/pemp/pdfs/pemp2005-04.pdf consultado a 15 de maio de 2013.

[64] Friedewald, M., Vildjiounaite, E., Punie, Y., & Wright, D. (2007). Privacy, Identity and Security in Ambient Intelligence: A Scenario Analysis. *Telematics and Informatics*, *24* (1), 15-29, p. 21. Disponível em: http://friedewald-family.de/Publikationen/Telematics24.2007.15.pdf consultado a 9 de maio de 2013.

[65] Costa, Â., Novais, P., Corchado, J. M., Neves, J. (2012). Increased Performance and Better Patient attendance in an Hospital With the Use of Smart Agendas. *Logic Journal of IGPL*, *20* (4), 689-698. DOI: 10.1093/jigpal/jzr021.

[66] Andrade, F., Costa, A., Novais, P. (2011). Privacidade e proteção de dados nos cuidados de saúde de idosos. In *Memórias do XV Congresso Ibero Americano de Derecho e Informática*, de FIADI – Federacion IberoAmericano de Asociaciones de Derecho e Informática e Asociación Argentina de Informática Jurídica Tomo 1, Buenos Aires, Argentina: Publicación elDial.com e Biblioteca Jurídica Online, p. 4. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/15197/1/2011%20-Congresso%20Direito%20Argentina.pdf consultado a 6 de abril de 2013.

processa-se através da receção de novos eventos pelo sistema e, usando um sistema de resolução de conflitos, procede à calendarização nos espaços livres, corrigindo erros e procurando ultrapassar incompatibilidades que possam decorrer deste processo. A função de gestão de tempos livres permite calendarização, na agenda do paciente/idoso, de atividades de lazer, procurando assim manter o utilizador ocupado e ativo[67].

A descentralização dos serviços de saúde e o desenvolvimento de tecnologias de assistência de saúde e assistência social à distância está a contribuir para a evolução de um sistema mais flexível, em que as pessoas são atendidas mais perto das suas habitações e das suas comunidades.[68] Casas inteligentes são um exemplo de um desenvolvimento tecnológico que facilita essa tendência de levar o sistema de cuidados de saúde e serviços sociais até o paciente, em vez de levar o paciente até o sistema de saúde[69].

Segundo o estudo da Comissão Europeia, a introdução das técnicas de monitorização de saúde à distância poderá potenciar mais altas antecipadas de pacientes hospitalizados, permitindo poupar 1,5 mil milhões de euros por ano só na Alemanha[70]. Os sistemas de AmI de reconhecimento de atividades e comportamentos[71], de monitorização de dieta e exercícios[72, 73] e de deteção de alterações ou anomalias[74] apoiam este objetivo.

O já referido projeto "iGenda" para além da calendarização automática e inteligente desenvolveu outra aplicação - *Sense Module*, cujo principal objetivo consiste na monitorização

---

[67] *Idem*, p.4.

[68] Augusto, J. C. (2010). Past, Present and Future of Ambient Intelligence and Smart Environments. In Joaquim Filipe, Ana Fred, Bernadette Sharp (Eds.), *Agents and Artificial Intelligence,* (pp. 3-15). Berlim: Springer, pp.4-5. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.212.1516 consultado a 20 de janeiro de 2013.

[69] Augusto J.C., Mccullagh, P. (2007), *op. cit.,* pp. 7-8.

[70] Comissão de Comunidades Europeias, *Envelhecer bem na sociedade da informação*, uma iniciativa i2010 Plano de Ação no domínio "Tecnologias da Informação e das Comunicações e Envelhecimento" (COM (2007) 332 final), de 14 de junho de 2007. Disponível em: http://europa.eu/legislation_summaries/information_society/strategies/l24292_pt.htm consultado a 8 de abril de 2014.

[71] Ogawa, M., Suzuki, R., Otake, S., Izutsu, T., Iwaya, T., Togawa, T. (2002). Long Term Remote Behavioral Monitoring of Elderly by Using Sensors Installed in Ordinary Houses. In *2nd Annual International IEEE-EMB Special Topic Conference on Microtechnologies in Medicine and Biology* (pp. 322-325). Madison, EUA: IEEE. DOI:10.1109/MMB.2002.1002339.

[72] Farringdon Farringdon, J., Nashold, S. (2005). Continuous Body Monitoring. In Y. Cai (Ed.), *Ambient Intelligence for Scientific Discovery* (pp. 202-223). Berlim: Springer. DOI: 10.1007/978-3-540-32263-4_10.

[73] Chang, K. H., Liu, S. Y., Chu, H. H., Hsu, J. Y. J., Chen, C., Lin, T. Y., Huang, P. (2006). The Diet-Aware Dining Table: Observing Dietary Behaviors Over a Tabletop Surface. In K. P. Fishkin, *et al.* (Eds.), *Proceedings of the International Conference on Pervasive computing. Lecture Notes in Computer Science* (Vol. 3968), (pp. 366-382). Berlim: Springer.

[74] Cook, D. J., Youngblood, G. M., Jain, G. (2008). Algorithms for Smart Spaces. In A. Helal, M. Mokhtari and B. Abdulrazak (Eds.), *The Engineering Handbook of Smart Technology for Aging, Disability and Independence* (pp.783-800). Nova Jérsia: John Wiley & Sons. Disponível em: http://eecs.wsu.edu/~cook/pubs/adi07.pdf consultado a 9 de abril de 2013.

móvel do paciente[75]. Esta aplicação baseia-se na utilização de um conjunto de sensores corporais que recolhem dados vitais do paciente, processa-os remotamente e no final enviam para o médico informação já atualizada sobre o estado de saúde do doente. Os sensores podem recolher dados de eletrocardiograma, pressão arterial, níveis de oxigenação do sangue e de deteção de quedas entre outros, sendo estes dados processados com vista a agregar informação sobre o estado geral de saúde do paciente. Os dados são posteriormente enviados ao médico do paciente para uma análise mais detalhada[76].

Através deste tipo de aplicações AmI os médicos ficarão mais disponíveis para os casos de verdadeira emergência, sem deixarem de manter o controlo diário sobre o estado de saúde de pacientes, a partir dos relatórios, e de tomar decisões com base nos seus conteúdos. Neste cenário, o interesse da integração do projeto "iGenda" é evidente, pois assegura a manutenção da ligação médico-utilizador.

Outro exemplo da utilização dos sistemas inteligentes na AAL é apresentado pelo projeto *VirtualECare* que consiste numa arquitetura baseada em tecnologia de agentes, suportando ambientes computacionais que permitam monitorizar e prover cuidados de saúde personalizados àqueles que deles necessitem. O aludido projeto pretende reproduzir os aspetos fundamentais deste tipo de cuidados na própria residência dos utentes, cuidando de proporcionar um ambiente adequado, adaptado às preferências e necessidades pessoais, e dando acesso ao consumidor a um conjunto alargado de serviços domésticos. O principal objetivo do *VirtualECare* é apresentar uma arquitetura baseada em ambientes capaz de monitorizar, interagir e fornecer aos seus clientes serviços de saúde de extrema qualidade. Esse sistema será interligado não só com outras instituições de saúde, mas também com centros de lazer, ginásios, lojas, familiares de pacientes, entre outros. A arquitetura do *VirtualECare* é distribuída, desempenhando cada um dos seus nós um papel diferente, com tarefas específicas, desde o *call center*, o sistema de apoio à decisão em grupo até aos dispositivos de monitorização[77].

[75] Carneiro, D., Novais, P., Costa, R., Gomes, P., Neves, J. (2009). EMon: Embodied Monitorization. In M. Tscheligi, *et al.* (Eds.), *Ambient Intelligence* (Vol. 5859), (pp. 133-142). Berlim: Springer.

[76] Andrade, F. (2011), *op. cit.,* p. 7

[77] Novais, P., et al. (2010), *op. cit.* pp. 179-190.

Trazer os cuidados de saúde às casas é um desenvolvimento interessante, mas a utilização de aplicações AmI nos hospitais revela-se também necessária. As aplicações AmI em hospitais podem contribuir para melhor segurança dos pacientes e dos próprios profissionais, ajudar a acompanhar a evolução de doentes após intervenção cirúrgica através da disponibilização de informação sobre o seu estado de saúde, recolha de informação administrativa e clínica e, por fim, providenciar pela marcação de terapias/tratamentos e pela otimização da cadeia de alarme em caso de emergência (por exemplo, no caso de um ataque cardíaco ou um acidente). Muitas das tecnologias AmI encontradas em casas inteligentes podem ser adaptadas com certas especificações para serem usadas em quartos ou áreas de um hospital[78].

Hospitais com recurso aos sistemas de AmI podem aumentar a eficiência dos seus serviços de vigilância de saúde e do processo de recuperação dos pacientes, bem como aumentar a segurança e reduzir a infeção cruzada, por exemplo, permitindo que apenas o pessoal autorizado e determinados pacientes possam ter acesso a áreas e dispositivos específicos[79].

Os cuidados de saúde determinam a vida e a morte das pessoas, e o acesso rápido às informações sobre a saúde de uma pessoa (por exemplo, alergias e doenças crónicas) pode ser muito importante em caso de emergência. Mas por outro lado as informações de saúde são altamente sensíveis[80]. As pessoas podem não estar dispostas a revelar os seus problemas de saúde mesmo aos parentes mais próximos, e muito menos aos seus superiores hierárquicos ou companhias de seguros. Assim, torna-se extremamente importante garantir que nos sistemas de AmI aplicados na área de saúde somente trabalhadores de emergência e médicos possam aceder às informações pessoais sempre que necessário, e mais ninguém sem que haja prévia autorização do titular dessas informações[81].

---

[78] Augusto, J. C. (2010), *op. cit.*, pp. 4, 9.

[79] Augusto J.C., Mccullagh, P. (2007), *op. cit.*, pp. 7-8.

[80] Artigo 7.º, n.º1 do Decreto- Lei n.º 67/98 de 26 de outubro: "É proibido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos".

[81] Friedewald, M., *et al.* (2006), *op. cit.*, pp. 126-127.

1.2.2. Educação

O rápido desenvolvimento das tecnologias de informação e comunicação (TIC) obriga a uma constante atualização de conhecimentos na área, por outro lado é a mesma tecnologia que moderniza e facilita a aprendizagem. A integração de ambientes inteligentes na educação está especialmente orientada para a organização do conhecimento.

A educação formal[82] com o recurso aos AmI vai tirar proveito não só da possibilidade de partilha de experiência e de promoção de colaboração independentemente da localização geográfica, mas também da utilização de museus e bibliotecas digitais. Estas bibliotecas fornecerão recursos integrados (impressão, fotografia, computação, etc.) e vários tipos de aprendizagem (formal, informal e profissional, etc.), proporcionando o intercâmbio de conhecimento detido por uma variedade de professores e alunos de diversas formas (multimédia, simulação, etc.). Os museus digitais permitirão acesso direto a exibições e outros valores de interesse científico e cultural através da tecnologia de multimédia interativa.

Para além disso, alunos com limitações físicas ou hospitalizados poderão ter acesso ao ensino completo e estar conetados juntamente com os seus colegas de turma. O mesmo poderá acontecer com alunos localizados em zonas rurais ou os que enfrentam obstáculos culturais que os impedem de estarem todos fisicamente juntos, bem como estudantes de diferentes nacionalidades e línguas reunidos por sistemas multilingues[83].

Os ambientes de aprendizagem inteligentes, por possuírem um modelo do conteúdo a ser ensinado e dos conhecimentos do aluno, são capazes de oferecer ensino e assistência personalizados[84]. Os AmIs podem auxiliar na solução de grandes desafios na Educação fornecendo métodos, técnicas e tecnologias que permitam desenvolver programas de assistência individualizada e inteligente do aluno, proporcionando uma maior interação social. As tecnologias AmI são um ótimo recurso a ser utilizado tanto como ferramenta de apoio a aprendizagem em sala de aula, bem como no ensino à distância, uma vez que fornecem um processo de ensino

[82] A educação formal é uma educação com reconhecimento oficial, oferecida nas escolas em cursos com níveis, graus, programas, currículos e diplomas. Desenvolve-se no seio de instituições próprias — escolas e universidades — onde o aluno deve seguir um programa pré-determinado. Cf. Chagas, I. (1993). Aprendizagem não formal/formal das ciências: Relações entre museus de ciência e escolas. *Revista de Educação 3* (1), 51-59. Disponível em: http://www.ie.ulisboa.pt/pls/portal/docs/1/298079.PDF consultado a 17 de dezembro de 2012.

[83] Ducatel, K., *et al.* (2001), *op. cit.*, p.109.

[84] Woolf B.P. (2009). *Building Intelligent Interactive Tutors: Student Centred Strategies for Revolutionizing E-learning.* Nova Jérsia: Elsevier, pp. 379 e ss.

individualizado. O principal destaque está na apresentação do material de aprendizagem (visualização, jogos, realidade virtual, etc.), na avaliação do progresso do aluno e na possibilidade de adaptar a apresentação de material e o ritmo de aprendizagem às necessidades e capacidades individuais de cada estudante, bem como na promoção da aprendizagem colaborativa que, por sua vez aumenta a eficiência e o prazer de aprender.

Igualmente, no ensino à distância, os sistemas de AmI podem oferecer assistência individual ao aluno, mesmo quando o professor não se encontra em linha, avaliando-o e controlando todo o processo de aprendizagem, como foi ilustrado no cenário "Annette e Salomão" de ISTAG[85]. O cenário apresenta possibilidade de existência de um assistente virtual que é um agente inteligente de *software* com as seguintes caraterísticas: perceção do ambiente, capacidade de interação, conhecimento, adaptação e representação gráfica. A perceção do ambiente contempla as observações do agente durante a interação e a troca de informações com o utilizador. O conhecimento do agente inteligente é constituído pelas informações que possui sobre o utilizador e o seu ambiente envolvente, o qual pode ser atualizado durante a interação. Quanto à caraterística de adaptação, o agente é capaz de aprender sobre o aluno e adaptar-se a ele a partir das novas informações que recolheu. Por exemplo, se o requerente solicita uma informação cuja área não está registada no seu perfil, o agente adiciona na sua base de conhecimento a solicitação do aluno, que constitui um novo conhecimento para o agente e que será usado posteriormente como uma evidência para o processo de atualização do perfil.

Na sala de aula, a utilização de ambientes inteligentes pode permitir ao professor dedicar mais tempo aos alunos com dificuldades especiais, bem como reduzir a sua carga de trabalho, auxiliando-o no planeamento e preparação de apresentações, na elaboração e registo do histórico pessoal de aprendizagem de cada aluno.

Uma sociedade tecnologicamente informativa envolve uma educação não formal, em especial das pessoas com pouca escolaridade, de modo a permitir a estas tirarem proveito das possibilidades oferecidas pela tecnologia[86]. A intenção desta educação é eliminar uma barreira

[85] Wright, D., *et al.* (2008), *op. cit.*, p.55.

[86] A educação não formal é aquela que "se processa fora da esfera escolar e é veiculada pelos museus, meios de comunicação e outras instituições que organizam eventos da diversa ordem, tais como cursos livres, feiras e encontros, com o propósito do ensinar ciência a um público heterogéneo". Chagas, I. (1993), *op. cit.*, p. 52.

que cresce em conjunto com o progresso tecnológico entre aqueles que são capazes de usar os novos equipamentos e tecnologias e os que não têm acesso a eles.

Por outro lado, a utilização de AmI na educação pode significar uma mudança de paradigma educacional, bem como o surgimento de novas formas de aprendizagem.[87]A disseminação das tecnologias de computação ubíqua e de localização, para além de causar impactos significativos em diversas áreas da sociedade, levou ao surgimento da educação ubíqua que permite a incorporação de atividades de aprendizagem individuais na vida quotidiana[88]. Neste cenário, torna-se necessário adaptar um novo modelo educacional, a fim de explorar recursos pedagógicos a qualquer hora e em qualquer lugar, permitindo a combinação perfeita de ambientes virtuais e espaços físicos.

A aprendizagem ubíqua é uma abordagem inovadora que integra comunicação sem fios, móvel, e tecnologias sensíveis ao contexto, capazes de detetar a situação particular do aluno no mundo real e fornecer uma orientação personalizada em conformidade com as necessidades de cada um estudante[89]. Ademais, aprendizagem ubíqua fornece informações relevantes sobre o meio envolvente, proporcionando, desta forma, oportunidades de auto-aprendizagem para os alunos. Portanto, não só permite aos alunos alcançar os objetivos de aprendizagem a qualquer hora e em qualquer lugar, mas também incentiva a capacidade de explorar novos conhecimentos e resolver problemas autonomamente, o que constitui uma das caraterísticas importantes da aprendizagem ubíqua[90].

---

[87] Bomsdorf, B. (2005). Adaptation of Learning Spaces: Supporting Ubiquitous Learning in Higher Distance Education. In Nigel Davies and Thomas Kirste and Heidrun Schumann (Eds.), *Dagstuhl Seminar Proceedings 05181, Mobile Computing and Ambient Intelligence: The Challenge of Multimedia* (pp.1-13). Leibniz:Internationales Begegnungs- und Forschungszentrum Center fur Informatik. Disponível em: http://drops.dagstuhl.de/opus/volltexte/2005/371/ consultado a 4 de março de 2013.

[88] Hwang, G. J., Tsai, C. C., & Yang, S. J. (2008). Criteria, Strategies and Research Issues of Context-Aware Ubiquitous Learning. *Educational Technology & Society*, *11* (2), 81-91. Disponível em: http://pdf.aminer.org/000/246/158/ubies_an_intelligent_expert_system_for_proactive_services_deploying_ubiquitous.pdf consultado a 2 de março de 2013.

[89] Hwang, G. J., Yang, T. C., Tsai, C. C. Yang, S. J. (2009). A Context-Aware Ubiquitous Learning Environment for Conducting Complex Science Experiments. *Computers & Education*, *53* (2), 402-413. DOI: 10.1016/j.compedu.2009.02.016.

[90] Mikulecký, P. (2012, abril). Smart Environments for Smart Learning. In *DIVAI 2012 - 9th International Scientific Conference on Distance Learning in Applied Informatics* (pp. 213-222). Sturovo, Eslováquia, p. 217. Disponível em: http://conferences.ukf.sk/public/conferences/1/divai2012_conference_proceedings.pdf consultado a 9 de janeiro de 2013.

Ideias interessantes sobre a aprendizagem em ambientes inteligentes podem ser encontradas em Winters, Walker e Rousos[91]. A aprendizagem pode ser vista agora como um processo social que acontece no tempo e lugar que o estudante escolher, continuando ao longo a vida. Winters, Walker e Rousos definem um ambiente inteligente como qualquer espaço onde a tecnologia omnipresente conduz o processo de aprendizagem de forma discreta, eficiente e colaborativa.[92] Assim, um ambiente inteligente pode ser uma sala "consciente" ou edifício que possui a perceção do contexto dos seus habitantes e trabalhadores/estudantes.

Em suma, uma grande proliferação e disponibilidade de informação conjugada com novas tecnologias baseadas nos ambientes inteligentes oferece a estudantes e professores possibilidade de desenvolver conteúdos de aprendizagem de várias formas e em diferentes composições de espaço-tempo.

1.2.3. Comércio

A forma de comércio tem sofrido profundas alterações não só nas questões de hábitos comerciais, mas também no tipo de transações e na sua logística. O comércio eletrónico[93] tem sido uma das histórias de sucesso da última década, enquanto os desenvolvimentos em comunicações sem fios e computação móvel anunciaram uma era do comércio móvel (*m – commerce* em inglês).

Por comércio eletrónico entende-se "a utilização de tecnologias de informação avançadas para aumento de eficiência de relações entre parceiros comerciais, para desenvolvimento de vendas e prestações de serviços, quer entre empresas, quer ao consumidor final"[94].

---

[91] Winters, N., Walker, K., Roussos, G. (2005, junho). Facilitating Learning in an Intelligent Environment. In *IEEE International Workshop on Intelligent Environments*, (pp. 74-79). Londres: Institute of Electrical Engineers. Disponível em: http://www.lkl.ac.uk/people/kevin/ie05.pdf consultado a 9 de janeiro de 2013.

[92] *Idem,* p. 74.

[93] Ao nível europeu existe a Diretiva 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000 que diz respeito a certos aspetos jurídicos da sociedade da informação, nomeadamente do comércio eletrónico, no mercado interno. Ao nível nacional encontra-se uma Lei do Comércio Eletrónico (Decreto-Lei n.º 7/2004, de 7 de janeiro, alterado pelo Decreto-Lei n.º62/2009, de 10 de Março e pela Lei n.º46/2012 de 29 de agosto) que regula a contratação sem intervenção humana e estabelece que: "À contratação celebrada exclusivamente por meio de computadores, sem intervenção humana, é aplicável o regime comum, salvo quando este pressupuser uma atuação" (artigo 33.º).

[94] Correia, Miguel J.A. Pupo (2011). *Direito Comercial, Direito da Empresa* (12.ª ed. Revista e Atualizada). Lisboa: Ediforum, p. 549.

Comércio eletrónico abrange todas as práticas contratuais que se fundam na utilização, entre as partes, de meios eletrónicos de processamento e transmissão de dados e têm por conteúdo a celebração de contratos comerciais (compra e venda e prestação de serviços) celebrados entre empresas, ou entre estas e consumidores finais[95].

O ponto mais específico do comércio eletrónico relativamente ao comércio tradicional consiste na caraterística do uso das novas tecnologias de comunicação enquanto meio de transmissão de informação, negociação e celebração de contratos. O comércio eletrónico é comummente percebido como sendo o resultado do fenomenal crescimento da Internet e tecnologias relacionadas, durante a última década.

O comércio móvel ou *m-commerce* tem por objetivo facilitar as transações de comércio eletrónico, ampliando o seu alcance para uma parte da população que anteriormente foi inacessível. Fundamental para comércio móvel é a disponibilidade de uma conexão de dados sem fios que permite o acesso do cliente à Internet. Por outras palavras, o comércio móvel é a capacidade de fazer transações comerciais em ambiente *wireless*.

As tecnologias baseadas nos ambientes inteligentes são capazes de fornecer uma infraestrutura omnipresente e inteligente para a implantação de serviços de comércio eletrónico e comércio móvel, o que por sua vez irá aumentar a flexibilidade do serviço implantado de comércio eletrónico e torná-lo mais amplamente disponível, resultando no que pode ser apropriadamente denominado comércio ubíquo (*u-commerce* de inglês)[96].

Este tipo de comércio, tendo por base os sistemas de AmI, apresenta quatro caraterísticas fundamentais: ubiquidade, universalidade, singularidade e unissonância (*ubiquity, universality, uniqueness and unision* em inglês)[97]. Ubiquidade permite ao utilizador o acesso à rede a qualquer hora e em qualquer lugar. A caraterística de singularidade consiste na identificação de utilizadores/clientes não apenas pela sua identidade e preferências, mas

---

[95] *Idem, ibidem.*

[96] Keegan, S., O'Hare, G. M., O'Grady, M. J. (2008). Easishop: Ambient Intelligence Assists Everyday Shopping. *Information Sciences*, *178* (3), 588-611, p.589. Disponível em: http://dl.acm.org/citation.cfm?id=1316219 consultado a 5 de janeiro de 2013.

[97] Galanxhi-Janaqi, H., & Nah, F. F. H. (2004). U-Commerce: Emerging Trends and Research ssues. *Industrial Management & Data Systems*, *104* (9), 744-755, p. 744. DOI: dx.doi.org/10.1108/02635570410567739.

também pela sua localização geográfica. Por sua vez, universalidade significa que um mesmo equipamento poderá ser utilizado independentemente do sítio/país, funcionando sempre da mesma forma, permitindo a multifuncionalidade e a interoperabilidade. Unissonância significa que os dados são integrados através de aplicações múltiplas, de modo que o utilizador visualiza suas informações em qualquer dispositivo utilizado.

Deste modo, o comércio ubíquo traduz uma convergência de todos os modelos de comércio virtual existentes, com o objetivo de converter as transações comerciais em operações independentes de dispositivo, de meio de transmissão de dados ou de posição geográfica.

Há certos autores que definem o comércio ubíquo, como sendo o uso de servidores de comércio eletrónico em conjunto com sensores distribuídos em lojas, oferecendo a conveniência do comércio móvel e permitindo aos clientes escolherem comprarem produtos e serviço a qualquer momento e em qualquer lugar, de forma inteligente e intuitiva[98].

Segundo Roussos, Gershman e Kourouthanassis[99], o comércio ubíquo está estritamente ligado ao comércio eletrónico e ao comércio móvel, utilizando a infraestrutura e os desenvolvimentos dos ambos, porém diferenciando-se por dois atributos: a identificação eletrónica de produtos físicos e o uso da infraestrutura ubíqua para promover serviços de negócios aos clientes.

Anatole Gershman apontou três objetivos principais do comércio ubíquo[100]:

- estar sempre conectado com o cliente;

- estar ciente em tempo real do contexto em que o cliente se encontra inserido;

---

[98] Lin, K. J., Yu, T., Shih, C. Y. (2005). The Design of a Personal and Intelligent Pervasive-Commerce System Architecture. In *WMCS'05. The Second IEEE International Workshop on Mobile Commerce and Services, 2005.* (pp. 163-173). Munique, Alemanha: IEEE. DOI: 10.1109/WMCS.2005.25.

[99] "Ubiquitous commerce is intimately related to electronic and mobile commerce and it uses its infrastructures and developed expertise but it is characterized by two extra features: the electronic identification of physical products (consumer or otherwise) and the seamless provisioning of business and consumer services over ubiquitous computing infrastructure". Cf. Roussos, G., Gershman, A., & Kourouthanassis, P. (2003, outubro). Ubiquitous Commerce. In *UbiComp 2003 Adjunct Proceedings,* (pp.1-4). Seattle, WA, EUA, p.2 Disponível em: http://www.dcs.bbk.ac.uk/~gr/u-commerce/ubicommerce.pdf consultado a 2 de abril de 2013.

[100] Gershman, A. (2002). Ubiquitous Commerce-always on, Always Aware, Always Pro-active. In *Proceedings of the 2002 Symposium on Applications and the Internet (SAINT 2002),* Nara, Japão (pp. 37-38). Washington, DC: IEEE Computer Society, p.38. DOI:10.1109/SAINT.2002.994443.

- ser pró-ativo, identificando, em tempo real, possíveis oportunidades para satisfazer necessidades do cliente.

Por sua vez, Olli Pitkänen afirma que o comércio ubíquo não é possível sem aplicação da ciência de contexto, isso porque se um sistema é ciente do contexto em que está inserido ele pode se adaptar e escolher um comportamento de acordo com o mesmo. O comércio ubíquo baseado na tecnologia inteligente e intuitiva deve possuir sensibilidade ao contexto, através do uso de sensores que identificam e podem extrair informações do ambiente envolvente, e mecanismos que trabalham continuamente avaliando desejos e ofertas para gerar oportunidades de negócio entre fornecedores e clientes[101].

Personalização dos serviços ou criação de perfis[102] é a principal diferencial do comércio ubíquo em comparação com outros tipos do comércio e consiste no processo de identificação de cliente e de reconhecimento das suas necessidades específicas de acordo com as quais empresas/fornecedores adaptam as suas ofertas[103]. As empresas vão querer possuir conhecimento detalhado sobre necessidades do cliente, os seus hábitos, o trabalho e tempos livre, levando-as a recolher o máximo possível de informações pessoais para a criação de perfis de clientes. Apesar de personalização trazer muitos benefícios, as suas desvantagens mais importantes prendem-se com o facto de cliente ser alvo de recolha massiva de informação pessoal por parte do fornecedor[104].

Como exemplo da utilização dos ambientes inteligentes no comércio ubíquo pode ser apontada a aplicação *iGrocer*[105], desenvolvida nos Estados Unidos da América que foi projetada para desempenhar um papel de assistente inteligente que auxilia nas compras em supermercados, consistindo o seu principal diferencial na possibilidade de manter e gerir o perfil nutricional das pessoas, através da sugestão de compra ou evitação de determinados produtos. Este recurso é particularmente útil para pessoas idosas ou que requerem cuidados especiais

---

[101] Pitkänen, O. (2003). Legal Challenges to Ubicommerce. In *UbiComp 2003 Adjunct Proceedings* (pp.16-19).Seattle, EUA, p.17. Disponível em: http://www.dcs.bbk.ac.uk/~gr/u-commerce/ubicommerce.pdf consultado a 19 de janeiro de 2013.

[102] "Profiling" em inglês.

[103] Roussos, G., Moussouri, T. (2004). Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce. *Personal and Ubiquitous Computing*, *8* (6), 416-429, pp.422-423. Disponível em: http://onemvweb.com/sources/sources/consumer_perception_commerce.pdf consultado a 4 de janeiro de 2013.

[104] *Idem, ibidem.*

[105] Shekar, S., Nair, P., Helal, A. S. (2003, março). iGrocer: A Ubiquitous and Pervasive Smart Grocery Shopping System. In *Proceedings of the 2003 ACM Symposium on Applied Computing* (pp. 645-652). Nova Iorque, EUA: ACM. DOI: 10.1145/952532.952658.

relacionados com certos alimentos[106]. Nestes casos, a aplicação realiza os devidos alertas e apresenta informações relativamente a produtos (sua composição, dados nutricionais, etc.), não existindo necessidade de utilizador ler o rótulo dos mesmos. Para sugerir produtos específicos, o sistema cruza os dados de perfil nutricional do cliente com a ESHA[107], uma base de dados com informações nutricionais mantidas pelo governo americano. A partir deste cruzamento, o sistema sugere produtos de acordo com a sua composição, emitindo alerta quanto a produtos que possam ser prejudiciais para a saúde do consumidor.

Outro sistema inteligente desenvolvido para auxiliar os clientes no processo de compra é aplicação *MyGrocer*[108]*.* O objetivo principal da *MyGrocer* consiste no controlo da reserva de produtos dentro da casa do consumidor. A aplicação emite um alerta quando algum *item* está em falta ou prestes a esgotar, por exemplo: em casa, o cliente armazena os produtos em compartimentos que possuem leitor de RFID (por exemplo, no frigorífico ou dispensa) que automaticamente atualizam as informações da sua reserva pessoal. Ademais, a partir de qualquer local o cliente pode aceder à sua lista de compras e consultar a reserva dos produtos em casa via Internet, acrescentando ou retirando *itens* para a próxima ida ao supermercado[109, 110].

1.2.4. Resolução de litígios em linha

Hoje em dia regista-se um número crescente de conflitos proveniente do exponencial aumento das transações comerciais e prestações de serviços via Internet. Devido à conveniência do comércio eletrónico, à ausência de limitações de tempo e de espaço conjugadas com uma disponibilidade de mais variados bens e serviços fizeram crescer as transações virtuais e ao mesmo tempo houve surto dos conflitos provenientes destas negociações. A atual tendência é a de que a maioria das controvérsias emergentes do comércio eletrónico seja resolvida pelos

---

[106] Os dados referentes a uma dieta específica, em alguns casos, podem ser considerados dados sensíveis, na medida em que são susceptíveis de revelar aspetos sensíveis da vida privada do indivíduo, por exemplo, as suas crenças religiosas ou/e o seu estado de saúde. *Vide* sobre a distinção entre dados sensíveis e não-sensíveis ponto 3.2.1. do presente trabalho.

[107] ESHA - *Elizabeth Stewart Hands and Associates.* The Oficial ESHA Nutrient Database Website. Disponível em: http://www.esha.com/product/database consultado a 27 de outubro de 2013.

[108] Kourouthanassis, P., Roussos, G. (2003). Developing Consumer-friendly Pervasive Retail Systems. *IEEE Pervasive Computing, 2*(2), 32-39. DOI: 10.1109/MPRV.2003.1203751.

[109] Kourouthanassis, P., & Roussos, G. (2003), *op. cit.,* pp.34-39.

[110] Roussos, G., Moussouri, T. (2004), *op. cit.*, pp. 419-422.

meios extrajudiciais, uma vez que estes desenvolvem uma política eficaz de crescimento das transações comerciais para o exterior e de captação de investimentos externos, encontrando-se o sistema judiciário ineficiente para atuar nestas questões.

O eventual obstáculo à utilização do comércio eletrónico não seria causado pela insuficiência técnica do sistema judiciário, mas pela potencial frustração de expetativa do consumidor. Da mesma forma que tais operações comerciais são efetuadas de forma muito célere, o consumidor certamente desejará que qualquer eventual conflito seja resolvido com a mesma rapidez e conforto.

Torna-se possível detalhar a nova realidade no Direito da Sociedade da Informação que consiste na aplicação conjunta dos meios extrajudiciais de resolução de conflitos via Internet, consistindo no método de resolução de conflitos alternativo ao judiciário, mais célere, simples e acessível através do computador.

A resposta para este tipo de problema pode ser dada através da possibilidade de resolução dos conflitos fora do tribunal comum, através de recurso aos meios alternativos como a negociação, mediação e arbitragem[111].

A arbitragem consiste "fundamentalmente num meio de resolução de conflitos que se carateriza pela atribuição da competência a fim de julgá-los a uma ou mais pessoas, escolhidas pelas próprias partes ou por terceiros, cujas decisões têm a mesma eficácia que possuem as sentenças judiciais"[112]. Desta forma, a arbitragem é um meio extrajudicial de composição de litígios e, ao mesmo tempo, é um meio alternativo da sua resolução de litígios (RAL ou ADR - *Alternative Dispute Resolution* do inglês) que se traduz numa solução de conflitos mais rápida, mais simples e menos dispendiosa do que no processo judicial. Os principais meios de resolução extrajudicial de litígios são a arbitragem, a mediação, a conciliação.

Tendo em conta os novos casos que surgiram com a evolução tecnológica a ADR precisou de suporte tecnológico para suas abordagens legais. Para dar respostas a estas abordagens, têm vindo a ser desenvolvidos sistemas focados em ajudar as partes a resolver os

[111] Brown, H. J., & Marriott, A. L. (1999). *ADR Principles andPpractice*. Londres: Sweet & Maxwell, p. 12.

[112] Vicente, Dário Moura. (2005). *Problemática internacional da sociedade da informação.* Coimbra: Almedina, p. 357.

seus conflitos através de novos meios tecnológicos, denominados sistemas de Resolução de Litígios em Linha (RLL ou ODR – do inglês *Online Dispute Resolution*) "[113].

Por sua vez, quando falamos de modos de RLL referimo-nos, de modo genérico, a meios de resolução de litígios que podem ou não visar uma decisão vinculativa tomada por um terceiro, implicando sempre o uso de tecnologias em linha de modo a facilitar a resolução dos litígios entre as partes[114]. Trata-se de um novo modelo de resolução de conflitos que ambiciona ser uma alternativa à litigância tradicional[115]. Pode contudo ir mais além que a RAL, uma vez que a introdução de ferramentas de suporte baseadas em tecnologias aumenta o número de soluções e os caminhos possíveis para chegar a elas. Este novo paradigma levanta algumas questões interessantes. Neste sentido, todo o processo decorre como se tratando de um processo de RAL, com a exceção de que as partes não estão em contacto pessoal mas fazem-no através de um meio de comunicação[116]. Enquanto plataforma técnica, a RLL pode ser considerada uma porta de entrada para os meio clássicos de resolução alternativa de litígios. Por acréscimo, entendemos que a RLL consiste em tecnologias de informação e de comunicação ao serviço da resolução de litígios[117].

Aliás, se a Internet dá origem a algumas disputas, parece oportuno utilizar o mesmo meio para lidar com elas[118]. Além disso, a RLL pode ser mais eficaz do que os métodos tradicionais em termos de tempo, conveniência e recursos financeiros envolvidos no processo de resolução de litígios.

---

[113] Café, A., Carneiro, D., Novais, P., Andrade, F. (2010). Sistema de resolução *online* de conflitos para partilhas de bens – divórcios e heranças. In Luís Barbosa, Miguel Correia (Eds.), *INFORUM- 2º Simpósio de Informática* (pp. 779-790). Braga: Inforum, p.780. Disponível em: http://inforum.org.pt/INForum2010/papers/sistemas-inteligentes/Paper064.pdf consultado a 5 de janeiro de 2013.

[114] United Nations Commission on International Trade Law. Working Group III (Online Dispute Resolution), Twenty-Second Session, Vienna, (13-17 December 2010), *Online Dispute Resolution for Cross-border Electronic Commerce Transactions*. Disponível em: http://daccess-dds-ny.un.org/doc/UNDOC/LTD/V10/574/10/PDF/V1057410.pdf?OpenElement consultado a 2 de maio de 2013.

[115] Neste contexto levanta-se a questão da possibilidade de sujeição da pessoa a uma decisão meramente tecnológica. A este respeito Catarina Sarmento e Castro fala num direito de não ficar sujeito a uma decisão individual automatizada. *Vide* Castro, Catarina Sarmento e. (2005). *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, pp.251-253. *Vide* igualmente o ponto 3.2.1. do presente trabalho.

[116] "ADR and ODR procedure's common features are: a) they are not carried in Court; b) they are activated through the express consent of the parties; c) they are aimed at preventing or solving disputes and they operate on the basis of the assistance, to a greater or lesser extent, of a third party chosen by the parties". Peruginelli, G., Chiti, G. (2002). Artificial Intelligence in Alternative Dispute Resolution. In *Proceedings of the Workshop on the Law of Electronic Agents–LEA. Workshop on the Law of Electronic Agents* (pp. 97–104). Bolonha: CIRSFID, p.98.

[117] "A ODR tem sido vista como a abordagem da ADR que se apoia nos meios tecnológicos para facilitar a resolução de conflitos, ou ainda, considerando a componente "*online*", é vista como um ambiente virtual no qual as partes possam reunir-se para resolver suas diferenças". Café, A., et al. (2010), *op. cit.*, p. 780.

[118] Hörnle, Julia (2003). Online Dispute Resolution: The Emperor's New Clothes?. *International Review of Law, Computers & Technology*, *17* (1), 27-37.

1.2.4.1 Tecnologia como quarta parte

A arquitetura de RLL baseia-se na utilização de infraestruturas e recursos tecnológicos síncronos[119] ou assíncronos[120], como por exemplo, as conversas eletrónicas, fóruns eletrónicos, correio eletrónico, teleconferência, áudio e videoconferência, salas de mediação virtuais[121]. Sendo estes sistemas conhecidos como a primeira geração dos sistemas de resolução de litígios em linha eles são mais próximos dos tradicionais meios de resolução extrajudicial de litígios, onde uma pessoa física se mantém como elemento central do processo de resolução levado a cabo. A tecnologia neste caso desempenha um papel essencial no suporte da comunicação das partes, sendo uma ferramenta valiosa na troca de informação através da rede entre os intervenientes do processo mas que não substitui a intervenção humana[122].

No que respeita aos meios de resolução de litígios em linha da segunda geração, estes já se afastam mais dos meios tradicionais, na medida em a tecnologia se assume como a quarta parte no processo da resolução que procura alcançar o entendimento entre as partes. O recurso às ferramentas telemáticas e o contributo da inteligência artificial, por meio de modelos matemáticos, proporcionam a resolução de conflitos pela avaliação sistémica das propostas das partes, elas mesmas auxiliadas por agentes informáticos num processo interativo que se baseia em esquemas negociais padronizados[123]. O papel da tecnologia em mediar a comunicação entre as partes é visto como a principal diferença entre RLL e outros métodos de resolução de litígio[124].

---

[119] A comunicação síncrona é a comunicação direta, com um intervalo de tempo mínimo entre o momento em que uma parte faz um comentário em uma discussão, e a outra parte recebe esta mensagem. A outra parte pode, por sua vez, reagir quase imediatamente. Isto é o caso da comunicação cara-a-cara, e em um ambiente em linha onde fóruns de discussão, audioconferência ou videoconferência podem ser usados. Cf. Rifkin, Janet. (2001). Online Dispute Resolution: Theory and Practice of the Fourth Party. *Conflict Resolution Quarterly*, *19* (1), 117-124, p.119.DOI: 10.1002/crq.3890190109.

[120] Na comunicação assíncrona, as partes não tomam parte na discussão ao mesmo tempo. Elas não recebem imediatamente a comunicação da outra parte, e também não precisam de reagir instantaneamente. Fóruns de discussão, correio eletrónico e de mensagens de texto (ou SMS) são os principais exemplos de comunicação assíncrona. É importante perceber que em ambas as formas de ODR de comunicação podem ser combinados. Cf. *Idem, ibidem.*

[121] Andrade, F., Carneiro, D., Novais, P. (2010). A Inteligência Artificial na resolução de conflitos em linha. *Scientia Ivridica, 59* (321), 137-164, p.138. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/19388/1/4%20-%202010b%20-%20Journal%20Scientia%20Ivridica.pdf consultado a 4 de março de 2013.

[122] *Idem, ibidem.*

[123] Comité Económico e Social Europeu, *Parecer sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à resolução de litígios de consumo em linha (Regulamento ODR)*, (COM (2011) 794 final-2011/0374 (COD)), de 28 de março de 2012, p.4. Disponível em:

No seu livro de 2001, Ethan Katsh e Janet Rifkin introduziram conceito de tecnologia como a "quarta parte"[125] no processo de resolução do litígio que poderá auxiliar um terceiro neutro (mediador ou árbitro) quanto ao correto planeamento da estratégia ou à tomada da melhor decisão. Neste domínio, surgem como elemento tecnológico de relevo os denominados sistemas periciais[126]. Eles podem auxiliar o terceiro (mediador ou árbitro) a tomar conhecimento de casos e decisões anteriores, bem como da respetiva aplicação da lei[127]. É preciso mencionar também sistemas de suporte à decisão que compilam e organizam conhecimento útil com o objetivo de facilitar o processo de tomada de decisão, sendo a tecnologia neste contexto uma ferramenta de armazenamento e gestão de dados e informação sobre o caso em análise[128].

Os referidos sistemas, nas suas representações mais avançadas, são capazes de aprender e ir aperfeiçoando soluções para litígios: eles não se limitam apenas a facultar a comunicação entre os intervenientes do processo ou tornar mais fácil o acesso à informação, mas possuem capacidade de gerar sugestões e soluções, ao nível da definição de estratégias e do processo de tomada de decisão, ao longo de todo ciclo de vida de conflito. Os referidos sistemas em conjugação com ambientes inteligentes possuem conhecimento contextual e capacidade de adaptar o processo de resolução de conflito de acordo com as alterações que possam ocorrer no contexto de interação[129].

---

https://toad.eesc.europa.eu/ViewDoc.aspx?doc=ces%5Cint%5Cint610%5CPT%5CR_CES96-2012_DT_PT.doc&docid=2819086 consultado 5 de abril de 2013.

[124] Rule, C. (2003). *Online Dispute Resolution for Business: B2B, Ecommerce, Consumer, Employment, Insurance, and Other Commercial Conflicts*. São Francisco, EUA: Jossey-Bass Wiley Company, p.45.

[125] Katsh, E. E., Katsh, M. E., Rifkin, J. (2001). *Online Dispute Resolution: Resolving Conflicts in Ciberspace*. São Francisco, EUA: Jossey-Bass Wiley Company, p.121.

[126] "Expert systems" em inglês. Cf. Lodder, A.Thiessen, E. (2003). The Role of Artificial Intelligence in Online Dispute Resolution. In D.Choi, E.Katsh (Eds.), *Workshop on Online Dispute Resolution at the International Conference on Artificial Intelligence and Law.* Edinburgh, Reino Unido, p. 4. Disponível em: http://www.mediate.com/Integrating/docs/lodder_thiessen.pdf consultado a 10 de março de 2013.

[127] Cf. Carneiro, D., Novais, P., Andrade, F., Zeleznikow, J., Neves, J. (2009). The Legal Precedent in Online Dispute Resolution. In Guido Governatori (Ed.), *Legal Knowledge and Information Systems, Jurix 2009: The Twenty Second Annual Conference* (pp. 47-52). Amsterdão: IOS Press, pp.50-52. Disponível em: http://repositorium.sdum.uminho.pt/handle/1822/19082 consultado a 3 de março de 2013.

[128] Katsh, E. E., Katsh, M. E.Rifkin, J. (2001), *op. cit.,* pp. 93 e ss.

[129] Carneiro, D., Novais, P., Neves, J. (2011). Toward Seamless Environments for Dispute Prevention and Resolution. In Paulo Novais, Davy Preuveneers, Juan M. Corchado (Eds.), *Ambient Intelligence-Software and Applications. 2nd International Symposium on Ambient Intelligence* (pp. 25-32). Berlim: Springer, p.27.

O *SmartSettle* é um dos exemplos dos sistemas inteligentes de suporte para resolução de litígios em linha[130]. Trata-se de um sistema de apoio à negociação que torna possível às partes solucionar os litígios com base em funções de satisfação por elas identificadas através de uma gama de ferramentas analíticas que permitem clarificar os interesses e as preferências, identificar as vantagens e desvantagens, reconhecer a satisfação das partes e gerar soluções[131]. O *SmartSettle* modela as preferências com fórmulas matemáticas e usa técnicas de otimização para gerar soluções ao mesmo tempo justas e ótimas, de acordo com as preferências das partes, que são representadas através de fórmulas de satisfação, passíveis de serem modificadas pelas partes em qualquer momento. Vários métodos podem ser usados para a negociação: troca de propostas, sugestões, reflexões. Se as partes não conseguirem chegar a uma solução, o sistema, após uma série de propostas e respostas dos intervenientes no processo, tendo em atenção as preferências das ambas as partes, gera uma solução matematicamente ótima para a disputa, maximizando o benefício que pode ser alcançado por ambas as partes[132].

1.2.4.2. Tecnologias de ambientes inteligentes em sistemas de resolução de litígios em linha

As plataformas de RLL utilizam interfaces inteligentes que compreendem um conjunto de interfaces dinâmicas que são adaptadas a cada utilizador específico, a fim de tornar a interação com a plataforma numa experiência mais intuitiva e fácil.

No âmbito dos sistemas RLL, as interfaces inteligentes podem ser usadas como tutores que fornecem informação às partes relativamente a temas ou tópicos específicos, como, *verbi gratia*, indicação das normas legais aplicáveis a uma determinada situação. Noutros casos, estas interfaces podem ser utilizadas para guiar as partes através do processo de resolução do litígio, ajudando a preencher informação em falta e dando conselhos e orientações úteis no momento certo[133].

---

[130] SmartSettle – Online Negotiation System. Disponível em: http://www.smartsettle.com consultado a 14 de novembro de 2012.

[131] Andrade F., Carneiro D., Novais P. (2010), *op. cit.,* pp. 161-162.

[132] *Idem, ibidem.*

[133] Carneiro, D., Novais, P., Neves, J. (2011), *op. cit.*, pp. 27-28.

Ao mesmo tempo, a maior crítica dirigida ao modelo de resolução de litígios em linha, onde a tecnologia assume papel do terceiro neutro, consiste na falta de "sensibilidade" para se aperceber das intenções e emoções das partes envolvidas na litigância o que, por sua vez leva à perda de uma quantidade significativa de informações relevantes para o processo. Esta informação pode incluir linguagem corporal, informação de contexto e estado emocional das partes. Tudo isto seria levado em atenção por um juiz ou um júri durante um litígio em tribunal, mas fica perdido quando se usa a ferramenta de RLL. Como resultado, os processos de resolução de conflitos em linha podem ficar "frios" e focados apenas na informação objetiva, deixando de lado as informações de contexto que podem ser muito importantes, principalmente do ponto de vista do mediador[134].

O uso da inteligência artificial[135] e, mais particularmente, das técnicas de ambientes inteligentes pode ajudar a preencher esta lacuna[136]. O principal objetivo consiste em superar algumas das principais desvantagens da comunicação em linha, ou seja, a falta de informação contextual, como linguagem corporal ou gestos, nível de stress, de fadiga e estilos conflituais das partes. Informações de contexto são necessárias não só para as partes tomarem melhores decisões e mais realistas, mas também para interpretar a evolução do estado emocional das partes litigantes a decorrer do processo de negociação. A ausência deste tipo de informações pode levar o terceiro neutro a tomar decisões arriscadas e menos acertadas, situação que seria facilmente detetada e evitada no caso da comunicação cara-a-cara[137]. Além disso, as informações de contexto são importantes para as partes terem consciência de que, do outro lado de ecrã/tela

[134] Novais, P., Carneiro, D., Gomes, M., Neves, J. (2013). The Relationship Between Stress and Conflict Handling Style in an ODR Environment. In Yoichi Motomura, Alastair Butler, Daisuke Bekki (Eds.), *Lecture Notes in Computer Science, New Frontiers in Artificial Intelligence. JSAI-isAI 2012 Workshops, LENLS, JURISIN, AMBN, ISS, Revised Selected Papers,* 7859 (pp. 125-140). Berlim: Springer. DOI: 10.1007/978-3-642-39931-2_10.

[135] Carneiro, D., Novais P., Andrade, F., Zeleznikow J., Neves J. (2014). Online Dispute Resolution: An Artificial Intelligence Perspective. *Artificial Intelligence Review*, *4* (2), 211-240. Paises Baixos: Springer.DOI: 10.1007/s10462-011-9305-z.

[136] Lodder, A., Thiessen, E. (2003), *op. cit.*, pp. 4-5.

[137] Friedman, R., Olekalns, M., Oh, S. H. (2007). Choosing Your Words Carefully: Managing'Face'During Online Dispute Resolution. In *IACM 20th Annual Conference 2007 Meetings Paper*. Budapeste, Hungria, p.4. Disponível em: http://ssrn.com/abstract=1111637 consultado a 11 de dezembro de 2012.

existem pessoas com sentimentos, desejos e receios e que cada decisão ou palavra deve ser bem calculada[138].

Ademais, o acesso à informação de contexto e estado emocional das partes pode revelar-se extremamente importante para o processo de tomada de decisão. Um mediador ou um terceiro neutro pode utilizar informações de contexto (captadas pelos sensores de ambiente e dispositivos não invasivos, etc., que determinam o nível de nervosismo, bem como permitem analisar o discurso[139] através de certas caraterísticas linguísticas e semânticas, mímica, tom de voz, entre outros) para aumentar as hipóteses de chegar a bons resultados através do planeamento ou recalculo da estratégia, tendo em atenção como cada proposta apresentada afeta as partes do processo[140].

Atualmente está a ser desenvolvido projeto *UMCourt* na Universidade do Minho, em Portugal, no contexto das TIARAC[141] (Telemática e Inteligência Artificial (AI) em Resolução Alternativa de Conflitos), o qual criou uma plataforma RLL baseada em agentes inteligentes de *software* e os AmI que não só fornecem ajuda na gestão e acesso à informação pelas partes e apresenta um rol de possíveis resultados, mas também apresenta um conjunto de funcionalidades inovadoras para apoiar a tomada de decisão, facilitando o acesso a informações de contexto, tais como o estilo de manipulação de conflito das partes ou os seus níveis de stress[142, 143, 144].

---

[138] "(...) contextinformation is needed for parties to keep in mind that at the other end of the screen there are people with feelings, desires and fears and that each decision or word has to be thought carefully". Cf. Carneiro, D., Castillo, J. C., Novais, P., Fernandéz-Caballero, A., Neves, J. (2012). Multimodal Behavioral Analysis for Non-invasive Stress Detection. *Expert Systems with Applications*, *39*(18), 13376-13389., p.13382. DOI: dx.doi.org/10.1016/j.eswa.2012.05.065.x.

[139] Broekens, J., Jonker, C. M., Meyer, J. J. C. (2010). Affective Negotiation Support Systems. *Journal of Ambient Intelligence and Smart Environments*, *2* (2), 121-144.

[140] Novais, P., et al. (2013), *op. cit.,* pp.126-128.

[141] TIARAC: Telemática e Inteligência Artificial na Resolução Alternativa de Conflitos. Grupo de Inteligência Artificial. Departamento de Informática da Universidade do Minho (Centro de Ciências e Tecnologias de Computação da Universidade do Minho). Braga, Portugal. Disponível em: http://islab.di.uminho.pt/tiarac/ consultado a 18 de novembro de 2012.

O sistema está a ser desenvolvido de modo a ser aplicado a diferentes domínios legais: direito do trabalho, direito de família, direito do consumidor.

[142] Andrade, F., Novais, P., Carneiro, D., Zeleznikow, J., Neves, J. (2010). Using BATNAs and WATNAs in Online Dispute Resolution. In K. Nakakoji, Y. Murakami, E. Mc- Cready (Eds.), *New Frontiers in Artificial Intelligence* (Vol. 6284), (pp. 5–18). Berlim: Springer**.** DOI:10.1007/978-3-642-14888-0_2.

[143] Carneiro, D., Novais, P., Andrade, F., Zeleznikow, J., Neves, J. (2010). Using Case-Based Reasoning to Support Alternative Dispute Resolution. In Andre Ponce de Leon F. de Carvalho, *et al.* (Eds.), *Distributed Computing and Artificial Intelligence*, (vol.79), (pp. 123-130). Berlim: Springer. DOI: 10.1007/978-3-642-14883-5_16.

A principal utilidade de um terceiro neutro está em determinar como cada aspeto do processo de resolução de disputa afeta a parte. Por isso, torna-se muito importante o desenvolvimento de sistemas de RLL com recurso a inteligência emocional para que sejam capazes, através da análise de informação contextual, compreender o estado afetivo das partes durante todo o processo de litigância. A principal caraterística da inteligência emocional é a capacidade de detetar e identificar o estado emocional de uma pessoa com quem estamos a comunicar. A inteligência emocional é um traço da inteligência humana que tem sido defendido como o mais importante, e até mesmo indispensável para uma vida social bem-sucedida[145].

O ser humano é muito afetado pelas emoções, humor e personalidade, portanto torna-se útil e necessário conceber ambientes inteligentes para sistemas de RLL, onde essa realidade seja considerada. Existe, portanto, a necessidade de recurso a inteligência emocional no campo da tecnologia de AmI com o objetivo de reconhecer emoções humanas ou expressar emoções por máquinas na interação homem-computador. Os sistemas interativos homem-máquina capazes de detetar stress[146] e de se adaptar e responder de forma apropriada aos estados afetivos do utilizador[147] irão, cada vez mais, ser vistos de uma forma mais natural e usados com maior confiança[148].

---

[144] Carneiro, D., Novais, P., Andrade, F., Neves, J. (2011). Retrieving Information in Online Dispute Resolution Platforms: A Hybrid Method. In Kevin D. Ashley & Tom M. van Engers (Eds.), *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Law* (pp. 224-228), University of Pittsburgh School of Law, Pittsburgh, Pennsylvania. Nova Iorque: ACM. Disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/14515/1/ICAIL11%20CNAN.pdf consultado a 2 de maio de 2013.

[145] Goleman, D. (1995). *Emotional Intelligence.* Nova Iorque: Bantam Books, pp. 46, 65, 95.

[146] Carneiro *et al.* (2012), *op. cit.*, p. 13378.

[147] Santos, R. J. da Silva (2010). *Sistema de apoio à argumentação em grupo em ambientes inteligentes e ubíquos considerando aspetos emocionais e de personalidade*. Dissertação de Doutoramento, Universidade de Trás-os-Montes e Alto Douro, Vila Real, Portugal, p. 47. Disponível em: http://hdl.handle.net/10348/2033 consultado a 19 de março de 2013.

[148] Contudo, este novo paradigma dos sofisticados sistemas interativos homem-máquina pode levantar uma série de questões a propósito de detetores de mentiras ou polígrafos que são basicamente a combinação de aparelhos médicos usados para detetar as alterações fisiológicas que acontecem no corpo. Quando uma pessoa é questionada sobre um acontecimento ou facto o examinador procura ver como os batimentos cardíacos, a pressão arterial, a frequência respiratória e a atividade eletrodérmica (suor dos dedos, nesse caso) de uma pessoa mudam em comparação aos níveis normais. Tais variações podem indicar se a pessoa está a mentir, mas os resultados dos exames estão abertos à interpretação do examinador. Na realidade, outras situações, como nervosismo, angústia, tristeza e embaraço, podem gerar mudanças nas batidas do coração, na pressão arterial, na respiração e na transpiração. Tais medidas podem distorcer o resultado do teste, comprometendo a idoneidade do valor da prova que se pretenderia obter com a utilização do polígrafo. *Vide* Lewis, J. A., & Cuppari, M. (2009). Polygraph: The Truth Lies Within, *The Journal Psychiatry & Law*, *37*, 85-92, e Fox, D. (2009). The Right to Silence as Protecting Mental Control. *The Akron Law Review*, *42*, 763-801. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1617410 consultado a 2 de agosto de 2014.

Como já foi referido, a Equipa de Investigação do Sistema, da Universidade do Minho está a desenvolver o projeto *VirtualECare*[149, 150], cujo objetivo consiste em desenvolver um ambiente baseado em agentes capazes de monitorizar, interagir e oferecer aos seus utilizadores serviços de extrema qualidade. Nesse sentido, o sistema é capaz de ler informação e caraterísticas de ambiente e de contexto no qual se encontra inserido o seu utilizador, incluindo condições ambientais, estado emocional, estado fisiológico, entre outros[151]. O *VirtualECare* aplicado nos sistemas RLL poderá aumentar a taxa de sucesso dos procedimentos de resolução de conflitos e aproximá-los do ambiente comunicativo cara-a-cara[152].

Do ponto de vista de um terceiro neutro, o acesso a informação contextual permitirá gerir melhor o processo, fazer pausas para prevenir a escalada de emoções ou aconselhar uma parte a ponderar com mais calma sobre uma determinada decisão ou proposta no caso de estar muito nervosa. Do ponto de vista das partes, isso permitirá a uma parte avaliar o estado emocional da oponente e perceber como a outra parte está a ser afetada por cada item do processo e, acima de tudo, tomar consciência de que, do outro lado existe alguém igual a ele/ela, com os mesmos receios, desejos e expectativas. Assim, as partes são obrigadas a ponderar melhor as suas decisões e palavras, sendo menos propensas a se atacarem ou a se ofenderem[153].

Tendo em conta tudo o que até agora se referiu, torna-se pertinente que as plataformas RLL possam ser complementadas por ambientes inteligentes capazes de adquirir informações importantes de meio envolvente e sobre as partes, nomeadamente o seu estado emocional. O acesso a este tipo de informação permitiria ao sistema RLL verificar em que medida uma sugestão, uma ação ou um determinado tópico afeta ou influencia cada parte e, desta forma,

---

[149] Costa, R., Novais, P., Lima, L., Carneiro, D., Samico, D., Oliveira, J., Machado, J., Neves. J. (2009). VirtualECare: Intelligent Assisted Living. In Dasun Weerasinghe (Ed.), *Electronic Healthcare* (pp. 138-144). Berlim: Springer.

[150] Costa, R., Carneiro, D., Novais, P., Lima, L., Machado, J., Marques, A., Neves, J. (2008). Ambient Assisted Living. In J. M. Corchado, D. Tapia, J. Bravo (Eds.), *Advances in Soft Computing, 3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008* (*Vol. 51*), (pp. 86-94). Berlim: Springer.

[151] Carneiro, D., Novais, P., Machado, L., Analide, C., Costa, N., Neves, J. (2011, janeiro). Role Playing Games and Emotions in Dispute Resolution Environments. In Emilio Corchado, *et al.* (Eds.), *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011* (pp. 155-162). Berlim: Springer, pp.156-159.

[152] Novais, P., Carneiro, D., Gomes, M., Neves, J. (2012). Non-invasive estimation of stress in conflict resolution environments. In Yves Demazeau, *et al.* (Eds.), *Advances on Practical Applications of Agents and Multi-Agent Systems* (pp. 153-159).Berlim: Springer, pp. 158-159.

[153] Carneiro *et al.* (2012), *op. cit.*, p. 13383.

adaptar também estratégias a fim de alcançar maior eficiência e o resultado final mais satisfatório para ambas as partes litigantes.

1.2.4.3 Proteção de dados pessoais na resolução de litígios em linha

Na era da Internet, o legislador está permanentemente a tentar recuperar o atraso em termos normativos relacionado com os desenvolvimentos nas tecnologias da informação e comunicação. No campo de resolução de disputas, o regime legal existente também está a ser modificado para acomodar novas tecnologias e as suas aplicações às formas tradicionais de resolução de litígios. Para dar resposta aos desafios provenientes da crescente dimensão digital do mercado interno da União Europeia (UE), entrou em vigor, em julho de 2013, a Diretiva n.º 2013/11/UE sobre a resolução alternativa de litígios de consumo (Diretiva RAL) e que altera a anterior Diretiva n.º 2009/22/CE, acompanhada do Regulamento n.º524/2013 sobre a resolução de litígios de consumo em linha (Regulamento RLL), que altera o anterior Regulamento (CE) n º 2006/2004. Estes dois diplomas legais constituem atualmente um novo quadro jurídico europeu em resolução alternativa de litígios de consumo, nomeadamente em RLL.

O Regulamento RLL tem por objetivo contribuir para o bom funcionamento do mercado interno, em particular do mercado interno digital, proporcionando uma plataforma eletrónica europeia de RLL ("plataforma de RLL") que facilite a resolução de litígios entre consumidores e comerciantes, em linha e por via extrajudicial, de forma independente, imparcial, transparente, eficaz, célere e justa e que operacionaliza o contacto entre consumidores e comerciantes para a procura de um entendimento satisfatório com intervenção de uma entidade de resolução alternativa (artigo 1.º do Regulamento RLL). O referido regulamento visa criar uma plataforma de RLL à escala da União Europeia. Essa plataforma assumirá a forma de um sítio *Web* interativo, com um ponto de entrada único para os consumidores e para os comerciantes que pretendam resolver litígios decorrentes de transações em linha por via extrajudicial.

Contudo, a questão vital para a legitimidade e eficácia da resolução de litígio em linha e, a que importa mais para o presente trabalho, reporta à confidencialidade e à privacidade e à proteção de dados e de informações pessoais tratados e armazenados na plataforma de RLL.

O tratamento de informações nos sistemas de resolução de litígios em linha está sujeito às regras em matéria de proteção de dados pessoais previstas na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[154, 155].

A expressão "dados de carácter pessoal" consta do artigo 8.º da Carta de Direitos Fundamentais da União Europeia (CDFUE)[156] e do artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE)[157], da Diretiva 95/46/CE no artigo 2.º[158], que dados pessoais no direito da União Europeia seriam: "qualquer informação relativa a uma pessoa singular, identificada ou identificável, direta ou indiretamente"[159].

Tal disposição encontra-se incorporada nas várias normativas europeias sobre o tema, em Portugal temos o artigo 3.º da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados ou LPDP)[160] que transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares

---

[154] Publicada no Jornal de Oficial das Comunidades Europeias, N.º L 281/31 em 23 de novembro de 1995.

[155] O regime de proteção de dados pessoais será abordado com mais detalhe no Capítulo 3 desta dissertação.

[156] O artigo 8.º da Carta de Direitos Fundamentais da União Europeia diz: " n.º1- Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito; n.º2 - Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação; n.º 3 - O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente".

[157] Artigo 16.º, n.º1 do Tratado sobre o Funcionamento da União Europeia: "Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito".

[158] Artigo 2.º da Diretiva 95/46/CE define a noção de dados pessoais como "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". *Vide* também Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, (01248/07/PT WP136), adotado em 20 de junho de 2007, p.4. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf consultado a 13 de março de 2014.

[159] Ou seja, não são apenas aqueles que de forma direta possibilitam a identificação de uma pessoa, como o caso de um número de identificação pessoal, mas também aqueles que indiretamente o permitem através de associação de conceitos ou conteúdos, como, por exemplo a matrícula de um veículo, o número de telefone/telemóvel, o *e-mail,* o valor de alguma retribuição ou remuneração, o som da voz, classificações escolares, o *curriculum vitae*, a história clínica, os créditos e as dívidas, o registo de quaisquer compras, o registo de pagamentos, etc.

[160] O referido diploma será analisado ao longo deste trabalho de acordo com os diferentes interesses em causa, contudo a análise mais aprofundada será feita no ponto 3.2.1.

no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[161]. A LPDP aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados[162, 163], (artigo 3.º, alínea a)), constituindo dados pessoais, toda a informação, seja ela numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo, relativa a uma pessoa física identificada ou identificável[164]. Nos termos do artigo 3.º, alínea a), segunda parte, da Lei n.º 67/98 considera-se "identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou a mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"[165]. É possível concluir que são identificáveis, não apenas aqueles que o próprio titular possa, pelos seus próprios meios identificar, mas que possa ainda identificar com recurso a meios de que disponha um terceiro[166].

A noção de tratamento de dados pessoais integra: a recolha de dados, o registo desses mesmos dados, a sua organização, conservação, adaptação, alteração, consulta, difusão, ou qualquer outra forma de colocação à disposição destes mesmos dados, bem como o bloqueio ou o apagamento/destruição (artigo 3.º alínea b) da Lei n.º 67/98, de 26 de outubro), independentemente da tecnologia ou técnica utilizada, e ainda do formato ou tipo, sejam texto, som ou imagem. De acordo com o artigo 6.º da LPDP o tratamento de dados pessoais só pode ser efetuado se o seu titular tiver fornecido de forma inequívoca o seu consentimento[167, 168] ou se o tratamento for necessário para fins expressamente estipulados no

---

[161] De acordo com a Diretiva 95/46/CE e a Lei da Proteção de Dados, são exemplos de dados pessoais, o nome, a morada, dados de identificação como o número de segurança social, de contribuinte, do bilhete de identidade, do passaporte, ou até de cliente de estabelecimento comercial, número de telefone, *o e-mail*, uma chapa de matrícula, o valor de uma retribuição, o som da voz registada para permitir o acesso a uma conta bancária, pois todos estes dados estando associados a uma pessoa permitem identificá-la. É o caso da impressão digital, da imagem biométrica do rosto, de uma imagem recolhida através do uso de uma câmara, v.g. vídeo vigilância, ou conjunto de fotografias divulgadas na Internet. As classificações escolares, o historial clínico, as dívidas, os créditos, as compras, os registos dos meios de pagamento, etc..

[162] Castro, Catarina Sarmento e. (2005), *op. cit.*, p. 106.

[163] Marques, José A. S. Garcia, Martins, Lourenço. (2006). *Direito da Informática*. (2ª ed.). Coimbra: Livraria Almedina, pp. 344-345.

[164] O conceito de dados pessoais será discutido com mais pormenor no ponto 3.2.1.

[165] Segundo artigo 2.º, alínea a) da Diretiva 95/46/CE: "«Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

[166] Castro, Catarina Sarmento e. (2005), *op. cit.*, pp. 72-73.

[167] O requisito de consentimento do titular de dados será analisado com mais detalhe no ponto 3.2.1.

[168] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.*, p. 339.

mesmo preceito legal, sendo exclusivamente essas as condições para a legitimidade do tratamento de dados pessoais[169].

De acordo com a alínea h) do artigo 3.º da LPDP, o consentimento deve, em geral, ser uma manifestação de vontade livre, específica e informada[170]. No caso de dados sensíveis, o consentimento deve ser ainda expresso, conforme o artigo 35.º, n.º3 da CRP e o artigo 7.º, n.º2 da LPDP. A Comissão Nacional de Dados (CNPD)[171] tem entendido que o consentimento será expresso quando o titular dos dados o der por escrito[172].

O consentimento só pode ser considerado livre quando seja dado[173] sem qualquer coação e quando possa ser retirado sem restrições ou oposição e, sem que o titular dos dados sofra qualquer consequência.[174] Será expressão de uma manifestação de vontade específica quando o consentimento for dado em função de um determinado período temporal e para finalidades conhecidas antecipadamente e sempre que a finalidade do tratamento sofra qualquer alteração, deve ser obtido novo consentimento[175]. De acordo com Catarina Sarmento e Castro só é possível

---

[169] Artigo 6.º da Lei n.º 67/98: "a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido;

b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c) Proteção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;

d) Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados".

[170] De acordo com Catarina Sarmento e Castro*:* "Enquanto condição geral de legitimidade, e ao contrário do que sucede quando funciona como condição para o tratamento de dados sensíveis, não se exige que o consentimento seja expresso. Daqui tem-se retirado que o consentimento, em geral, poderá ser um consentimento meramente oral, não sendo necessário que este seja obtido por escrito". Cf. Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 207.

[171] Comissão Nacional de Proteção de Dados, criada nos moldes previstos pela Lei n.º 10/95, atualmente substituída pela Lei n.º67/98, designada pela sigla CNDP, é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia de República e tem, segundo o artigo 22.º da mesma Lei, a atribuição genérica de controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pela liberdades e garantias consagradas na Constituição e na lei. Mais sobre CNPD *vide* ponto 3.2.1.

[172] *Vide* a Autorização n.º45/96 e a Autorização n.º17/96, ambas publicadas no relatório da CNPD, de 1996.

[173] O consentimento prestado pelo titular dos dados pessoais pode em qualquer momento ser revogado, nos termos do artigo 81.º do CC e não funcione em termos retroactivo. *Vide* Vasconcelos, Pedro Pais de. (1999). Proteção de dados pessoais e direito à privacidade. In AA.VV., *Direito da sociedade da informação* (Vol.1), (pp. 241-253). Coimbra: Coimbra Editora, p.252.

[174] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 206.

[175] *Idem*, p. 207.

considerar como consentimento informado aquele que for dado havendo o titular de dados tomado conhecimento da finalidade e da extensão exata do seu consentimento[176].

Os titulares de dados, neste caso as partes litigantes do processo de RLL, deverão ser informados, e dar o seu consentimento, no que se refere ao tratamento dos seus dados pessoais na plataforma de RLL, e devem ser informados quanto aos seus direitos no que respeita a esse tratamento, por meio de uma declaração de confidencialidade dos dados que deve ser tornada pública e que deverá explicar, numa linguagem simples e clara, as operações de tratamento levadas a cabo sob a responsabilidade dos vários intervenientes da plataforma, nos termos dos artigos 10.º e 11.º da Lei n.º 67/98, de 26 de outubro que correspondem aos artigos 10.º e 11.º da Diretiva 95/46/CE.

Em primeiro lugar, os titulares de dados têm direito de acesso aos dados objeto de tratamento (artigo 11.º Lei n.º 67/98). É um direito à informação não sujeito a qualquer justificação por parte do titular, basta haver a intenção de consultar os dados que lhe dizem respeito, e sempre que tal seja legalmente exigido, o cumprimento de obrigações de registo, autorização, notificação à Comissão Nacional de Proteção de Dados[177]. No caso de RLL as partes devem ter acesso aos dados processados e tratados durante a resolução do conflito. Para além disso, o titular de dados tem também direito a saber da finalidade do tratamento dos seus dados pessoais, se existe comunicação dos dados a outras entidades, como e em que condições foi realizado o seu tratamento (artigo 10.º da Lei n.º 67/98). Tudo isto concretiza o direito à informação do titular dos dados juntamente como o princípio de proporcionalidade[178].

Os dados devem ser conservados apenas durante o período necessário de acordo com as finalidades da recolha e do tratamento (artigo 5.º n.º 1, alínea e) da Lei n.º 67/98). Se os dados estão incorretos ou se são conservados para além do prazo limite, o titular tem o direito que os mesmos sejam eliminados ou, pelo menos, o acesso aos mesmos bloqueados, de acordo

[176] Por exemplo: a identidade do responsável pelo tratamento e do seu representante, os destinatários dos dados ou categorias de destinatários, em caso de comunicação de dados pessoais e da existência de direito de acesso e das suas condições. *Idem,* pp. 206-207.

[177] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 247.

[178] *Idem*, pp. 236-237.

com o artigo 11.º n.º1, alínea d) do referido diploma[179]. Todavia, há que salientar que a LPDP no mesmo artigo 5.º n.º2 permite o prorrogação do prazo, ainda que tenha sido cumprida a finalidade do tratamento, se fins históricos, científicos ou estatísticos o justifiquem; desde que não incompatíveis com o escopo de tratamento original. Por isso, é importante assegurar que os dados apresentados na queixa sejam eliminados logo que já não se mostrem necessários e depois de certo prazo ou imediatamente, quando fica claro que uma queixa é infundada. O artigo 12.º n.º3. do Regulamento RLL prevê que os dados pessoais referentes a litígios sejam automaticamente apagados seis meses após a data de conclusão do mesmo.

Para além disso, o titular dos dados tem ainda o direito à retificação dos dados inexatos ou incompletos, e também à atualização dos mesmos, consagrado no artigo 11.º n.º1, alínea d) da Lei n.º 67/98, com vista ao cumprimento de um verdadeiro controlo pelo titular, o direito à correção dos dados dentro de prazos determinados. Não depende isto da iniciativa do titular, mas é antes um dever que impende sobre o responsável pelo tratamento dos dados.

O direito de oposição, previsto no artigo 12.º da Lei da Proteção de Dados, consiste, em geral, na faculdade concedida ao titular dos dados de se opor ao tratamento dos seus dados pessoais, com base em razões ponderosas e legítimas relacionadas com a sua situação particular[180].

A Lei da Proteção de Dados atribuiu ao titular dos dados pessoais o direito a não ficar sujeito a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento (artigo 13.º)[181]. Cria-se, assim, uma proibição geral relativa à tomada de decisões individuais automatizadas, apenas ressalvada nos termos do n.º 2 e 3. Admite-se que os dados armazenados de forma automatizada possam ser utilizados para ajudar uma tomada de decisão, *verbi gratia,* fornecendo mais informação, ou sugerindo a atuação apropriada, mas os

[179] *Idem,* p. 251.

[180] *Idem,* p. 254.

[181] A respeito desta questão Catarina Sarmento e Castro fala num direito a não se ficar sujeito a uma decisão individual automatizada: *Idem,* pp. 251-253. *Vide* igualmente o ponto 3.2.1. do presente trabalho.

computadores e os dados que armazenam não devem ser utilizados como único meio para encontrar a solução[182]. Daí a exceção do artigo 13.º n.º 2, da Lei da Proteção de Dados, que admite a submissão a decisão automatizada, desde que existam "medidas adequadas que garantam a defesa dos seus (titular dos dados) interesses legítimos, designadamente o seu direito de representação e expressão" ou quando a decisão "ocorra no âmbito da celebração ou execução de um contrato, e sob condição de o seu (do titular dos dados) pedido de celebração ou execução do contrato ter sido deferido" (artigo 13.º n.º 2). Assim sendo, apenas quando a decisão é exclusivamente tomada com uso da informática, e não ocorra "no âmbito da celebração ou execução de um contrato", ou, quando ocorra neste caso, sirva para negar o seu pedido, é que é decisão automática é proibida[183].

Contudo há um determinado tipo de dados cujo tratamento está constitucionalmente proibido no n.º 3 do artigo 35.º da CRP: "A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica", sendo tal limitação reafirmada pelo n.º 1 do artigo 7.º da LPDP que diz que é proibido o tratamento de dados sensíveis, ali qualificados como dados pessoais relativos a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, inclusive dados genéticos (a mesma proibição encontra-se plasmada no artigo 8.º da Diretiva 95/46/CE)[184].

Pode acontecer, nos sistemas RLL aliados com ambientes inteligentes, que os dados aparentemente pouco relevantes e de carácter não sensível, depois de serem submetidos ao tratamento (que poderá implicar criação de perfis, cruzamento de dados) passem a revelar informações sensíveis, permitindo a elaboração do conhecimento sobre a pessoa em causa, sobretudo se conjugado com outros elementos que possam induzir caraterísticas, preferências, opiniões políticas, crenças religiosas, estado de saúde, etc.[185], pelo que, deve tal informação receber a mesma proteção.

---

[182] *Idem,* p. 254.

[183] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.*, p. 359.

[184] *Idem,* p. 337.

[185] Rouvroy, A. (2008). Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. *Studies in Ethics, Law, and Technology*, *2* (1), 1-51, p.41. DOI: 10.2202/1941-6008.1001. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 consultado a 9 de dezembro de 2012.

Conforme o que foi dito supra, o tratamento de dados sensíveis é constitucionalmente proibido por força do n.º 3 do artigo 35.º da CRP. No entanto, o mesmo dispositivo constitucional acima mencionado prevê a excecionalidade do tratamento de dados sensíveis em alguns casos, mediante o consentimento expresso do titular ou autorização prevista em lei, sempre com garantias de não discriminação, ou para processamento com escopo estatístico, mediante o uso de dados que não permitam a identificação do respetivo titular[186].

Em suma, há que salientar que no âmbito de resolução de litígios em linha o tratamento de informações deve forçosamente respeitar as normas e os princípios em matéria de proteção de dados pessoais estabelecidos na Diretiva 95/46/CE e no Decreto-Lei n.º 67/98, de 26 de outubro a fim de serem processados de modo leal e legal. A correta aplicação dos princípios de proteção de dados estabelecidos na Diretiva 95/46/CE é condição *sine qua non* para o êxito da implantação e aceitação geral dos sistemas de RLL na sociedade.

1.3. Considerações

O presente Capítulo começou por abordar o conceito de Ambientes Inteligentes através de um breve histórico e por descrever as suas principais caraterísticas juntamente com uma série de áreas de possível aplicação. Foi apresentada uma visão do mundo rodeado por uma grande quantidade de dispositivos eletrónicos, introduzidos num determinado ambiente físico que se adapta às diferentes necessidades e situações dos utilizadores, tendo autonomia para agir e sendo programado para reconhecer ou, até mesmo, aprender o comportamento do utilizador que vive nesse ambiente.

Foram apresentados vários sistemas no âmbito de ambientes inteligentes que interagem com a vida das pessoas a diferentes níveis, desde ambiente doméstico, até áreas como saúde, comércio eletrónico, educação e resolução de conflitos em linha.

Contudo, apesar de inúmeros benefícios inerentes à aplicação de ambientes inteligentes, o estudo desenvolvido ao longo do presente trabalho pretende focar-se nas ameaças à

[186] *Vide* Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.*, pp. 247-252.

privacidade e à segurança de dados pessoais no contexto de AmI. Como ficou demonstrado, o objetivo final do ambiente inteligente é facilitar e melhorar a vida das pessoas através da recolha de grandes quantidades de informação e a sua análise com vista a fornecer um ambiente personalizado, exclusivo e o mais adequado para os seus utilizadores, o que, por sua vez, implicará uma elevada utilização e armazenamento de dados e informação pessoal, incluindo a criação e gestão de perfis de utilizador.

Ao mesmo tempo, uma certa opacidade do funcionamento dos sistemas de vigilância emergentes acarreta o risco de um processamento indevido e não solicitado de dados pessoais, tornando os aspetos de segurança e privacidade críticos. A invisibilidade de terminais dos sistemas de ambientes inteligentes e a inclusão de modelos de serviços descentralizados não permite ao titular de dados ter uma visão compreensiva de como os seus dados são processados nem ter consciência das implicações daí decorrentes.

Deste modo, estratégias para segurança e privacidade em sistemas de AmI exigem desafios adicionais, pois os mesmos recursos que podem facilitar a interação entre humano e máquina podem igualmente potenciar o acesso ou a divulgação não autorizados de dados pessoais, a vigilância de atividades desenvolvidas pelo utilizador, o armazenamento de informações pessoais de forma insegura ou até mesmo a transferência de tais informações a terceiros sem autorização prévia da posterior utilização dos dados para fins diferentes dos que levaram à sua recolha, etc..

Torna-se pertinente nesta fase do estudo considerar os novos desafios que se colocam à privacidade e proteção de dados pessoais introduzidos pelo paradigma de ambientes inteligentes e a consequente necessidade de repensar questões relacionadas com segurança, confiança, autonomia, identidade e autodeterminação da pessoa humana que serão discutidos no Capítulo seguinte.

CAPÍTULO 2 – POTENCIAIS AMEAÇAS DA TECNOLOGIA DE AMBIENTES INTELIGENTES

2.1. Vigilância e monitorização

O aumento da quantidade de sensores incorporados em ambientes ou em dispositivos pessoais e objetos que as pessoas transportam contribui para o correspondente crescimento da quantidade de dados gerados. A tecnologia baseada nos AmI refere-se a um mundo em que as pessoas estão rodeadas de interfaces intuitivas e inteligentes que são incorporadas em quaisquer tipos de objetos ou lugares[187]. Os dispositivos por detrás dessas interfaces são sensíveis à presença e às necessidades do indivíduo, oferecendo serviços e tratamento personalizados de acordo com os requisitos pessoais, capazes de prever comportamentos através de uma permanente aprendizagem e criação de perfis de utilizadores[188].

O objetivo dessa monitorização consiste na prestação de serviços personalizados ou adaptação do ambiente de acordo com as ordens expressas e necessidades do utilizador, interpretando as informações do contexto envolvente e relacionando as preferências dos seus utilizadores[189].

Nos AmI os espaços estão equipados com um conjunto de tecnologias, infraestruturas, aplicações e serviços implantados em diversos domínios e ambientes, tais como carros, casas, fábricas, escritórios, cidades, etc.. O objetivo final dos ambientes inteligentes consiste na recolha de grandes quantidades de dados, no seu armazenamento e na sua análise com vista a fornecer um ambiente exclusivo, personalizado e o mais adequado para os seus utilizadores[190].

---

[187] Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F., & Rohs, M. (2005). Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In Werner Weber, Jan M. Rabaey & Emilie H.L. Aarts (Eds.), *Ambient Intelligence (pp. 5-29).* Berlim: Springer, p. 5.

[188] Cf. Punie, Y. (2005), *op. cit.*, pp. 141–165.

[189] ČAS Johann. (2011). Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions. In Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes (Eds.), *Computers, Privacy and Data Protection an Element of Choice* (pp. 139-169). Londres: Springer, p. 142.

[190] Lindwer, M., Marculescu, D., Basten, T., Zimmennann, R., Marculescu, R., Jung, S., Cantatore, E. (2003). Ambient Intelligence Visions and Achievements: Linking Abstract Ideas to Real-world Concepts. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition, 2003* (pp. 10-15). Munique, Alemanha: IEEE, p.10. DOI: 10.1109/DATE.2003.1253580.

Ao mesmo tempo que os ambientes inteligentes se tornam convenientes, da mesma forma tornam a privacidade vulnerável a novos ataques e contribuem para a utilização indevida da informação pessoal. As questões de privacidade dizem respeito à recolha nesses ambientes de dados sobre os utilizadores que podem ser partilhados sem o consentimento dos mesmos, por exemplo, informação sobre os interesses, objetivos e planos do utilizador, os quais podem ser explorados por terceiros. Por exemplo, os dispositivos que controlam a posição geográfica das pessoas são muito úteis, mas a divulgação desses mesmos dados poderá não só ameaçar a privacidade do seu utilizador, como também facilitar os ataques terroristas, o roubo ou o sequestro[191].

Os ambientes inteligentes referem-se a espaços físicos, o que, por sua vez, torna indispensável recorrer a vários tipos de sensores, uma vez que se não houver sensores capazes de recolher a informação, o processamento e a complexidade de algoritmos para tratamento de dados presentes nestes sistemas de AmI não representarão utilidade alguma. A monitorização e identificação de pessoas num ambiente são um requisito para funcionamento dos sistemas de AmI.

Os algoritmos[192] de *software* dos sistemas de AmI dependem de dados sensoriais provenientes do mundo físico que permitem ao sistema ter a perceção do ambiente em que se encontram inseridos de forma a auxiliar a tomar decisões correstamete. A qualidade da informação nestes ambientes está diretamente relacionada com a quantidade de sensores existentes e a sua variedade. Assim, quanto maior o número de sensores, mais informação poderá ser captada e processada, o que, por sua vez, melhorará a perceção do sistema sobre o meio envolvente.

Existe grande variedade de sensores, alguns deles foram desenhados para a deteção de produtos químicos e humidade,[193] medição de distância ou indicação do posicionamento geográfico,[194] indicação de temperatura, luminosidade, radiação, som, pressão, velocidade e direção, bem como já foi referido no Capítulo anterior, para a monitorização ao nível fisiológico

[191] Wright D., *et al.* (2008), *op. cit.*, p. 162.

[192] Em informática: conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas. Disponível em:http://www.lexico.pt/algoritmo/ consultado a 5 de outubro de 2013.

[193] Delapierre, G., Grange, H., Chambaz, B., & Destannes, L. (1983). Polymer-based Capacitive Humidity Sensor: Characteristics and Experimental Results.*Sensors and Actuators*, *4*, 97-104, pp. 98.

[194] Wolffenbuttel, R. F., Mahmoud, K. M., & Regtien, P. P. (1990). Compliant Capacitive Wrist Sensor for Use in Industrial Robots. *Instrumentation and Measurement, IEEE Transactions on*, *39*(6), 991-997, pp. 992 e ss.

nos cuidados de saúde[195, 196]. Estes sensores são normalmente de pequenas dimensões e podem ser facilmente integrados em qualquer aplicação ou sistema de ambientes inteligentes.

A tarefa mais complexa para o sistema de AmI consiste em perceber o significado da informação que é apreendida. A análise de dados nos sistemas de AmI pode ser efetuada através do recurso ao modelo centralizado ou descentralizado[197]. No modelo centralizado a informação captada pelos sensores é transmitida a um servidor central onde é analisada. Por sua vez, no caso do modelo descentralizado, cada sensor possui capacidades de processamento local da informação recolhida, que posteriormente será transmitida a outros nós na rede de sensores. A escolha do modelo depende da arquitetura computacional e das tarefas que os sensores realizam num determinado sistema[198].

Os sensores fisiológicos poderão ser utilizados para o reconhecimento de estado afetivo do utilizador, o que poderá facilmente violar a privacidade do indivíduo, revelando as verdadeiras emoções de pessoas, que normalmente tendem a escondê-las por trás de expressões faciais neutras ou falsas. Os sensores podem servir para avaliar o estado de saúde e serem capazes de monitorização contínua e de deteção de anomalias[199], incluindo as fatais, como ataques cardíaco, sendo verdadeiros "laboratório em um chip" capazes de realizar vários testes fisiológicos[200].

De forma geral, os dados são matéria-prima bruta. No momento em que o utilizador atribui a esses dados algum significado especial, eles convertem-se em informação[201]. Quando os especialistas elaboram ou encontram um modelo, realizando a interpretação de informação e esse modelo apresenta um valor acrescentado, então referimo-nos ao conhecimento.

---

[195] Stanford, V. (2004). Biosignals Offer Potential for Direct Interfaces and Health Monitoring. *Pervasive Computing, 3* (1), 99-103, pp. 99-100. DOI: OI: 10.1109/MPRV.2004.1269140.

[196] Najafi, B., Aminian, K.Paraschiv-Ionescu, A., Leow, F., Bula, C. J. R, Robert P. (2003). Ambulatory System for Human Motion Analysis Using a Kinematic Sensor: Monitoring of Daily Physical Activity in the Elderly. *Biomedical Engineering, IEEE Transactions on*, *50* (6), 711-723. DOI:10.1109/TBME.2003.812189.

[197] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002). A Survey on Sensor Networks. *Communications Magazine, IEEE*, *40*(8), 102-114.

[198] Cook, D. J., Augusto, J.C., Jakkula, V. R. (2009), *op. cit.,* p. 281.

[199] Vardasca, R., Costa, A., Mendes, P. M., Novais, P., Simões, R. (2013). Information and Technology Implementation Issues in AAL Solutions. *International Journal of E-Health and Medical Communications (IJEHMC)*, *4*(2), 1-17. DOI:dx.doi.org/10.4018/jehmc.2013040101.

[200] " AmI sensors for evaluating health conditions will be tiny, very sophisticated (the "lab on a chip" capable of performing various physiological tests) and capable of continuous monitoring and detection of anomalies, including life-threatening ones such as heart attacks". Cf. Wright D., *et al.* (2008), *op. cit.,* p. 17.

[201] "Information is the communication of instructive knowledge, informations and numbers.Date is more restrictive word which means thing assumed as fact and made the basis of reasoning on calculation."- Jones, P., & Marsh, D. (1993). *Essentials of EDI Law: A Straightforward Legal Framework to Protect Your Business.*Ontário: Electronic Data Interchange Council of Canada, p. 7.

Outra forma de obter informações sobre utilizadores, para além de monitorização direta, consiste na mineração de dados[202]. O termo "mineração de dados", também conhecido como "Descoberta de Conhecimentos em Bancos de Dados", ou KDD (do inglês, "Knowledge Discovery in Databases"), refere-se à técnica que tem como objetivo o processamento de grandes volumes de dados, com o objetivo de estabelecer relações, associações e padrões em grandes bases de dados preexistentes, transformando dados brutos em informação útil. Para o efeito são utilizados algoritmos de aprendizagem ou classificação baseados em redes neurais e estatística[203]. As técnicas de mineração de dados foram desenvolvidas principalmente pela comunidade de inteligência artificial (a aprendizagem da máquina e o reconhecimento de padrões) e pela comunidade das matemáticas (as estatísticas e o processamento da incerteza).

A mineração de dados refere-se genericamente ao processo de extração de conhecimento útil a partir de grandes volumes de dados que pode ser utilizado em qualquer tipo de base de dados desde que, antecipadamente, seja realizada uma limpeza nos dados de forma que fiquem somente os mais importantes e necessários. A mineração de dados apresenta as seguintes etapas[204]:

- Seleção de dados: recuperação de dados que são relevantes para análise a fim de obter resultados com informações úteis;

- Pré-processamento: nesta fase é efetuada limpeza e a correção de dados incompletos e inconsistentes, de forma a não comprometer a qualidade dos modelos de conhecimento a serem extraídos ao final do processo da KDD;

- Transformação de dados: os dados importantes que foram extraídos no processo anterior são consolidados na forma apropriada para que a mineração possa ser realizada. É efetuada análise dos dados e a sua reorganização de uma forma específica, por meio da aplicação de operações, tais como sumarização e agregação, para depois serem interpretados por um *software* de mineração de dados;

---

[202] *"Data mining"* em inglês

[203] Witten, I. H., Frank, E. (2005). *Data Mining: Practical Machine Learning Tools and Techniques*. São Francisco, EUA: Morgan Kaufmann, pp.5-9, 60 e ss.

[204] Jiawei, H., Kamber, M. (2001). *Data Mining: Concepts and Techniques*. São Francisco, EUA: Morgan Kaufmann, pp.5-7.

- Mineração dos dados: depois de transformados os dados são lidos e interpretados através da aplicação de métodos baseados em técnicas da área de inteligência computacional para a descoberta de padrões. A mineração faz com que meros dados sejam transformados em informações;

- Análise de resultados: após a interpretação poderão surgir padrões, correlações e descoberta de novos factos e informações;

- Apresentação do conhecimento: nesta fase é feita utilização de técnicas de visualização e representação de conhecimento para apresentar novas informações e o conhecimento extraído ao utilizador.

As informações sobre a relação entre dados e, posteriormente, a descoberta de novos conhecimentos, podem ser muito úteis para realizar atividades de tomada de decisão. A técnica de mineração de dados tem sido aplicada em diversas áreas como, por exemplo, o comércio, a saúde, as ações contra-terrorismo, as atividades de fiscalização, etc.[205].

Assim, os dados correlacionados que poderiam ser considerados irrelevantes ou mesmo triviais, caso analisados isoladamente, graças as novas tecnologias baseadas nos AmI, conseguem fornecer informação sobre, por exemplo, o estilo de vida, os gostos e as preferência ou os riscos para a saúde de pessoa, especialmente quando conjugadas com a técnica de vigilância. Isso demonstra o potencial de algumas aplicações do ambiente inteligente, que poderão alterar a natureza dos dados envolvidos.

Ademais, a difusão de recolha e a possibilidade de cruzamento de dados pessoais esbatem a distinção entre os dados sensíveis e não-sensíveis. Primeiro, uma captura persistente e generalizada de dados também inclui itens de natureza sensível; em segundo lugar, o tratamento e cruzamento de dados pouco relevantes pode revelar informações sensíveis, permitindo a elaboração do conhecimento sobre a pessoa em causa.

---

[205] Por exemplo o cruzamento dos dados fiscais e dos pagamentos com cartões de crédito e de débito permitiram ao Governo detetar que, desde 2012, 16 mil contribuintes declararam rendimentos abaixo dos pagamentos que receberam, num montante de 400 milhões de euros. *Vide* em: Lusa. (2013, 4 de dezembro). Cruzamento de dados descobre milhares de pessoas a enganar o Estado. *Expresso.* Disponível em:http://expresso.sapo.pt/cruzamento-de-dados-descobre-milhares-de-pessoas-a-enganaroestado=f844457#ixzz36n3WaWXb consultado a 10 de dezembro de 2013.

Em geral, a computação ubíqua faz sentido somente se os sistemas forem capazes de aprender com o passado, para completar e corrigir perfis pessoais de modo constante e adaptar os serviços em conformidade com necessidades de cada utilizador, o que por sua vez exige que os sistemas de AmI possuam memória[206], ou seja, sejam capazes de armazenar dados pessoais. Nos ambientes inteligentes haverá sempre maneira de restabelecer a identidade pessoal dos indivíduos, uma vez capturada.

No sistema de AmI os utilizadores estão permanentemente observados e o seu comportamento e as ações autonomamente interpretados, tendo em conta a localização e outras informações contextuais. Os resultados destinam-se a um processo de aprendizagem contínua, que formará a base de decisões autónomas por parte do sistema.

A possibilidade de monitorizar o comportamento de compra de bens e serviços dos clientes pode não só conduzir a uma cadeia de fornecimento mais personalizado, mas também pode contribuir para uma situação em que o cliente poderá estar sujeito a controlo e manipulação. Os críticos temem que os fornecedores com acesso à infraestrutura AmI a usem apenas para o seu próprio benefício, apresentando aos seus clientes apenas os produtos que querem promover, em vez de produtos que os clientes realmente precisam ou de que poderiam beneficiar[207].

Em alguns casos, as pessoas estão de facto obrigadas a fornecer (muitas vezes desnecessariamente) informações pessoais, se querem ter acesso a um determinado bem ou serviço, por exemplo, quando pedem um crédito no banco, se candidatam a um emprego, celebram um contrato de seguro, alugam um apartamento, entre outras situações afins.[208] Este ato "voluntário" pode obrigar tanto a uma aceitação das regras impostas, quanto, em caso de rejeição, à recusa dos serviços prestados ou ao abandono do local em que a vigilância é realizada. A título de exemplo: a videovigilância apresenta-se como uma atividade (aparentemente) pouco invasiva para o indivíduo em que, em troco do chamado "bem comum" como a segurança pública (ou mesmo de uma recompensa[209]), é manipulado para cooperar com

[206] Wright D., *et al.* (2008), *op. cit.,* p. 210.

[207] Čas Johann. (2011), *op. cit.,* p. 146.

[208] Wright D., *et al.* (2008), *op. cit.*,pp. 210, 160-165.

[209] Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, *17* (5), 559-596, p. 558.

as autoridades ou com outras entidades, cedendo a sua informação pessoal para fins que não eram inicialmente previstos[210].

Em suma, as aplicações dos AmI estão previstas para serem implementadas em muitas esferas do quotidiano - mesmo aquelas onde a privacidade tem sido considerada sagrada, como em casas das pessoas – o que para alguns críticos levanta o espetro do estado Orwelliano.

O polémico ex-analista da agência de segurança norte-americana NSA Edward Snowden alertou recentemente para a existência de uma ameaça global à privacidade. Snowden, depois de ter revelado a existência de uma rede de espionagem eletrónica por parte dos Estados Unidos, argumentou que os mecanismos de recolha de informação para controlo dos cidadãos descritos pelo escritor George Orwell que já alertara sobre os perigos desse tipo de recolha de informações e dados pessoais no romance "1984", não são nada, comparados com o que existe atualmente[211]. Acrescenta: "Temos detetores em nossos bolsos que nos seguem aonde quer que vamos (...)"[212], apontando para a atual difusão global de *smartphones* e sensores de GPS. Segundo Snowden " (...) uma criança nascida hoje crescerá sem a menor noção de privacidade. Ela nunca saberá o que significa ter um momento privado, para si, de pensamentos não gravados nem analisados"[213].

A crescente vigilância pode ter consequências muito concretas para o cidadão: a divulgação de dados de saúde, preferências pessoais, hábitos e estilo de vida a uma companhia de seguros ou a um empregador pode facilmente levar à discriminação (por exemplo: contribuições de seguros mais elevados, diminuição de perspetivas de subir na carreira, até mesmo a recusa de cobertura de seguro, o despedimento, etc.), a chantagem e os problemas nas relações humanas.

---

[210] Esta questão será discutida no próximo ponto 2.7.1.

[211] "Great Britain's George Orwell warned us of the danger of this kind of information. The types of collection in the book - microphones and video cameras, TVs that watch us - are nothing compared to what we have available today." Snowden Edward. (2013, dezembro 25). Alternative Christmas Message 2013. *Channel 4* . Disponível em: http://www.channel4.com/programmes/alternative-christmas-message consultado a 28 de dezembro de 2013.

[212] Tradução nossa. *Idem*: "We have sensors in our pockets that track us everywhere we go".

[213] Tradução nossa. *Idem*: "A child born today will grow up with no conception of privacy at all. They'll never know what it means to have a private moment to themselves, an unrecorded, unanalyzed thought."

2.2. Criação de perfis

A criação de perfis nos AmI consiste na recolha constante e no processamento de uma ampla gama de dados de várias fontes que estão relacionados com a identidade do utilizador, com as suas atividades, caraterísticas e preferências em ambientes específicos.

Com base em perfis construídos, os sistemas de AmI são capazes de responder às necessidades do utilizador – ou, pelo menos, o que é assumido como serem necessidades inferidas a partir de interpretação da informação recolhida[214]. Esta técnica pode ser aplicada a um indivíduo, a um ou vários grupos de pessoas, bem como aos animais, aos objetos e às relações existentes entre todos eles. Tal atividade de criação de perfis produz, portanto, um determinado tipo de conhecimento, por meio do processo supra referido, como a descoberta de conhecimento útil em bases de dados.

A descoberta de informação em bases de dados pretende processar automaticamente grandes quantidades de informações para extrair um conhecimento útil a partir deles, permitindo ao seu utilizador o uso desta informação valiosa para a sua conveniência.

Porém, o conhecimento produzido não representa necessariamente o estado atual das coisas, uma vez que os perfis são padrões probabilísticos resultantes de um processamento de dados[215]. Levado para um nível mais abstrato, através de recurso à mineração de dados é possível definir determinados padrões a partir dos dados do passado que podem servir para criar o conhecimento probabilístico sobre indivíduos, grupos de humanos e não-humanos no presente e no futuro. Desta forma, o perfil é, em si, um tipo de produção de conhecimento: ele tende a criar a "realidade" através de inferências realizadas a partir de acontecimentos passados.

Uma questão ligada a esta técnica é o facto de que ela pode levar à dissociação entre os factos representados pela informação armazenada e o contexto no qual estes se encontram e dentro do qual assumem seu significado próprio. Deste modo, dificilmente se poderá denominar um perfil desta natureza como um perfil representativo das preferências de uma pessoa.

---

[214] Wright D., *et al.* (2008), *op. cit.* pp. 148- 152.

[215] Poullet, Y. (2010). About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In Serge Gutwirth, Yves Poullet, Paul De Hert (Eds.), *Data Protection in a Profiled World* (pp. 3-30). Paises Baixos: Springer, p. 31.

A qualidade de um perfil pessoal depende tanto do âmbito e da qualidade dos dados de entrada, bem como do adequado processamento dos mesmos. No entanto, os perfis desenvolvidos a partir de dados recolhidos representam - na melhor das hipóteses – apenas meras aproximações das preferências reais do utilizador. As informações recolhidas por sensores dos sistemas de AmI são baseadas principalmente na observação do comportamento. Além disso, se as preferências individuais relativamente a uma aplicação específica ou situação tendem a mudar com frequência e de forma dinâmica, neste caso, a oportunidade de criação de um perfil é significativamente reduzida. A criação de perfis pode igualmente apresentar ameaças à confiança, pois leva a erros de interpretação em relação às necessidades dos utilizadores. Assim, o perfil pode apenas capturar um extrato simplificado de uma realidade complexa.

O perfil inadequado poderá obrigar o utilizador a tentar encaixar-se num determinado perfil. Por exemplo, se as companhias de seguros podem aplicar prémios de seguro mais altos sobre os utilizadores cujo estilo de vida é considerado "inseguro" (por exemplo, determinado consumo de alimentos, comportamento de condução ou atividade recreativa que não se encaixam em padrões de comportamento dito ”normal”), os utilizadores ficam com a opção de pagar mais ou mudar o seu comportamento de acordo com os desejos de companhias de seguros[216].

Na criação de perfil estão em causa não apenas a privacidade do consumidor, mas também a sua própria autonomia na tomada de decisão e a liberdade de escolha, valendo aqui um relance ao que Yves Poullet carateriza como sendo as duas faces da privacidade moderna. Por um lado, a proteção da intimidade e, por outro, a garantia da autodeterminação e da própria liberdade dos consumidores[217]. A criação de perfis de utilizador pode apresentar ameaças à identidade porque as escolhas, apresentadas pelos sistemas de AmI, forçam as pessoas a comportar-se de uma maneira que elas não teriam escolhido sem intervenção desses sistemas. Deste modo, as pessoas sentem-se obrigadas a aceitar o curso apresentado pelo AmI[218].

Os dados fornecidos pelo próprio utilizador, dados obtidos a partir de análise de hábitos de navegação ou mesmo a partir de terceiros, podem conduzir à limitação da diversidade e do

---

[216] Wright D., *et al.* (2008), *op. cit.,* p. 163.

[217] Poullet, Y. (2009). Data protection legislation: What is at stake for our society and democracy?. *Compute Law & Escurita Review*, *25* (3), 211-226, pp. 214-215. Disponível em: http://users.ecs.soton.ac.uk/pw6g08/notes/info2009/resource4.pdf consultado a 8 de dezembro de 2012.

[218] Wright D., *et al.* (2008), *op. cit.,* p. 148.

rol de escolhas futuras de uma determinada pessoa a partir de um perfil que lhe foi atribuído com base no seu comportamento passado[219].

Em nome de segurança pública, os cidadãos muitas vezes são convidados a fornecer informação pessoal como um pré-requisito para aceder a um determinado serviço: são as autoridades de segurança públicas que estabelecem determinados requisitos, enquanto que as empresas privadas e outras entidades (por exemplo, serviços de transporte e aeroportos) são obrigadas a implementá-los. No entanto, em casos de recusa de serviço, os fundamentos em que essa mesma decisão se baseou não são sempre claros e transparentes. Outras razões para a recusa dos serviços podem decorrer da interoperabilidade inadequada dos sistemas de informação ou, no caso de pessoas de regiões menos desenvolvidas, devido à própria inexistência de dados de perfis pessoais.

Acresce ainda que a criação de perfis, bem como os perfis incompletos e/ou as informações descontextualizadas podem gerar represálias[220]. Uma pessoa inocente poderá erroneamente ser identificada como um criminoso ou como uma potencial ameaça à segurança ou mesmo como um terrorista[221]. A probabilidade de erros e a suspeita infundada podem aumentar caso as necessidades da segurança e os direitos da privacidade não sejam equilibrados de forma adequada[222].

O artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) é fundamental para preservar a privacidade e a proteção dos dados pessoais face às novas tecnologias de vigilância e monitorização, determinando no seu n.º 2 que as restrições à privacidade devem estar expressamente previstas na lei, mas também devem ser necessárias numa sociedade democrática[223].

---

[219] *Idem*, p.162.

[220] *Idem,* p. 165.

[221] Como acontece com um dos heróis do livro do Pepetela. (2007). *O Terrorista de Berkeley, Califórnia.* Lisboa: Dom Quixote de Portugal. Trata-se de uma sátira à paranoia do terrorismo que surgiu nos Estados Unidos, após o atentado terrorista de 11 de setembro de 2001 e trata das atitudes catuais sobre terrorismo e também de aspetos da tecnologia presente na sociedade moderna.

[222] *Vide* mais sobre as restrições ao direito à privacidade no ponto 2.7.1.

[223] Artigo 8.º, n.º2 da CEDH:" Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."

Ademais, tanto o Tribunal Europeu dos Direitos do Homem (TEDH), como o Tribunal de Justiça da União Europeia (TJUE) têm afirmado repetidamente que a aplicação e a interpretação do artigo 8.º da CEDH e do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia exigem a conciliação com outros direitos[224].

Questão interessante relativa ao armazenamento de dados sensíveis colocou-se no caso S. e Marper contra Reino Unido, de 4 de dezembro de 2008[225] e julgado pelo Tribunal Europeu dos Direitos do Homem (TEDH), sendo o seu acórdão considerado pela doutrina como revolucionário na jurisprudência do Tribunal. Em traços muito gerais, na sequência da suspeita de prática de tentativa de roubo, foram retiradas impressões digitais e ADN a Marper e a S. (na altura era menor). Ambos foram absolvidos e solicitaram que fossem destruídos aqueles dados sensíveis, o que foi recusado em várias ocasiões e por várias entidades após recursos. O governo britânico alegou a necessidade de preservação dos dados biométricos recolhidos por razões de prevenção e deteção e, em particular, na luta contra o terrorismo, permitindo a identificação das pessoas de uma forma antes impossível, tendo por base legal *"Police and Criminal Evidence Act"* de 1984[226].

O TEDH reconheceu que havia uma violação do direito à privacidade previsto no artigo 8.º, n.º1º da CEDH e decidiu que a manutenção de amostras celulares e perfis de ADN, sem limite temporal (indefinidamente) ou independentemente do tipo de facto praticado, pela informação que continham sobre o visado e os seus familiares, e pelo risco de estigma

---

[224] *Vide* Acórdão do Tribunal Europeu dos Direitos do Homem de 7 de fevereiro de 2012, *Von Hannover contra Alemanha (n.º 2)*, pedidos n.ºs 40660/08 e 60641/08. Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109029#{"itemid":["001-109029"]} consultado a 6 de dezembro de 2013; Acórdão do Tribunal de Justiça da União Europeia de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, n.º 48. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d54572c3c048834df2957684a99bb943cf.e34KaxiLc3eQc40LaxqMbN4ObhaKe0?text=&docid=115205&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=48954 consultado a 6 de dezembro de 2013; Acórdão do Tribunal de Justiça da União Europeia de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, n.º 68. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=49163 consultado a 6 de dezembro de 2013.

[225] Acórdão do Tribunal Europeu dos Direitos do Homem de 4 de dezembro de 2008, *S. e Marper contra Reino Unido* (pedidos n.ºs 30562/04 e 30566/04. ECHR 1581 (4 de dezembro de 2008). Disponível em: http://www.bailii.org/cgi-bin/markup.cgi?doc=/eu/cases/ECHR/2008/1581.html&query=title+ (+marper+) &method=boolean consultado a 28 de março de 2014.

[226] *Police and Criminal Evidence Act.* (1984). Disponível em: http://www.legislation.gov.uk/ukpga/1984/60/contents consultado a 25 de março de 2014.

contendia com a previsão do artigo 8.º da CEDH de respeitar o direito à vida privada seria injustificada face à absolvição e não tratava o visado como inocente.

O Tribunal analisou se esta violação da privacidade podia enquadrar-se na limitação prevista no n.º2 do artigo 8.º da CEDH, sendo necessário para o efeito a satisfação dos três requisitos: a restrição ao direito da privacidade deve estar prevista na lei, para um fim legítimo e necessário numa sociedade democrática. Segundo o TEDH os dois requisitos - a base legal e o fim legítimo que consistia em prevenção de crimes - estavam satisfeitos. A terceira condição, a necessidade numa sociedade democrática, não estava satisfeita. O Tribunal reconheceu a utilidade das bases de dados para finalidades de deteção de crimes, mas referiu o perigo da estigmatização derivado de certos procedimentos de segurança, existindo risco de criar a categoria do "perpétuo suspeito".

O Tribunal considerou que a manutenção e a inserção na base de dados da polícia manteria a suspeita acerca da prática dos factos, já que o visado, não obstante ter sido absolvido, estaria a ser tratado como criminoso, o que seria discriminatório, não respeitaria a sua vida privada e não seria necessário numa sociedade democrática. As conclusões do Tribunal assumem importância particular na avaliação das novas medidas tecnológicas de segurança, nomeadamente nos cenários dos ambientes inteligentes em que pode existir o armazenamento ilimitado de dados sensíveis e criação de perfis.

Contudo, não somente os motivos de segurança pública, mas também as considerações do lucro e do mercado podem levar à violação do direito à privacidade. Por exemplo, os clientes podem ser coagidos a fornecer os seus dados pessoais sensíveis, caso desejem desfrutar de certos privilégios ou serviços (prémios de seguros especiais e descontos). Quanto mais sofisticados forem os serviços oferecidos, maior é a quantidade de dados pessoais que é deixada pelo indivíduo nas mãos do provedor do serviço, e tal informação poderá servir para a criação de perfis individuais e coletivos de utilizadores. Além disso, quanto mais extensa for a rede dos serviços, maiores as possibilidades de interconexão entre os bancos de dados e a disseminação da informação recolhida.

Na sociedade atual a tutela dos dados pessoais está sujeita, por um lado, à pressão do Estado para aumentar a quantidade e a qualidade de informações sobre os cidadãos sob pretexto da garantia da segurança e da saúde públicas e, por outro lado, à pressão do mercado,

tendo em vista a comercialização de dados pessoais de consumidores devido ao valor económico que eles representam[227]. Deste modo, numa sociedade pronta a renunciar aos seus direitos, neste caso o direito à privacidade, em nome da Segurança e das vantagens económicas, acabam por prevalecer as razões do Estado e os interesses do mercado, enquanto que os dados pessoais passam a constituir um elemento central tanto no controlo social como na produção de riquezas.

Hoje, com a grande penetração da rede Internet conjugada com a introdução de tecnologia de AmI, é possível estabelecer o "perfil" de um consumidor a partir do seu comportamento que é justamente o conjunto de hábitos de sua navegação na Internet, conforme observa o Grupo de Trabalho do Artigo 29º de Proteção de Dados Pessoais no seu Parecer 2/2010 sobre publicidade comportamental em linha, adotado em 22 de junho de 2010: "A publicidade comportamental tem por base a observação do comportamento das pessoas ao longo do tempo, procurando estudar as caraterísticas deste comportamento através das suas ações (várias visitas ao mesmo sítio Web, interações, palavras-chave, produção de conteúdo em linha, etc.), com vista a criar um perfil específico e, deste modo, apresentar-lhes anúncios que correspondem aos interesses implícitos no seu comportamento"[228].

A recolha e a agregação de dados sobre os consumidores e a criação de seus perfis são condições preliminares para a publicidade comportamental. A partir deste perfil, o consumidor fica sujeito a uma mensagem publicitária individualmente direcionada, cujas possibilidades de se encaixar dentro de seus interesses e preferências são presumivelmente maiores.

Em especial, o Parecer[229] salienta que os fornecedores de redes de publicidade estão sujeitos ao artigo 5.º, n.º 3, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao Tratamento de Dados Pessoais e à Proteção da Privacidade no Sector das Comunicações Eletrónicas (Diretiva relativa à privacidade e às comunicações

---

[227] Kroft, Steve. (2014, 9 março). The Data Brokers Selling Your Personal Information. *CBSNEWS*. Disponível em: http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ consultado a 10 de agosto de 2014.

[228] O Grupo de Trabalho foi instituído pelo artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e de privacidade. As suas tarefas são definidas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE. *Vide* em*:* http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

[229] Grupo de Trabalho de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 2/2010 do sobre publicidade comportamental em linha,* (0909/10/PTWP171), adotado em 22 de junho de 2010, p.5. Disponível em:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf consultado a 13 de março de 2014.

eletrónicas ou Diretiva da Privacidade Eletrónica)[230], nos termos do qual a instalação de testemunhos de conexão[231] ou de dispositivos análogos no equipamento terminal de utilizadores, bem como a obtenção de informações através de tais dispositivos, depende do consentimento prévio e informado do utilizador que se traduz em qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objeto de tratamento.

O artigo 2.º, alínea h), da Diretiva 95/46/CE define consentimento 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". O artigo 7.º da Diretiva, que estabelece a base jurídica para o tratamento de dados pessoais, prevê o consentimento inequívoco como um dos fundamentos legais. O artigo 8.º requer o consentimento explícito como um fundamento legal para o tratamento de dados sensíveis. O artigo 26.º n.º 1, da Diretiva 95/46/CE, assim como várias disposições da Diretiva 2002/58/CE, requerem o consentimento para que possam ser realizadas atividades de tratamento de dados específicas no seu âmbito de aplicação.

O consentimento é um dos fundamentos legais para o tratamento de dados pessoais que confere algum controlo à pessoa em causa relativamente ao tratamento dos seus dados pessoais. O consentimento tem de ser obtido antes da recolha dos dados pessoais para que as pessoas em causa possam compreender que estão a dar o seu consentimento e qual o âmbito desse consentimento. A importância do consentimento, enquanto fator da autonomia e

[230] Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas que foi alterada pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho. Em Portugal a Diretiva foi transposta para o ordenamento jurídico através da Lei n.º 41/2004, de 18 de agosto e alterada pela Lei n.º 46/2012, de 29 de agosto por transposição da Diretiva n.º 2009/136/CE do Parlamento Europeu e do Conselho de 25 de novembro.

[231] "*Cookies"* em inglês. O conceito de testemunhos de conexão "abrange todas as tecnologias baseadas no princípio do armazenamento de informações no equipamento terminal do utilizador e do acesso às informações já armazenadas no mesmo." Grupo de Trabalho de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 2/2010 do sobre publicidade comportamental em linha*, *op.cit.*, p. 7.

autodeterminação informativa[232] da pessoa, baseia-se no seu uso no contexto certo, estando reunidos os elementos necessários[233].

Os operadores apenas podem recolher os dados pessoais de uma pessoa mediante o consentimento da mesma ou caso exista uma justificação para essa recolha. Somente nos casos em que a recolha é necessária por imperativos legais ou por requisitos contratuais (ex. para vender uma viagem aérea, uma companhia aérea têm de recolher os dados dos viajantes) é que o operador pode dispensar o consentimento da pessoa para recolher os seus dados pessoais. Todavia, tanto numa situação como noutra, o operador deve informar sempre a pessoa da finalidade para a qual está a recolher os seus dados pessoais.

O consentimento deve ser prestado antes do tratamento de dados, mas pode também ser necessário no decurso do tratamento, sempre que exista um novo objetivo. A Diretiva 2002/58/CE refere esta questão em várias das suas disposições, quer através da exigência expressa de um consentimento "prévio" (por ex., artigo 6.º n.º 3) ou através da redação das disposições (por ex., artigo 5.º n.º3)[234].

O consentimento livre traduz-se na liberdade fundamental[235]. Segundo o Grupo de Trabalho do Artigo 29.º um consentimento livre consiste em "uma decisão voluntária, tomada por uma pessoa na posse de todas as suas faculdades, sem qualquer tipo de coerção, de carácter social, financeiro, psicológico ou outro, (...) o recurso ao consentimento deve limitar-se a casos em que a pessoa em causa tenha uma liberdade de escolha genuína e possa subsequentemente retirar o consentimento sem correr riscos"[236, 237]. O titular de dados ainda tem direito de revogar o seu consentimento a qualquer momento, evitando que o tratamento dos seus dados continue. Trata-se de um direito indisponível, a que a pessoa não pode renunciar[238].

---

[232] Sobre o direito à autodeterminação informativa *vide* Castro, Catarina Sarmento e. (2005), *op. cit.,* pp. 22 a 29. *Vide* também o ponto 3.2. do presente trabalho.

[233] Grupo de Trabalho de Proteção de Dados Pessoias do Artigo 29.º, *Parecer 15/2011 sobre a definição de consentimento,* (01197/11/PT WP187), adotado em 13 julho de 2011, p.37. Disponível em: http://www.gpdp. gov.mo/uploadfile/others/wp187_pt.pdf consultado a 12 de outubro de 2014.

[234] *Idem,* p. 14.

[235] Kosta, Eleni. (2013). *Consent in European Data Protection Law.* Países Baixos: Martinus Nijhoff Publisher, p. 171.

[236] Grupo de Trabalho de Proteção de Dados Pessoias do Artigo 29.º, *Parecer 15/2011 sobre a definição de consentimento, op.cit.,* p. 15.

[237] Contudo, as vezes acontece que a aceitação ou não do testemunho de conexão pode influenciar o acesso do utilizador ao conteúdo em causa, nestas situações não há lugar a uma verdadeira escolha. *Vide* Kosta, Eleni. (2013), *op. cit.*, p. 312.

[238] *Vide* Kosta, Eleni. (2013), *op. cit.*, p. 251.

O artigo 7.º da Diretiva 95/46/CE estabelece a base jurídica para o tratamento de dados pessoais e prevê o consentimento inequívoco como um dos fundamentos legais, "o que obriga ao uso de mecanismos para obter o consentimento que não deixem qualquer dúvida de que a pessoa em causa teve a intenção de dar o seu consentimento"[239].

O requisito de um consentimento livre[240] e inequívoco tem de estar em permanente relação com os princípios reconhecidos pela lei e pela doutrina para a permissão do tratamento de dados pessoais: em primeiro lugar, um princípio geral de transparência, o que quer dizer que o responsável pelo tratamento dos dados tem que estar claramente identificado, tendo de informar claramente o titular dos dados sobre as finalidades[241] e os prazos para o tratamento e conservação dos dados ou sobre a sua comunicação a terceiros. O consentimento deve ser específico, ou seja, um consentimento genérico, que não especifique as finalidades exatas do tratamento, não satisfaz este requisito[242].

Ao basear-se no consentimento para tratar os dados pessoais, o responsável pelo tratamento não fica dispensado da obrigação de preencher os demais requisitos do quadro normativo da proteção de dados, designadamente a observância do princípio da proporcionalidade, nos termos do artigo 6.º n.º 1, alínea c) da Diretiva 95/46/CE, a segurança do tratamento, artigo 17.º, etc.[243].

A utilização de testemunhos de conexão para ser considerada legítima nos termos do art, 5.º, n.º3 da Diretiva da Privacidade Eletrónica; exige um fornecimento de informações claras e completas ao utilizador, nos termos da Diretiva 95/46/CE, (nomeadamente sobre os objetivos do tratamento) e a obtenção do consentimento do utilizador depois de lhe terem sido dadas todas aquelas informações.

O Grupo do Artigo 29.º chama igualmente a atenção para o facto de que segundo o considerando 25 da Diretiva da Privacidade Eletrónica "a configuração dos programas de

---

[239] Grupo de Trabalho de Proteção de Dados Pessoias do Artigo 29.º, *Parecer 15/2011 sobre a definição de consentimento*, *op. cit.,* p. 39.

[240] "Significa isto que não pode existir risco de fraude, intimidação ou consequências negativas importantes para a pessoa em causa se esta recusar o seu consentimento."- *Idem*, pp. 38-39.

[241] Sobre o princípio da finalidade *vide* Castro, Catarina Sarmento e. (2005), *op. cit.*, pp. 229-237.

[242] Grupo de Trabalho de Proteção de Dados Pessoias do Artigo 29.º, *Parecer 15/2011 sobre a definição de consentimento*, *op. cit.,* p. 39.

[243] *Idem*, p. 38.

navegação e os mecanismos de autoexclusão só permitirem que o consentimento seja validamente prestado num número muito restrito de casos", existindo por isso, "uma necessidade de criação de mecanismos de aceitação prévia, que exijam que as pessoas em causa pratiquem um ato voluntário, manifestando a intenção de receber testemunhos de conexão ou dispositivos análogos e a aceitação de que o seu comportamento de navegação seja posteriormente monitorizado para fins de apresentação de publicidade personalizada"[244].

Por conseguinte, para cumprir os requisitos do artigo 5.º n.º 3 da Diretiva 2002/58/CE, não se torna necessário solicitar o consentimento para cada leitura do testemunho. Contudo, para manter os utilizadores cientes dessa monitorização, os fornecedores de redes de publicidade devem estabelecer um prazo de validade para o consentimento que deverá ser facilmente revogável em qualquer momento, bem como disponibilizar aos utilizadores ferramentas visíveis, que seriam apresentadas sempre que a monitorização tivesse lugar[245].

Dada a natureza da publicidade comportamental, o cumprimento dos requisitos de transparência é requisito indispensável para que as pessoas possam autorizar a recolha e o tratamento dos seus dados pessoais e ter uma verdadeira escolha nesta matéria.

Como foi visto, as diversas técnicas destinadas à criação deste perfil fazem com que o consumidor seja caraterizado a partir de seus hábitos e comportamentos. Tendo em conta os comportamentos observados a partir de históricos de compras, produtos visualizados e outros dados pessoais disponíveis, estabelece-se uma presunção de quais seriam os seus interesses. O estabelecimento de um perfil para um determinado consumidor não é um mal em si, muito embora apresente grande potencial para se tornar um mal caso o consumidor não tenha consciência efetiva do que ocorre.

Uma outra atividade questionável resultante da criação de perfis consiste nos chamados preços dinâmicos que consistem na variação do preço a ser cobrado por um produto ou serviço, tendo em conta o perfil do consumidor, identificando os que estariam dispostos a pagar mais por

---

[244] Grupo de Trabalho de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 2/2010 do sobre publicidade comportamental em linha*, *op.cit.*, p.3.

[245] O Grupo do Artigo 29.º considera que esta prática "permitiria resolver o problema de sobrecarregar os utilizadores com inúmeros avisos, assegurando simultaneamente que o envio de testemunhos de conexão e a posterior monitorização do comportamento de navegação na Internet para fins de apresentação de publicidade personalizada apenas teria lugar com o consentimento informado das pessoas em causa". *Idem, ibidem.*

possuírem perfis demonstrativos essa inclinação[246]. Desta forma, torna-se possível discriminar consumidores a partir de critérios individuais, o que viola o princípio da igualdade dos consumidores perante o mercado e configura diretamente uma prática discriminatória. É evidente, por outro lado, que a prática de preços dinâmicos pode parecer uma pálida ameaça comparando com outras possíveis utilidades potenciais destes dados comportamentais em atividades ilícitas, como a aplicação de ataques através da Internet especialmente modelados segundo o perfil e as vulnerabilidades específicas do utilizador.

Outra possibilidade concreta de desvio da finalidade dos dados recolhidos para a elaboração de perfis de consumidores é a própria discriminação de determinados consumidores em sentido estrito. Nesta hipótese, determinados perfis poderiam levar à recusa de acesso a determinados bens ou serviços.

Uma base de dados ou perfil informatizados podem guardar um número quase ilimitado de informações. A necessidade de proteger o cidadão diante das novas técnicas informaticas baseia-se no valor económico que os dados representam, ou seja, pela possibilidade da sua comercialização. Pretende-se evitar, assim, que o cidadão seja transformado em números, sendo tratado como uma mercadoria, sem a consideração dos seus aspetos subjetivos.

2.3. Identidade

Como já foi referido anteriormente, os sistemas de AmI podem ser caraterizados, por um lado, pela sua invisibilidade, discrição e, por outro lado, pela sua sensibilidade e interatividade, e pela capacidade de resposta personalizada. Desta forma, os ambientes inteligentes, graças às suas técnicas inovadoras de criação de perfis, aos sensores embutidos e sofisticados agentes de *software,* prometem não só revolucionar a forma como as pessoas vivem e interagem, mas também afetarão e mudarão o sentido e a definição de identidade pessoal.

[246] "*Dynamic pricing"* em inglês." Profiling can present threats to privacy, because aggregated data can be used by governments and companies to support behavioural targeting and/or to implement dynamic pricing. A modern incarnation of price discrimination, dynamic pricing means that different prices are offered to customers based on their characteristics". Cf. Wright, D., *et al.* (2008), *op. cit.,* p.162.

O cenário dos AmI realizará uma série de transformações importantes no modo como a identidade de uma pessoa é capturada, representada e disseminada[247]. Essas mudanças derivam de uma série de novas caraterísticas e tendências presentes na tecnologia de AmI.

Antes de mais, no mundo dos AmI existirá uma contínua digitalização da informação pessoal, sua captura, análise, processamento e armazenamento em grandes quantidades[248]. Tal irá provocar mudanças nos processos de identificação, bem como no modo como as identidades dos indivíduos serão representadas e utilizadas. Este aumento de informação pessoal vai advir tanto dos objetos inteligentes, como das próprias pessoas[249]. Os sistemas eletrónicos, os sensores e os objetos inteligentes distribuídos e incorporados no mundo físico - através do acompanhamento constante de ações e comportamentos do utilizador -, vão gerar e produzir grandes quantidades de dados pessoais e informações sobre a identidade e o comportamento do indivíduo[250].

O aumento de informações pessoais também virá dos próprios utilizadores, uma vez que as pessoas serão capazes de criar, descrever e definir as suas identidades através de um grande número de instrumentos e plataformas. Ao mesmo tempo as tecnologias AmI vão fazer desaparecer a distinção entre mundo físico e digital[251]. As fronteiras que demarcam o território físico do digital tornar-se-ão cada vez mais difíceis de distinguir, na medida em que os espaços tendem a convergir num ambiente de computação contínuo, de avançada tecnologia da rede e com as mais variadas interfaces[252].

---

[247] Andrade, Norberto Nuno Gomes de. (2011). Future Trends in the Regulation of Personal Identity and Legal Personality in the Context of Ambient Intelligence Environments: The Right to Multiple Identities and the Rise of the Alvatars. In Sam Muller, *et al.* (Eds.), *The Law of the Future and the Future of Law*, FICHL Publication Series n.º 11, (pp. 567-585). Oslo: Torkel Opsahl Academic EPublisher, p. 572.

[248] Hildebrandt, M. (2009). Profiling and AmI. In Kai Rannenberg, Denis Royer, Andre Deuker (Eds.), *The Future of Identity in the Information Society* (pp. 273-310). Berlim: Springer, p. 274.

[249] Andrade, Norberto Nuno Gomes de. (2011), *op. cit.*, *loc.cit.*

[250] *Idem,* p. 572: "The increase of personal information will, moreover, derive from both the embedded smart objects, as well as from people themselves. In this way, electronic systems, sensors and other objects distributed throughout the physical world – via the constant monitoring of our actions and behavior – will, themselves, generate and produce massive amounts of personal data and information concerning our identity and behavior."

[251] Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 101–158, p.115.

[252] ISTAG - Information Society Technologies Advisory Group. (2005). Ambient Intelligence: From Vision to Reality. In G. Riva, *et al.* (Eds.), *Ambient Intelligence. The Evolution of Technology, Communication and Cognition Towards the Future of Human–Computer Interaction. Emerging Communication* (Vol. 6), (pp. 45-68). Amsterdão: IOS Press, p.47. Disponível em: http://www.neurovr.org/emerging/volume6.html consultado a 2 de fevereiro de 2013.

Com o gradual e inexorável desaparecimento de fronteiras entre mundos *offline* e *online* surgirá uma nova identidade que vai trazer ao mundo físico muitas das caraterísticas presentes no mundo *online*, tais como o rastreamento massivo e a criação de perfis referidos anteriormente[253].

Igualmente, este novo ambiente tecnológico irá favorecer a multiplicação de identidades.[254] Esta tendência é caraterizada pela virtualização cada vez mais crescente e pela multiplicação de distintas identidades, como, por exemplo, as identidades virtuais e parciais criadas pelas mais diversas razões e finalidades. (segurança, negócios, conveniência ou entretenimento)[255].

Ademais, os sistemas de AmI apresentarão uma capacidade mais abrangente e sofisticada de identificar, distinguir e classificar cada ser humano. Entidades públicas e privadas, por meio de tecnologias automatizadas de criação de perfis, de biometria, de tecnologias de vigilância e de localização, terão ao seu dispor um conjunto dos mais sofisticados instrumentos para identificar, rastrear e monitorizar os seus cidadãos ou os (potencias) clientes. Esse novo aparelho tecnológico irá tornar vários elementos e aspetos de uma identidade, protegidos pelo direito à identidade pessoal (como a aparência física, a voz e as caraterísticas psicológicas), mais facilmente detetáveis e, o que é pior, mais facilmente reproduzíveis no mundo dos ambientes inteligentes.

Neste sentido, e tendo em conta as tecnologias AmI, juntamente com as suas principais caraterísticas e finalidades, é perfeitamente possível imaginar uma nova geração de agentes eletrónicos programados para agir em nome do próprio utilizador. Em suma, o conceito de identidade no mundo dos AmI será essencialmente caraterizado pelas suas múltiplas facetas e omnipresença[256].

---

[253] Nabeth, Thierry. (2009). Identity of Identity. In K. Rannenberg, D. Royer, A. Deuker (Eds.), *The Future of Identity in the Information Society: Challenges and Opportunities* (pp. 19-69). Berlim, Londres: Springer, p. 23: "(...) disappearing of the frontier between the offline and the online world, the new identity that will emerge will bring in the physical world many of the characteristics presente in the online worlds, such as increased transparency and massive tracking and profiling".

[254] Fenómenos recorrentemente observados na Internet e as suas plataformas de interação e comunicação: redes sociais, mundos virtuais, *blogs* - espaços que oferecem diferentes "vidas" e "existências".

[255] Andrade, Norberto Nuno Gomes de. (2011), *op. cit.*, pp. 573-574.

[256] Nabeth, Thierry. (2009), *op. cit.*,p. 53. Mais sobre esta questão *vide* o ponto seguinte 2.3.1.

Quanto ao seu caráter omnipresente, os dados de uma identidade estarão dispersos, descentralizados e permanentemente registados. A identidade omnipresente pressupõe que os dados ou aspetos de identidade se encontram dispersos no ambiente, espalhados em objetos e interfaces inteligentes, bases de dados e na rede. A fusão entre esferas *online* e *offline*, bem como a proliferação de comunicações, de disseminação de dados pessoais do utilizador e seu armazenamento por meio de vários tipos de tecnologia, de sensores e de dispositivos, implicará certamente a omnipresença de informações sobre a identidade do utilizador[257]. Ao mesmo tempo, a identidade omnipresente[258] significa que os dados de uma identidade, por mais dispersos que sejam, também tornar-se-ão descentralizados, ou seja, a nossa identidade poderá sair do nosso controlo[259].

Com os AmI, essa tendência agravar-se-á, a nossa identidade pessoal não será apenas suscetível de ser (mal) representada por outras pessoas, mas também pela própria tecnologia e pelos agentes inteligentes autónomos. O mesmo aspeto de uma identidade (como eu sou percebido e representado por outros) não só irá abranger as perceções que outras pessoas têm sobre a nossa identidade, mas também os perfis e as representações de uma identidade construída pelos sistemas de AmI e pelos agentes de *software* (nomeadamente através dos processos automatizados de criação de perfis).

Além de mais, os aspetos de uma identidade vão se espalhar não só no mundo físico-digital dos AmI (espaço híbrido), mas também vão ser permanentemente armazenados e registados (como já acontece com a Internet). Esse caráter tendencialmente eterno das caraterísticas de uma identidade chama a nossa atenção para a necessidade de incorporar o chamado direito ao esquecimento[260] como salvaguarda para o direito à identidade pessoal. Quanto ao aspeto multifacetado da identidade, é de sublinhar que uma série de desenvolvimentos técnicos observados na Internet coloca um desafio sério à compreensão tradicional da identidade. No mundo dos AmI a conexão entre "uma pessoa - uma identidade"[261]

---

[257] Andrade, Norberto Nuno Gomes de. (2011), *op. cit.*, p. 574: "Regarding its ubiquitous character, traces of one's identity will become dispersed, decentered and permanently registered. In the first place, ubiquitous identity presupposes that traces of our identity will be dispersed in the environment, scattered throughout smart objects, intelligent interfaces, databases and networks located everywhere".

[258] Nabeth, Thierry (2009), *op. cit.*, p. 53.

[259] Andrade, Norberto Nuno Gomes de (2011), *op. cit.*, *loc. cit.:* "Secondly, ubiquitous identity will also mean that the traces of one's identity, further to being dispersed, will also become decentered, that is, outside oneself sphere of command".

[260] A questão relacionada com o direito ao esquecimento será discutida no próximo ponto 3.3.1.

deixa de existir, uma vez que a identidade será cada vez mais indeterminada, variável e fragmentada. Este fenómeno já pode ser visto hoje, através de diferentes casos e exemplos. Atualmente as pessoas criam diferentes identidades simultâneas através de suas contas de correio eletrónico, em redes sociais, em fóruns em linha, etc.. Outra situação que também ocorre com bastante frequência é quando as identidades individuais estão a ser partilhadas e geridas por várias pessoas (como é, por exemplo, o caso de uma conta de correio eletrónico de uma determinada instituição compartilhada pelos seus membros).

O sentido de identidade do utilizador no mundo dos AmI também pode estar comprometido. Se o ambiente baseado nas aplicações dos AmI assume que, com base na atividade passada e nas preferências pode prever um determinado comportamento no futuro, existe a possibilidade de ser apresentado um curso de ação que não teria sido a primeira escolha do utilizador. Pior, o utilizador pode sentir-se obrigado a aceitar a ação proposta pela aplicação AmI, e, desta forma, o seu sentido de identidade começa a deteriorar-se. Esta situação pode também ser considerada não só prejudicial para a liberdade pessoal, mas também para a própria democracia[262].

A identidade é um conceito cada vez mais complexo, multifacetado e mutável.[263] Nesta perspetiva, a ideia de uma identidade única e estável assume contornos pré-históricos, já que as pessoas tendem cada vez mais a apresentar diferentes identidades, dissociadas uma das outras e, muitas vezes, construídas a partir da profunda incongruência. Neste sentido, os indivíduos são não só diferentes uns dos outros, mas também dentro de si, sendo objeto de constantes variações. Eles têm identidades dissociadas que são construídas com base nas suas contradições internas e nas forças antagónicas. Tendo em conta esta tendência, o direito a múltiplas identidades pode ser considerado como um elemento importante do direito à identidade e como uma derivação do direito ao livre desenvolvimento da personalidade.

---

[262] "Users may even start experiencing cognitive dissonance, when they believe they want one thing but a smart object tells them they want something else." Cf. Brey, P. (2005). Freedom and Privacy in Ambient Intelligence. *Ethics and Information Technology,7* (3), 157-166, p. 162. Disponível em: http://www.utwente.nl/gw/wijsb/organization/brey/Publicaties_Brey/Brey_2006_Freedom-Privacy_AI.pdf consultado a 1 de fevereiro de 2013.

[263] Wright, D. (Ed.) (2006). *Safeguards in a World of Ambient Intelligence: Final Report*, *SWAMI Deliverable D4.* Karlsruhe: Fraunhofer Institute for Systems and Innovation Research, p.81. Disponível em: http://is.jrc.ec.europa.eu/pages/TFS/documents/SWAMID4-final.pdf consultado a 2 de fevereiro de 2013.

Como já foi visto previamente, o tradicional conceito "uma pessoa - uma identidade" tornou-se obsoleto. É importante notar que com os desenvolvimentos tecnológicos, com destaque para os ambientes inteligentes, assiste-se a uma profunda fragmentação da identidade pessoal em vários conceitos e diferentes identidades[264], parciais e virtuais, como avatares, pseudónimos, perfis, etc.. Na medida em que os indivíduos tendem cada vez mais assumir diferentes papéis ao longo da sua vida, diferentes conjuntos de caraterísticas correspondentes a diferentes finalidades são usados para representar a sua identidade[265]. Tendo em conta as considerações anteriores sobre a fragmentação e a multiplicação de identidades parece importante o reconhecimento do direito a identidades múltiplas.

O direito a identidades múltiplas permitiria criar diferentes representações de si mesmo, mantendo-as separadas uma das outras. O direito a identidades múltiplas diz respeito à necessidade de cada indivíduo ter, de acordo com o determinado contexto em que atua, as suas identidades parciais (tanto digitais como físicas) reconhecidas por lei. Este reconhecimento implicaria, além disso, que cada identidade parcial estaria sujeita apenas à identificação de acordo com os elementos específicos, impedindo que esta determinada identidade de alguma forma possa vir a ser ligada a outros elementos de identificação ou caraterísticas e, assim, a outras identidades parciais. Tal aspeto não só poderá servir aos interesses da privacidade do sujeito (mantendo os aspetos importantes da sua privada vida ocultos), mas também contribuirá para a minimização da divulgação de dados pessoais[266].

A proposta de um direito a identidades múltiplas pretende chamar a atenção para a necessidade de adaptar o atual quadro jurídico ao mundo tecnológico, onde as identidades diferentes e simultâneas podem ser facilmente criadas e utilizadas.

---

[264] Jaquet-Chiffelle, D. O., Benoist, E., Haenni, R., Wenger, F., & Zwingelberg, H. (2009). Virtual Persons and Identities. In K. Rannenberg, Denis Royer and André Deuker (Eds.), *The Future of identity in the Information Society* (pp. 75-122). Berlim: Springer, p. 76.

[265] Andrade, Norberto Nuno Gomes de. (2011), *op. cit.,* pp. 573-574.

[266] *Idem*, pp. 576-577.

2.3.1. Os ' Alvatars ' ou a nova geração de agentes inteligentes

Graças aos avanços tecnológicos no campo da miniaturização, da computação, da inteligência artificial e da comunicação sem fios, os AmI irão introduzir no quotidiano um número infinito de objetos inteligentes[267]. Como tal, qualquer tipo de material, objeto ou substância será transformado em unidades de computação, dotadas da capacidade de explorar e sentir o ambiente, interagindo e respondendo a seres humanos, bem como da capacidade de localizar e reconhecer objetos e pessoas, incluindo até mesmo o estado emocional e as intenções dos últimos[268], adaptando-se e respondendo de forma eficaz às necessidades dos utilizadores[269].

Para alcançar esse nível de personalização, Norberto Nuno Gomes de Andrade apresenta uma visão da nova geração de agentes inteligentes de *software* – Alvatars: (AI + Avatares) que representam avatares[270] dirigidos pela inteligência artificial (AI) e que operam no contexto de ambientes inteligentes[271], altamente personalizados e intuitivos, meticulosamente programados de acordo com perfil, personalidade e caráter do utilizador.

Uma das principais caraterísticas dos Alvatars, que os distingue dos "tradicionais" agentes de *software*, é o seu grau de personalização, ou seja, o volume de informação sobre o utilizador que o Alvatar será capaz de reter e processar. A computação afetiva e as tecnologias que permitem o processo de aprendizagem do agente de *software,* tornam possível o surgimento do Alvatar (réplica digital do utilizador), bem como, contrinuem para a personalização do ambiente de acordo com cada indivíduo.

Relativamente ao primeiro tipo, os Alvatars vão integrar tecnologias de aprendizagem, permitindo-lhes analisar o comportamento passado e as preferências do utilizador, a fim de prever necessidades e personalizar os serviços. Os agentes de *software* no contexto dos AmI

---

[267] Bohn J., *et al.* (2005), *op. cit.*, 5.

[268] Gaggioli, Andrea. (2005). Optimal Experience in Ambient Intelligence. In G. Riva, *et al.* (Eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction* (pp. 35-43). Amsterdão: IOS Press, p.35.

[269] ISTAG- Information Society Technologies Advisory Group. (2005), *op. cit.*, pp. 47, 67.

[270] Avatar- representação gráfica de um utilizador numa comunidade virtual. In Infopédia Porto: Porto Editora. Disponível em: www: http://www.infopedia.pt/lingua-portuguesa/avatar consultado a 5 de dezembro de 2012.

[271] Andrade, Norberto Nuno Gomes de. (2011), *op. cit.,* 577.

serão capazes, deste modo, de agir em nome do utilizador, aprendendo sobre seus hábitos, gostos e preferências[272].

Quanto à computação afetiva, trata-se de um termo inventado por Picard, que a definiu como computação que se relaciona com, surge de ou deliberadamente influencia, emoções[273]. A tecnologia de computação afetiva aplicada a agentes inteligentes permitirá aos Alvatars detetar de forma intuitiva e interpretar o estado de espírito e as emoções do utilizador e, com base nisso, tirar conclusões e tomar decisões[274]. Como tal, o reconhecimento do estado afetivo do utilizador poderá ser feito através de meios como medição de sinais fisiológicos, análise de expressões faciais, tom de voz, gestos, força com que as teclas são pressionadas, etc., bem como, por inferência do estado emocional habitual do utilizador, a partir do conhecimento de objetivos e planos do utilizador, os seus comportamentos passados, entre outros, e de uma avaliação da situação concreta em que o utilizador se encontra[275].

Desta forma, esses agentes inteligentes, incorporados no ambiente físico (relógio de pulso, roupas, casa, carro, etc.) e em sintonia com as necessidades do utilizador poderão atuar não somente de forma reativa, agindo sob o comando e instruções, mas também, e fundamentalmente, de forma pró-ativa, operando de forma autónoma, em nome do próprio utilizador[276].

Para além da capacidade de reconhecer os indivíduos e as suas particularidades, estes agentes também serão capazes de perceber o estado emocional do seu utilizador[277]. Apoiados

---

[272] *Idem,* p. 579.

[273] "I call ´affective computing`, computing that relates to, arises from or deliberately influences emotion." Cf. Picard, R. W. (1997). *Affective Computing*. Cambridge, Massachusetts: MIT Press, p. 3.

[274] Andrade, Norberto Nuno Gomes de. (2011), *op. cit., loc. cit.*

[275] Alcañiz, M., Rey, B. (2005). New Technologies for Ambient Technology. In G. Riva *et al.* (Eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction* (pp.3-15). Amsterdão: IOS Press, p. 14.

[276] Andrade, Norberto Nuno Gomes de. (2011), *op. cit., loc.cit.*

[277] Ferenstein, Gregory. (2012, 27 agosto). Brain Hacking Scientist Extract Personal Secrets With Commercial Hardware. Disponível em: http://techcrunch.com/2012/08/27/brain-hacking-scientists-extract-personal-secrets-with-commercial-hardware/ consultado a 5 de janeiro de 2014; Gholipour, Bahar. (2013, agosto 26). *Reading Minds: Brain Scans Create Pictures of What You See.* Disponível em: http://www.livescience.com/39175-brain-scans-read-letters.html consultado a 5 de janeiro de 2014; Euronews: SCI-Tech Innovation. (2012, 20 dezembro). A Machine Wich Can Read Your Mind. *Euronews*. Disponível em: http://www.euronews.com/2012/12/20/a-machine-which-can-read-your-mind/ consultado a 5 de janeiro de 2014; Eveleth, Rose. (2014, 18 julho). Neuroscience: 'I Built a Brain Decoder'. *BBC.* Disponível em: http://www.bbc.com/future/story/20140717-i-can-read-your-mind consultado a 10 de agosto de 2014.

por um exército de sensores, e atuadores dispersos por todo o meio físico, e equipados com tecnologias inteligentes de criação de perfis, máquinas de aprendizagem e de computação afetiva, os Alvatars irão capturar e processar quantidades inimagináveis de dados e informações, acabando por saber sobre o utilizador mais do que ele sobre si próprio[278].

Desta forma, o Alvatar vai emergir como uma espécie de "clone digital", em "representação do utilizador", que refletirá a sua personalidade e imitará, de forma autónoma, o próprio comportamento do utilizador num determinado contexto, de acordo com suas reais intenções e desejos.

Como consequência do conhecimento meticuloso que o Alvatar terá sobre o utilizador (personalização) e do ambiente mais amplo no qual ele funcionará (os AmI), a gama de decisões e ações disponíveis para o agente será incomensuravelmente maior. Como tal, o Alvatar terá maior espaço de manobra para agir e operar em nome do utilizador, quando comparado com os atuais agentes de *software* inteligentes. Os Alvatars irão "pensar" autonomamente e antecipar a decisão do utilizador, prevendo as suas necessidades e atuando em conformidade. Como tal, o Alvatar vai, por exemplo, sugerir o caminho que o utilizador poderá seguir, a fim de evitar o trânsito e chegar ao trabalho na hora certa, ou adiar automaticamente uma reunião, em caso do atraso do utilizador, etc..

Os exemplos referidos acima revelam que os Alvatars não serão limitados a objetivos e determinadas finalidades, apenas auxiliando o indivíduo em contextos particulares e abordando exclusivamente necessidades específicas. Como agentes extremamente personalizados, os Alvatars vão lidar com todas as necessidades e atividades possíveis relacionadas com o indivíduo. Como tal, os Alvatars vão distinguir-se dos agentes de *software* inteligentes atuais, que tendem a operar de forma ocasional e apenas em setores específicos de atividade (entretenimento, serviços bancários, compras, etc.). O agente AmI vai, para além disso, crescer com o utilizador, acompanhar o indivíduo de forma permanente, a partir de tenra idade de um indivíduo (ou possivelmente a partir do seu nascimento) até a sua morte[279]. Durante todo este conjunto educação homem/máquina, o Alvatar irá constantemente aprender sobre o utilizador

[278] Andrade, Norberto Nuno Gomes de. (2011), *op. cit.*, p. 580.

[279] *Idem*, p. 583.

(ou seja, a partir de ações, conversas, decisões e atitudes tomadas pelo indivíduo, monitorizados e gravados pelo agente), aperfeiçoando a sua réplica do perfil do utilizador.

A personalização e a criação de perfis realizada por Alvatars será contínua, difundida, mas também invisível e discreta. Todas estas caraterísticas combinadas tornam a personalização da tecnologia extremamente problemática do ponto de vista da privacidade, uma vez que os dados serão coletados e processados, não só através do fluxo de informações conscientemente aprovadas e transmitidas pelo utilizador, mas também (e fundamentalmente), através de uma quantidade enorme de informações recolhidas pelos agentes sem o consentimento e/ou o conhecimento do utilizador (por exemplo, através de biossensores, etc.).

A solução passará não pela proibição de recolha dos dados pessoais (que é indispensável para a implementação da visão dos ambientes inteligentes), mas pela confidencialidade e segurança dos dados, dando controlo sobre essa informação ao utilizador e deixando o último decidir se quer manter essa informação confidencial ou permitir que ela seja compartilhada ou divulgada.

2.4. Autonomia nos sistemas de ambientes inteligentes e perda do controlo

Uma das questões éticas fundamentais que se prende com os ambientes inteligentes é saber em que medida as pessoas vão perder ou não o controlo sobre esses sistemas. O controlo sobre a informação pessoal é o controlo sobre um aspeto da identidade que o indivíduo projeta para o mundo e o direito à privacidade permite liberdade de constrangimentos excessivos na construção da própria identidade[280].

A autonomia é fundamental para o desenvolvimento humano e é muitas vezes definida como autocontrolo, ou seja, capacidade de construir as suas próprias metas e valores, e ter a

[280] "(..) control over personal information is control over an aspect of the identity one projects to the world, and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity." Agre, P. E., & Rotenberg, M. (Eds.) (1998). *Technology and Privacy: The New Landscape*. Cambridge, MA: Mit Press, p. 3.

liberdade[281] de tomar as suas próprias decisões e realizar ações com base nessas decisões. O ideal de autonomia está fortemente relacionado com o ideal de liberdade. Como Isaiah Berlin[282] argumentou no seu famoso ensaio, a liberdade pode ser positiva e negativa. A liberdade positiva significa "ser livre para" agir, a liberdade de cada um decidir o seu futuro, a liberdade para atuar com autonomia. Por liberdade negativa entende-se o "ser livre de", é a capacidade de agir sem obstrução ou interferência de terceiros. Ambos os tipos de liberdade envolvem controlo. Liberdade positiva envolve o controlo sobre o meio ambiente; liberdade negativa envolve autocontrolo, ou controlo sobre próprios pensamentos e decisões.

Uma das principais razões para a criação e implementação dos sistemas de AmI é contribuir para gestão de processos complexos, que anteriormente tinham de ser realizados pelo utilizador. Assim, o objetivo declarado do sistema de AmI consiste em assumir uma certa carga de tarefas do utilizador – principalmente tarefas padronizadas com repetições frequentes –, com vista a aumentar o nível de segurança, conveniência e / ou eficiência. A tecnologia dos AmI permitirá ao utilizador libertar-se de tarefas de rotina tediosas e alcançar mais controlo sobre o ambiente que o rodeia, fornecendo ao utilizador informações personalizadas e detalhadas sobre o seu ambiente, que lhe permitirá interagir com ele com mais êxito[283].

Paradoxalmente, os seres humanos podem ganhar mais controlo sobre tarefas importantes, delegando outras menos relevantes para sistemas inteligentes, desde que estes dispositivos estejam programados para antecipar e responder às suas necessidades[284].

Quanto ao controlo do utilizador sobre a tecnologia, os seus níveis podem variar consideravelmente em função da aplicação[285]. Os AmI apresentam um nível de controlo elevado

---

[281] Brey, P. (2005), *op. cit.,* p. 160.

[282] Berlin, I. (1969). Two Concepts of Liberty. In Isaiah Berlin, *Four Essays on Liberty* (pp. 118-172). Oxford: Oxford University Press, pp. 124-125.

[283] "Ambient Intelligence may hence help humans gain more control over the environments with which they interact, and it may take away control as well. Let us now consider more carefully how such gains or losses in control are realized. There are at least three distinct ways in which AmI may confer control to its users. First, AmI may make the human environment more controllable by making it more responsive to voluntary action. AmI may make it easier for humans to reach particular goals or outcomes in an environment in which they operate by requiring less cognitive or physical effort from users in their use of objects in the environment." - Cf. Brey, P. (2005), *op. cit., loc.cit.*

[284] "Proponents of Ambient Intelligence claim that it will help humans gain more control over the environments with which they interact because it will become more responsive to their needs and intentions. Paradoxically, however, this control is supposed to be gained through a delegation of control to machines. In other words, control is to be gained by giving it away."- Cf. Brey, P. (2005), *op. cit.,loc.cit.*

[285] Wright D., *et al.* (2008), *op. cit.*, pp. 206-207.

quando agem em nome do próprio utilizador, por exemplo: no caso em que aplicação decide rejeitar/efetuar uma chamada telefónica ou negar transmissão de dados pessoais[286].

Os AmI demonstram um nível de controlo médio, quando se limitam a apresentar um conselho ou uma sugestão, por exemplo: para reduzir a velocidade do carro devido a uma curva na estrada. Por sua vez, os AmI têm um nível baixo de controlo quando só executam comandos do utilizador.

Na maioria dos cenários da vida moderna e em todos os cenários de um futuro próximo, os AmI terão um alto nível de controlo sobre a segurança (na forma do controlo de acesso a casas, carros, trabalho, dados de saúde, pagamentos, passaportes e do controlo de imigração) e as questões de privacidade[287].

Atualmente, as aplicações, onde a vida de uma pessoa depende dos AmI e onde os AmI apresentam um alto nível de controlo, incluem a mobilidade segura, especialmente no caso de condução (através da deteção dos obstáculos, do controlo da velocidade do carro e da garantia de que o carro permanece na estrada), a vigilância de saúde e a deteção de uma crise (como ataque cardíaco).

Ao mesmo tempo que existem indícios de que a tecnologia dos AmI poder melhorar o controlo dos utilizadores sobre o ambiente envolvente, essa mesma tecnologia apresenta um sério risco em retirar o controlo das mãos dos utilizadores. O risco da perda do controlo surge nos casos em que as máquinas decidem autónoma e descontroladamente em nome e, em princípio, no melhor interesse do utilizador[288].

Os objetos inteligentes podem realizar ações que podem não corresponder às necessidades ou intenções de seu utilizador. Tal poderá acontecer quando o AmI interfere incorretamente sobre o utilizador, sobre o seu comportamento, sobre as suas necessidades e preferências[289]. Ao mesmo tempo, a combinação da dependência da tecnologia e a falta de compreensão do seu funcionamento pode provocar stress e revolta, especialmente nos casos

---

[286] Friedewald, M., *et al.* (2006), *op. cit.*, p. 129.

[287] Wright D., *et al.* (2008), *op. cit.,* p. 207.

[288] Spiekermann, S., Pallas, F. (2006). Technology Paternalism–Wider Implications of Ubiquitous Computing. *Poiesis & Praxis*, *4* (1), 6-18, pp.8-9. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=761111 consultado a 6 de agosto de 2013.

[289] Brey, P. (2005), *op. cit.,* p. 162.

em que o sistema não funciona como é esperado[290]. O utilizador poderá sentir pressão psicológica resultante de ir contra a vontade de um objeto inteligente que supostamente deveria ter uma boa compreensão das suas necessidades e intenções[291]. Como referiu Milon Gupta: "De certa forma, é um alívio saber que todas as coisas em sua casa, incluindo o seu PC e seu sistema de aquecimento, são mudos. Eles dão-lhe a sensação de que está sempre a controlar. Este sentimento está em perigo, se frigoríficos, torradeiras, lâmpadas e pintura da parede de repente se tornarem inteligentes. A própria vantagem de ambiente inteligente poderá, paradoxalmente, reverter-se: dispositivos e aplicações, que se tornaram fisicamente discretos, podem vir a ser psicologicamente intrusivos"[292].

Outro tipo de perda de controlo ocorre quando um perfil de utilizador ou uma base de conhecimento de um objeto inteligente não representam somente as necessidades do utilizador, mas também interesses de terceiros. Isto pode acontecer, por exemplo, quando um objeto inteligente foi projetado para prosseguir certos interesses comerciais e fornecer a empresas comerciais o acesso ao perfil do utilizador[293].

A perda de controlo pode ocorrer quando objetos inteligentes são utilizados por terceiros para recolha de dados e vigilância. Assim, informações captadas sobre preferências, comportamentos, interações sociais e experiências podem ser utilizadas por terceiros para prejudicar os interesses do utilizador e exercer controlo sobre o mesmo.

É provável que no futuro o AmI representará fortemente os interesses comerciais, ao lado dos interesses do utilizador[294]. Desenvolvimento atual dos AmI é impulsionado pela ideia de que podem suportar novos modelos de negócio e funcionar como uma nova forma para as

---

[290] Wright, David (Ed.) (2006), *op. cit.,* p. 92.

[291] "This loss of control may not only be due to the additionally required effort, but also to the psychological pressure that results from going against the will of a smart object that is suppose to have a good understanding of one's needs and desires". Cf. Brey, P. (2005), *op. cit., loc.cit.*

[292] Tradução nossa. "In a way, it is quite a relief to know that all things in your home, including your PC and your heating system, are dumb. They give you the feeling that you are always in control. This feeling is in danger, if fridges, toasters, lamps, and wall paint suddenly turn smartigo The very advantage of Ambient Intelligence could become paradoxically reverted: Devices and applications, which have become physically unobtrusive, could turn out to be psychologically obtrusive". Cf. Gupta, Milon. (2002). *Walls with Ears and Brains. The Unobtrusive Intrusion of Ambient Intelligence.* Disponível em: http://archive.eurescom.eu/message/messageDec2002/A_bit_beyond.asp consultado a 3 de janeiro de 2013.

[293] "A third type of loss of control occurs when a user profile or knowledge base in a smart object does not just represent the needs of the user, but also the interests of third parties. This may happen, for example, when a smart object has either been designed to take certain commercial interests into account, or gives commercial firms access to the user profile or knowledge base. This may result in a smart object either recommending a purchase or making a silent purchase which is not based on the user's real needs but on needs that a commercial firm assigns to the user."- Cf. Brey, P. (2005), *op. cit., loc.cit.*

[294] *Idem, op. cit.,* p. 163.

empresas obterem informações sobre seus clientes, alcançá-los com publicidade direcionada e vender-lhes bens e serviços no local. AmI oferecem um grande potencial a empresas comerciais, prometendo-lhes total transparência do mercado e acesso direto aos consumidores[295].

As companhias de seguros também podem facilmente aproveitar objetos inteligentes para seu benefício. Um objeto inteligente pode, por exemplo, recusar-se a envolver-se em ações que são consideradas muito arriscadas pela seguradora, mesmo se o utilizador quiser que o objeto execute tais ações. Deste modo, essas políticas aplicadas a objetos inteligentes poderiam torná-los desleais para com os seus proprietários[296].

Em conclusão, os AmI possuem um potencial para melhorar a liberdade positiva dos utilizadores através de sua capacidade de melhorar o controlo sobre o ambiente, tornando-o mais sensível às suas necessidades e intenções. No entanto, esta tecnologia é capaz de limitar a liberdade, em ambos os sentidos: positivo e negativo. Pode limitar a liberdade positiva do utilizador em situações em que os objetos inteligentes agem autonomamente contra os seus desejos, tais ações podem ser o resultado de imperfeições da própria tecnologia ou quando a tecnologia tem em conta não apenas os interesses do utilizador mas também os dos terceiros[297].

Quando os objetos inteligentes conseguem inferir corretamente quais são as necessidades do utilizador, e informá-lo acerca disso, poderão igualmente aumentar a liberdade negativa do utilizador, melhorando a sua auto-compreensão e, assim, ajudar-lhe a tornar-se mais autónomo. Mas, como foi referido anteriormente, tais inferências sobre as necessidades do utilizador podem, muitas vezes, conter vícios e imperfeições, apresentando uma falsa imagem de quem é e do que quer, e, nesses casos, os AmI diminuirão a autonomia do utilizador se este confiar no seu julgamento, pondo em risco a sua capacidade genuína para autodeterminação individual e reflexiva.

---

[295] "AmI offers great potential for commercial firms, promising them total market transparency and direct access to consumers. It offers them very direct ways to find out about their customers and to reach them with targeted advertising and sell them new goods and services on the spot". *Idem, ibidem.*

[296] Bohn J., *et al.* (2005), *op. cit.*, p. 20

[297] Brey, P. (2005), *op. cit.,* p. 164.

2.5. Perda de confiança e falta de tansparência

Como já foi referido anteriormente, uma das caraterísticas centrais das aplicações dos AmI é a sua capacidade de operar em segundo plano, passando despercebidas ao utilizador[298]. Embora esta caraterística tenha os seus méritos, sem dúvida, em termos de usabilidade, conveniência e eficiência, pode também ter efeitos adversos quanto à confiança do utilizador e à aceitação dos serviços dos sistemas baseados nos AmI. Como os utilizadores sabem que os sistemas de AmI podem operar de forma invisível, autónoma e impercetível, podem surgir as preocupações sobre o controlo do sistema e a utilização indevida dos dados recolhidos.

A utilização dos AmI nos cuidados de saúde pode levantar dúvidas se os sistemas de acompanhamento médico e de diagnóstico são suficientemente transparentes para que um utilizador típico (geralmente idosos) possua o entendimento pleno sobre o tipo de dados que são recolhidos, onde são armazenados, para onde são transmitidos, e o que acontece posteriormente com eles.

A solução para reduzir a desconfiança consiste em disponibilizar aos utilizadores informação completa sobre os procedimentos do sistema, os seus objetivos e as suas responsabilidades[299].

Nos sistemas de AmI é importante garantir a transparência de recolha e processamento de dados em relação ao sujeito, e assegurar um equilíbrio adequado entre a informação prestada pelo sujeito e a que é retirada a partir dele. O acesso aos dados de perfis e também ao conhecimento daí derivado permitiria às pessoas uma melhor compreensão das decisões tomadas com base no seu perfil, mas também tornaria possível provar a responsabilidade em caso de dano e servir como salvaguarda contra a manipulação, contestando a lógica das decisões tomadas.

Atualmente a legislação prevê o dever de informação, mas mesmo assim é questionável se os requisitos permitem aos indivíduos compreender efetivamente o processamento dos seus dados e as suas implicações, no meio de tanta informação.

---

[298] Aarts, E., Harwig R., Schuurmans M. (2002) Ambient Intelligence. In P. Denning (Eds.), *The Invisible Future: The Seamless Integration of Technology in Everyday Life* (pp. 235- 250). Nova Iorque: McGraw-Hill, p.239.

[299] Wright, David (Ed.) (2006), *op. cit.*, p. 34.

2.6. Infoexclusão

No contexto do mundo digital, o acesso às TIC tornou-se importante e indispensável, uma vez que os indivíduos que não possuem acesso às novas tecnologias são altamente desfavorecidos ou até mesmo excluídos. No futuro próximo a tecnologia será, sem dúvida, muito mais difundida e o acesso e o uso das tecnologias dos AmI tornar-se-ão ainda mais importantes na medida em que farão realmente parte da vida quotidiana do ser humano.

Neste contexto, a exclusão digital é uma questão crucial para as sociedades e torna-se importante considerá-la: será que as tecnologias dos AmI irão contribuir para a diminuição ou incremento da exclusão digital? Especificamente, em termos de acesso físico ao equipamento e à infraestrutura dos AmI, este é suscetível de melhorar, uma vez que as aplicações dos AmI irão fazer parte do dia a dia das pessoas.

Por outro lado, haverá ainda uma percentagem da população que não terá acesso às aplicações AmI e até mesmo uma percentagem ainda maior terá acesso somente à infraestrutura básica e não aos equipamentos mais sofisticados, limitando assim o seu acesso aos benefícios dos AmI. Além disso, a habilidades e o conhecimento continuam a ser fatores limitadores[300].

Na sociedade com altos níveis da difusão de tecnologia, os indivíduos que não possuem conhecimento ou habilidades para utilizar as tecnologias dos AmI em alguma medida serão ainda mais sujeitos à exclusão. Pode-se argumentar que, embora a divisão em termos dos conhecimentos e habilidades possa diminuir no futuro, o fosso digital a existir, será muito mais grave e mais perigoso[301].

---

[300] "Apurando os valores sobre a utilização de Internet, verifica-se que 55,2% dos inquiridos utilizam a Internet, contra 44,8% que não utilizam. Entre os não utilizadores, é de salientar que 6,5% deixaram de utilizar a Internet em 2013 e 38,3% nunca utilizaram este recurso. A maioria dos utilizadores de Internet portugueses utilizam a Internet diariamente (72,9%), mas apenas 38,5% acedem através de dispositivos móveis (telemóvel, smartphone ou tablet). A utilização de Internet é feita de forma equilibrada em termos de género (51,0% de utilizadores do género masculino e 49,0% do Feminino) mas não em termos de idade (a taxa de utilização decresce drasticamente com o aumento da idade dos inquiridos) e de escolaridade (a taxa de utilização sobe drasticamente com o aumento do grau de escolaridade)." - *Vide* Cardoso, G., Mendonça, S., Lima,T., Paisana,M. e Neves.M. (2014, janeiro). *A Internet em Portugal – Sociedade em Rede 2014.* Lisboa: Publicações OberCom-Observatório da Comunicação, p. 4, 6, 7, 10. Disponível em: http://www.obercom.pt/client/?newsId=548&fileName=internet_portugal_2014.pdf consultado a 2 de setembro de 2014.

[301] Wright, David (Ed.) (2006), *op. cit.,* pp. 101-103.

Nos sistemas de AmI a existência do perfil é um pré-requisito para muitos aplicativos, proporcionará mais oportunidades para as empresas e outras organizações, no sentido atingir apenas grupos específicos, selecionando clientes mais ou menos "valiosos" e, por sua vez, discriminar e excluir um grande número de pessoas do acesso a serviços básicos e oportunidades com base nos perfis criados[302].

Deste modo, o uso indevido de dados de perfis por parte de empresas ou outras entidades pode levar à discriminação de pessoas de acordo com a raça, etnia ou nível socioeconómico, exacerbando assim a exclusão e alargando o fosso digital. A tecnologia dos AmI pode realmente ser um motor da dupla exclusão: as pessoas não são apenas excluídas da informação, mas também pela informação[303].

Os custos elevados da manutenção e da atualização das tecnologias dos AmI podem levar ao alargamento do fosso digital dentro das sociedades, onde algumas das pessoas seriam capazes de suportar os custos de manutenção, enquanto outras ficariam arredadas dessa possibilidade. Com o surgimento de novas tecnologias a dimensão global do fosso digital entre os países desenvolvidos e em vias de desenvolvimento provavelmente irá manter-se ao mesmo nível ou poderá até crescer[304]. Não obstante a crescente democratização de suportes informáticos que facultam o acesso à informação, verifica-se que determinados grupos de pessoas – por serem idosos, emigrantes, detentores de deficiência física ou mental, iletrados e ou iletrados tecnológicos, com dificuldades económicas ou em situação social marginal – são excluídos da atual sociedade digital[305].

Finalmente, as aplicações e os serviços dos AmI não serão gratuitos, e por conseguinte, nem todos os cidadãos irão desfrutar de benefícios que a tecnologias dos AmI pode oferecer - mesmo nas áreas que possuam utilidade pública (na área de saúde, educação, etc.). Não há garantias de que os serviços dos AmI farão parte dos serviços públicos para o benefício de todos.

---

[302] Kruger, D. (1998). *Access Denied?: Preventing Information Exclusion* (Vol. 18). Londres: Demos, pp. 33-34.

[303] Wright D., *et al.* (2008), *op. cit.*, pp. 153-154.

[304] *Idem,* p. 208.

[305] *Vide* Assistência Médica Internacional - AMI. *Infoexclusão.* Disponível em: http://www.ami.org.pt/default.asp?id=p1p211p215p340p364&l=1 consultado a 3 de fevereiro de 2013.

Devido à sua facilidade de utilização e ao caráter intuitivo, a tecnologia dos AmI possui potencial para suavizar alguns aspetos do atual fosso digital. No entanto, essa mesma tecnologia também pode ampliar outros aspetos da desigualdade no seu acesso.

2.7. Problemas de privacidade e proteção de dados pessoais face aos ambientes inteligentes

Em 1890, nos Estados Unidos da América, os juristas Samuel Warren e Louis Brandeis definiram no seu artigo *"The right to privacy"* o conceito de privacidade como um "direito a ser deixado em paz"[306]. O artigo marca a "passagem da *privacy property* para a *privacy personality*"[307], ou seja, do direito de propriedade[308] para um direito autónomo, ligado à personalidade, determinando o início da automatização do direito à privacidade[309].

Este novo conceito baseou-se no princípio de que a nossa casa deveria ser considerada um espaço fechado, onde nos poderíamos exprimir sem sermos observados ou examinados por terceiros. Os dados sensíveis, como as opiniões filosóficas, políticas ou religiosas, não só deveriam ser protegidos devido ao seu caráter íntimo, uma vez que apelam às liberdades constitucionais das pessoas, mas também com vista a evitar o risco de discriminação associada à sua utilização por terceiros[310]. Em resumo, tratava-se de um direito de aceção negativa[311].

A conceção negativa[312] de privacidade definida como um direito de opacidade ou de não interferência dos terceiros na vida privada de cada um tem sido progressivamente considerada

---

[306] Warren, S. D., Brandeis, L. D. (1890, dezembro). The Right to Privacy. *Harvard Law Review*, *4*(15), 193-220.

[307] Moreira, Teresa Alexandra Coelho. (2010). *A privacidade dos trabalhadores e as novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder do controlo eletrónico do empregador.* Vila Nova de Gaia: Almedina, p. 109.

[308] "O núcleo original do direito à vida privada era constituído pela relação entre os direitos da pessoa e o direito de propriedade, sendo que esta era condição necessária para aceder à intimidade. A propriedade e o contrato eram o suporte jurídico desta privacy mais ´primitiva`, sendo que a sua vulneração só podia verificar-se por meio de intrusões físicas. Assim, o direito a ser deixado só e a ter uma esfera própria era, especificamente, o de estar só dentro dos ´muros domésticos`, onde por natureza, a esfera era delimitada pela propriedade das coisas". Cf. Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* pp. 114-115.

[309] *Vide* Castro, Catarina Sarmento e. (2005), *op. cit.*, p. 17, e Marques, José A. S. Garcia e Martins, Lourenço. (2006), *op. cit.,*p. 140-141, e Moreira, Teresa Alexandra Coelho.(2010), *op. cit.,* pp. 117 e ss.

[310] Poullet, Y. (2010), *op. cit.*, p. 3-4.

[311] "Este direito goza de um duplo âmbito de poder. Por um lado, traduz-se na faculdade de impedir a tomada de conhecimento injustificado ou intrusivo e, por outro, o direito a opor-se à instrumentalização do seu conhecimento mediante a divulgação ilegítima."- Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* p. 123.

[312] Castro, Catarina Sarmento e. (2005),*op. cit.,* p. 27.

na atual Sociedade da Informação como insuficiente. Este direito à privacidade não era ainda associado ao uso das novas tecnologias de informação, nem ameaçado, como hoje, por meios de comunicação eletrónica sofisticados. Foi entendido numa conceção abrangente, enquanto direito geral de personalidade, precisamente com o objetivo de promover a proteção de dimensões variadas da personalidade humana, até então desprovidas de garantias, que deveriam ser, segundo Warren e Brandeis, protegidas da "curiosidade popular"[313].

A possibilidade de armazenar e processar grandes quantidades de dados através de computadores modificou em grande medida o equilíbrio do poder informativo por um lado, entre as entidades públicas e privadas – detentoras da "informação" - e, por outro lado, os cidadãos, que não têm acesso a essa informação[314]. Além do mais, o desequilíbrio da balança de controlo sobre a informação tem-se agravado com a opacidade de funcionamento dos sistemas de informação que rodeiam cada vez mais os cidadãos. Esta mutação da sociedade da informação[315], onde as pessoas estão quase permanentemente ligadas à rede (*"networked person"*[316] ou "*homo conectus"*[317]), exigiu novos princípios e a necessidade de uma maior proteção de dados pessoais.

O advento das tecnologias da informação[318] e o grande poder de processamento de dados pelos computadores foi responsável pelo surgimento da moderna legislação nessa área[319]. São muitas as normas internacionais e europeias que atualmente visam a proteção da reserva

---

[313] *Idem*, pp. 17-18.

[314] Poullet, Y. (2010), *op. cit.*, *loc.cit.*

[315] "O direito à privacidade, assumindo o carácter evolutivo, vai-se ampliando nos finais do século XIX e no século XX, relacionado com o desenvolvimento de novas tecnologias e com o objetivo de abranger novas realidades relacionadas com estas inovações. Já Warren e Brandeis tinham advertido que as invenções e os avanços da técnica poderiam trazer sérios riscos para as liberdades dos indivíduos, e, concretamente, para o seu âmbito mais privado. (...) Contudo, na época em que se desenvolveu esta tutela do direito à privacidade o perigo que enfrentava as pessoas não estava relacionado com a era da informática. O objetivo passava por criar um sistema que defendesse a privacidade da pessoa perante a ´incipiente e descarada atividade desenvolvida pela imprensa". Cf. Moreira, Teresa Alexandra Coelho. (2010), *op. cit.*, pp. 119-120

[316] Rodotà, S. (2009). Data Protection as a Fundamental Right. In Serge Gutwirth, *et al.* (Eds.), *Reinventing Data Protection?* (pp. 77-82). Paises Baixos: Springer, p.81.

[317] Andrade, F. (2012a). Comunicações eletrónicas e Direitos do Homem: o perigo do "homo conectus". In Mário Ferreira Monte, Paulo de Tarso Brandão (Coord.), *Direitos humanos e sua efetivação na era da transnacionalidade: debate luso-brasileiro* (pp. 207-226). Curitiba:Juruá Editora, p. 207.

[318] Entre nós, relaciona-se com a instituição do projeto do Registo Nacional de Identificação nos anos 70. *Vide* Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit., pp.* 131-133.

[319] "A tecnologia contribuiu para o surgimento de uma nova esfera privada que, embora mais rica, também se apresenta mais frágil, por estar mais exposta a terceiros, o que origina a necessidade de um reforço da proteção jurídica e de um alargamento das fronteiras do conceito de privacidade."- Moreira, Teresa Alexandra Coelho. (2010), *op. cit.*,p. 120.

da vida privada, diretamente respeitantes à proteção de dados ou informações pessoais[320]. Não se trata já, todavia, do mesmo direito, mas do direito à privacidade na sua perspetiva positiva[321]: protege-se, neste caso, um direito à autodeterminação informativa[322], regulando a proteção de dados pessoais. Em muitos contextos, este direito aparece referido ao tratamento de informações mediante o uso da informática. O direito à autodeterminação informativa, consagrado, na Constituição Portuguesa, no artigo 35.º, assuma-se como um poder de proteção do indivíduo face às agressões do Estado e de terceiros, permitindo-lhe opor-se à recolha, difusão, ou a qualquer outro modo de tratamento da sua informação pessoal[323]. Mas é também uma liberdade na medida em que constitui um poder de determinar ou controlar o uso dos seus dados pessoais[324].

Segundo Catarina Sarmento e Castro o direito à autodeterminação informativa" traduz-se num feixe de prerrogativas que pretendem garantir que cada um de nós não caminhe nu, desprovido de um manto de penumbra, numa sociedade que sabe cada vez mais acerca de cada indivíduo. É um direito a não viver num mundo com paredes de vidro, é um direito a não ser transparente, por isso, desenha-se como um direito de proteção, de sentido negativo"[325].

---

[320] O artigo 12.º da Declaração Universal dos Direitos do Homem refere-se expressamente à proteção da privacidade: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei." Em redação semelhante, o artigo 17.º do Pacto Internacional relativo aos Direitos Civis e Políticos também protege a privacidade. A mesma proteção genérica da vida privada resulta do artigo 8.º da Convenção Europeia dos Direitos do Homem (Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais) que prevê *que* "qualquer pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Ao nível comunitário são duas Diretivas respeitantes à proteção de dados pessoais: a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas que foi alterada pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho.

[321] Rouvroy, A., Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In Serge Gutwirth *et al.* (Eds.), *Reinventing Data Protection?* (pp. 45-76). Paises Baixos: Springer, p.51.

[322] "*Recht auf informationelle Selbstimmung"*em alemão. Sobre o direito à autodeterminação informativa, *vide* Castro, Catarina Sarmento e. (2005), *op. cit.*, pp. 22-29.

[323] Castro, Catarina Sarmento e. (2003, dezembro). O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro. In *VIII Congresso Ibero-Americano de Direito Constitucional*. Sevilha. Disponível em: http://www.estig.ipbeja.pt/~ac_direito/CatarinaCastro.pdf consultado a 5 de novembro de 2013, p.10.

[324] Pode ser visto enquanto direito do indivíduo de decidir " até onde vai a sombra que deseja que paire sobre as informações que lhe respeitem." *Vide* Castro, Catarina Sarmento e. (2005),*op. cit.*, p. 28.

[325] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit., loc.cit.*

Estes novos direitos digitais são hoje ameaçados por entidades públicas de segurança que, em nome da garantia do direito à liberdade e à segurança, procuram controlar cada vez mais as informações pessoais, transformando o indivíduo num ser transparente[326]. Como refere a mesma autora: "(...) hoje as ameaças à privacidade advêm também da revolução provocada pelas possibilidades abertas através do tratamento automatizado dos dados pessoais, que permite que sejamos "perseguidos" durante todo o dia, e nos transformou em "pessoas eletrónicas", encerradas num mundo de vidro (...)"[327].

Um dos principais argumentos para a implantação do sistema de AmI prende-se com a possibilidade de contextualizar e personalizar o ambiente de acordo com as presumidas necessidades ou desejos do utilizador. A fim de atingir esse objetivo, os sistemas têm de recolher e tratar grandes quantidades de dados pessoais e definir os perfis dos utilizadores. Estes dados são frequentemente recolhidos e processados sem notificação do sujeito, através de diferentes dispositivos ou técnicas, tais como testemunhos de conexão, etiquetas RFID que efetuam um rastreio silencioso e contínuo de hábitos pessoais e de comportamentos do utilizador, violando um dos seus requisitos fundamentais - a existência do consentimento do titular de dados[328].

No caso do AmI existe uma certa opacidade de funcionamento nos sistemas de vigilância emergentes que acarretam o risco de um processamento indevido e não solicitado de dados pessoais. No mundo dos AmI pode-se esperar estar sob a vigilância constante onde quer que estejamos, porque a recolha de informação pessoal é permanente, efetuada em tempo real e o seu tratamento posterior é um pré-requisito para o funcionamento da tecnologia de AmI.

Os sistemas de AmI contribuem também para o esbatimento de fronteiras entre a esfera pública e privada[329]: inserido no meio da multidão o indivíduo pode ser rastreado, enquanto que

---

[326] *Idem*, p. 26.

[327] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 19.

[328] A questão de consentimento enquanto o fundamento de tratamento de dados pessoais será abordado ao longo do presente trabalho, nomeadamente com mais detalhe no ponto 3.2.1.

[329] Beslay, L., & Hakala, H. (2007). Digital Territory: Bubbles. In Paul. T. Kidd (Ed.), *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society* (pp. 69-78). Nova Deli: Vision Book, p.74.

na sua casa pode ser monitorizado através do GPS, da RFID, dos sensores, das pulseiras com chips embutidos, da utilização da TV interativa e do seu computador com ligação à Internet[330].

O Tribunal Europeu dos Direitos do Homem introduziu a noção de "razoável expectativa de privacidade"[331], ou seja, o direito à privacidade do indivíduo não se estenderia apenas à sua casa e aos documentos, mas também a qualquer lugar (público) no qual pudesse ter razoável expectativa de privacidade (como, por exemplo, no seu ambiente de trabalho). Nesta perspetiva, questiona-se se ainda é possível uma razoável expectativa de privacidade se tudo o que indivíduo faz é constantemente monitorizado? O desenvolvimento das tecnologias de AmI e a crescente preocupação com a Segurança poderão levar à erosão da privacidade; a razoável expectativa de privacidade transformar-se-á na expectativa de estar a ser monitorizado[332].

Face à natureza invasiva dos AmI e ao facto de se basearem na recolha e no processamento de dados pessoais, torna-se pertinente defender a privacidade e o direito à autodeterminação informativa dos cidadãos, fornecendo-lhe não só proteção contra as utilizações abusivas das suas informações, como também garantias de que suas escolhas sobre a utilização de seus próprios dados serão livres e transparentes.

Como foi possível perceber ao longo do presente Capítulo, a tecnologia de AmI pode constituir um grande risco de os dados serem usados para tornar o indivíduo num objeto sob constante vigilância e monitorização, o que não é compatível com a verdadeira natureza do direito à privacidade e o direito à proteção de dados, enquanto direitos fundamentais cuja expressão se traduz na ideia universal da autonomia[333], da liberdade pessoal e da dignidade de cada ser humano, que lhe confere o direito a desenvolver a sua personalidade e ter controlo sobre os assuntos que diretamente lhe dizem respeito[334].

---

[330] De Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., & Fuster, G. G. (2009). Legal Safeguards for Privacy and Data Protection in Ambient Intelligence. *Personal and Ubiquitous Computing*, *13* (6), 435-444, p. 436. DOI 10.1007/s00779-008-0211-6.

[331] *Vide* Acórdão do Tribunal Europeu dos Direitos do Homem de 3 de abril de 2007, petição n.º 62617/00, *Copland contra Reino Unido.* Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996#{"itemid":["001-79996"]} consultado a 5 de novembro de 2013. Neste caso ficou estabelecido pelo Tribunal que a recolha, o armazenamento e a utilização de informações pessoais dos trabalhadores, tais como o uso da Internet, a correspondência eletrónica e os telefonemas, sem o conhecimento do indivíduo vigiado, contradizem o direito de privacidade tutelado pelo texto normativo do Artigo 8.º da CEDH.

[332] De Hert, P., *et al.* (2009), *op. cit.,* pp. 438-439.

[333] *Vide* Rouvroy, A., & Poullet, Y. (2009), *op. cit.,* pp. 59-6.

[334] Sobre a previsão legal dos direitos à privacidade e à proteção de dados pessoais *vide* os pontos 3.1 e 3.2 do presente trabalho respetivamente.

2.7.1. Privacidade e Segurança: a procura do equilíbrio

Os trágicos acontecimentos de 11 de setembro de 2001 têm vindo a dar relevo crescente às políticas de proteção do direito à liberdade e à segurança dos Estados, conferindo maior ênfase no combate ao terrorismo e criminalidade organizada, acompanhado do desenvolvimento e da implementação dos novos tipos de tecnologias de deteção e vigilância em massa.

O direito à liberdade e à segurança do indivíduo encontra-se expressamente previsto nos vários diplomas internacionais e nacionais: a Declaração Universal dos Direitos do Homem (artigo 3.º), a Convenção Europeia dos Direitos do Homem (artigo 5.º), a Carta dos Direitos Fundamentais da União Europeia (artigo 6.º) e no caso de Portugal, a Constituição da República Portuguesa (artigo 27.º).

Hoje em dia, o direito à segurança é considerado um direito de proteção de sentido negativo – consubstancia-se no dever dos Estados em se absterem de violar a segurança do indivíduo, mas assume cada vez mais importância num contexto de aparecimento de novas formas de terrorismo, enquanto direito positivo de proteção, impondo às autoridades públicas um dever de proteção do cidadão contra as ameaças de terceiros[335].

Neste contexto, a necessidade de combater com maior eficácia a criminalidade e terrorismo global acaba inevitavelmente por impor a adoção de medidas e mecanismos suscetíveis de pôr em risco liberdades fundamentais, *maxime*, a privacidade, limitando o direito à autodeterminação informativa dos cidadãos através da derrogação dos princípios gerais aplicáveis ao tratamento de dados pessoais[336].

A guerra desencadeada contra o terrorismo pelo mundo ocidental levou à adoção de técnicas de vigilância com recurso à mineração de dados e à criação de perfis como instrumentos da deteção e prevenção criminal, da auxiliar de investigação policial, permitindo identificar atividades suspeitas e potenciais terroristas. Aliás, hoje em dia, os próprios cidadãos, com base no medo e na pressão do terror instalados, estão mais sensibilizados para a adoção

[335] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.,* p. 22.

[336] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,*p. 179.

de mediadas protetoras cada vez mais rigorosas, acabando por fazer facilmente uma troca da sua Privacidade pela Segurança.

O armazenamento, o processamento e a troca de dados pessoais pelas agências de segurança e pelas entidades governamentais, conjugados com a técnica de mineração de dados podem pôr em risco os princípios protetores do tratamento de dados pessoais, aproveitando os dados já recolhidos para diferentes finalidades e partilhando os mesmos com outras instituições sem o consentimento dos titulares. Apesar da utilidade prática da criação destas bases de dados para finalidades de deteção de crimes e prevenção criminal, existe um perigo latente da estigmatização ou da criação da categoria do "potencial suspeito", disseminando a desconfiança e a suspeita sobre pessoas inocentes ou mesmo membros de determinados grupos sociais, culturais ou étnicos. Como exemplo pode ser apontada a situação das informações susceptíveis de serem retiradas do uso da televisão interativa pelo cidadão, funcionando como alerta para a agência de segurança no caso do visionamento sistemático de programas considerados impróprios e "perigosos" (pornografia, incitamento à violência e ao ódio, etc.)[337]. Os dados decorrentes do pagamento numa bomba de gasolina, da passagem numa autoestrada, da entrada e saída num edifício ou da utilização de um computador, mediante o uso de um sistema biométrico (impressões digitais, íris, voz, geometria da mão) podem ser utilizados para investigação e vigilância dos passos e compartamentos do cidadão e conservados para, no futuro, serem utilizados para fins de eventual investigação policial[338].

É por isso que a transparência é um requisito fundamental para que as pessoas possam exercer o controlo sobre os seus próprios dados e garantir a sua proteção efetiva. O regime legal vigente requer que os titulares dos dados sejam informados acerca da forma como a recolha e o

[337] É do conhecimento público que a agência secreta norte-americana NSA (Agência de Segurança Nacional) espia milhões de cidadãos em todo o mundo e fá-lo com a intenção de vigiar alvos potenciais e eliminar ameaças de terrorismo. A verdade é que a maior parte dos dados recolhidos pertencem a cidadãos comuns. Relatório feito pelo *Washington Post* conclui que nove em cada dez documentos e ficheiros da NSA referem-se a cidadãos comuns e não aos alvos que estavam a ser vigiados. O jornal norte-americano analisou dezenas de milhares de comunicações e documentos da agência. *E-mails*, *SMS* ou mensagens instantâneas, fotografias e documentos foram escrutinados e conclui-se que a maior parte, 90%, referem-se ou são de cidadãos que podem ou não estar ligados diretamente ao alvo estudado. Nove em cada dez contas intercetadas (89%), escreve o *Washington Post*, não cabiam dentro do âmbito da investigação da NSA. E entre o material catalogado estão histórias de amor, de relações sexuais ilícitas, conversas sobre política e religião – e tantas outras informações que foi conservada mesmo tendo a NSA considerado inútil essa informação que o *Washington Post* descreve como "surpreendentemente íntima" e de "teor voyeurista". Notícia disponível em linha: Gellman, Barton. (2014, julho 11). How 160,000 Intercepted Communications Led to Our Latest NSA Story. *Washington Post*. Disponível em http://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html consultado a 10 de agosto de 2014.

[338] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,*pp. 182-183.

processamento de dados são organizados e efetuados – artigo 10.º da Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.[339] Contudo, esses requisitos de informação dificilmente permitem oferecer ao titular dos dados uma visão esclarecedora sobre os métodos de processamento dos seus dados pessoais e das implicações daí decorrentes, uma vez que a complexa e secreta natureza dos processos de mineração de dados e de criação de perfis torna difícil ou, quase impossível, a demonstração da situação da interferência abusiva no direito à privacidade e eventuais violações da proteção de dados pessoais e, consequentemente, a possibilidade de contestar as decisões tomadas pelas autoridades com base neles[340].

Em face da intensificação das políticas europeias de combate ao terrorismo e ao crime desencadeadas pelos ataques terroristas de Nova Iorque em 2001, Madrid em 2004, e Londres em 2005, que geraram um investimento crescente nos sistemas de informação e vigilância, houve um aumento de partilha de informação, entre entidades policiais nacionais e internacionais, ou a estas disponibilizada, como no caso dos acordos sobre o fornecimento dos registos de identificação de passageiros aéreos (PNR – "*Passenger Name Record*"), celebrados com o governo dos EUA, obrigando as companhias aéreas a transmitir ao Departamento de Segurança Interna dados sobre os passageiros de voos em direção aos EUA ("*Homeland Security Department*")[341].

---

[339] Artigo 10.º: "Os Estados-membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento a que os dados se destinam; c) Outras informações, tais como: - os destinatários ou categorias de destinatários dos dados, - o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder, - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos".

[340] A respeito desta questão Catarina Sarmento e Castro fala num direito a não ficar sujeito a uma decisão individual automatizada: Castro, Catarina Sarmento e. (2005), *op. cit.,* pp. 251-253. *Vide* igualmente o ponto 3.2.1. do presente trabalho.

[341] Decisão 2007/551/PESC/JAI do Conselho da União Europeia, de 23 de julho de 2007, relativa à assinatura, em nome da União Europeia, do Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento (Acordo PNR 2007). Publicada no Jornal Oficial da União Europeia em 4 de agosto de 2007 – série L204. Este acordo de 2007 foi revogado e substituído pelo Acordo entre os Estados Unidos da América e a União Europeia aprovado pela Decisão do Conselho de 26 de abril de 2012 sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna (DSI) dos Estados Unidos, publicado no Jornal Oficial da União Europeia em 11 de agosto de 2012 - série L 215/5.

É também hoje conhecido um sistema global de interceção de comunicações privadas e económicas, funcionando na base de uma cooperação entre os Estados Unidos, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia - o *ECHELON*[342], que tem capacidade praticamente global de vigilância, uma vez que, recorrendo principalmente a estações recetoras via satélite e a satélites de espionagem, se torna possível intercetar qualquer informação via telefone, telefax, Internet ou correio eletrónico, emitida seja por quem for, de forma a aceder ao respetivo conteúdo[343].

Ao propósito do problema discutido, Catarina Sarmento e Castro refere: "Assistimos hoje ao confronto entre dois vetores fundamentais à vida humana: a segurança (e a ela associada, a transparência) e a privacidade. (...) Neste caso, trata-se de encontrar o equilíbrio entre o direito à autodeterminação informativa e o direito à segurança, o que não deixa de ser a procura da harmonia entre a liberdade individual (neste caso, essencialmente informática) e a segurança: a primeira, sem a segunda, gera o caos e a anarquia, a segunda, sem a primeira, conduzirá à construção de Estados totalitários"[344].

Como ficou demonstrado, depois dos atentados às Torres Gémeas a segurança tornou-se no problema central, criando um clima propício à legislação, onde os direitos individuais, incluindo o direito à reserva da vida privada, passaram para segundo plano. Um pouco por todo o lado, os Estados foram assumindo uma nova direção quanto ao tratamento de dados pessoais, e o que até aí poderia ser considerado como uma violação dos princípios de proteção de dados relativos, por exemplo, ao período de conservação de dados, passou a ser admitido, em nome da segurança[345].

Um claro exemplo disso foi a criação de uma legislação para a conservação de dados a nível europeu, Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de

---

[342] Mais sobre a espionagem e o Sistema ECHELON *vide* Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,*pp. 213-225.

[343] Mais detalhadamente sobre o assunto *vide* Comissão Temporária do Parlamento Europeu sobre o Sistema de Intercepção ECHELON, Relator: Gerhard Schmid, *Relatório sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON")*, (2001/2098 (INI)), de 11 de julho de 2001. Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=PT consultado a 8 de novembro de 2012.

[344] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.,* p. 24.

[345] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.*, p. 179.

comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações[346], transposta para o ordenamento jurídico português pela Lei n.º 32/2008, de 17 de julho, e que altera a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais à proteção da privacidade no setor das comunicações eletrónicas.

Nascida no contexto dos atentados terrorista de Londres em 2005, a Diretiva visa harmonizar as disposições nos Estados Membros relativas à conservação de determinados dados, impondo aos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicação a obrigação de conservação de dados de tráfego, de dados de localização e de dados conexos, com vista à investigação, deteção e repressão de crimes graves e terrorismo pelas autoridades nacionais competentes.

Para o efeito, a Diretiva obriga à adoção, pelos Estados membros, de medidas destinadas a garantir a disponibilidade, durante um período mínimo de 6 meses e máximo de 2 anos, de dados de tráfego e de localização, bem como de dados conexos necessários para identificar o utilizador de serviços de comunicações eletrónicas, tais como: dados de localização (dados que indiquem a posição geográfica do utilizador, obtidos nas redes wireless); dados de conteúdo (dados que dizem respeito ao conteúdo de uma comunicação); dados de base (dados pessoais referentes à conexão de rede, nomeadamente o número, identidade e morada do utilizador); dados de tráfego (dados informáticos ou técnicos indicando a origem da comunicação, o destino, os trajetos, a hora, a data, o tamanho, a duração e o tipo de serviço subjacente; por exemplo o endereço IP[347], o endereço do correio eletrónico)[348].

---

[346] Esta Diretiva foi transposta para o ordenamento jurídico português pela Lei n.º 32/2008 de 17 de julho, que estabeleceu a obrigação de conservação dos dados pessoais dos assinantes e/ou utilizadores pelo prazo de um ano (outros Estados Membros adotaram diferentes prazos, dentro dos limites da Diretiva).

[347] O endereço IP (*Internet Protocol* ou Protocolo de Internet), de forma genérica, é uma identificação numérica de um dispositivo (computador, impressora, etc.) em uma rede local ou pública. Cada computador na Internet possui um IP único, que é o meio em que as máquinas usam para se comunicarem na Internet. O Grupo de Trabalho de Proteção de Dados do Artigo 29.ºconsidera expressamente os endereços IP como dados pessoais no seu Parecer 4/2007 sobre o conceito de dados pessoais. Contudo, esta posição é discutível. Há situações em que os dados IP, por si só, não são de forma alguma identificáveis. Um exemplo poderia ser o endereço IP atribuído a um computador num ciber-café, onde não é exigida a identificação dos clientes. Aiás, já o próprio Considerando 24 do Relatório sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (COM (2012) 0011 – C7-0025/2012 – 2012/0011 (COD)) menciona que os endereços IP não devem ser necessariamente considerados como dados pessoais em todas as circunstâncias, afirmando que: "Ao utilizarem os serviços em linha, as pessoas singulares podem ser associadas a identificadores em linha, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como por exemplo, endereços IP (Protocolo Internet) Estes identificadores podem deixar vestígios que, em combinação com identificadores únicos e outras informações recebidas

Porém, recentemente, em resposta a dois pedidos de reenvio prejudicial, do High Court irlandês (Tribunal Supremo, Irlanda) e do Verfassungsgerichts austríaco (Tribunal Constitucional, Áustria)[349], o Tribunal de Justiça da União Europeia (TJUE) considerou que a Diretiva 2006/24/CE não respeita o princípio da proporcionalidade à luz dos artigos 7.º, 8.º e 52.º, n.º1, da Carta de Direitos Fundamentais da União Europeia, declarando a mesma inválida, uma vez que constitui uma invasão desproporcional na vida privada dos cidadãos utilizadores de meios de comunicação eletrónica, violando direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais.

O Tribunal entendeu que os dados conservados ao abrigo desta Diretiva permitem, no seu todo, retirar conclusões precisas sobre a vida privada dos titulares dos dados retidos, tal como os hábitos quotidianos, os locais permanentes ou temporários de residência, os seus movimentos diários, locais frequentados, bem como atividades desenvolvidas e relações sociais.

---

pelos servidores, podem ser utilizadas para a definição de perfis e a identificação das pessoas. Daí decorre que deve examinar-se, caso a caso e em função dos progressos tecnológicos, se números de identificação, dados de localização, identificadores em linha ou outros elementos específicos têm de ser necessariamente considerados como dados pessoais, devendo ser considerados como tal quando processados com o intuito de direcionar conteúdos específicos para um indivíduo ou de assinalar esse indivíduo por qualquer outro motivo".

A propósito da questão de endereço IP *vide* Procuradoria-Geral da República – Gabinete Cibercrime (3 de abril de 2013). *A obtenção do endereço IP - súmula da jurisprudência recente.* Nota Prática n.º 2/2013. Disponível em: http://cibercrime.pgr.pt/documentos/2013_04_03%20nota%20pratica%20-%20jurispridencia%20sobre%20I.pdf consultado a 10 de outubro de 2014, citado: "A jurisprudência tem-se pronunciado dominantemente no sentido de que o pedido de identificação do utilizador de um determinado endereço IP, num dado dia e hora, não deve ser submetido ao regime dos dados de tráfego, por se entender que este pedido não se refere a informação sobre o percurso dessa comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. Segundo a jurisprudência maioritária que o pedido, feito a um operador, sobre a identificação do seu cliente que utilizou um determinado endereço IP num determinado dia e hora, apenas pretende confirmar que uma comunicação (e apenas essa) foi efetuada por via daquele número técnico de acesso à Internet. Portanto, com esta informação, apenas se estabelece a ligação entre uma determinada comunicação, que se conhece já, e a respetiva origem. A mesma jurisprudência assume que o mesmo não acontecerá quando se pretende, numa investigação, obter informação sobre um alargado período de tempo ou sobre as múltiplas comunicações efetuadas por um suspeito: nesse caso, estar-se-á claramente já no âmbito do tráfego." Para o efeito *vide* Acórdão da Relação de Évora de 7 de dezembro de 2012 no Processo n.º 315/11.2PBPTG-A.E1. Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/6f0b16b32262478f80257abc00517327?OpenDocument; Acórdão da Relação de Lisboa de 22 de janeiro de 2013 no Processo n.º581/12.6PLSNT-A-L1-5. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument; Acórdão da Relação de Évora de 22 de dezembro de 2012 no processo 72/11.2DFTR-4.E1. Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/050470526baad26f80257ada0044b126?OpenDocument

[348] Lopes, J. M., Cabreiro, C. A. (2006). A emergência da prova digital na investigação da criminalidade informática. *Sub Júdice-Justiça e Sociedade*, *35*, 71-79, pp.74-75.

[349] *Vide* Acórdão do Tribunal de Justiça da União Europeia (Grande Secção) de 8 de abril de 2014 nos Processos Apensos C-293/12 *(Digital Rights Ireland)* e C-594/12 *(Seitlinger)*. Disponível em em:http://curia.europa.eu/juris/document/document.jsf?docid=150642&text=&doclang=PT consultado a 20 de maio de 2014.

O Tribunal de Justiça considerou que, ao impor a conservação desses dados e ao permitir o acesso às autoridades nacionais competentes, a Diretiva em questão imiscui-se de forma particularmente grave nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais.

Ademais, o facto de a conservação e posterior utilização dos dados serem efetuadas sem que o assinante ou o utilizador de serviços de comunicações eletrónicas seja informado é suscetível de provocar nas pessoas em causa a sensação de que a sua vida privada é objeto de vigilância e monitorização constantes.

O Tribunal, apesar de reconhecer a importância que o combate à criminalidade grave e ao terrorismo reveste para a garantia da segurança pública, entendeu que a vantagem conferida pelos mecanismos previstos na Diretiva no âmbito da investigação criminal deste tipo de crimes não justifica a imposição de medidas desta natureza a um âmbito tão alargado de indivíduos e sem qualquer restrição subjetiva, geográfica ou temporal. O Tribunal concluiu, assim, que a Diretiva não estabelece regras suficientemente claras e precisas quanto ao alcance da limitação dos direitos fundamentais da reserva da intimidade da vida privada e à proteção de dados pessoais consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, nem prevê garantias suficientes para assegurar a proteção efetiva dos dados pessoais conservados contra o risco de práticas abusivas ou de acesso e utilização não autorizados dos mesmos, para além de não garantir a destruição irreversível dos dados no fim do período de conservação.

Face ao exposto, o TJUE decidiu, pela invalidade da Diretiva, por violação dos direitos à reserva da intimidade da vida privada e à proteção de dados pessoais e ao princípio da proporcionalidade – servindo-se, para o efeito, das normas contidas nos artigos 7.º, 8.º e 52.º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia, em vigor desde 1 de dezembro de 2009 (artigo 6.º do Tratado da União Europeia).

Perante o que foi referido, torna-se pertinente compatibilizar a utilização das mais sofisticadas tecnologias suscetíveis de proteger eficazmente os cidadãos contra o terrorismo com respeito pelas suas liberdades individuais. O objetivo, fácil de enunciar mas de difícil concretização, consiste em encontrar um ponto de equilíbrio capaz de, por um lado, proteger melhor a segurança dos cidadãos e, por outro, de não violar as suas liberdades, *maxime*, o

direito à privacidade, sendo os dois direitos fundamentais, a que acresce a qualidade de estarem incluídos entre os direitos, liberdades e garantias[350].

Assim, a Recomendação n.º R (87) 15 do Conselho da Europa[351], que regula a utilização de dados pessoais no setor da polícia, sublinha a necessidade "de conciliar, de um lado, o interesse da sociedade na prevenção e repressão das infrações penais e na manutenção da ordem pública e, do outro lado, os interesses do indivíduo e o direito ao respeito pela sua vida privada"[352]. Segundo o referido diploma parece existir a possibilidade de reduzir as garantias sobre a proteção de dados pessoais para fins de aplicação de medidas de prevenção e repressão criminal. Importa, em concreto, ter presente o sentido e alcance de certas normas de proteção inscritas em instrumentos normativos elaborados após ponderada reflexão.

Recentemente, a União Europeia aprovou a Diretiva 2014/41/UE, relativa à Decisão Europeia de Investigação em matéria penal, publicada no Jornal Oficial no passado dia 1 de maio de 2014.

A Decisão Europeia de Investigação (DEI) é uma decisão judicial emitida ou validada por uma autoridade judiciária de um Estado-Membro («Estado de emissão») para que sejam executadas noutro Estado-Membro («Estado de execução») uma ou várias medidas de investigação específicas, tendo em vista a obtenção de elementos de prova ou para obtenção de elementos de prova que já estejam na posse das autoridades competentes do Estado de execução.

Com a aludida Diretiva é estabelecido um regime único para a obtenção de elementos de prova e são definidas regras para a execução de medidas de investigação, em todas as fases do processo penal, inclusive a fase de julgamento, se necessário com a participação da pessoa em causa com vista à recolha de provas.

---

[350] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* p. 180.

[351] Committee of Ministers, *Recommendation N.ºR (87) 15 and Explanatory Memorandum of the regulating the use of personal data in the police sector,* adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies. Disponível em: http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf consultado a 10 de outubro de 2014.

[352] *Idem*, p. 1: "Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other".

A Diretiva surge, assim, na sequência do estabelecido no Programa de Estocolmo[353], aprovado pelo Conselho Europeu de 11 de dezembro de 2009, onde se considerou que os trabalhos para a criação de um sistema global de obtenção de elementos de prova nos processos de dimensão transfronteiriça, com base no princípio do reconhecimento mútuo, deveriam ser prosseguidos.

A Diretiva 2014/41/EU no seu Considerando 40 declara expressamente que a proteção das pessoas singulares no que toca ao processamento de dados é um direito fundamental e em conformidade com o artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16.º, n.º1, do Tratado sobre o Funcionamento da União Europeia, no qual todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Tal preceito obriga os Estados-Membros a adotar, na aplicação da referida Diretiva, uma política de transparência no que diz respeito ao tratamento de dados e ao exercício dos direitos dos titulares a vias de recurso para a proteção dos seus dados pessoais (conforme o Considerando 41 da Diretiva)[354].

Assim, estabelece-se o princípio-regra de que os dados pessoais obtidos ao abrigo da Diretiva só deverão ser tratados quando necessário, e deverão ser proporcionais em relação aos fins compatíveis com a prevenção, a investigação ou com a aplicação de sanções penais e o exercício do direito à defesa. Nota-se que apenas as pessoas autorizadas deverão ter acesso às informações que contenham dados pessoais passíveis de serem obtidos através de processos de autenticação[355].

Por força do artigo 20.º da referida Diretiva, os Estados-Membros devem assegurar que os dados pessoais são protegidos e só podem ser tratados nos termos da Decisão-Quadro

---

[353] O Programa de Estocolmo estabelece as prioridades da União Europeia (UE) para o espaço de justiça, liberdade e segurança para o período de 2010 a 2014 visa dar resposta aos desafios futuros e fortalecer o espaço de justiça, liberdade e segurança com ações centradas nos interesses e nas necessidades dos cidadãos. Para mais informações consultar: Conselho Europeu, *Programa de Estocolmo - uma Europa aberta e segura que sirva e proteja os cidadãos,* ((2010/C 115/01)), Jornal Oficial C115, de 4 de maio de 2010. Disponível em: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0034_pt.htm consultado a 26 de janeiro de 2013.

[354] Considerando 41 da Diretiva 2014/41/EU: "Os Estados-Membros deverão adotar, na aplicação da presente diretiva, uma política de transparência no que diz respeito ao tratamento de dados pessoais e ao exercício dos direitos dos titulares a vias de recurso para a proteção dos seus dados pessoais".

[355] Considerando 42 da Diretiva 2014/41/EU.

2008/977/JAI do Conselho[356] (que definiu os direitos dos sujeitos no contexto da investigação criminal e outras práticas policiais, incluindo a criação de perfis: o direito de ser informado, o direito ao acesso, retificação e apagamento dos dados, atividades que devem ser dadas a conhecer aos terceiros a quem os dados tenham sido comunicados e ainda uma obrigação específica de assegurar uma alta qualidade dos dados a fim de garantir a correção dos consequentes perfis), e de acordo com os princípios consagrados na Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (Convenção 108), adotada e aberta à assinatura em Estrasburgo, a 28 de janeiro de 1981, e no seu Protocolo Adicional[357], cumprindo a exigência dos princípios gerais aplicados ao tratamento de dados pessoais- i.e., ao princípio da transparência, da qualidade dos dados (licitude; lealdade; conservação pelo tempo necessário; adequação; pertinência; proporcionalidade) e da finalidade[358].

Tendo em conta que foi dito, pode-se argumentar que, atualmente, os Estados procuram um maior controlo das atividades particulares, em nome do interesse público da segurança e do bem-estar social. O cerne do problema reside na discussão sobre até onde pode o Estado intervir na liberdade individual, mais concretamente no direito à privacidade, em benefício do interesse público, mediante um apertado controlo da sociedade.

---

[356] Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, sobre a proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (publicada no Jornal Oficial da União Europeia em 30 de dezembro de 2008, em série L 350, pp.60-71. Em 2008, a Decisão-Quadro 2008/977/JAI do Conselho, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, veio regular a matéria no espaço de liberdade, segurança e justiça. Por se restringir à cooperação entre Estados-Membros e por limitar a proteção dos dados por uma série de exceções aos princípios da limitação de finalidade e do consentimento, esta decisão foi considerada em geral insatisfatória. Atualmente, no contexto da corrente reforma do regime jurídico de proteção de dados pessoais da EU, uma proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados visa revogar a Decisão-Quadro 2008/977 e alargar o seu âmbito de aplicação às atividades de tratamento de dados realizadas pelas autoridades policiais e judiciárias a nível meramente nacional.

[357] Todos os Estados-Membros da UE ratificaram a Convenção 108. Em 1999, a Convenção foi alterada para permitir a adesão da UE. (Alterações à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (STCE n.º 108.) que permitem a adesão das Comunidades Europeias, adotadas pelo Comité de Ministros em Estrasburgo, em 15 de junho de 1999; artigo 23.º, n.º 2, da Convenção 108 na redação em vigor). Em 2001 foi adotado um protocolo adicional à Convenção 108 que estabelece disposições sobre fluxos transfronteiriços de dados para Estados não signatários, os chamados países terceiros, e sobre a criação obrigatória de autoridades nacionais de controlo de proteção de dados - Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, STCE n.º 181, 2001.

[358] Igualmente consagrados na Lei n.º67/98, de 26 de outubro e na Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

A necessidade de prevenção de futuros delitos criminais pode levar à intromissão no direito fundamental à autodeterminação informacional que, no contexto das novas tecnologias da informação e comunicação, é entendido como o direito de o titular controlar os fluxos de sua informação.

A previsão de possibilidade de terceiros poderem aceder a dados pessoais no artigo 5.°, n.º 1[359] e n.º 2 do artigo 8.° da Convenção Europeia dos Direitos do Homem[360], aponta para a natureza não absoluta do direito à reserva da vida privada, o que igualmente decorre da leitura do artigo 26.° da Constituição da República Portuguesa[361].

O artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) é fundamental para preservar a privacidade e a proteção dos dados pessoais face às novas tecnologias de vigilância e monitorização, uma vez que o seu n.º 2 determina que as restrições à privacidade devem estar expressamente previstas na lei e somente para atingir um fim legítimo e necessário numa sociedade democrática[362]. Este preceito bem interpretado e aplicado pode constituir uma ferramenta eficaz para preservar a privacidade e a proteção de dados pessoais.

O TEDH pronunciou-se através da sua jurisprudência, sobre muitas situações em que foi suscitada a questão da proteção de dados, entre as quais importa destacar questões relacionadas com a interceção de comunicações[363], diversas formas de vigilância[364] e proteção contra o armazenamento de dados pessoais pelas autoridades públicas[365]. O TEDH esclareceu que o artigo 8.º da CEDH não só obriga os Estados a absterem-se de praticar atos suscetíveis de

[359] Artigo 5.°, n.°1 da CEDH: "Toda a pessoa tem direito à liberdade e segurança (...)".

[360] A CEDH foi adotada pela República Portuguesa através da Lei n.º 65/78, de 13 de outubro. O seu artigo 8.°, n.°1 dispõe que " Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência."

[361] Artigo 26.°, n.°4 diz: "A privação da cidadania e as restrições à capacidade civil só podem efetuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos".

[362] Artigo 8.°, n.°2 da CEDH: "Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros".

[363] *Vide*, por exemplo, TEDH, acórdão *Copland c. Reino Unido*, *op.cit.*

[364] *Vide*, por exemplo, Acórdão do Tribunal Europeu dos Direitos do Homem de 2 de setembro de 2010, petição n.º 35623/05, *Uzun contra Alemanha.* Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-100293#{"itemid":["001-100293"]} consultado a 5 de novembro de 2013.

[365] Foi o que se revelou no caso *S. e Marper contra Reino Unido* supra discutido no ponto 2.2.

violar este direito consagrado na Convenção como impõe também, em certos casos, uma obrigação positiva de assegurar ativamente o respeito efetivo pela vida privada e familiar[366].

A própria Constituição da República Portuguesa prevê que os direitos fundamentais enquanto direitos subjetivos, segundo artigo 18.º da CRP, beneficiam de aplicabilidade imediata e vinculação geral (artigo 18.º, n.º 1 da CRP), apenas podendo ser restringidos nos casos expressamente previstos na Constituição e somente na medida em que tal se torne indispensável à salvaguarda de outros direitos liberdades e garantias constitucionalmente protegidos (artigo 18.º, n.º2 da CRP) sem que seja aniquilado o conteúdo essencial do respetivo direito atingindo (artigo 18.º, n.º3 CRP).

O número 2.º, primeira parte do artigo 18.º da CRP, diz que: "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição (...) ". As normas constitucionais consagradoras de direitos, liberdades e garantias não estão dependentes de nenhuma lei concretizadora, o que explica o sentido da imposição constitucional da sua aplicabilidade direta.

Segundo Gomes Canotilho e Vital Moreira "aplicabilidade direta transporta, em regra, direitos subjetivos, o que permite (...) invocar as normas consagradoras de direitos, liberdades e garantias na ausência de lei (...) e a invalidade dos atos normativos que, de forma direta, ou mediante interpretação infrinjam os preceitos consagradores de direitos, liberdades e garantias, impondo-se, assim, na solução dos casos concretos, contra a lei e em vez da lei, ou contra determinada interpretação da lei"[367].

Assim, as necessidades de prevenção de delitos criminais e garantia de segurança pública são, também fundamentais à realização da autonomia, liberdade e dignidade da pessoa humana e podem em casos previstos da lei justificar a limitação do direito à intimidade da vida privada.

---

[366] *Vide*, por exemplo, Acórdão do Tribunal Europeu dos Direitos do Homem de 17 de julho de 2008, petição n.º 20511/03, *I. contra Finlândia.* Disponível em http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87510#{"itemid":["001-87510"]} consultado a 5 de novembro de 2013; Acórdão do Tribunal Europeu dos Direitos do Homem de 2 de dezembro de 2008, petição n.º 2872/02, *K.U. contra Finlândia.* Disponível em http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]} consultado a 5 de novembro de 2013.

[367] Canotilho, José Joaquim Gomes, Moreira, Vital. (2007). *Constituição da República Portuguesa Anotada* (4ª ed. Revista), Volume 1º, Artigos 1º a 107º. Coimbra: Coimbra Editora, p. 283.

A reserva da privacidade deve ser considerada a regra e não a exceção, atendendo à própria natureza do direito à privacidade como direito de personalidade e, por outro lado, à sua consagração constitucional como direito fundamental[368].

O direito à privacidade só pode ser licitamente limitado quando um interesse público superior o exija, em termos e com intensidade tais que o contrário possa provocar prejuízos gravíssimos para a comunidade.

De acordo com Pedro Pais Vasconcelos "a ofensa é lícita quando os interesses públicos em jogo sejam de tal modo ponderosos e a necessidade da ofensa seja de tal modo imperiosa que o exercício do direito à privacidade se torne abusivo, quando exceda manifestamente os limites impostos pela boa-fé, pelos bons costumes ou pelo fim social ou económico desse direito"[369].

A estas exceções aplica-se o regime das restrições aos direitos, liberdades e garantias do artigo 18.º da CRP. Do referido preceito constitucional deriva a ideia de que todo o direito fundamental apenas pode ser limitado nas situações expressamente admitidas pela Constituição, a eventual restrição deve ser adequada e justificada pela necessidade de promover ou salvaguardar outro direito ou interesse constitucionalmente valioso (artigo 18.º, n.º 2) e só na proporção dessa necessidade, com recurso a medidas que envolvem um menor sacrifício para o direito fundamental conflituante e sem que seja aniquilado o conteúdo essencial do respetivo direito atingindo[370].

De acordo com José Vieira de Andrade, "a Constituição portuguesa refere-se expressamente no n.º2 do artigo 18.º à necessidade da restrição, referência que deve ser entendida como consagração do princípio da proporcionalidade em sentido amplo, incluindo a proibição de restrições inadequadas, desnecessárias ou desproporcionais dos direitos, liberdades e garantias, independentemente de tais restrições afetarem o conteúdo essencial (absoluto) dos preceitos constitucionais"[371].

---

[368] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* p. 250.

[369] *Idem*, p. 251.

[370] Andrade, José Carlos Vieira de. (2012). *Os Direitos Fundamentais na Constituição Portuguesa de 1976.* (5ª ed.). Coimbra: Almedina, p. 287.

[371] *Idem*, p. 284.

Em geral, a CRP estabelece um conjunto importante de requisitos de validade das leis restritivas de direitos, liberdades e garantias: têm de revestir caráter geral e abstrato, não podem ter efeitos retroativos, as restrições têm de limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos, não podendo em caso algum diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais (artigo 18.º, n.ºs 2 e 3)[372].

Nos termos do artigo 18.º, n.º 3, a lei restritiva tem de ser geral e abstrata, isto é, deve ser aplicável a todas as pessoas ou a toda uma categoria de pessoas e deve ser suscetível de aplicação a um número indeterminável de casos[373]. De acordo com José Vieira de Andrade, "definição teórica de generalidade e abstração, deve entender-se que, no domínio dos direitos fundamentais, este imperativo se refere em primeira linha ao princípio de igualdade, enquanto manifestação do caráter universal dos direitos fundamentais e proibição de privilégios e de discriminação e segregações arbitrárias ou injustificadas"[374].

A doutrina consagrada no artigo 18.º, n.º 2 da CRP[375] estabelece critérios rigorosos para que, em caso de conflito de direitos ou valores da mesma matriz (como no caso do direito à segurança e do direito à privacidade), a limitação legítima de um direito fundamental possa ocorrer, impondo ao legislador o respeito pelo princípio da proporcionalidade e a realização de uma ponderação concreta dos valores conflituantes, a fim de encontrar justo equilíbrio entre os vários bens constitucionalmente protegidos e para que a referida restrição possa trazer mais benefícios para o interesse da comunidade do que os sacrifícios que são impostos ao titular do direito atingido[376].

Neste sentido, José Vieira de Andrade acrescenta que, "a dignidade do homem livre constitui para nós a base dos direitos fundamentais e o princípio da sua unidade material. Se a existência de outros princípios ou valores (inegável numa constituição particularmente marcada por precauções de caráter social) justifica que os direitos possam ser restringidos (ou os limita logo no plano constitucional), a ideia do homem como ser digno e livre, que está na base dos

[372] *Idem*, p. 282.

[373] *Idem*, p. 289.

[374] *Idem, ibidem.*

[375] Artigo 18.º, n.º 2 da CRP: "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos".

[376] Andrade, José Carlos Vieira de. (2012), *op. cit.,* p. 286

direitos e que constitui, muito especialmente, a essência dos direitos, liberdade e garantias, tem de ser vista como um limite absoluto a esse poder de restrição"[377].

A interpretação dos preceitos constitucionais que autorizem a restrição legislativa dos direitos fundamentais deve ser feita de harmonia com a Declaração Universal dos Direitos do Homem, nos termos do n.º 2 do artigo 16.º da Constituição da República Portuguesa[378]. A Declaração Universal dos Direitos do Homem no seu artigo 29.º permite genericamente que o legislador estabeleça limites aos direitos fundamentais para garantir o reconhecimento ou o respeito dos valores aí enunciados: «direitos e liberdades de outrem», «justas exigências da moral, da ordem pública e do bem-estar geral numa sociedade democrática»[379].

Igualmente no artigo 5º, alínea d) da LPDP, na ausência de consentimento do titular dos dados pessoais, o seu tratamento só será legalmente admissível se for indispensável para "prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados."

Mais adiante, o mesmo diploma, no artigo 8.º, n.º 3 enuncia que, "o tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infração determinada, para o exercício de competências previstas no respetivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que Portugal seja parte."

Como todos os direitos fundamentais, o direito à segurança e à intimidade da vida privada não são ilimitados nem absolutos. Mas não se pode resolver o seu conflito com recurso a uma hierarquia de direitos, o que ia levar ao completo aniquilamento de um deles[380]. Isto é, não se pode defender uma hierarquização de direitos que pudesse determinar a exclusão de um direito à privacidade, em favor de um direito à segurança[381].

---

[377] *Idem,* pp. 284-285.

[378] Artigo 16.ºn.º2 da CRP: 'Os preceitos constitucionais e legais relativos aos direitos fundamentais devem ser interpretados e integrados de harmonia com a Declaração Universal dos Direitos do Homem."

[379] Andrade, José Carlos Vieira de. (2012), *op. cit.*, p. 279.

[380] *Idem,* p. 300.

[381] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.,* pp. 25-26.

É possível admitir que o Estado possa aplicar restrições à vida particular, desde que legítimas, com o respeito por princípios fundamentais em matéria de proteção de dados e, sobretudo, na observância dos princípios da proporcionalidade e razoabilidade na sua tríplice dimensão, princípio da adequação, da necessidade e da proporcionalidade *strictu sensu*, sendo a hermenêutica jurídica constitucional um instrumento adequado para resolver o conflito entre liberdade particular e interesse público.

As soluções tecnológicas também podem auxiliar no combate ao terrorismo e criminalidade organizada. O nível técnico dos sistemas de vigilância deve permitir que eles próprios possam ser controlados e fiscalizados, assegurando a sua transparência e integridade dos seus procedimentos quanto ao tratamento de dados pessoais.

Relativamente à partilha de informações detidas pelos serviços policiais dos Estados, assume particular importância que esta ocorra apenas entre autoridades policiais, e não entre quaisquer outras com vista a evitar os reaproveitamentos de dados e o seu tratamento para finalidades distintas da finalidade que esteve na origem da sua recolha. Devem ser tidos cuidados acrescidos com uma das principais ameaças do tratamento automatizado de dados pessoais: a sua inexatidão.

O uso de dados pessoais para fins policiais apenas deverá ter lugar de forma pontual, quando esteja em causa prevenir um perigo concreto ou reprimir uma infração penal determinada, devendo limitar-se aos dados estritamente necessários, cumprindo o princípio do mínimo de intromissão que requer a exaustão das técnicas menos intrusivas antes do recurso a outras[382].

São estes alguns dos princípios fundamentais cujo respeito parece hoje depender a justa medida em matéria de tratamento de informações pessoais para garantia do direito à segurança. Em suma, um leque de salvaguardas legais precisa de ser trabalhado com as melhores práticas internacionais para ajudar os Estados a avaliar a necessidade, proporcionalidade e a razoabilidade das medidas de segurança, bem como criar normas claras para garantir transparência e controlo público das condições da realização de tratamentos de dados pessoais por mecanismos de vigilância[383].

---

[382] *Idem*, *ibidem*.

[383] *Idem, ibidem.*

2.8. Considerações

No presente Capítulo foram abordadas de forma multidisciplinar as ameaças emergentes da tecnologia de AmI referentes à privacidade e à proteção dos dados pessoais. Após uma breve consideração da evolução doutrinária do conceito legal de privacidade foi possível inferir que o paradigma de ambientes inteligentes introduz novos desafios e obriga a repensar questões relacionadas com a segurança, a autonomia, a identidade e a autodeterminação da pessoa humana.Os sistemas de AmI apresentarão uma capacidade mais abrangente e sofisticada de identificar, distinguir e classificar cada ser humano. Graças às suas técnicas inovadoras de criação de perfis, sensores embutidos e sofisticados agentes de *software,* os ambientes inteligentes prometem não só revolucionar o estilo de vida das pessoas e de interagir na sociedade, mas também vão afetar e mudar o sentido e a definição de identidade pessoal.

Por outro lado, o facto de os sistemas de AmI poderem operar de forma invisível, autónoma e impercetível, pode levantar preocupações sobre o controlo do sistema, a perda de confiança do indivíduo no ambiente tecnológico e a um processamento indevido e não solicitado de dados pessoas.

Entidades públicas e privadas, por meio de tecnologias automatizadas de criação de perfis, de biometria, de tecnologias de vigilância e de localização, terão ao seu dispor um conjunto de instrumentos sofisticados para identificar, rastrear e monitorizar os seus cidadãos ou os (potencias) clientes, o que, por sua vez, poderá levar à discriminação de pessoas de acordo com sua raça, etnia ou nível socioeconómico, assim exacerbando a exclusão e alargando o fosso digital. Na criação de perfil está em causa não apenas privacidade do consumidor, mas também a sua própria autonomia na tomada de decisão e liberdade de escolha.

Ficou claro que os acontecimentos de 11 de setembro de 2001 levaram ao reforço das políticas de segurança dos Estados, acompanhado de desenvolvimento e implementação dos novos tipos de tecnologias de deteção e vigilância em massa, o que acaba inevitavelmente por impor a adoção de medidas e mecanismos suscetíveis de pôr em risco liberdades fundamentais,

maxime, a privacidade, limitando o direito à autodeterminação informativa dos cidadãos através da derrogação dos princípios gerais aplicáveis ao tratamento de dados pessoais.

A natureza invasiva de AmI e o facto de se basearem na recolha e processamento de dados pessoais podem efetivamente colocar em risco a privacidade do indivíduo, tornam as salvaguardas do direito à privacidade e a regulação da proteção de dados pessoais cada vez mais necessárias. Deste modo, torna-se pertinente responder à questão de como é que se pode salvaguardar os direitos fundamentais, nomeadamente os direitos à privacidade e à proteção de dados, face aos ambientes inteligentes, bem como avaliar a relevância, aplicabilidade e adequação do quadro legal da proteção de dados pessoais vigente na União Europeia e ao nível nacional no contexto desta nova realidade tecnológica.

CAPÍTULO 3 - UM QUADRO LEGAL PARA OS AMBIENTES INTELIGENTES: GARANTIAS ESPECÍFICAS PARA A PRIVACIDADE E PROTEÇÃO DE DADOS

3.1. Direito à privacidade enquanto um Direito Fundamental: artigo 8.º da Convenção Europeia dos Direitos do Homem

Dentro do sistema jurídico ocidental, a privacidade é protegida principalmente por disposições explícitas, tanto em tratados internacionais de direitos humanos, como nas constituições.

A primeira disposição de mencionar ao nível do Direito Internacional é o artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) que, apesar de não dar uma definição clara de privacidade, destaca o respeito pela vida privada, na ordem europeia de direitos humanos[384].

O artigo 8 º da CEDH (Direito ao respeito pela vida privada e familiar) declara:

"1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

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

Esta disposição é a fonte para a legislação da União Europeia relativa à privacidade e à proteção dos dados pessoais, bem como para a legislação nacional. De acordo com o artigo 8.º, privacidade traduz o esforço político para garantir a não-interferência em assuntos individuais e passa a proteger a privacidade do indivíduo na perspetiva do tratamento dos seus dados pessoais, consagrando, deste modo, a perspetiva positiva do direito à autodeterminação informativa[385]. Como tal, funciona como um escudo e protege a opacidade do indivíduo, sempre

[384] *Vide* Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* p.167.

[385] Neste sentido Castro, Catarina Sarmento e. (2005), *op. cit.*, p.40.

que o uso de tecnologias invasivas como as dos AmI põe em causa a privacidade e o sigilo dos dados pessoais. O mesmo artigo 8.º pode, portanto, ser invocado contra invasões de autonomia e autodeterminação informativa[386].

É ainda importante referir que o artigo 8.º da CEDH não formula a privacidade como um direito absoluto. O segundo parágrafo da disposição prevê as possíveis exceções[387]. De acordo com o n.º 2 do artigo 8.º da CEDH a restrição de privacidade deve ser imperativamente prevista por lei - ou por uma fonte legal equivalente, o que constitui critério formal. Por sua vez esta restrição pode ser aplicada somente quando for considerada necessária numa sociedade democrática (o critério de necessidade) e só pode ser aplicada para alcançar um dos objetivos específicos previstos no artigo 8.º da CEDH: segurança nacional, segurança pública, bem-estar económico do país, defesa da ordem e prevenção das infrações penais, proteção da saúde ou da moral, ou proteção dos direitos e das liberdades de terceiros (o critério de legitimidade)[388].

Finalmente, deve ser referido o artigo 12.º da Declaração Universal dos Direitos do Homem proclamada pela Assembleia Geral da ONU (Organização das Nações Unidas) a 10 de dezembro de 1948[389].

Deve ser referido o artigo 12.º da Declaração Universal dos Direitos do Homem proclamada pela Assembleia Geral da ONU a 10 de dezembro de 1948 que consagrou pela primeira vez num instrumento jurídico internacional o direito à proteção contra intromissões de terceiros, especialmente do Estado, na vida privada[390].

---

[386] Como sublinha Catarina Sarmento e Castro: "A própria jurisprudência do Tribunal Europeu dos Direitos do Homem, em pequenos passos, a partir da ideia mais geral da proteção da privacidade consagrada no artigo 8.º da Convenção Europeia dos Direitos do Homem, ajudou à construção de princípios da proteção dos dados pessoais."- Castro, Catarina Sarmento e (2005), *op. cit.*, p.25. Mais sobre a análise do artigo 8.º da CEDH pela jurisprudência do Tribunal Europeu dos Direitos do Homem, *vide* Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* pp. 123 e ss.

[387] Artigo 8.º, n.º 2 da CEDH:" Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."

[388] A questão de possibilidade de restrição de direitos fundamentais foi discutido no ponto 2.7.1.

[389] O artigo 12.º da Declaração Universal dos Direitos do Homem*:* "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."

[390] O artigo 12.º da Declaração Universal dos Direitos do Homem*: "*Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."

O artigo 17.º do Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), aprovado pela ONU em 1966, visa igualmente proteger a privacidade, na medida em que reproduz o artigo 12.º da Declaração Universal dos Direitos do Homem[391].

Em direito internacional convencional, é importante destacar a Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal do Conselho da Europa (Convenção 108) adotada em 1980 e aberta à assinatura em 28 de janeiro de 1981, em Estrasburgo, que tem por finalidade "garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado de dados de carácter pessoal que lhe digam respeito"[392].

A Convenção, além de reconhecer o controlo da pessoa sobre os seus dados (artigo 8.º), consagrou princípios fundamentais de proteção de dados pessoais que vieram, posteriormente, a integrar a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, como os princípios da finalidade, da adequação, da pertinência, da exatidão, garantias da retificação e da informação, etc. (artigo 5.º da Convenção n.º108)[393].

Como afirma Teresa Coelho Moreira, "a Convenção (108) é o primeiro documento internacional destinado a garantir o direito à liberdade informática ou direito à autodeterminação informacional e ficou estabelecido o marco genérico de proteção da pessoa perante possíveis intromissões na sua privacidade, ou lesão de outros direitos de personalidade, através da informática"[394].

Quanto ao direito comunitário, são relevantes fundamentalmente duas Diretivas vulgarmente conhecidas por *privacy Directives*: a Diretiva 95/46/CE, do Parlamento Europeu e

[391] O artigo 17.º do Pacto Internacional sobre Direitos Civis e Políticos:" 1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação.2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados." Portugal subscreveu o Pacto Internacional sobre os Direitos Civis e Políticos em 7 de outubro de 1976.

[392] Mais sobre o percurso do Conselho da Europa na tutela do direito à privacidade *vide* Moreira, Teresa Alexandra Coelho. (2010), *op. cit.*, pp.165 e ss.

[393] Castro, Catarina Sarmento e. (2005), *op. cit.*, p.40.

[394] Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,*, pp.171-172.

do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que deu corpo aos princípios do direito à privacidade já consagrados na Convenção 108 e alargou a sua aplicação, e a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas[395] que foi alterada pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações[396] e pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho[397]. Todas elas influenciaram a proteção concedida em matéria de dados pessoais pelos Estados Membros da União Europeia, em virtude da obrigatoriedade da sua transposição.

A Diretiva 95/46/CE foi aprovada numa altura em que vários Estados-Membros tinham já adotado leis nacionais sobre proteção de dados e visava assegurar o funcionamento do mercado único e a proteção efetiva dos direitos e das liberdades fundamentais das pessoas singulares, que só seria possível se os Estados-Membros pudessem confiar na existência de um nível uniformemente elevado de proteção de dados. Todavia, actualmente as regras em vigor não asseguram o grau de harmonização que se exige nem a eficácia necessária para garantir o direito à proteção dos dados pessoais.

Tendo em conta as alterações trazidas pelo Tratado de Lisboa no seu artigo 16.º do TFUE, que atribui à UE competência legislativa complementar para aprovar normas harmonizadas sobre proteção de dados, e com o objetivo de conferir plena eficácia à CEDH na era digital (que consagrou no seu artigo 8.º o novo direito fundamental à proteção de dados pessoais, juridicamente vinculativo para as instituições da União Europeia e para os Estados-Membros quando apliquem o direito da União), em 2010 a Comissão Europeia propôs uma

[395] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), JO L 201, 2002.

[396] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE. A Diretiva 2006/24/CE foi considerada inválida pelo TJUE em 8 de abril de 2014, tal como já foi referido no ponto 2.7.1. do presente trabalho.

[397] Directiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor.

reforma de fundo do quadro legislativo da UE em matéria de proteção de dados, que uniformizou, atualizou e modernizou os princípios estabelecidos na Diretiva 95/46/CE, de 24 de outubro e incluiu uma comunicação[398] que apresentava duas propostas legislativas: uma proposta de Regulamento Geral de Proteção de Dados (RGPD)[399] que define o quadro geral europeu para a proteção dos dados e uma proposta de Diretiva[400] do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, que substitui Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008. Em 12 de março de 2014 o Parlamento Europeu aprovou[401] a última versão[402] do RGPD. As alterações às propostas da Comissão aprovadas pelo Parlamento Europeu têm ainda de ser negociadas com o Conselho de Ministros da UE, sendo provável que o acordo final será feito até 2015.

Desde o tempo em que a UE introduziu, há 19 anos, a sua Diretiva de proteção de dados, a evolução tecnológica e a globalização transformaram e criaram novas formas como os grandes volumes de dados pessoais são recolhidos, analisados, utilizados, transferidos e conservados. Ao mesmo tempo, as novas tecnologias permitem às empresas privadas e autoridades a utilização de dados pessoais a uma escala sem precedentes na persecução das

---

[398] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Proteção da privacidade num mundo interligado; Um quadro europeu de proteção de dados para o século XXI*, (COM (2012) 9 final), de 25 de janeiro de 2012. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:PT:PDF consultado a 14 de outubro de 2013.

[399] Parlamento Europeu e Conselho Europeu, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)*, (COM (2012) 11 final), de 25 de janeiro de 2012. Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf consultado a 15 de novembro de 2012.

[400] Parlamento Europeu e Conselho Europeu, *Proposta de Diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados*, (COM (2012) 10 final), de 25 de janeiro de 2012. Disponível em:http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:PT:PDF consultado a 6 de junho de 2013.

[401] Parlamento Europeu, *Resolução legislativa, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,* (COM(2012)0011 –MC7-0025/2012 – 2012/0011(COD)), de 12 de março de 2014. Estrasburgo. Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=PT&ring=A7-2013-0402 consultado a 1 de abril de 2014.

[402] Na mesma versão aprovada pela Comissão das Liberdades Cívicas, Justiça e dos Assuntos Internos em outubro de 2013.

suas atividades. Aliás, as próprias pessoas disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global[403].

Para assegurar a continuidade da proteção de dados e adaptar as regras à evolução tecnológica a reforma do regime jurídico de proteção de dados irá transformar o modo como os dados pessoais são protegidos e regulados na UE.

3.1.2. Direito à privacidade no ordenamento jurídico português: direito à privacidade enquanto um Direito de Personalidade

No ordenamento jurídico português o direito à privacidade é reconhecido pela Constituição da República Portuguesa, no artigo 26.º, n.º1, e pelo Código Civil, no artigo 80.º, como direito fundamental e como direito de personalidade, respetivamente[404].

A privacidade e a proteção de dados é assim uma preocupação importante para o legislador, contudo existe uma certa fluidez do conceito de privacidade, que, aliás, nem a própria Constituição nem a lei ajudam a fixar. Ao mesmo tempo Paulo Mota Pinto, na tentativa definir o conceito de privacidade, conclui que existe dificuldade na definição de um conceito que "é necessariamente indeterminado, acaba por se revelar imprestável, como um verdadeiro "conceito elástico" [405].

Gomes Canotilho e Vital Moreira defendem que o âmbito do direito à intimidade da vida privada deve ser analisado em dois direitos "(a) o direito a impedir o acesso de estranhos a

[403] "Dados disponibilizados nos perfis de redes sociais, em Portugal, em 2013 os dados mais divulgados são o Nome,Fotografia pessoal, Localidade e Data de Nascimento, com percentagens de 96,1%, 84,7%, 76,0% e 74,5%. Os dados relativos a formas de contacto pessoal, tais como o Telefone fixo, Telemóvel e Endereço de email são os menos divulgados pelos internautas portugueses nas redes sociais, com percentagens de 0,4%, 3,3% e 18,8%, respetivamente." *Vide* Cardoso, G., et al. (2014, janeiro), *op. cit.*, p.17.

[404] Pinto, P. M. (2000). A limitação voluntária do direito à reserva sobre a intimidade da vida privada. In Jorge Dias de Figueiredo *et al.* (Eds.), *Estudos em homenagem a Cunha Rodrigues* (Vol. 2), (pp. 527- 558). Coimbra: Coimbra Editora, p.527.

[405] Pinto, P. M. (1993). O direito à reserva sobre a intimidade da vida privada. *Boletim da Faculdade de Direito da Universidade de Coimbra*, *69*, 479-586, pp. 504-505; 523-524.

informações sobre a vida privada e familiar e (b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem (artigo 80.° Do Código Civil)"[406].

Por sua vez, Garcia Marques entende o conceito da vida privada como "aquele conjunto de atividades, situações, atitudes ou comportamentos individuais que, não tendo relação com a vida pública (privada entendida como separado da coisa pública), respeitam estritamente à vida pessoal e familiar de uma pessoa"[407], consistindo numa interpretação mais ampla e flexível que a de Canotilho e Moreira.

Na tentativa de delimitar o âmbito material do direito à reserva da vida privada, ou seja, alcance do seu conteúdo, é importante ressaltar a teoria das três esferas defendida fundamentalmente pela doutrina alemã *(Sphärentheorie),* que reconhece três níveis na reserva da vida privada: a esfera íntima ou esfera de segredo que abrange dados e informações pertencentes à intimidade do indivíduo como as opiniões filosóficas, políticas ou religiosas, a origem racial ou étnica e os dados relativos à intimidade sexual, ao estado de saúde, incluindo dados genéticos[408] e que devem, em absoluto, ser subtraídos ao conhecimento de outrem; esfera privada que engloba os comportamentos, os acontecimentos e a informação que diz respeito às relações pessoais do indivíduo que ele partilha com um número limitado de pessoas[409] e, por fim, esfera pública dados que o titular está disposto a apresentar voluntariamente, por corresponder a eventos suscetíveis de serem conhecidos por todos, respeita à participação de cada um na vida da coletividade[410].

Nos termos da Lei da Proteção de Dados Pessoais na esfera pública estariam os dados que foram manifestamente tornados públicos pelo seu titular, como se refere o artigo 7.º n.º 3, alínea c) da Lei da Proteção de dados. Da esfera privada fariam parte os chamados dados não sensíveis, definidos na alínea a) do artigo 3.º da Lei n.º 67/98 como "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável". A esfera íntima englobaria os chamados

[406] Canotilho, José Joaquim Gomes e Moreira, Vital (2007), *op. cit.,* pp.467-468.

[407] Marques, J. A. G. (2004). Internet e privacidade. In Alberto de Sá e Melo, *et al.* (Eds.), *Direito da Sociedade da Informação*, *5*, 23-64. Coimbra: Coimbra Editora, p.24.

[408] Silva, Hugo Lança. (2006, setembro). Monitorização da internet: onde fica o direito à privacidade? In *Verbo Jurídico,* p.7. Disponível em: http://www.verbojuridico.com/doutrina/tecnologia/monitorizacaointernet.pdf consultado a 6 de setembro de 2013.

[409] Castro, Catarina Sarmento e. (2005), *op. cit.,* p.24.

[410] Andrade, Manuel da Costa. (2006). *Sobre as Proibições de Prova em Processo Penal*, 1.ª reimp., Coimbra: Coimbra Editora, pp. 94 -96.

dados sensíveis, que a Lei no artigo 7.º refere como "dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica", bem como "o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos"[411].

Segundo Farinho o conteúdo reconhecido a estas três esferas segue um critério de valoração da intimidade, na medida em que as esferas que exigem maior proteção são aquelas que estão mais próximas de experiências definidoras da identidade do indivíduo, encontrando-se fora do objeto do direito sob estudo toda e qualquer informação divulgada pelo próprio titular quando feita num local público, isto é, no qual se cruzam ou podem cruzar destinatários não compreendidos nas outras esferas, pela ausência de relações próximas com o titular[412].

No entanto, de acordo com o mesmo autor "a mera determinação pelo indivíduo em tornar pública uma certa informação não é suficiente se for feita num círculo aparentemente determinado de destinatários, uma vez que, nestes casos, o sujeito pode assumir que a informação divulgada foi controlada quanto aos destinatários"[413].

Em Portugal o direito à reserva da intimidade da vida privada está consagrado no artigo 26.º da Constituição da República Portuguesa[414]. O n.º 1 do artigo 26.º da Constituição, na redação que lhe foi dada pela revisão constitucional de 1997, tutela entre outros "direitos de personalidade"[415], os "direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação". O artigo 26.º da CRP ao proclamar que a todos os cidadãos são reconhecidos os direitos à identidade e historicidade pessoal, bem como o direito à reserva da intimidade da vida

[411] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* p.250.

[412] Farinho, Domingos Soares. (2006), *op. cit.,* p.46.

[413] *Idem, ibidem.*

[414] Constituição da República Portuguesa, artigo 1.º: "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação." Artigo 2.º: "A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias."

[415] Segundo Orlando de Carvalho, o direito geral de personalidade é "um direito que abrange todas as manifestações previsíveis e imprevisíveis da personalidade, pois é, a um tempo, direito à pessoa-ser e à pessoa-devir, ou melhor, à pessoa-ser em devir, entidade não estática mas dinâmica e com jus à sua "liberdade de desabrochar" (com direito ao 'livre desenvolvimento da personalidade' de que falam já certos textos jurídicos). Trata-se de um jus in se ipsum radical, em que a pessoa é o bem protegido, correspondendo à sua necessidade intrínseca de autodeterminação (...). Só um tal direito ilimitado e ilimitável permite uma tutela suficiente do homem ante os riscos de violação que lhe oferece a sociedade moderna". Cf. Carvalho, Orlando de.(1981). *Teoria geral do Direito Civil.* Coimbra: Centelha, p. 90.

privada no seu n.º 2.º enuncia o estabelecimento de garantias efetivas contra a utilização abusiva ou contrária à dignidade humana, de toda a informação relativa às pessoas e às famílias.

Nesse sentido, Jorge Miranda e Rui Medeiros esclarecem: "O artigo 26.º constitui expressão direta do postulado básico da dignidade humana que a Constituição consagra logo no artigo 1.º como valor básico logicamente anterior à própria ideia do Estado de Direito democrático e que constitui referência primeira em matéria de direitos fundamentais. Simultaneamente, a dignidade humana encontra aqui uma sede fundamental de definição normativa: quem invoca a dignidade humana não poderá deixar de ter em conta, simultaneamente, os direitos aqui consagrados, pois estes dão-lhe expressão mais definida"[416].

Os autores referem ainda que, além do direito de oposição e respeito pela vida privada, a mencionada premissa compreende atualmente uma dimensão positiva que se traduz na autodeterminação informativa[417], conferindo ao cidadão um autêntico controlo sobre seus dados pessoais, regulando o acesso e a utilização dos mesmos por terceiros[418].

No entendimento de Paulo Mota Pinto, o direito à autodeterminação informativa[419] do direito a um controlo da informação sobre a vida privada, que diz respeito não apenas à recolha de informação sobre a vida privada, mas também à sua divulgação[420].

Deste modo, em Portugal[421] o direito à privacidade é reconhecido no artigo 35.º da Constituição da República Portuguesa que contempla um direito à autodeterminação informativa

---

[416] Miranda Jorge, Medeiros Rui. (2010). *Constituição Portuguesa Anotada*. Tomo I (2ª ed.) Coimbra: Coimbra Editora, pp. 607.

[417] *Vide* ponto 2.7 do presente trabalho.

[418] Miranda Jorge, Medeiros Rui. (2010), *op. cit.,* p.620.

[419] Segundo Teresa Coelho Moreira: "Com este novo direito (o direito à autodeterminação informacional) toda a pessoa tem o direito de preservar a sua identidade, controlando a revelação e o uso dos dados que lhe dizem respeito e protegendo-se perante a capacidade ilimitada de arquivá-los, relacioná-los e transmiti-los, objetivo que se pretende atingir atribuindo ao cidadão uma série de faculdades tendentes a garantir que o titular dos dados tenha consentido na recolha e no tratamento dos seus dados pessoais ou, pelo menos, os tenha conhecido, dispondo do direito de aceder, retificar e cancelar, quando for necessário, tais informações."- Moreira, Teresa Alexandra Coelho. (2010), *op. cit.*, p.295.

[420] Pinto, P. M. (2000), *op. cit.,* p.529.

[421] "Portugal foi o primeiro Estado europeu que reconheceu de forma expressa no seu contexto constitucional um direito à proteção de dados pessoais, distinto do direito à reserva sobre a intimidade da vida privada. Desde a sua versão de 1976m que a CRP consagra um direito à autodeterminação informativa no artigo 35.º ". - Teresa Alexandra Coelho. (2010), *op. cit.*, pp.295-296.

que, na linha da jurisprudência germânica[422], assume uma dimensão de proteção da intimidade da vida privada perante o tratamento e utilização de dados na informática[423].

O direito consagrado no artigo 35.º da CRP[424] atribui ao indivíduo não apenas o poder (direito de natureza negativa)[425] de negar ou se opor à recolha, difusão e tratamento de dados pessoais mas, sobretudo, o poder positivo[426] de dispor sobre os seus dados pessoais, evitando que o indivíduo seja transformado em "objeto de informações"[427], vinculando o estado a tomar medidas legislativas para a realização plena da autodeterminação da pessoa em face do uso da informática.

O direito à autodeterminação informativa, segundo Catarina Sarmento e Castro, pode ser encarado numa dupla perspetiva[428]: subjetiva e objetiva[429]. A dimensão subjetiva traduz-se na capacidade jurídica de titulares de dados de se defenderem dos abusos que estes podem sofrer por parte do Estado quanto à utilização da informação pessoal. Esta dimensão subjetiva pode manifestar-se na abstenção do Estado em proceder ao tratamento de dados pessoais, tirando os casos excecionais previstos na Constituição, bem como pode constituir uma imposição ou obrigação do Estado de definir normas jurídicas reguladoras da utilização e tratamento dos dados pessoais e criar uma entidade administrativa independente para sua salvaguarda.[430] Por sua vez, a perspetiva objetiva impõe ao Estado a adoção de providências de defesa contra agressões de terceiros ao direito à privacidade[431].

---

[422] A primeira decisão sobre o assunto foi proferida no Acórdão *BVerfGE* 65,1 do Tribunal Constitucional Federal Alemão de 15 de dezembro de 1983 relativa à Lei do Censo (*Volkszählungsurteil*).

[423] Farinho, Domingos Soares. (2006), *op. cit.*, p.43.

[424] A análise mais detalhada do artigo 35.º da CRP será feita no ponto 3.2.1.

[425] Miranda Jorge, Medeiros Rui. (2010), *op. cit.,* p.380.

[426] "Longe de ser um mero direito contra as intrusões do Estado ou de outros indivíduos, que devem abster-se de proceder a tratamentos dos seus dados pessoais, é um direito a decidir até onde vai a sombra que deseja que paire sobre as informações que lhe respeitam, construindo-se como uma liberdade, como um poder de determinar o uso dos seus dados pessoais."- Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.*, p.11.

[427] Canotilho, José Joaquim Gomes e Moreira, Vital. (2007), *op. cit.*, p. 551.

[428] Neste sentido Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* pp.301-302.

[429] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.*, p.12.

[430] Canotilho, José Joaquim Gomes. (2000). *Direito Constitucional e Teoria da Constituição* (4.ª ed.). Coimbra: Almedina, p. 1218.

[431] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit., loc.cit.*

Como sintetiza Teresa Coelho Moreira, "o direito à autodeterminação informativa é um verdadeiro direito fundamental com o conteúdo próprio, e não apenas uma garantia do direito da reserva sobre a intimidade da vida privada (...)"[432].

O direito à privacidade é também um direito de personalidade que encontra os seus fundamentos na proteção da dignidade da pessoa humana, na proteção da individualidade e autonomia de cada um, perante agressões decorrentes do uso dessas informações no contexto de meios tecnológicos emergentes e do crescente recurso a meios eletrónicos[433].

A lei portuguesa consagra direito à reserva sobre a intimidade da vida privada, incluindo-o entre os chamados "direitos de personalidade" (artigos 70.º a 80.º do Código Civil). Foi em 1966 que o direito à intimidade da vida privada passou a ser consagrado expressamente no ordenamento jurídico português[434].

O artigo 80.º do Código Civil estabelece:

"1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem.

2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas".

Pedro Pais de Vasconcelos defende a ideia de que o direito à privacidade prevalece sobre a necessidade de recolha e tratamento de dados pessoais[435]. Esta prevalência decorre, desde logo, da natureza do direito à privacidade, como direito de personalidade.

Segundo o autor "os direitos de personalidade são aqueles sem os quais as pessoas não são tratadas como pessoas, são direitos que são exigidos pela sua radical dignidade como e enquanto Pessoas Humanas, constituem fundamento ontológico da personalidade e da dignidade humana"[436].

---

[432] Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* p.301.

[433] Pinto, P. M. (1993), *op. cit.,* p.480.

[434] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* p.157.

[435] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* p.249.

[436] *Idem,* p.250.

Daí conclui-se que os direitos de personalidade - entre os quais o direito à privacidade - são supra legais, por isso, são hierarquicamente superiores aos outros direitos, inclusivamente aos direitos fundamentais que não sejam direitos de personalidade[437].

Além da referência aos normativos do Código Civil e da Constituição da República Portuguesa, torna-se pertinente referir outros meio normativos da ordem jurídica portuguesa na matéria da privacidade.

Uma outra área do ordenamento jurídico, onde a intimidade encontra tutela específica, é o direito penal. O artigo 193.º do Código Penal (devassa por meio informático) pune com pena de prisão até dois anos e com pena de multa até 240 dias "quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica", igualmente a Lei n.º67/98, prevê nos seus artigos de 35.º a 49.º a responsabilidade contravencional e criminal em matéria de proteção de dados pessoais.

Os meios administrativos de proteção de dados pessoais concentram-se na Comissão Nacional de Proteção de Dados, criada nos moldes previstos pela Lei n.º 10/95, atualmente substituída pela Lei n.º67/98, designada pela sigla CNDP. Esta Comissão é, nas palavras da Lei (artigo 21.º, n.º1, da Lei n.º67/98), uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia de República e tem, segundo o artigo 22.º da mesma Lei, a atribuição genérica de controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pela liberdades e garantias consagradas na Constituição e na lei. A CNDP, segundo a Lei n.º67/98, possui amplas competências: tem poderes de investigação e de inquérito, de autoridade e de emitir pareceres prévios ao tratamento de dados pessoais[438].

O direito à privacidade procura minimizar a interferência em assuntos particulares e individuais; oferece um instrumento para salvaguardar a opacidade do indivíduo e coloca limites à interferência por parte de terceiros ou do próprio Estado na autonomia do indivíduo. Observa-se hoje que a expetativa razoável de privacidade está a ser ameaçada devido à emergência de

---

[437] É o caso do direito de imprensa que, tendo a consagração constitucional, não tem todavia a dignidade de um direito de personalidade. *Vide* Gonçalves, Maria Eduarda. (2003). *Direito da Informação - Novos direitos e formas de regulação na Sociedade da Informação.* Coimbra: Almedina, e Correia, Luís Brito. (2000). *Direito da comunicação social* (Vol.I). Coimbra: Almedina.

[438] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* p.243.

novas tecnologias e às possibilidades de vigilância, especialmente nos sistemas de AmI, onde recolha e o processamento de dados pessoais são quase um pré-requisito. Há uma série de instrumentos legais que poderiam servir como garantias à privacidade, no entanto, a sua utilidade como salvaguardas não é suficiente uma vez que existem diversas lacunas que precisam de ser corrigidas, assim torna-se forçoso recorrer a novas ferramentas de opacidade, como as técnicas de anonimato, as tecnologias de proteção da privacidade e o direito ao esquecimento, entre outros[439].

3.2. Proteção de dados pessoais enquanto Direito Fundamental

Na ordem jurídica da União Europeia o direito à proteção de dados pessoais é reconhecido como um direito fundamental autónomo. Está previsto de forma expressa no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.

O Tratado de Lisboa[440], com a sua entrada em vigor a 1 de dezembro de 2009[441], introduziu uma base jurídica para a proteção de dados pessoais na União Europeia, conferindo à Carta dos Direitos Fundamentais da União Europeia (CDFUE)[442] o mesmo valor jurídico dos tratados constitutivos com o efeito jurídico vinculativo[443], consagrando nos artigos 7.º e 8.º o respeito pela vida privada e familiar e a proteção de dados pessoais, respetivamente.

Esta Carta prevê no artigo 8.º a proteção dos dados pessoais enquanto direito fundamental protegido pela ordem jurídica europeia[444], enquanto uma ferramenta fundamental para o livre desenvolvimento da personalidade humana. Com efeito, a proteção de dados pessoais que objeto de tratamento foi autonomizável do direito ao respeito à vida privada (artigo 7.º da Carta), o que traduz a relevância atribuída, pelo ordenamento jurídico da UE,

---

[439] Sobre estas e outras ferramentas de opacidade ver o ponto seguinte 3.3.

[440] Publicado no Jornal Oficial da União Europeia em 17 de dezembro de 2007, C-306.

[441] Artigo 6.º, n.º2 do Tratado de Lisboa.

[442] A CDFUE foi proclamada em Nice em 2000, contudo a sua entrada em vigor só acorreu com o Tratado de Lisboa em 2009.

[443] Artigo 6.º, n.º1 do Tratado da União Europeia.

[444] Por sua vez o artigo 8.º da Carta é inspirado pelo artigo 8.º da Convenção Europeia dos Direitos do Homem e na Convenção 108 do Conselho da Europa, bem como no artigo 286.º do Tratado que institui a Comunidade Europeia (atualmente corresponde ao artigo 16.º do Tratado sobre o Funcionamento da União Europeia) e na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

ao direito fundamental da proteção dos dados pessoais enquanto um instrumento imprescindível para o livre desenvolvimento da personalidade humana e, sobretudo, como um direito distinto e autónomo do do respeito à vida privada previsto no artigo 7.º da Carta que representa a visão negativa do direito à privacidade.

De acordo com o artigo 8.º n.º1 da CDFUE: "Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhe digam respeito". Neste sentido protegem-se não só dados íntimos e privados, mas também os dados pessoais, ou seja, todos os dados relativos a uma pessoa, por outro lado, a referida disposição abrange todos os cidadãos e não apenas cidadão da União Europeia.

Na primeira parte do n.º2, o artigo 8.º reconhece o princípio de licitude e o princípio de finalidade para efeitos da recolha e de tratamento de dados pessoais, afirmando que os dados recolhidos devem ser objeto de um tratamento leal e apenas para fins específicos. Mais, a referida disposição enuncia que este tratamento deve ser realizado sempre com base no consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, estabelecendo expressamente o princípio de consentimento, enquanto fundamento legal do tratamento de dados pessoais. Ao mesmo tempo, na segunda parte do n.º2 do artigo 8.º da Carta encontra-se reconhecido a todos os titulares de dados o direito de acesso aos dados e o de retificação de dados inexatos ou incompletos, protegendo o direito à autodeterminação informativa das pessoas[445].

Em suma, como refere Teresa Moreira, o artigo 8.º da Carta "consagra a consciencialização dos desequilíbrios de poder entre a pessoa e o responsável pelo tratamento de dados e, também, o impacto que este tratamento pode ter sobre as diversas liberdades do cidadão"[446].

Aliás, a Constituição da República Portuguesa desde a sua versão originária de 1976 consagra um direito à autodeterminação informativa[447] no artigo 35.º, tendo sido o seu texto revisto em 1982, em 1989 e em 1997. Na sua versão inicial, o artigo referia-se ao uso de dados

[445] Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,*pp. 196-197.

[446] *Idem*, p. 196.

[447] Mais sobre o direito à autodeterminação informativa ver no ponto anterior 3.1.2.

mecanográficos[448]. Deste modo, Portugal foi o primeiro país a estabelecer constitucionalmente um direito fundamental à proteção dos dados pessoais, objeto de tratamento automatizado[449, 450].

O artigo 35.º da CRP consagra a proteção dos cidadãos perante o tratamento de dados pessoais informatizados:

Artigo 35.º (Utilização da informática)

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a leio regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

---

[448] Só a Revisão da Constituição de 1982 substituiu os "registos mecanográficos" pelos "registos informáticos". Na versão atual refere-se "dados informatizados" e "tratamento automatizado". A versão original da Constituição Portuguesa de 1976 já atribuía ao indivíduo o direito de tomar conhecimento dos dados constantes de registos mecanográficos e do seu fim, o direito de atualização e de retificação dos mesmos, a par das proibições de atribuição de um número nacional único e da realização de tratamentos de dados sensíveis.

[449] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.,* p. 10.

[450] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.*, pp. 282 e ss.

7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

O artigo em questão confere ao indivíduo o direito de negar informação pessoal e de se opor à sua recolha, difusão, ou qualquer outro modo de tratamento. Segundo Catarina Sarmento e Castro, evita-se, deste modo, que o indivíduo seja transformado em "simples objeto de informações", na medida em que se lhe atribui um poder positivo de dispor sobre as suas informações pessoais, que se traduz em poder de autotutela, de controlo, sobre os seus dados pessoais, permitindo "preservar a sua própria identidade informática"[451].

No entendimento de Teresa Coelho Moreira, "o direito consagrado neste artigo 35.º traduz-se, assim, num acervo de prerrogativas que pretendem garantir que cada um tenha o direito a manter secreto uma parte dos seus dados pessoais, a não ser objeto de um controlo total, ou de ser visto como uma pessoa transparente"[452].

O artigo 35.º no seu n.º2 contempla "o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei".

É importante referir que este direito à informação ultrapassa o mero direito de aceder/conhecer e corrigir os dados tratados. Constitui antes e segundo Gomes Canotilho e Vital Moreira "uma espécie de direito básico" - *habeas data* - que se traduz em vários direitos: "a) o direito de acesso, ou seja, o direito de conhecer os dados constantes de registos informáticos, quaisquer que eles sejam (públicos ou privados); b) o direito ao conhecimento da identidade dos responsáveis bem como o direito ao esclarecimento sobre a finalidade dos dados; c) o direito à contestação, ou seja, o direito à retificação dos dados e sobre a identidade e endereço do responsável; d) o direito à atualização (cujo escopo fundamental é a correção do conteúdo dos dados em caso de desatualização); e finalmente, o direito à eliminação dos dados cujo registo é interdito"[453].

Segundo Gomes Canotilho e Vital Moreira "o enunciado linguístico dados é o plural da expressão latina datum e está utilizada na Constituição no sentido que hoje lhe empresta a

[451] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.*, p. 11.

[452] Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* p. 300.

[453] Canotilho, José Joaquim Gomes e Moreira, Vital. (2007), *op. cit.*, pp. 551-552.

ciência informática: representação convencional de informação sob a forma analógica ou digital possibilitadora do seu tratamento automático (introdução, organização, gestão e processamento de dados)"[454].

O artigo 35.º prevê direitos e garantias para os titulares de dados pessoais e cria obrigações para os responsáveis pela sua recolha e tratamento, no que se refere à qualidade e segurança da informação, assim como às condições em que estes dados podem ser utilizados.

Hoje, a tipificação dos direitos fundamentais prevista pelo artigo 35.º, n.º 1 da CRP, contempla o direito ao conhecimento de dados pessoais existentes em registos informáticos que se desdobra em vários direitos: o direito de acesso, retificação e atualização de dados pessoais, o direito ao conhecimento da identidade dos responsáveis, bem como o direito ao esclarecimento sobre a finalidade dos dados, o direito de contestação, o direito à eliminação de dados, nomeadamente quando existem dados incorretos ou obsoletos, ou quando o tratamento destes é proibido.

Do artigo 35.º, n.º2 consta ainda a imposição dirigida ao legislador para que defina o conceito de dados pessoais, as condições do seu tratamento automatizado, da sua conexão, transmissão e utilização.[455] Através desta obrigação o legislador constituinte define este direito fundamental como um direito que impõe ao Estado deveres positivos, de prestação normativa, obrigando-o a definir mecanismos através dos quais o titular do direito possa exercer a sua liberdade informacional face à comunidade.

O n.º2 do artigo 35.º da CRP reveste uma especial relevância por mencionar a previsão constitucional de uma entidade administrativa independente – a Comissão Nacional de Proteção de Dados, cujo objetivo principal consiste na proteção de dados pessoais do cidadão, sendo o seu estatuto regulado pela Lei n.º67/98, de 26 de outubro.

A Constituição no n.º3 do artigo 35.º estipula a proibição absoluta do tratamento de certos tipos de dados pessoais, os chamados dados sensíveis[456], respeitantes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante

---

[454] *Idem*, pp. 550 – 558.

[455] O regime que consta hoje da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados) concretiza aspetos importantes do direito à autodeterminação informativa, precisando garantias de proteção.

[456] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* p. 294.

expresso consentimento do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não identificáveis individualmente.

O n.º4 do mesmo artigo refere ainda a proibição do acesso aos dados pessoais de terceiros, salvo em casos excecionais previstos na lei. Como sublinha Catarina Sarmento e Castro, esta proibição "deve ser entendida num sentido amplo: pretende-se impedir que as informações prestadas a um particular ou entidade possam ser por estes divulgadas a outras pessoas, bem como que aqueles concedam a terceiros o acesso aos dados tratados"[457]. A proibição de acesso a dados pessoais por parte de terceiros terceiros é explicada pelo risco que a informática pode representar para a esfera da vida privada e resulta sobretudo da perda de controlo das informações pessoais prestadas a um particular ou entidade quando as mesmas são divulgadas ou acedidas indevidamente. Esta proibição de acesso e da divulgação de dados está ligada a uma outra proibição relevante: a do tratamento de dados para finalidades distintas da finalidade que esteve na origem do seu tratamento[458].

A Constituição prevê exceções a esta proibição autorizando o legislador a definir os casos em que poderá haver acesso de terceiros e interconexão de dados. A estas exceções aplica-se o regime das restrições aos direitos, liberdades e garantias do artigo 18.º da CRP, o que significa que essas só podem ser admitidas quando exigidas pela necessidade de defesa de direitos ou bens constitucionalmente protegidos.

O número 5.º prevê a proibição da atribuição de um número nacional único aos cidadãos[459], que possa funcionar como identificador universal, sendo certo que tal proibição não impede que a cada cidadão, apenas e só para certo efeito limitado, seja atribuído um número que o distingue dos demais em certas áreas, por exemplo, o número de cartão de cidadão, do número de identificação fiscal ou o número de segurança social.

O artigo 35.º da Constituição estabelece no seu número 6.º a garantia do livre acesso às redes informáticas de uso público. Este direito ao digital ultrapassa o contexto do direito à autodeterminação informativa, para pressupor já um direito a uma prestação do Estado que fica

[457] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 36.

[458] *Idem*, *ibidem.*

[459] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* pp. 295-296.

obrigado a tomar medidas com vista a garantir o acesso geral às redes informáticas de uso público por parte de qualquer indivíduo[460].

O mesmo número do artigo 35.º obriga também o legislador à definição de normas reguladoras do fluxo de dados transfronteiras e da proteção adequada de dados pessoais e de outros, cuja salvaguarda se justifique por razões de interesse nacional. A Lei da Proteção de Dados concretizou este aspeto através da transposição da Diretiva 95/46/CE.

Através do 7.º, e último número do artigo 35.º, da Constituição atribui-se aos ficheiros manuais uma proteção idêntica à prevista no texto constitucional para os ficheiros automáticos[461], cabendo à lei essa definição[462]. Gomes Canotilho e Vital Moreira referem que o termo tratamento de dados pessoais informatizados "abrange não apenas a individualização, afixação e recolha de dados, mas também a sua conexão, transmissão, utilização e publicação"[463].

Apesar o artigo 35.º ser a principal norma reguladora da proteção da privacidade no que diz respeito ao tratamento de dados pessoais, outros artigos da Constituição assumem um papel igualmente importante nestas matérias, como é o caso do já mencionado artigo 26.º da CRP que reconhece o "direito à reserva da intimidade da vida privada", e que o artigo 35.º da CRP pretende salvaguardar.

Também enquanto garantia do direito à reserva da intimidade da vida privada a Constituição estabeleceu o artigo 34.º que protege a inviolabilidade do "sigilo da correspondência e dos outros meios de comunicação privada" (n.º1), proibindo "toda a ingerência das autoridades públicas (...) nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em processo criminal" (n.º4), bem como o artigo 32.º, n.º8 que, no âmbito das garantias do processo criminal, considera nulas "todas as provas obtidas mediante (...) abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações"[464].

A inclusão do direito à proteção de dados pessoais do Título II da Constituição, relativo aos direitos, liberdades e garantias, submete-o ao regime especial desses direitos fundamentais, o

[460] Castro, Catarina Sarmento e. (2005), *op. cit.*, p. 37.

[461] Mais sobre esta questão *vide* Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* pp. 297-299.

[462] Neste sentido Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 33.

[463] Canotilho, José Joaquim Gomes e Moreira, Vital. (2007), *op. cit.,* p. 550.

[464] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 39.

que é particularmente significativo em matéria de restrições, além, naturalmente, de lhes ser aplicado o regime geral dos direitos fundamentais[465].

É possível concluir que, que quer ao nível da Carta dos Direitos Fundamentais da União Europeia, quer ao nível constitucional no ordenamento jurídico português, o direito à proteção de dados pessoais, não só está expressamente referido, como ocupa lugar de destaque, enquanto valor jurídico no qual devem assentar os pilares fundamentais da sociedade.

Apesar das inúmeras novas oportunidades oferecidas pela tecnologia dos AmI, existe um grande risco de os dados serem usados para tornar o indivíduo num objeto sob constante vigilância e monitorização[466], o que não é compatível com a verdadeira natureza da proteção de dados como direito fundamental que é vista como expressão da liberdade pessoal e da dignidade.

3.2.1. Proteção de dados pessoais no ordenamento jurídico português: Lei n.º 67/98, de 26 de outubro

Tomando como ponto de partida a Convenção 108 do Conselho da Europa, o Parlamento Europeu e o Conselho da União Europeia aprovaram em 24 de outubro de 1995, a Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos, aplicável no âmbito do mercado interno. A aprovação da Diretiva resultou da necessidade de harmonizar as legislações dos Estados-Membros da União em matéria de proteção de dados pessoais mas, sobretudo, pretendeu, como refere Teresa Coelho Moreira "criar um Documento que conseguisse uma livre circulação de dados pessoais nos vários Estados- Membros que não colocasse entraves ao mercado interno e que realizasse uma aproximação entre as várias legislações internas, já que disparidade de legislações nacionais criava perigosas «distorções» da concorrência no mercado europeu"[467].

Contudo, a referida Diretiva no momento da sua aprovação só tinha em atenção transmissão de informações em bancos de dados não necessariamente em rede ou, unicamente

[465] Castro, Catarina Sarmento e. (2003, dezembro), *op. cit.*, p. 13.

[466] De Hert, P., *et al.* (2009), *op. cit.,* pp. 439-440.

[467] Moreira, Teresa Alexandra Coelho. (2010), *op. cit.,* p. 199.

em redes fechadas, não existindo ainda preocupação da exposição destes dados em rede aberta como a Internet com os seus riscos. Por outro lado as técnicas de recolha e transmissão de dados não tinham ainda atingido o grau de sofisticação hoje conhecido[468].

Em conformidade com o artigo 8.º, n.º1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16.º, n.º1, do Tratado sobre o Funcionamento da União Europeia (TFUE), todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. De acordo com o artigo 2.º, n.º2 e o artigo 16º, n.º2 conjugado com artigo 4.º, n.º 2, alínea a), do TFUE, a proteção de dados é um domínio ao qual o Tratado atribui à União Europeia competência partilhada com os Estados-Membros, o que significa que estes exercem a sua competência na medida em que a União não tenha exercido a sua[469]. Tendo em atenção que a EU já exerceu a sua competência nesta matéria através da adoção em 24 de outubro de 1995 da Diretiva 95/46/CE do Parlamento Europeu e o Conselho da União Europeia, a iniciativa legislativa dos Estados-Membros sobre a matéria de proteção de dados pessoais ficou inibida. Em Portugal foi a Lei n.º 67/98 (Lei de Proteção de Dados Pessoais ou LPDP), de 26 de outubro que procedeu à transposição da Diretiva n.º 95/46/CE para o ordenamento jurídico nacional que deverá ser interpretada à luz do direito da União Europeia, revogando a antiga Lei de Proteção de Dados Pessoais (Lei n.º 10/91, de 29 de abril) e Lei n.º 28/94, de 29 de agosto. É igualmente importante referir que a LPDP assumiu um papel importante ao regulamentar a alteração do disposto no artigo 35.º da CRP, fruto da 4ª Revisão Constitucional de 1997, influenciada pela Diretiva 95/46/CE.

Ademais, desde a 4ª Revisão constitucional, o artigo 35.º da CRP no seu n.º2 passou a prever a existência de uma autoridade administrativa independente.[470] No entanto, e apesar da referida imposição constitucional ter sido criada só em 1997, o legislador ordinário já tinhacriado esta entidade em 1991 pela Lei n.º 10/91, de 29 de abril – a, então designada, Comissão Nacional de Proteção de Dados Pessoais Informatizados - tendo sido instituída em 1994. Desde 1998 esta entidade administrativa independente é conhecida por Comissão Nacional de

[468] Farinho, Domingos Soares. (2006), *op. cit.,* p. 78.

[469] Artigo 2.º, n.º 2 do TFUE:"Quando os Tratados atribuam à União competência partilhada com os Estados-Membros em determinado domínio, a União e os Estados-Membros podem legislar e adotar atos juridicamente vinculativos nesse domínio. Os Estados-Membros exercem a sua competência na medida em que a União não tenha exercido a sua. Os Estados-Membros voltam a exercer a sua competência na medida em que a União tenha decidido deixar de exercer a sua."

[470] É de referir que a CDFUE no seu artigo 8.º, n.º 3 igualmente prevê a existência de uma autoridade independente que terá por objetivo a fiscalização do cumprimento das regras em matéria de proteção de dados pessoais.

Proteção de Dados, (o seu estatuto foi regulado e as suas competência substancialmente reforçadas pela LPDP), que possui poderes de autoridade e com atribuição de controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais (artigo 22.º, n.º1 da LPDP), que funciona junto da Assembleia da República (artigo 21.º, n.º1 da LPDP)[471].

As atribuições e competências (definidas nos artigos 21.º a 24.º da LPDP) da CNPD foram reforçadas, passando a dispor de poderes de fiscalização[472], nomeadamente de investigação e de poderes de autoridade, "designadamente o de ordenar bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português" – artigo 22.º, n.º3. Destaca-se, igualmente, a competência para emitir pareceres nos termos dos artigos 22.º, n.º3, alínea c), e 23.º, n.º1, alínea a).

Torna-se obrigatória a consulta da CNPD "sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias ou internacionais, relativos ao tratamento de dados pessoais" – artigo 22.º, n.º2.

Cabe, ainda, à CNPD um conjunto de poderes previstos no artigo 23.º, n.º3, tais como: autorizar ou registar, consoante os casos, os tratamentos de dados pessoais, autorizar, em casos excecionais, a utilização de dados pessoais para finalidades não determinantes da recolha, autorizar, em casos excecionais, a interconexão de tratamentos de dados pessoais, autorizar a transferência internacional de dados pessoais, fixar o prazo de conservação dos dados, em função da finalidade, assegurar o direito de acesso, retificação e atualização, autorizar a fixação de custos ou de periodicidade para o exercício do direito de acesso, fixar prazos máximos de cumprimento do exercício do direito de acesso em cada setor de atividade, apreciar as queixas e reclamações dos particulares, deliberar sobre a aplicação de coimas, promover e apreciar códigos de conduta, entre outros.

---

[471] Na mesma altura, sai a Lei n.º 69/98 de 28 de outubro, que vem regular a proteção de dados pessoais e a defesa da privacidade no sector das telecomunicações, transpondo a denominada Diretiva das Telecomunicações (Diretiva 97/66/CE), e que também atribui à CNPD competências nesta matéria. Em 2004, é revogada a Lei n.º 69/98, com a publicação da Lei n.º 41/2004, de 18 de agosto, que regula a proteção de dados pessoais no sector das comunicações eletrónicas, transpondo a Diretiva 2002/58/CE.

É também publicada legislação complementar, que atribui competências à Comissão como autoridade nacional de controlo em matérias de proteção de dados pessoais relativas a *Schengen* (Lei n.º 2/94 de 19 de fevereiro) e à Europol (Lei n.º 68/98, de 26 de outubro).

[472] Castro, Catarina Sarmento e. (2005), *op. cit.*, p. 332.

Por último, a CNPD passa a poder divulgar a sua atividade e, pedagogicamente, tentar convencer os responsáveis pelo tratamento de dados a respeitarem os critérios que propõe através da elaboração e publicação de um relatório anual, artigo 23.º, n.º1, alínea p)[473].

Voltando à discussão sobre a LPDP, a mesma começa por proclamar, no seu artigo 2º, o princípio geral que determina que "o deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais".

Na alínea a) do artigo 3.º, a lei consagra a definição de dados pessoais como "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»)"; enquanto por tratamento de dados pessoais "pressupõe-se qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição" – artigo 3.º, alínea b) da LPDP.

Esta definição representa um conceito alargado de dados pessoais que se traduz na expressão "qualquer informação" que visa abranger todo tipo de informação, independentemente da veracidade dessa informação ou do formato em que a mesma se apresenta[474].

Torna-se pertinente referir que o Tribunal de Justiça da UE teve oportunidade de se pronunciar acerca da interpretação da noção de "dados pessoais" da Diretiva 95/46, considerando no Acórdão Lindqvist[475] que este conceito abrange "seguramente, o nome de uma pessoa a par do seu contacto telefónico ou de informações relativas às suas condições de trabalho ou ao seus passatempos"[476].

---

[473] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* p. 365.

[474] Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, *op.cit.*, pp.4 e 6.

[475] Acórdão *Lindqvist* do Tribunal de Justiça de 6 de novembro de 2003 proferido no âmbito do Processo C-101/01 de 6 de novembro de 2003, Coletânea da Jurisprudência 2003 I-12971. Disponível em: http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-101/01 consultado a 3 de maio de 2013.

[476] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 71.

Por sua vez, os dados referem-se a uma pessoa quando dizem respeito à identidade, caraterísticas ou comportamento de uma pessoa ou se tal informação for utilizada para determinar ou influenciar a forma como essa pessoa é tratada ou avaliada[477]. Quando os dados não permitem identificar uma pessoa, mesmo que sejam dados que se referem, em abstrato, a pessoas, não são dados pessoais: é o caso de dados estatísticos através dos quais não é possível fazer essa ligação[478].

Assim, e segundo Catarina Sarmento e Castro, dado pessoal é "toda informação, seja ela numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo, relativa a uma pessoa física identificada ou identificável"[479].

Conforme a definição elencada na LPDP é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social. Consequentemente, são identificáveis, não apenas aqueles que o próprio titular possa, pelos seus meios identificar, mas que possa identificar, ainda que com recurso a meios que um terceiro disponha. A utilização do termo "indiretamente" significa que a proteção abranje toda a pessoa que, de uma forma ou outra, por associação de conceitos ou conteúdos, mesmo que não exista uma referência direta a ela, possa ser identificada ou identificável.

O Considerando 26 da Diretiva 95/46/CE ajuda a determinar o que se deve entender por pessoa identificável: "para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa". Destaca-se uma preocupação em não deixar depender a atribuição do caráter de dado pessoal à mera possibilidade de o próprio ou um qualquer terceiro poder identificar a pessoa. Pelo contrário, o caráter de dado pessoal só será atribuído se a pessoa puder ser identificável através de meios suscetíveis de serem razoavelmente utilizados para efetuar essa identificação, impondo, deste modo, uma ponderação[480].

---

[477] Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, *op. cit.,* p.8.

[478] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 71.

[479] *Idem, ibidem.*

[480] *Idem*, p. 73.

O tratamento de dados pode constituir uma intromissão na esfera do titular dos dados. Por isso é necessária a existência do consentimento que funciona como condição da legitimidade do tratamento de dados, sobretudo quando se trata de um tratamento de dados sensíveis, n.º2 do artigo 7º da LPDP[481].

Conforme resulta da alínea h) do artigo 3.º da LPDP, o consentimento deve, em geral, ser uma manifestação de vontade livre, específica e informada[482]. No caso de dados sensíveis, o consentimento deve ser ainda expresso, de acordo com artigo 35.º, n.º3 da CRP e artigo 7.º, n.º2 da LPDP. A CNPD entende que o consentimento será expresso quando o titular dos dados der o seu consentimento por escrito. O consentimento só pode ser considerado livre quando seja dado sem qualquer coação e quando possa ser retirado sem restrições ou oposição e, sem que o titular dos dados sofra qualquer consequência[483].

Será expressão de uma manifestação de vontade específica quando o consentimento seja dado em função de um determinado período temporal e para finalidades conhecidas antecipadamente. Não estarão preenchidos os requisitos do consentimento quando este seja dado para tratamento de finalidade vaga ou genérica. Sempre que a finalidade do tratamento sofra qualquer alteração deve ser obtido novo consentimento[484].

De acordo com Catarina Sarmento e Castro só é possível considerar como consentimento informado ou esclarecido aquele que for dado havendo o titular de dados tomado conhecimento da finalidade e da extensão exata do seu consentimento, da identidade do responsável pelo tratamento e do seu representante, dos destinatários dos dados ou categorias de destinatários, em caso de comunicação de dados pessoais e da existência de direito de acesso e das suas condições[485].

---

[481] Esta matéria já foi tratada no ponto 1.2.4.3. do presente trabalho.

[482] O Regulamento Geral de Proteção de Dados vem reforça o consentimento, acrescentando o termo explícito à sua definição. O artigo 7.º clarifica as condições para que o consentimento seja válido enquanto fundamento jurídico para o tratamento lícito. Por suas vez, o silêncio ou a omissão não devem, por conseguinte, constituir um consentimento, (Considerando 25 do RGPD). Acrescenta-se ainda que, sempre que o tratamento for realizado com base nesse consentimento, sobre o responsável pelo tratamento passa recair o ónus de provar o consentimento da pessoa em causa, (Considerando 32 do RGPD).Além disso, o RGPD no seu artigo 8.º estabelece condições suplementares para a licitude do tratamento de dados pessoais de crianças: o tratamento de dados pessoais de uma criança com idade inferior a 13 anos só é lícito se, e na medida em que, para tal o consentimento seja dado ou autorizado pelo progenitor ou pelo titular da guarda dessa criança.

[483] Castro, Catarina Sarmento e. (2005), *op. cit.*, p. 206.

[484] *Idem,* p. 207.

[485] *Idem,* pp. 206-207.

Por sua vez, Garcia Marques e Lourenço Martins indicam um conjunto de requisitos para que o consentimento se possa considerar esclarecido*:* "a) a informação, oral ou escrita, tem de exprimir-se em linguagem corrente; b) os elementos relevantes serão aqueles que um padrão médio de cidadão, no quadro que o caso concreta apresenta, julgaria necessários para tomar uma decisão; c) nos casos em que tal informação tenha sido fornecida ao responsável pelo banco de dados, a informação deve incluir elementos que, embora, em geral, possam ser irrelevantes, sejam importantes para o concreto titular de dados (...); d) entre o dever de informar e o dever de obter o consentimento, intercede o dever de averiguar se o interessado compreendeu as explicações; e) o consentimento informado tem de ser prestado para cada ato de tratamento de dados"[486].

O consentimento prestado pelo titular dos dados pessoais pode, em qualquer momento, ser revogado, nos termos do artigo 81.º do CC e não funciona em termos retroativos. A revogação do consentimento deve dar lugar à imediata destruição de dados e é lícita, embora o titular possa incorrer na obrigação de indemnizar os danos causados pela revogação[487].

O tratamento de dados pessoais contra ou sem o consentimento do seu titular constitui uma violação gravíssima dos direitos de personalidade, nomeadamente do direito à privacidade.

A Diretiva e, consequentemente, a LPDP visam proteger os direitos e a liberdade das pessoas no que diz respeito ao tratamento de dados pessoais através da aplicação de um leque de princípios orientadores que determinam a legitimidade desses tratamentos, estabelecendo limites estritos à recolha e à utilização de dados pessoais: princípio geral de transparência, princípio da finalidade, princípio da exatidão e atualização dos dados, princípio da licitude e lealdade, princípio da adequação, pertinência e proporcionalidade[488].

O princípio geral da transparência, estabelecido no Considerando 25 e no artigo 10.º da Diretiva 95/46/CE e no caso de Portugal no artigo 2.º da Lei da Proteção de Dados Pessoais, está intrinsecamente ligado aos direitos de acesso (artigo 10.º do mesmo diploma) e informação (artigo 11.º) do titular dos dados, e consequente dever do responsável em facultar tais informações, concretizando deste modo, o direito à autodeterminação informativa, impondo que

---

[486] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* p. 339.

[487] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* p. 250.

[488] Nesta parte *vide* Castro, Catarina Sarmento e. (2005), *op. cit.,* pp. 229-237, e Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* pp. 129 - 442.

em todo o processo de tratamento de dados pessoais, sejam facultados ao titular dos dados a identificação do responsável pelo procedimento, bem como indicadas as categorias de dados tratados juntamente com as finalidades do seu tratamento, período de conservação dos dados, eventuais comunicações dos mesmos a terceiros, além de qualquer outra informação que seja ou possa ser relevante ao titular para o exercício de seus direitos[489].

Ademais, o próprio dever de notificação à Comissão Nacional de Proteção de Dados Pessoais para efeitos de registo ou autorização de tratamentos de dados pessoais materializa também uma vertente desse princípio da transparência, precisamente nos artigos 18.º e 19.º da Diretiva 95/46/CE e artigo 10.º e 11.º da Lei de Proteção de Dados Pessoais[490]. Este princípio sofre, atualmente, violações constantes, sobretudo no que concerne às recolhas e tratamento invisíveis de dados pessoais sem a consciência pelo seu titular que especialmente possam ocorrer nos AmI. Nestes casos a captação das informações e o seu posterior tratamento são ilícitos face a este princípio.

O princípio da finalidade encontra-se plasmado na alínea b) do artigo 6.º da Diretiva 95/46/CE, na alínea b), n.º1 do artigo 5.º da Convenção 108 do Conselho da Europa e na alínea b), n.º1 do artigo 5.º da Lei n.º 67/98, de 26 de outubro, que estabelece que os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com as referidas finalidades (embora um processamento adicional dos dados para fins históricos, estatísticos ou científicos não seja considerado incompatível, desde que salvaguardas apropriadas sejam fornecidas pelos Estados-Membros e que tais garantias devam em especial impedir a utilização de dados em apoio de medidas ou decisões relativas a qualquer indivíduo em particular).

Este princípio também é designado como o princípio da limitação do uso de dados e como princípio da especificação dos fins.[491] A finalidade deve ser determinada e conhecida antes do início do tratamento e explícita, excluindo-se o tratamento de dados para fins pouco claros e vagos. Nos documentos de recolha de dados pessoais deve constar a descrição da finalidade da sua recolha e os objetivos do seu tratamento.

[489] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 229.

[490] *Idem, Ibidem.*

[491] *Idem*, p. 230.

Porém, em certas circunstâncias, é possível proceder ao tratamento dos dados recolhidos para um fim diverso daquele que foi determinado no momento da sua recolha, desde que seja compatível com a finalidade primordialmente definida perante a autorização da Comissão Nacional da Proteção de Dados Pessoais nos termos do artigo 28.º da Lei n.º 67/98. Cabe à CNPD a função de avaliar a compatibilidade e, sendo o caso, autorizar o tratamento para finalidade diversa[492].

De acordo com a alínea c), n.º1 do artigo 5.º da Lei n.º 67/98, de 26 de outubro e alínea c), n.º1 do artigo 6.º da Diretiva 95/46/CE os dados pessoais devem ser pertinentes, não excessivos e adequados em relação à finalidade para que são recolhidos e posteriormente tratados e a sua qualidade deve ser idónea para as finalidades daquele tratamento[493]. Do próprio dispositivo legal supra citado é possível verificar a existência de uma íntima ligação entre o primado em questão e o princípio da finalidade anteriormente referido.

Ademais, numa avaliação de pertinência, é preciso aferir a medida de utilização dos dados em relação à finalidade originária, excluindo-se o tratamento de informação que apesar de ser idónea não seja pertinente para a finalidade do tratamento.

No que concerne à proibição de excessos, a lei exige um juízo final para aferir se a extensão do tratamento realizado não extrapolará o estritamente necessário para aquela finalidade[494]. Este princípio de exatidão e atualização dos dados encontra-se previsto na alínea d), n.º1 do artigo 6.º da Diretiva e na alínea d), n.º1 do artigo 5.º da Lei de Proteção de Dados Pessoais e exige que os dados pessoais sejam exatos e, caso necessário, atualizados, determinando a adoção das medidas necessárias para a retificação ou eliminação de dados incompletos ou inexatos, sempre em função das finalidades da recolha e tratamento posterior. É importante que sejam realizadas atualizações periódicas destes dados armazenados conforme a necessidade para que os mesmos sejam fiéis à realidade.

O referido princípio obriga o responsável pelo tratamento de dados a corrigir informações incorretas ou obsoletos, bem como, sendo o caso, a apagar dados desnecessários ou impertinentes. Na medida em que a não atualização de dados obsoletos ou a manutenção de dados incompletos poderá causar sérios prejuízos ao seu titular (por exemplo, no caso da

[492] Castro, Catarina Sarmento e. (2005), *op. cit.,* pp. 230-231.

[493] *Idem*, p. 236.

[494] *Idem*, *ibidem.*

avaliação de crédito para a celebração de um contrato), decorre do princípio em causa, o correspondente direito ao titular dos dados de exigir do responsável pelo tratamento consoante o caso, a retificação, o apagamento ou o bloqueio dos dado cujo tratamento não cumpra o disposto na Diretiva, nomeadamente devido ao seu caráter incompleto ou inexato, nos termos do artigo 12.º, alínea b) da Diretiva e artigo 11.º, n.º 1, alínea d) da Lei de Proteção de Dados Pessoais.

O princípio da licitude e lealdade previsto na alínea a), n.º1 do artigo 6.º da Diretiva e na alínea a) do n.º1 do artigo 6.º da LPDP determina que os dados pessoais devem ser tratados de forma lícita e com respeito à boa-fé, ou seja, os dados devem ser recolhidos e tratados de forma transparente[495]: com o conhecimento do respetivo titular que tem direito a ser informado acerca da finalidade do tratamento e da identidade do responsável, vedando-se a recolha de dados por terceiros ou quando o titular dos dados não pode opor-se à sua recolha, facto que impediria o exercício da autodeterminação pelo indivíduo[496].

A licitude do tratamento é aferida pelo cumprimento dos normativos nacionais, comunitários, europeus e internacionais, estando ainda sujeito aos princípios gerais de direito, nomeadamente ao princípio da boa-fé[497].

Do corpo do artigo 6.º da Lei n.º 67/98 pode retirar-se um princípio de voluntariedade que legitima e constitui o fundamento para a recolha e o tratamento de dados pessoais[498]. Nos termos do artigo 6.º da Lei da Proteção de Dados Pessoais, o tratamento de dados pessoais só pode ter lugar quando exista uma condição de legitimidade que o fundamente, ou seja, o tratamento de dados pessoais é, em princípio, proibido, salvo se existir um fundamento legitimante. Deste modo, nos termos do artigo 6.º da LPDP o tratamento só pode ser efetuado se o seu titular tiver dado de forma inequívoca o seu consentimento ou se o tratamento for necessário para:

a) Execução de contrato ou contratos em que o titular dos dados seja part,e ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido, por

[495] *Idem*, p. 235.

[496] *Idem,* pp. 205-206.

[497] *Idem*, p. 235.

[498] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* pp. 246-247.

exemplo, no caso da solicitação de um cartão de crédito de um estabelecimento comercial ou contratação dos serviços de acesso á rede de telecomunicações, Internet;

b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito*, verbi gratia,* no âmbito do Direito do Trabalho o empregador é obrigado a comunicar os dados a outras entidades públicas relativas à segurança social ou para efeitos fiscais[499];
c) Proteção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento[500];
d) Execução de uma missão de interesse público ou no exercício de autoridade pública[501] em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados[502];
e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados[503];

Sendo exclusivamente as supra referidas as condições para a legitimidade do tratamento de dados pessoais.

Nos artigos 10.º a 13.º, a Lei n.º67/98 reconhece aos titulares de dados o direito de informação sobre os dados que lhe respeitem, o respetivo tratamento, caraterísticas e finalidade da base de dados e identidade do respetivo responsável (artigo 10.º), o direito de acesso aos

[499] Por vezes existe uma obrigação legal do responsável pelo tratamento de comunicar os dados pessoais a um terceiro, uma vez que a comunicação de dados é um tratamento, ou da obrigação de criação de uma base de dados, cabendo a CNPD a emissão de parecer sobre as disposições legais que exigem esse tratamento, nos termos do artigo 23.º, n.º1 alínea a) da LPDP. *Vide* Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 208.

[500] No entendimento de Catarina Castro e Sarmento, este fundamento abrange também as situações em que o titular de dados se encontra impedido de consentir, por exemplo quando está em estado de coma ou inconsciência, bem como quando o titular dos dados seja um menor e não for possível, em tempo útil, contactar o seu representante. *Vide* Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 210.

[501] Para maior esclarecimento *vide* Autorizações n.º11/97 e n.º51/99 da CNPD.

[502] A execução de interesse público pode ser atribuído igualmente a pessoas coletivas privadas que desempenham funções de interesse público, estando para o efeito investidas em poder de autoridade. *Vide* Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 212. Ademais, a utilização de dados pessoais por autoridades que atuam na esfera pública também está sujeita ao artigo 8.º da CEDH.

[503] *Vide* CNPD, *Parecer 22/2001 acerca da comunicação a terceiros de dados pessoais contidos na Base de Dados do Recenseamento Eleitoral,* de 2001. Disponível em: http://www.cnpd.pt/bin/orientacoes/ACESSO-BDRE-2001.pdf consultado a 16 de fevereiro de 2013.

dados em questão para seu conhecimento e eventual retificação (artigo 11.º) e o direito de oposição ao tratamento desses dados, entre outros[504].

O direito ao acesso aos dados, objeto de tratamento previsto no artigo 11.º da LPDP[505], é um direito à informação não sujeito a qualquer justificação por parte do titular, basta haver a intenção de consultar os dados que lhe dizem respeito[506].

Para além disso, o titular tem também direito a saber da finalidade do tratamento dos seus dados pessoais, se existe comunicação dos dados a outras entidades, e a maneira como foi realizado o tratamento ou as condições do mesmo. Tudo isto concretiza o direito à informação do titular dos dados (artigo 10.º da LPDP, igualmente consagrado no artigo 8.º, alínea a), da Convenção 108 do Conselho da Europa e no artigo 10.º e artigo 11.º da Diretiva 95/46/CE.

O titular goza ainda do direito ao apagamento dos dados, nos termos do artigo 5.º n.º1, alínea e), da LPDP[507]: os dados só devem ser tratados e conservados por um determinado período de tempo, exigindo-se a sua extinção ou apagamento aquando da expiração de certo prazo.[508] E este prazo tem de ser adequado às finalidades do tratamento

---

[504] Igualmente, no quadro da Diretiva 2002/58/CE são reconhecidos, entre os direitos e os deveres específicos deste setor, os seguintes: os deveres de adotar as medidas de segurança adequadas e de informar da falta de segurança (artigo 4.º, n.º 2); o direito à confidencialidade das comunicações (artigo 5.º); o direito à destruição dos dados de tráfego e à faturação (artigo 6.º); os direitos sobre a faturação (artigo 7.º); a identificação da linha chamadora e da linha conectada (artigo 8.º); o direito de oposição ao tratamento dos dados de localização (artigo 9.º); o direito de pôr termo ao reencaminhamento automático de chamadas (artigo 11.º); o direito a ser informado das finalidades a que se destinam as listas de assinantes impressas ou eletrónicas publicamente disponíveis (artigo 12.º); a proibição da prática do envio de correio eletrónico para fins de comercialização direta (artigo 13.º, n.º 4).

[505] Também consagrado no artigo 8.º, alínea b), da Convenção 108 do Conselho da Europa e no artigo 12.º da Diretiva 95/46/CE.

[506] Segundo Catarina Sarmento e Castro, o direito de acesso " traduz aquilo que expressivamente foi, em língua francesa, apelidado de «droit de regard», um direito de «olhar», ou seja, um direito de aceder às informações que lhe respeitem, para conhecê-las." *Vide* Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 247.

[507] Existe disposição com o mesmo sentido no artigo 8.º, alínea e), da Convenção 108 do Conselho da Europa e no artigo 6.º, n.º1, alínea e) e no artigo 12.º, alínea b) da Diretiva 95/46/CE.

[508] O direito a ser esquecido tem estado no centro da discussão sobre a reforma das regras europeias sobre a proteção dos dados pessoais desencadeada em 25 de janeiro de 2012 pela Comissão Europeia, nomeadamente no âmbito da proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados que foi, na sua última versão, aprovada pelo Parlamento Europeu em 12 de Março de 2014. O direito a ser esquecido prende-se com a possibilidade de pessoas gerirem melhor os riscos em matéria de proteção de dados em linha através da supressão definitiva dos seus dados das páginas da Internet e das referências aos mesmos feitas por motores de busca caso não existirem motivos legítimos para a sua conservação, o que conduz à implementação do chamado "direito ao apagamento" dos dados nos termos do artigo 17.º da proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. O artigo 17.º confere ao titular de dados o direito a ser esquecido, desenvolve e especifica mais detalhadamente o direito ao apagamento consagrado no artigo 12.º, alínea b) e no artigo 6.º, n.º1, alínea e) da Diretiva 95/46/CE e no artigo

dos dados, sendo definindo pela Comissão Nacional da Proteção de Dados, tendo em conta cada finalidade, nos termos do artigo 23.º, n.º1, alínea f) da LPDP.

Para além disso, o titular dos dados tem ainda o direito à retificação dos dados inexatos ou incompletos, e também à atualização dos mesmos, não dependendo da iniciativa do titular, mas é antes um dever que impende sobre o responsável pelo tratamento dos dados, alínea d) do n.º1 do artigo 11º. De acordo com Catarina Sarmento e Castro é a própria qualidade dos dados pessoais que exige a garantia desse direito, nos termos do artigo 5.º, n.º1, alínea d), primeira parte da LPDP que determina que os dados pessoais devem ser "exatos e, se necessário, atualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos"[509].

A LPDP no seu artigo 13.º ainda prevê o direito de não ficar sujeito a uma decisão individual automatizada[510], ou seja, uma decisão que produza efeitos na esfera jurídica do destinatário e que seja tomada exclusivamente com base na avaliação automatizada de certos aspetos, como, por exemplo, a solvabilidade para a concessão de crédito pessoal bancário, ou a rejeição de um candidato com base apenas nos testes de avaliação psicotécnicos computadorizados, sem qualquer intervenção humana[511].

Contudo, nos termos do mesmo artigo 13.º, n.ºs 2 e 3[512], esta proibição não é, apesar de tudo, absoluta, uma vez que os dados armazenados de forma automatizada também podem ajudar a chegar a uma certa decisão, i.e., o que se proíbe é que os sistemas informáticos e os dados que estes armazenam sejam os exclusivos responsáveis

---

5.º n.º1, alínea e), da LPDP. *Vide* Parlamento Europeu, *Resolução legislativa, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, op.cit.* No mesmo sentido sobre o direito ao esquecimento *vide* Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 1/2012 sobre as propostas de reforma em matéria de proteção de dados*, (00530/12/PT WP 191), adotado em 23 de março de 2013, pp.14-15. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_pt.pdf consultado a 2 de fevereiro de 2013. A questão relacionada com o direito ao esquecimento será igualmente discutida no próximo ponto 3.3.1.

[509] Castro, Catarina Sarmento e. (2005), *op. cit.,* pp. 250-251.

[510] Previsto no artigo 15.º da Diretiva 95/46/CE.

[511] Sobre esta questão *vide* Castro, Catarina Sarmento e. (2005), *op. cit.,* pp. 251-253.

[512] Garcia Marques e Lourenço Martins não concordam com as referidas exceções argumentando que, "o princípio da «justiça» -que encontra normal aplicação no tocante ao exercício de poderes discricionários e no quadro da chamada «discricionariedade técnica» - exige o respeito do critério do «exame individual», não sendo compatível com qualquer procedimento exclusivamente baseado no tratamento automatizado de dados", o que leva, na opinião dos autores " a inaplicabilidade das referidas exceções na medida em que possa relevar o princípio da Justiça, consagrado no artigo 266.º, n.º2, da Constituição". Cf. Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.,* p. 360.

pela decisão[513]. Caso contrário estar-se-ia a comprometer o contraditório e que certas caraterísticas e/ou circunstâncias específicas também fossem tidas em conta. De qualquer forma, desde que se garanta a defesa de interesses legítimos dos titulares de dados este processo automatizado não é necessariamente inviabilizado, basta que se assegure a maneira de as pessoas terem conhecimento da lógica subjacente ao tratamento dos dados autonomizados que lhe digam respeito e trazer à decisão o seu ponto de vista pessoal[514].

Também no artigo 12.º encontra-se previsto o direito de oposição ao tratamento dos seus dados (*v.g.,* à sua recolha ou à sua comunicação)[515]: tanto com base em razões preponderantes e legítimas relacionadas com a sua situação particular, bem como infundadamente (sem ter de o justificar), de forma gratuita e, em qualquer altura, sempre que o tratamento de dados tenha a finalidade de *marketing* direto[516].

O tratamento de um determinado tipo de dados está constitucionalmente proibido no n.º3 do artigo 35.º da CRP: "A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica", sendo tal limitação reafirmada pelo n.º 1 do artigo 7.º da LPDP que diz que é proibido o tratamento de dados sensíveis, ali qualificados como dados pessoais relativos a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, inclusive dados genéticos[517].

Os dados sensíveis, por serem suscetíveis de denunciar aspetos mais íntimos da vida privada de seu titular e em função dos valores envolvidos, geralmente, não podem ser submetidos ao tratamento; tal proibição serve para evitar eventual conduta discriminatória[518, 519].

---

[513] Como exemplo podem ser referidos os sistemas periciais e os sistemas de suporte à decisão, que já foram abordados no ponto 1.2.4.1.

[514] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 253.

[515] Artigo 14º da Diretiva 95/46/CE.

[516] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 254.

[517] *Idem,* p. 89, nota 158.

[518] *Idem*, *ibidem.*

[519] Neste sentido Garcia Marques e Lourenço Martins: "Em regra, a doutrina mostrou-se pouco disposta a definir um tal conjunto de dados, por entender que tais dados, quaisquer que sejam, não são sensíveis em si mesmos, mas sim em função do contexto em que são usados." *Vide* Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.* p. 337.

No entanto, as aplicações dos ambientes inteligentes possuem potencial para alterar a natureza dos dados envolvidos o que levanta várias questões, uma vez que é possível, em alguns casos através da coleta e análise de dados não sensíveis, especialmente se conjugado com outros elementos que possam induzir caraterísticas, preferências, opiniões políticas, crenças religiosas, estado de saúde, etc., chegar as informações altamente sensíveis, que deverão, obviamente, merecer o mesma proteção prevista no n.º 1 do artigo 7.º da LPDP[520].

Conforme o que foi dito supra, o tratamento de dados sensíveis é constitucionalmente proibido por força do n.º3 do artigo 35.º da CRP. No entanto, o mesmo dispositivo constitucional acima mencionado prevê a excecionalidade do tratamento de dados sensíveis em alguns casos, mediante o consentimento expresso do titular ou autorização prevista em lei, sempre com garantias de não discriminação, ou para processamento com escopo estatístico, mediante o uso de dados que não permitam a identificação do respetivo titular.

Por sua vez, a LPDP, no n.º2 do artigo 7.º, permitiu o tratamento de dados sensíveis, mediante disposição legal ou autorização da CNPD, quando por motivos de "interesse público" importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º[521].

Deste modo, o n.º2 do artigo 7.º da LPDP veio posicionar ao lado da autorização por disposição legal, a autorização da CNPD, o que para alguns autores pode configurar uma norma de constitucionalidade duvidosa, especialmente tendo em conta o artigo 35.º n.º 3 da CRP que admite enquanto fundamento legitimante do tratamento de dados sensíveis o consentimento expresso do titular e a autorização prevista por lei[522]. Neste sentido, Garcia Marques e Lourenço Martins apontam para "o facto de a Constituição da República ter previsto que a lei pudesse autorizar o tratamento dos dados mais sensíveis, não habilitava a lei ordinária (de proteção de dados) a alargar tal faculdade- sempre excecional e sujeita a condições (garantias de não

[520] De Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., & Fuster, G. G. (2009). Legal safeguards for privacy and data protection in ambient intelligence. *Personal and ubiquitous computing*, *13* (6), 435-444, pp. 439-440. DOI 10.1007/s00779-008-0211-6.

[521] Marques, José A. S. Garcia, Martins, Lourenço. (2006), *op. cit.* pp. 348-349.

[522] *Idem*, p. 348.

discriminação e medidas de segurança adequadas) - a uma simples autorização administrativa da autoridade do controlo"[523]. O que leva Catarina Sarmento e Castro a concluir sobre a inadmissibilidade de considerar "a intervenção da CNPD, em si mesma, isoladamente, sem o consentimento, como fundamento legitimante de tratamento de dados sensíveis, ainda que se descortinasse um interesse público importante e indispensável", sendo indispensável para o efeito "a existência de duas (leis e consentimento) e não três, as fontes legitimadoras do tratamento de dados sensíveis"[524].

Como já foi referido antes, no caso de se tratar de dados sensíveis o consentimento deve ser, de acordo com artigo 7.º, n.º2 da LPDP, expresso e redigido por escrito conforme o entendimento da CNPD[525], bem como ser uma manifestação de vontade livre, específica e informada, conforme a exigência do artigo 3.º, alínea h) da LPDP. A CNPD deverá verificar as condições em que é dado o consentimento do cidadão, bem como deverá avaliar a existência do mesmo interesse público e prossecução das atribuições legais ou estatuárias do responsável[526].

Acrescente-se que o tratamento de dados sensíveis é ainda permitido nos casos expressamente previstos nas alíneas do n.º3 do artigo 7.º:

a) Mediante disposição legal ou autorização de Comissão, pode ser permitido o tratamento de dados sensíveis " quando por motivos de interesse público importante esse tratamento for indispensável ao exercício de atribuições legais ou estatutários do seu responsável ", "com garantias de não discriminação" e com medidas de segurança;

b) Quando o titular dos dados tiver dado o seu consentimento expresso para o seu tratamento, "com garantias de não discriminação" e com medidas de segurança;

c) Ser necessário para proteger interesses vitais do titular dos dados ou de uma ou outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;

d) Ser efetuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas atividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às

---

[523] *Idem*, p. 350.

[524] Castro, Catarina Sarmento e. (2005), *op. cit*, p. 219.

[525] *Vide* a Autorização n.º45/96 e a Autorização n.º17/96, ambas publicadas no relatório da CNPDI, de 1996.

[526] Castro, Catarina Sarmento e. (2005), *op. cit.*, p. 221.

pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;

e) Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;

f) Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efetuado exclusivamente com essa finalidade.

No n.º4 do artigo 7.º a LPDP prevê uma exceção à proibição de tratamento de dados sensíveis referentes à saúde e à vida sexual, incluindo os dados genéticos, sendo, no entanto, permitido quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde. Contudo, segundo a lei, o tratamento desses dados deve se efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional e notificado à Comissão nos termos da lei, bem como devem ser garantidas medidas adequadas de segurança da informação.

Igualmente, a Lei n.º67/98 autonomiza, no artigo 8.º, o que pode ser denominado como dados de justiça, relativa a pessoas suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias. De acordo com Pedro Pais de Vasconcelos só podem ser criados e mantidos registos centrais destes dados por serviços públicos com competência específica em rigorosa observância das normas de proteção de dados pessoais mediante prévio parecer da CNPD, podendo ser objeto de tratamento mediante a sua autorização, quando tal for indispensável à execução de finalidades legítimas do seu responsável[527]. Para além disso, o autor sublinha que o tratamento de dados pessoais para fins de investigação "deve limitar-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infração determinada, para o exercício de competências previstas no respetivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que Portugal seja parte"[528].

[527] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* p. 248

[528] *Idem, ibidem.*

A privacidade é igualmente garantida pela segurança de dados, sendo uma obrigação legal do responsável pelo tratamento de dados pessoais nos termos do artigo 14.º da LPDP, que o obriga à adoção de mecanismos de garantia preventivos e atuações da solução[529].

De acordo com a lei o responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, garantindo a sua confidencialidade, i.e., segundo Catarina Castro e Sarmento "garantia da segurança traduz-se na salvaguarda da informação, mas também na manutenção da sua integridade, através da adoção de medidas que impeçam a alteração dos dados, que permitam detetar disfuncionalidades e corrigí-las"[530].

As garantias de segurança das informações podem ser relativas à segurança física das instalações ou aos mecanismos de segurança implementados no próprio sistema[531, 532]. No caso da segurança física das instalações, como exemplo pode ser apontado o acesso restrito de pessoas às instalações ou a existência de alarme de segurança e de controlo. Quanto aos mecanismos de segurança implementados no próprio sistema, é indispensável a existência de palavra-passe de acesso às informações, cópias de segurança dos dados[533], bem como deve ser feito o recurso às técnicas de encriptação e anonimato[534]. Ademais, o sistema deverá permitir a identificação de qualquer acesso ou intromissão de dados[535].

A LPDP estabelece, ainda, em seu artigo 15.º, um conjunto de medidas especiais para garantir a segurança no tratamento de dados sensíveis e dos dados referidos no n.º 1 do artigo 8.º, devendo o responsável pelo tratamento dos dados tomar as medidas adequadas para: impedir o acesso de pessoa não autorizada às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações); impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados); impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção); impedir que

[529] Castro, Catarina Sarmento e. (2005), *op. cit,* p. 267.

[530] *Idem, ibidem.*

[531] Ver o ponto seguinte 3.3.5. sobre o reforço da segurança e controlo sobre dados pessoais através do recurso à tecnologia.

[532] Castro, Catarina Sarmento e. (2005), *op. cit,* p. 267-268.

[533] "*backup"* em inglês.

[534] Sobre anonimato ver o ponto 3.3.2.

[535] Castro, Catarina Sarmento e. (2005), *op. cit,* pp. 268-269.

sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização); garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso); garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão); garantir que possa verificar-se *a posteriori*, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada setor, quais os dados pessoais introduzidos quando e por quem (controlo da introdução); impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

A Lei de Proteção de Dados Pessoais deve ser interpretada, integrada e concretizada com respeito pelo direito de personalidade e sempre que for preciso decidir quanto à recolha, tratamento, interconexão ou transferência de dados pessoais sem existência do consentimento expresso do seu titular, não bastará que a dispensa de prévio consentimento expresso encontre o seu fundamento formal nas disposições da LPDP[536]. Deste modo, segundo Pedro Pais de Vasconcelos "quando estejam em causa direitos de personalidade, designadamente o direito à privacidade, será necessário encontrar para tal prática o fundamento de ordem pública, uma necessidade insuperável de interesse coletivo, que não permita uma solução alternativa e que justifique em termos éticos uma tal agressão. Quando assim for, todavia, a agressão necessária deverá ser a mais limitada possível, de modo a reduzir ao mínimo a lesão do direito à privacidade"[537].

3.3. Privacidade e proteção de dados pessoais nos AmI: possíveis soluções

A introdução das tecnologias de informação e comunicação e, nomeadamente, dos AmI no quotidiano, acompanhado pelo crescimento exponencial de comunicação em linha, comércio e serviços eletrónicos, que vão além das fronteiras territoriais dos Estados-Membros, deram

[536] Vasconcelos, Pedro Pais de. (1999), *op. cit.,* p. 253.

[537] *Idem, ibidem.*

origem a inúmeras iniciativas de segurança nacionais e internacionais com um impacto de longo alcance sobre os direitos humanos.

O desenvolvimento das novas tecnologias, especialmente dos ambientes inteligentes, apesar de proporcionar inúmeros benefícios que já foram referidos nos capítulos anteriores, apresenta um enorme desafio para a privacidade, na medida em que fomenta o aumento da vigilância e da recolha invisível de dados pessoais.

É importante avaliar a adequação do quadro legal da proteção de dados pessoais vigente na União Europeia face aos desafios levantados pelos ambientes inteligentes.

3.3.1. Direito ao esquecimento

A discussão sobre a reforma da legislação comunitária sobre proteção de dados pessoais levantou uma série de questões muito relevantes, uma das quais prende-se, por exemplo, com a possibilidade de pessoas gerirem melhor os riscos em matéria de proteção de dados em linha através da supressão definitiva dos seus dados das páginas da Internet e das referências aos mesmos feitas por motores de busca, caso não existam motivos legítimos para a sua conservação, o que conduz à implementação do chamado "direito a ser esquecido" dos dados nos termos do artigo 17.º da Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos (regulamento geral sobre a proteção de dados).

Esta questão torna-se particularmente relevante quando se percebe que a Internet tende a gravar tudo e a esquecer nada. O artigo 17.º confere ao titular de dados o direito a ser esquecido, desenvolve e especifica mais detalhadamente o direito ao apagamento consagrado no artigo 12.º, alínea b), da Diretiva 95/46/CE, e prevê as condições do direito ao esquecimento, nomeadamente o dever do responsável pelo tratamento que tornou públicos os dados pessoais de informar terceiros sobre o pedido da pessoa em causa de apagamento de quaisquer ligações para esses dados, ou cópias ou reproduções que tenham sido efetuadas. Em Portugal, segundo a Lei n.º 67/98 o titular de dados pessoais detém o direito ao apagamento,

que impõe que os dados sejam conservados apenas durante o período estritamente necessário aos fins para os quais foram recolhidos.

Em termos práticos, a polémica do direito a ser esquecido gira em torno da questão da concessão (ou não) aos utilizadores de Internet da possibilidade de exclusão de dados pessoais (como imagens, textos, opiniões, documentos oficiais, certidões e quaisquer outros tipo de dados pessoais capazes descrever ou referir comportamentos e ações passadas, etc.), a partir das listas de resultados apresentadas pelos motores de busca, *sites*, redes sociais, *blogs*, etc., independentemente de tal disponibilização ter sido autorizada ou até mesmo efetuada pelo próprio titular. Tendo em conta o que foi dito anteriormente sobre a proliferação de dados no cenário dos ambientes inteligentes, a questão da admissibilidade de um direito a ser esquecido torna-se pertinente. O facto de os dados pessoais serem públicos não significa que os requisitos da diretiva sobre proteção de dados não se apliquem. Pelo contrário: mesmo depois de serem tornados públicos, os dados pessoais não deixam de ser pessoais e, consequentemente, os titulares não podem ser privados da proteção a que têm direito no que toca ao tratamento dos seus dados, direito este consagrado constitucionalmente no artigo 35.º da CRP[538, 539].

Em relação à articulação entre o direito a ser esquecido e outros direitos, é importante ter em atenção que o interesse (privado) e o direito ao apagamento de dados precisam de ser equilibrados com outros direitos concorrentes e interesses importantes. Este é o caso do interesse público e social de acesso à informação (direito à informação), o direito à liberdade de expressão e da necessidade de preservar a memória coletiva e histórica.

Além disso, e em casos particulares, é importante reconhecer que o direito a ser esquecido não deve prevalecer sempre. O direito ao esquecimento também poderá enfrentar dificuldades quando estão em causa determinados membros da sociedade (políticos, figuras públicas), cuja transparência é importante do ponto de vista da democracia.

---

[538] Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 3/1999 no que diz respeito ao tratamento de dados pessoais relativo a informação do sector público e proteção de dados pessoais. Contribuição para a consulta iniciada com o Livro Verde da Comissão Europeia intitulado "Informação do sector público: um recurso fundamental para a Europa",* (COM (1998) 585 WP 20), adotado em 3 de maio de 1999. Disponível em:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp20pt.pdf consultado a 5 de novembro de 2013.

[539] Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 2/2003 sobre a aplicação dos princípios de proteção de dados às listas Whois,* (10972/03/PT final WP 76), adotado em 13 de junho de 2003. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_pt.pdf consultado a 5 de novembro de 2013.

Tradicionalmente ligado ao direito à privacidade, a questão do esquecimento também tem uma forte ligação com o direito à identidade. O direito a ser esquecido pode desenvolver um papel extremamente importante ao permitir a um indivíduo reconstruir a sua identidade, conferindo a possibilidade de ter partes da nossa identidade apagada, tornando-as indisponíveis ao público[540]. Deve-se levar em consideração que, ao contrário dos outros direitos de personalidade, a identidade pessoal sofre alterações com a evolução e o envelhecimento da pessoa, apresentando um caráter mutável.

Neste sentido, o direito a ser esquecido - como parte do direito à identidade pessoal - está intimamente ligado à capacidade de se reinventar e de ter oportunidade de iniciar de novo e apresentar uma identidade renovada para o mundo, impedindo que ela seja deturpada, mal representada ou falsificada[541]. Como tal, o direito ao esquecimento parece encontrar uma raiz normativa adequada no direito à identidade pessoal. O direito a ser esquecido é, portanto, um importante instrumento jurídico que serve para reconstruir a identidade, permitindo que um indivíduo se recrie, exercendo um maior controlo sobre a própria identidade.

Neste sentido, a enunciação taxativa das informações que poderão ser do conhecimento público e o estabelecimento de limites temporais definitivos à sua divulgação constituem bons pontos de partida para contrariar a constatação feita pela comissária europeia Viviane Reding de que "Deus perdoa e esquece, mas a Internet não"[542].

Recentemente, o Tribunal de Justiça da União Europeia proferiu um acórdão inédito[543] no âmbito do processo C-131/12, dando razão a um cidadão espanhol, M. Costeja González, que

---

[540] Andrade, Norberto Nuno Gomes de. (2011), *op. cit.,* p. 90: "Being traditionally connected to the right to privacy, the issue of forgetfulness also bears an important association with the right to identity. Recurring again to the idea and metaphor of personal identity as narrative, the question that lies beneath the right to oblivion is the possibility of having parts of our identity narrative erased, preventing them from being accessed and acknowledged by the larger public."

[541] *Idem,* p. 91: "In this sense, the right to be forgotten – as part of the right to personal identity – is intimately connected to the ability to reinvent oneself, to have a second chance to start-over and present a renewed identity to the world. As such, the right to oblivion seems to find an appropriate normative root in the right to personal identity."

[542] Tradução nossa. *"*God forgives and forgets but the Web never does!" - *vide* discurso de Reding, Viviane. (16 de março de 2011). Your Data, Your Rights: Safeguarding Your Privacy in a Connected World. *Press Releases Database of the European Commission***.** Disponível em: http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm consultado a 9 de maio de 2013.

[543] Acórdão do Tribunal de Justiça da União Europeia (Grande Secção) de 13 de maio de 2014 no Processo C-131/12. Coletânea geral, *Google Spain SL, Google Inc. contra Agência Espanhola de Proteção de Dados, Mario Costeja González.* Disponível em:

em 2010 apresentou na Agência Espanhola de Proteção de Dados, AEPD *(Agencia Española de Protección de Datos)* uma reclamação contra a "*La Vanguardia Ediciones SL"* (editor de um jornal diário de grande tiragem em Espanha, designadamente na região da Catalunha) e contra a *Google Spain* e a *Google Inc.,* alegando que, quando um internauta inseria o seu nome no motor de busca do grupo *Google («Google Search»),* a lista de resultados exibia ligações para duas páginas do jornal diário da "*La Vanguardia"*, datadas de janeiro e março de 1998, que anunciavam, designadamente, uma venda de imóveis em hasta pública organizada na sequência de um arresto destinado a cobrar as dívidas de M. Costeja González à Segurança Social. Com esta reclamação, Costeja González quis apagar da Internet a referência a esse acontecimento da sua vida.

O Tribunal considerou que o direito ao apagamento dos dados e direito de oposição ao tratamento dos mesmos, já existentes na Diretiva 95/46/CE, devem ser interpretados no sentido de o operador de um motor de busca ser obrigado a suprimir da lista de resultados de uma pesquisa feita com o nome de uma pessoa, as ligações a outras páginas publicadas por terceiros com informações sobre essa pessoa[544].

O Tribunal sublinhou que o tratamento de dados pessoais realizado por um operador de um motor de busca permite a qualquer internauta, quando realiza uma pesquisa a partir do nome de uma pessoa singular, obter, com a lista de resultados, uma visão global e estruturada das informações sobre essa pessoa na Internet. Ademais, o Tribunal salientou que essas informações podem referir-se a numerosos aspetos da vida privada que, sem o motor de busca, não poderiam ou só muito dificilmente poderiam ter sido relacionadas, permitindo, deste modo, aos internautas estabelecer um perfil mais ou menos detalhado das pessoas alvo de pesquisas.

Para além disso, segundo o mesmo Tribunal o efeito de ingerência nos direitos da pessoa é multiplicado devido ao importante papel desempenhado pela Internet e pelos motores de busca na sociedade moderna, que conferem o caráter de ubiquidade às informações contidas nas listas de resultados.

---

http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd893c7971ed634404b9dbce9953fc6761.e34KaxiLc3qMb40Rch0SaxuNbxf0?text=&docid=152065&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=140038 consultado a 3 de junho de 2014.

[544] Depois da decisão do Tribunal de Justiça da União Europeia o motor de busca Google, até a data de hoje, já recebeu mais de 182 mil pedidos de cidadãos europeus que pretendem exercer este direito. *Vide* Google. *Relatório de transparência*. Disponível em: https://www.google.com/transparencyreport/removals/europeprivacy/ consultado a 8 de dezembro de 2014.

A Jurisprudência afirmada por esta decisão torna-se especialmente relevante numa altura em que decorre a reforma da legislação na União Europeia em matéria de proteção de dados pessoais. O direito a ser esquecido tem estado no centro da discussão da proposta de Regulamento Geral de Proteção de Dados e, na sua última versão RGPD (tal como foi aprovado pela Comissão das Liberdades Cívicas, Justiça e dos Assuntos Internos em outubro de 2013), aprovada em março de 2014 pelo Parlamento Europeu, até a sua designação foi alterada para "direito ao apagamento de dados"[545], que se traduz no direito a obter do responsável pelo tratamento o apagamento dos dados pessoais que lhe digam respeito e a comunicação ulterior desses dados – nada de novo, portanto –, e ainda de obter de terceiros o apagamento de quaisquer ligações para esses dados pessoais, cópias ou reproduções dos mesmos sempre que: os dados deixarem de ser necessários em relação à finalidade que motivou a sua recolha ou tratamento[546]; o titular dos dados retire o consentimento sobre o qual é baseado o tratamento, ou se o período de conservação consentido tiver terminado e não existir outro fundamento jurídico para o tratamento dos dados[547]; se o titular dos dados se opuser ao tratamento de dados pessoais[548] ou se os dados forem tratados ilicitamente[549].

3.3.2 Anonimato

A principal diferença entre as aplicações de rede existentes e aplicações emergentes baseadas nos sistemas de AmI consiste, em primeiro lugar, na possibilidade do utilizador, no caso das aplicações de rede, ter conhecimento do tipo de dados que estão a ser recolhidos em relação a ele e, em segundo lugar, ter acesso a alguns meios para limitar essa mesma captação de dados: por exemplo, o utilizador pode aceder a certas páginas da Internet de forma anónima através do computador público, pode desligar o telemóvel, pode pagar em dinheiro, em vez de usar o cartão de crédito ou o pagamento via Internet, etc..

---

[545] Artigo 17.° de RGPD.

[546] Artigo 17.°, n.° 1, alínea a) de RGPD.

[547] Artigo 17.°, n.°1, alínea b) de RGPD.

[548] Artigo 17.°, n.°1, alínea c) de RGPD.

[549] Artigo 17.°, n.°1, alínea d) de RGPD.

Enquanto no caso dos sistemas de AmI as pessoas estão perante um ambiente cheio de sensores invisíveis, tornando difícil, se não impossível, para o utilizador ter conhecimento e controlar a recolha de dados, bem como alcançar o anonimato. O processamento dos dados através do recurso aos algoritmos de raciocínio inteligente, limitando o cruzamento de dados e o controlo de acesso aos dados recolhidos, parece ser uma das principais formas de proteção da privacidade em tais aplicações. O uso de diferentes identidades com o mínimo de dados pessoais em cada aplicação ajuda a prevenir a descoberta, a ligação/correlação entre a identidade do utilizador e os seus dados pessoais, bem como entre as diferentes ações do mesmo utilizador[550, 551].

Contudo, o anonimato ainda é capaz de garantir um considerável nível de opacidade do indivíduo, uma vez que consiste na possibilidade de usar um recurso ou serviço sem divulgação da identidade do utilizador. Os dados consideram-se anonimizados se todos os elementos de identificação tiverem sido eliminados de um conjunto de dados pessoais: não pode ser deixado nas informações nenhum item que possa servir, exercendo um esforço razoável, para reidentificar a pessoa em causa[552]. Quando os dados são eficazmente anonimizados, deixam de ser dados pessoais.

Por sua vez, a Directiva 95/46/CE no seu artigo 6.º, n.º 1, al. e) e a Convenção 108 no artigo 5.º, al. e) permitem, nos casos em que os dados pessoais deixam de servir a sua finalidade inicial, que estes sejam conservados sem anonimização para fins históricos, estatísticos ou científicos, desde que sejam aplicadas garantias adequadas contra a sua utilização abusiva.

O anonimato pode ser visto enquanto manifestação do direito à reserva da intimidade da vida privada, protegido nos termos do disposto no artigo 26.º da CRP. Garcia Marques considera

---

[550] Sobre direito a identidades múltiplas falou-se no ponto 2.3.

[551] Relacionados com o problema de anonimato na Internet apresentam-se dois interessantes artigos de Frances M. T. Brazier que discutem a possibilidade de aplicação de técnicas de anonimato a agentes de *software* no âmbito de comércio eletrónico e nas aplicações de governação eletrónica do ponto de vista jurídico e técnico. *Vide* Brazier, F., Oskamp, A., Prins, C., Schellekens, M., & Wijngaards, N. (2003). Are Anonymous Agents Realistic? In A. Oskamp, E. Weitzenböck (Eds.), *Proceedings of the LEA 2003: The Law and Electronic Agents* (pp. 69-79). Oslo: Unipub. Disponível em: http://www.iids.org/publications/lea03_anonymity.pdf consultado a 3 de fevereiro de 2013, e Brazier, F., Oskamp, A., Prins, C., Schellekens, M., & Wijngaards, N. (2004). Anonymity and Software Agents: An Interdisciplinary Challenge. *Artificial Intelligence and Law*, *12*(1-2), 137-157. Disponível 2013 em:http://link.springer.com/article/10.1007/s10506-004-6488-5#page-1 consultado a 3 de fevereiro de 2013.

[552] Considerando 26 da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.

que o anonimato é um direito ligado a direitos constitucionais, como a liberdade de expressão (artigo 37.º da CRP), o sigilo da correspondência e das comunicações (artigo 34.º da CRP e artigos 75.º a 78.º do Código Civil)), entre outros[553]. Segundo o autor "o anonimato, além de garantir a intimidade, reforça a liberdade de expressão, uma vez que os utilizadores podem participar livremente na rede sem receio de que os seus rastos sejam seguidos"[554].

O direito ao anonimato das comunicações e o correspondente dever de confidencialidade que poderá limitar qualquer forma de interceção ou vigilância por quem não seja o remetente ou o destinatário, salvo esteja expressamente prevista na lei[555]. O Grupo de Proteção de Dados do Artigo 29º considerou anonimato como uma importante salvaguarda para o direito à privacidade[556]. O Grupo referiu que a capacidade de poder optar pelo anonimato é essencial para que as pessoas possam dispor da mesma proteção em termos de privacidade em linha que a atualmente disponível fora de linha[557]. Porém, o Grupo do Artigo 29º sublinha que o anonimato não se justifica em todas e quaisquer circunstâncias: "A definição das circunstâncias em que se justifica a "opção do anonimato" e aquelas em que sucede o inverso requer uma ponderação cuidadosa dos direitos fundamentais em jogo, não apenas em matéria de privacidade como também a nível da liberdade de expressão, juntamente com outros objetivos políticos importantes como a prevenção do crime"[558]. Por sua vez, as eventuais restrições jurídicas em matéria de direito ao anonimato devem ser sempre proporcionadas e restringir-se ao necessário para proteger u interesse público específico numa sociedade democrática.

As modalidades de acesso anónimo à Internet (por exemplo, espaços públicos da Internet, cartões de pré-pagamento) e os meios de pagamento anónimos são dois elementos essenciais para assegurar o anonimato efetivo em linha. O Grupo do Artigo 29º defende que deve ser possível o envio de correio eletrónico, a consulta passiva de sítios na *World Wide Web* e a aquisição da maioria dos bens e serviços através da Internet de forma anónima.[559]

---

[553] Marques, J. A. G. (2004), *op. cit.*, pp. 61-62.

[554] *Idem*, p. 62.

[555] *Idem, Ibidem.*

[556] Article 29 Data Protection Working Party, *Recommendation 3/97: Anonymity on the Internet,* (XV D /5022/97 final WP 6), adotado em 3 de dezembro de 1997, p.6. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf consultado a 15 de maio de 2013.

[557] *Idem*, p.12.

[558] *Idem, ibidem.*

[559] *Idem, ibidem.*

Torna-se necessária a existência de um certo controlo no que diz respeito às pessoas que contribuem com material em linha para as instâncias públicas (*"newsgroups"* ou fóruns, etc.), mas a imposição de um requisito no sentido de que as pessoas se identifiquem é, segundo a opinião do Grupo do Artigo 29º, em muitos casos, desproporcionado e inexequível, argumentando que "os direitos fundamentais à privacidade e de liberdade de expressão não devem ser restringidos de forma desproporcionada através de sistemas de identificação obrigatória, nomeadamente, sempre que existam outros meios mais proporcionados de controlar e moderar o conteúdo do material assim divulgado"[560].

A intervenção sob anónimato pode assumir uma dupla face: se, para o utilizador, pode representar uma defesa, preservando a "liberdade de expressão", o certo é que, para terceiros, a navegação com ocultação da identidade pode ser fonte de riscos acrescidos, sendo também fonte de maiores dificuldades para a investigação policial. Daí que o anonimato apresente problemas jurídicos, uma vez que permite ocultar a identidade na rede daqueles que cometem infrações por este meio[561].

Contudo, parece ser inegável a legitimidade de as pessoas poderem proteger a sua privacidade com recurso às técnicas do anonimato, evitando que os dados pessoais sejam alvo de tratamento e armazenamento em ficheiros automatizados de dados pessoais para finalidades desconhecidas e sem consentimento dos seus legítimos titulares[562].

Hugo Lança Silva reconhece a necessidade da existência do anonimato, mas sublinha que este não é um direito absoluto, antes deve ser analisado de acordo com o caso concreto: "decorrente da privacidade individual, urge reconhecer um verdadeiro direito ao anonimato na rede, permitindo a utilização lícita na rede alicerçada em qualquer pseudónimo criado especificamente para o efeito", contudo, "o anonimato, a defesa da privacidade não pode ser entendido como um valor absoluto, mas, como tudo na vida e no Direito, de ser relativizado em

---

[560] *Idem,* p.9.

[561] Marques, J. A. G. (2004), *op. cit.,* p. 42.

[562] Veiga, A., Rodrigues, B. S. (2007). A monitorização de dados pessoais de tráfego nas comunicações eletrónicas. *Raízes Jurídicas*, *3* (2), 59-110, p.83. Disponível em: http://www.estig.ipbeja.pt/~ac_direito/monitorizacao.pdf consultado a 5 de janeiro de 2014.

cada caso concreto, de forma a arquitetar a consagração de uma solução justa"[563]. Neste sentido, o autor afirma que o anonimato encontra a sua base legal no direito à privacidade, bem como na defesa dos direitos da personalidade do individuo[564]. Por outro lado, Hugo Lança Silva considera não só possível mas também necessário compatibilizar privacidade, o anonimato e a responsabilização: "no que diz respeito à trilogia da privacidade – anonimato – responsabilização impõe-se o reconhecimento da sua compatibilidade. Pessoalmente, reiteramos o que sempre sublinhamos: a defesa da privacidade do utilizador da Internet tem de ser superiormente protegida"[565].

No entanto, o anonimato pode inviabilizar a responsabilização pelos atos ilícitos realizados na rede, uma vez que torna difícil determinar o agente do crime[566]. O anonimato é já uma necessidade reconhecida no uso da Internet, "mas quando sai do âmbito do direito à reserva da vida privada e entra na impossibilidade de punição dos atores dos atos ilícitos, é abdicável"[567].

Neste caso, torna-se importante referir a legislação que regula a responsabilidade dos prestadores de serviços em rede [568]. Exemplo disso é o Decreto-Lei n.º 7/2004, de 7 de janeiro, alterado pelo Decreto-Lei n.º 62/2009, de 10 de março que transpôs para a ordem jurídica nacional a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico no mercado interno.

---

[563] Silva, Hugo Lança. (2005, dezembro). Os Internet Service Providers e o direito: são criminosos, são cúmplices, são parceiros da justiça, polícias ou juízes? In *Verbo Jurídico*, p.6. Disponível em: http://www.verbojuridico.com/doutrina/tecnologia/isp.pdf consultado a 6 de junho de 2014.

[564] *Idem*, pp. 8-9.

[565] *Idem*, p. 6.

[566] Luís Menezes Leitão rejeita a hipótese de aplicação de medidas para impedir o anonimato na Internet, afirmando que "a imposição de identificação apresentar-se-ia como excessiva dado que há inúmeras razões legítimas para o utilizador querer permanecer anónimo". *Vide* Leitão, Luís Menezes. (2001, janeiro). A responsabilidade civil na Internet. *Revista da Ordem dos Advogados, 61* (1), 171-192, p.184.

[567] Dias, Vera E. M. (2009). A responsabilidade dos prestadores de serviços em rede - as inovações do Decreto-Lei n.º 7/2004. Relatório de Direito da Sociedade de Informação. In *Verbo Jurídico,* p.8. Disponível em: http://www.verbojuridico.com/doutrina/2011/veradias_responsabilidadeprestadoresservicosrede.pdf consultado a 9 de outubro de 2013.

[568] "*Internet service providers*" em inglês. Manuel Carneiro da Frada entende por prestadores de serviços em rede "aquelas entidades que, intervindo de forma autónoma, permanente e organizada no circuito informático, prestam, normalmente com escopo lucrativo, serviços na, ou através, da rede eletrónica". - Frada, M. Carneiro da. (2001). Vinho Novo em Odres Velhos? A Responsabilidade Civil das «Operadoras de Internet» e a Doutrina Comum da Imputação de Danos. *Direito da Sociedade da Informação*, *2*, 7-32, p. 10.

O ordenamento jurídico português estabeleceu, de forma inequívoca, o princípio da irresponsabilidade dos prestadores intermediários de serviços em rede[569] pelos conteúdos de terceiros, baseada na ausência do dever geral de vigilância[570], pelo que só em casos excecionais – quando preencham os requisitos previstos nos artigos 13.º a 17.º do Decreto-Lei n.º 7/2004, de 7 de janeiro -, é legítima a perseguição judicial dos prestadores de serviço na Internet[571]. A Lei n.º 7/2004, de 7 de janeiro distingue entre prestadores intermediários de serviço de simples transporte (artigo 14.º), prestadores intermediários de serviço de armazenagem intermediária (artigo 15.º), prestadores intermediários de serviço de armazenagem principal (artigo 16.º) e prestadores intermediários de serviços de associação de conteúdos (artigo 17.º). Tendo em conta a atividade que o prestador intermediário de serviços desempenha têm de preencher determinados requisitos para poder beneficiar da isenção de responsabilidade. Por outras palavras, se limitarem a sua atividade e não interferirem na criação e edição dos conteúdos ilícitos não incorrem em responsabilidade[572]. Ao mesmo tempo, estão ainda sujeitos a alguns deveres como o de informar e colaborar com as autoridades e o de retirar ou bloquear os conteúdos se aquelas o determinarem, de acordo com artigo 13.º da Lei n.º 7/2004. Mais concretamente, a referida lei na alínea b) do seu artigo 13.º exige que as operadoras satisfaçam os pedidos judiciais de identificar os destinatários dos serviços com quem possuem acordos de armazenamento de dados, quando lhes for pedido. Deste modo, entende-se que o indivíduo na Internet tem direito pleno à privacidade, mas caso o utilizador anónimo cometa um ato ilícito na rede, as autoridades judiciais terão legitimidade para solicitar junto dos prestadores de serviços intermediários desse utilizador os meios conducentes à identificação dos alegados infratores.

Em suma, o tema do anonimato tem vindo a assumir uma importância notável no estudo da sociedade contemporânea, nomeadamente numa conjuntura em que os sistemas de ambientes inteligentes procuram um conhecimento cada vez maior da pessoa, tentando identificá-la, rastreá-la e reconhecê-la. Neste contexto o Regulamento Geral de Proteção de

---

[569] «Prestadores intermediários de serviços em rede» são os que prestam serviços técnicos para o acesso, disponibilização e utilização de informações ou serviços «Prestadores intermediários de serviços em rede» são os que prestam serviços técnicos para o acesso, disponibilização e utilização de informações ou serviços, - artigo 4.º, n.º5 do Decreto-Lei n.º 7/2004, de 7 de janeiro

[570] Artigo 12.º Decreto-Lei n.º 7/2004, de 7 de janeiro:" Os prestadores intermediários de serviços em rede não estão sujeitos a uma obrigação geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito."

[571] Silva, Hugo Lança (2005, dezembro), *op. cit*, p. 28

[572] No entendimento de Hugo Lança Silva, solução fácil de responsabilizar sempre as operadoras de serviço "seria um propulsor do sentido de impunidade dos utilizadores da rede, mais tranquilos ao sentirem que os seus atos desvaliosos iriam onerar terceiros." Silva, Hugo Lança (2005, dezembro), *op. cit*, p. 16.

Dados encoraja a utilização das técnicas com recurso ao anonimato e clarifica o significado de dados anónimos e, em conformidade com o Considerando 23, exclui explicitamente esses dados do âmbito de aplicação do referido regulamento[573].

3.3.3. Redefinição do conceito legal de dados pessoais

A definição de dados pessoais constante da Diretiva 95/46/CE refere que por dados pessoais entende-se qualquer informação relativa a uma pessoa singular identificada ou identificável, considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

Da perspetiva do conteúdo da informação, o conceito de dados pessoais inclui dados que fornecem qualquer tipo de informação. Isto abrange, como é evidente, informação pessoal que, devido à sua natureza de risco especial, é considerada como "dados sensíveis" no artigo 8.º da Diretiva, mas também tipos mais gerais de informação. A expressão "dados pessoais" abrange a informação referente à esfera da vida privada e familiar da pessoa *stricto sensu*, mas inclui também informação sobre qualquer tipo de atividade realizada pela pessoa, por exemplo no que toca às relações de trabalho ou ao seu comportamento económico e social[574].

Este conceito de dados pessoais face a novas técnicas de recolha de dados em ambientes inteligentes torna-se insuficiente, devido à agregação massiva de dados, ao seu cruzamento e à capacidade de processamento dos computadores, os indivíduos tornam-se facilmente identificáveis[575].

Como se viu, o atual quadro jurídico da UE no artigo 8.º da Diretiva 95/46/CE proíbe o tratamento de dados sensíveis, isto é, dados que revelem a origem racial ou étnica, as opiniões

---

[573] Considerando 23 do RGPD: "Os princípios de proteção de dados não devem (...) ser aplicáveis a dados anónimos, que correspondem às informações não respeitantes a uma pessoa singular identificada ou identificável. O presente regulamento não diz por isso respeito ao tratamento de tais dados anónimos, incluindo para fins estatísticos ou de investigação."

[574] Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, *op. cit.,* p.8.

[575] Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M., Moscibroda, A. (2009). Privacy, Trust and Policy-Making: Challenges and Responses. *Computer Law & Security Review*, *25* (1), 69-83, p.81-82. DOI: 10.1016/j.clsr.2008.11.004.

políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual, havendo um número limitado de exceções, com determinadas condições e garantias[576]. No entanto, esta distinção entre dados sensíveis e não-sensíveis pode ser posta em causa nos ambientes inteligentes, na medida em que simples informações sobre os hábitos de consumo podem revelar dados pessoais sensíveis, como por exemplo relativos à saúde ou religião[577].

Antoinette Rouvroy refere que a monitorização das preferências de um consumidor num supermercado pode revelar aspetos sensíveis da sua vida privada: uma dieta específica pode revelar crenças religiosas, a compra de determinados medicamentos pode indicar estado de saúde, por sua vez a criação de perfis das pessoas na base dos seus programas de entretenimento preferidos e no contexto de uma televisão interativa pode sugerir opiniões políticas de determinada pessoa ou em relação às suas crenças filosóficas ou religiosas, etc.[578].

Os ambientes inteligentes permitem recolher grandes quantidades de dados relativos à situação pessoal do utilizador, aos seus comportamentos e as suas escolhas, sendo bastante elucidativos quanto à personalidade do utilizador, às suas preferências e os seus gostos, ao seu estatuto social ou estado de saúde, permitindo estabelecer um perfil[579]. As aplicações dos ambientes inteligentes possuem potencial para alterar a natureza dos dados envolvidos, o que levanta várias questões, uma vez que, em alguns casos, é possível chegar as informações sensíveis através da recolha e análise de dados inicialmente não sensíveis.

Outra preocupação é suscitada pelo uso da tecnologia RFID que, além de efetuar um rastreio silencioso e contínuo de hábitos pessoais e de comportamentos do utilizador, violando um dos seus requisitos fundamentais - a existência do consentimento do titular de dados, implica a localização de pessoas e a obtenção do acesso a dados pessoais. De facto, os artigos com etiquetas usados pelas pessoas contêm identificadores únicos que podem ser lidos à distância que poderão ser utilizados para reconhecer determinada pessoa ao longo do tempo, tornando-a "identificável"[580]. Isto poderá levantar a questão de terceiros poderem localizar as pessoas sem o seu conhecimento. Tal como foi sublinhado no Parecer 4/2007 do Grupo de

[576] Cf. Artigo 8.º da Diretiva 95/46/CE.

[577] Ver sobre a distinção entre dados sensíveis e não-sensíveis o ponto 3.2.1.

[578] Rouvroy, A. (2008), *op. cit.,* p. 41.

[579] Poullet, Y. (2010), *op. cit.*, p. 16.

[580] De Hert, P. (2009), *op. cit.,* pp. 437-438.

Trabalho do Artigo 29º sobre o conceito de dados pessoais, quando um identificador único está associado a uma pessoa, enquadra-se na definição de dados pessoais estabelecida na Diretiva 95/46/CE, ainda que a identidade social (nome, morada, etc.) da pessoa se mantenha desconhecida (ou seja, a pessoa é "identificável", mas não necessariamente "identificada")[581].

Além disso, o número único contido numa etiqueta pode também ser usado para identificar à distância a natureza dos bens transportados por uma pessoa, o que por sua vez pode revelar informações sobre o seu estatuto social, saúde, etc.. Portanto, mesmo nos casos em que uma etiqueta contém apenas um número - que é único num contexto específico e não contém outros dados pessoais - terá de haver precaução ao abordar potenciais problemas de privacidade e segurança, caso a etiqueta se destine a ser usada por várias pessoas.[582] As normas de proteção de dados apenas se aplicam se os dados na etiqueta forem suscetíveis de levar à identificação de uma pessoa. O problema coloca-se se essa identificação não é possível de uma forma simples, mas se torna possível quando os dados da etiqueta forem comparados com outros dados disponíveis, ou se o número de série do chip da etiqueta servir como identificador mesmo sem ser feita uma ligação direta com a identidade real da pessoa (por exemplo, quando a etiqueta contém um único identificador que ajuda a identificar o proprietário dos dados)[583].

Deverá ser feita uma referência especial aos dados biométricos, na medida em que a sua utilização garante uma identificação exata do indivíduo. A própria biometria apresenta-se como uma tecnologia capaz de converter as caraterísticas físicas de seres vivos em dados digitais[584]. Estes dados podem ser definidos como propriedades biológicas, caraterísticas fisiológicas, traços físicos ou caraterísticas comportamentais, na medida em que essas caraterísticas e/ou ações são simultaneamente únicos a essa pessoa e mensuráveis, mesmo que os padrões utilizados na prática para medí-las tecnicamente envolvam um certo grau de probabilidade.

---

[581] Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, *op. cit.,* p.15-16.

[582] Grupo de Proteção de Dados do Artigo 29.º, *Parecer 9/2011 sobre a proposta revista da indústria relativa a um quadro para as avaliações do impacto das aplicações RFID na proteção da privacidade e dos dados,* (00327/11/PT WP180), adotado em 11 de fevereiro de 2011, p.6. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_pt.pdf consultado a 13 de março de 2014.

[583] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*,(10107/05/EN WP 105), de 19 de janeiro de 2005. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf consultado a 3 de abril de 2013.

[584] Andrade, F. (2012b). Consideração jurídica das assinaturas dinâmicas no ordenamento jurídico português. *In Memórias do XVI Congresso Ibero Americano de Derecho e Informática.* Quito, p.9.

Segundo Francisco Pacheco Andrade, é possível distinguir na biometria duas dimensões fundamentais: "de um lado, aquilo que poderemos designar por dimensão fisiológica - a captura, mediação, digitação de certas caraterísticas, tais como impressões digitais, forma do rosto, geometria da mão, reconhecimento da iris; de outro lado, aquilo a que podemos chamar de dimensão comportamental – a captura, medição, digitação de outras caraterísticas, como o modo como alguém fala (reconhecimento de voz), ou o modo como alguém bate no teclado de um computador ou assina (reconhecimento de modo de assinar caligraficamente), aquilo que, por essa razão, designaremos por «biometria comportamental»"[585].

Exemplos típicos de dados biométricos são as impressões digitais, os padrões da retina, a estrutura facial, a voz, mas também a geometria das mãos, os padrões das veias ou mesmo uma habilidade profundamente enraizada ou outra caraterística comportamental (tal como a assinatura dinâmica[586], forma particular de andar ou falar, etc.). Uma particularidade dos dados biométricos é que estes podem ser considerados como conteúdo da informação sobre uma determinada pessoa, bem como um elemento para estabelecer uma ligação entre uma informação e a pessoa. Assim sendo, podem funcionar como "identificadores"[587].

De facto, devido à sua ligação única com uma determinada pessoa, os dados biométricos podem ser utilizados para identificar a pessoa. Este caráter duplo também surge no caso de dados de ADN[588] que fornecem informação sobre o corpo humano e permitem uma identificação clara e única da pessoa em causa[589]. As amostras de tecidos humanos (tal como uma amostra de sangue) são fontes de que se podem extrair dados biométricos, mas, no entanto, não são em si dados biométricos (tal como, por exemplo, um padrão de impressões é um dado biométrico, mas o próprio dedo não o é). Como tal, a extração de informação das amostras é uma recolha de dados pessoais à qual são aplicáveis as regras da Diretiva 95/46/CE.

---

[585] *Idem*, *ibidem.*

[586] Francisco Pacheco Andrade define assinatura dinâmica (baseada na biometria comportamental) como como conjunto de "técnicas de processamento digital da assinatura manuscrita de uma pessoa, (...), traduzindo e processando digitalmente as características dinâmicas do processo de assinatura manuscrita, transferindo assim para o ambiente digital as principais características e funcionalidades que tornam uma "assinatura" um sinal de identificação única para cada indivíduo. É importante referir a propósito que esta técnica não apenas permite capturar a forma da assinatura, mas também os seus dados biométricos, através de elementos como a velocidade, aceleração e sequência de riscos, numa combinação de elementos realmente única para cada indivíduo". Andrade, F. (2012b), *op. cit.*, p. 11.

[587] Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, *op. cit.*, p.9.

[588] A proteção de dados genéticos, enquanto dados sensíveis, já se encontra expressamente prevista na LPDP no artigo 7.º, n.º1.

[589] *Vide* sobre a questão de dados genéticos Castro, Catarina Sarmento e. (2005), *op. cit.,* pp. 94-95.

Devido aos desenvolvimentos tecnológicos torna-se necessário rever as normas em vigor aplicáveis aos dados sensíveis, ponderar a eventual junção de outras categorias de dados e clarificar ainda mais as condições para o tratamento destes dados[590]. Deve existir uma maior clarificação e harmonização das condições necessárias para o tratamento das diferentes categorias de dados sensíveis. Nenhuma lei prevê estas situações mesmo que a ligação possa ser usada para conduzir à criação de perfis e monitorização, o que torna imprescindível a criação de novos instrumentos legais para os ambientes inteligentes[591]. O AmI obriga a refletir sobre noção legal de dados pessoais do quadro jurídico atual da União Europeia pois pode vir a ser inviável no futuro, devido a tecnologias de vigilância e amplas possibilidades de perfis aumentarem ainda mais a disponibilidade e o cruzamento de dados entre vários sistemas e dispositivos e, consequentemente, entre as diferentes esferas da vida privada da pessoa[592].

Parece que nos dias de hoje o direito ao anonimato, à privacidade e à confidencialidade das pessoas está em risco devido ao uso de novas tecnologias de informação e comunicação que atuam como um forte mecanismo de recolha massiva de informação pessoal. Assim, a possibilidade de agir anonimamente estará também em vias de extinção, uma vez que, tendencialmente, todos passamos a poder ser identificados, no sentido de conhecidos e reconhecidos[593]. Até agora os considerados dados "anónimos" passam a ser ligados a uma pessoa, o que leva a concluir que praticamente todos os dados, no contexto de AmI, são dados pessoais[594].

Deste modo, com o surgimento de AmI, a definição de dados pessoais deve ser reconsiderada. Coloca-se a questão de saber se a distinção entre dados pessoais e outro tipo de dados pode ser sustentada no mundo de AmI, já que esta tecnologia pode ter impacto sobre o comportamento de uma pessoa mesmo sem a necessidade de a identificar. No entendimento de alguns autores seria o momento oportuno para explorar a possibilidade de passagem de

---

[590] Trata-se, por exemplo, dos dados biométricos que neste momento não são expressamente integrados na categoria dos dados sensíveis.

[591] E especialmente de normas dirigidas especificamente para a identificação por radiofrequências.

[592] De Hert, P., *et al.* (2009), *op. cit.*, pp. 439-440.

[593] Um exemplo disso é o cruzamento das informações que constam nos registos em linha e as que ficam armazenadas nos testemunhos de conexão que pode implicar a ligação de informações anónimas a pessoas reais. A questão não se resume apenas ao cruzamento destas informações, mas envolve, inclusive, a mecânica de rastreamento e incorporação dos dados que os consumidores dão sobre si nos registos em linha.

[594] Wright, D., *et al.* (2009), *op. cit.,* p. 82.

proteção de dados pessoais para a proteção de dados *tout court*[595]: uma nova geração de normas legais de proteção de dados, que não se baseariam no critério de "identificabilidade" das pessoas, mas apenas seriam acionadas quando os dados e o conhecimento desenvolvidos pelas AmI afetassem os comportamento e as decisões dos titulares de dados, independentemente da sua capacidade de identificar os indivíduos[596].

No âmbito da já referida reforma do regime jurídico da EU em matéria de proteção de dados, o Regulamento Geral de Proteção de Dados vem atualizar as definições legais, introduzindo expressamente dados genéticos, artigo 4.º, n.º10, dados biométricos, artigo 4.º, n.º 11, dados relativos à saúde, artigo 4.º, n.º 12. O RGPD procedeu à redefinição do conceito de dados pessoais, fazendo expressamente referência a dados genéticos, dados de localização e identificador único (RFIDs). Assim, segundo artigo 4.º, n.º2 os dados pessoais são "qualquer informação relativa a uma pessoa singular identificada ou identificável («titular de dados»). É considerada identificável a pessoa que possa ser identificada, direta ou indiretamente, nomeadamente por referência a um identificador, tal como o nome, um número de identificação, dados de localização, um identificador único, ou a um ou mais elementos específicos da identidade física, fisiológica, genética, psíquica, económica, cultural, social ou de género dessa pessoa". Igualmente o artigo 9.º n.º1 refere categorias especiais de dados (dados de natureza sensível), cujo tratamento é proibido, incluído expressamente dados genéticos: "É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a orientação sexual ou a identidade de género, a filiação e as atividades sindicais, bem como o tratamento de dados genéticos ou dados relativos à saúde ou à orientação sexual, às sanções administrativas, aos julgamentos, aos delitos penais ou presumidos, a condenações ou medidas de segurança conexas". Deste modo no RGDP o conceito de dados pessoais é clarificado mediante critérios objetivos (artigo 4.º, n.º 1, e Considerandos 23 e 24).

Ademais o novo regulamento introduz a definição e regulamenta a criação de perfis que se traduzem "em qualquer forma de tratamento automatizado de dados pessoais destinado a avaliar determinados aspetos pessoais relativos a uma pessoa singular ou a analisar ou prever

[595] Gutwirth, S., De Hert, P. (2008). Regulating Profiling in a Democratic Constitutional State. In M. Hildebrandt, S. Gutwirth (Eds.), *Profiling the European Citizen: Cross Disciplinary Perspectives* (pp. 271-302). Dordrecht: Springer, p.289.

[596] *Idem*, pp. 367-268.

em particular o seu desempenho profissional, a sua situação económica, localização, saúde, preferências pessoais, fiabilidade ou comportamento" (artigo 4.º n.º3-A). Para assegurar que as atividades de definição de perfis beneficiem de um consentimento informado, o RGPD impõe também novos limites à criação de perfis, (artigo 4.º, ponto 3-B, artigo 14.º, n.º 1, alíneas g), g-A) e g-B), artigo 15.º, n.º 1, e artigo 20.º).

De acordo com o Considerando 58 e artigo 20.º do RGPD as pessoas singulares têm direito a não ser objeto de uma medida baseada na definição de perfis através de tratamento automatizado que produza efeitos na sua esfera jurídica ou que as afete de modo significativo, sendo permitida só nos casos expressamente autorizados por lei, se for aplicada no âmbito da celebração ou da execução de um contrato, ou mediante o consentimento da pessoa em causa. Nestes casos o tratamento deve ser acompanhado de garantias adequadas, incluindo uma informação específica do titular dos dados e o direito de obter a intervenção humana, e que tal medida não diga respeito a uma criança.

Por fim, o referido regulamento passa a ser aplicável ao tratamento envolvendo identificadores fornecidos por aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (Protocolo Internet), testemunhos de conexão (*cookie*) e etiquetas de identificação por radiofrequências (RFID), salvo se estes identificadores não estiverem associados a uma pessoa singular identificada ou identificável.[597] Neste sentido, os números de identificação, os dados de localização, os identificadores em linha ou outros fatores específicos não têm necessariamente de ser considerados dados pessoais em todas as circunstâncias, uma vez que os referidos identificadores podem deixar vestígios que, em combinação com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e para a identificação das pessoas, sendo necessário examinar caso a caso e em função da evolução tecnológica, se números de identificação, dados de localização, identificadores em linha ou outros elementos específicos devem ser necessariamente considerados como dados pessoais.

[597] Considerando 24 do RGPD.

3.3.4. Territórios digitais

O desenvolvimento da computação ubíqua e de ambientes inteligentes fomenta a circulação de informação e dados em redes a partir dos mais variados dispositivos e sensores, que é efetuada cada vez mais na interseção dos espaços físicos e eletrónicos[598], criando uma zona de troca de dados entre utilizadores, lugares e objetos[599].

A proteção da privacidade e do anonimato só será eficaz com o reconhecimento de que os lugares físicos passam a ter fronteiras eletrónicas e informacionais, criando uma nova territorialidade - território digital ou informacional- que pode ser visto como uma espécie de membrana invisível que gere o fluxo de informação de e para o utilizador[600].

Beslay e Hakala usam a imagem da bolha para definir território digital[601]. As bolhas

---

[598] André Lemos apresenta o seguinte exemplo: "(...) ao sentar em um café e falar no telefone celular, ao usar um laptop para enviar e receber informações em rede Wi-Fi, estamos fazendo transitar, por fronteiras invisíveis, informações pessoais que podem ser captadas e usadas sem o nosso conhecimento ou consentimento. Claro, estamos ainda em um café, mas este passa a ser dotado de novas funções informacionais. Vemos aqui uma nova tensão de controlo, logo, uma novo território, informacional, criado por redes sem fios e dispositivos digitais nos lugares. Posso assim ser monitorado, controlado ou vigiado nesse café se estiver usando o celular, o laptop ou se houver um reder que acione a etiqueta RFID da minha caneta. Sem essa camada informacional, sem esse território informacional, não há como circular informação digital e o café seria apenas esse lugar tradicional para se tomar um café ou ler o jornal. Mas trata-se agora de um ciber-café." Lemos, André. (2009). Mídias locativas e vigilância: sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais. In Rodrigo Firmino, Fernanda Bruno, Marta Kanashiro (Coord.), *Anais do evento "Vigilância, segurança e controle social na América Latina"* (pp. 621-648). Curitiba: Editora Universitária Champagnat, PUCPR, pp.639-640. Disponível em: www2.pucpr.br/reol/index.php/SSSCLA?dd1=2696&dd99=pdf consultado a 9 de outubro de 2014.

[599] Beslay, L., Hakala, H. (2007), *op. cit.,* pp. 75, 78: "a growing number of emerging technologies, such as location-based services, fourth generation mobile telephones, closed circuit television, biometrics, etc., tend to establish links and bridges between a specific physical location and digitized knowledge and information. If the added value for the user is obvious, the potential new threats are not always highlighted. (...) Location-based services, radio frequency identification tags, body implants, ambient intelligence sensors, etc. will permit the implementation of a trustworthy environment and therefore the domestication of the ambient intelligence space by the individual. The vision will facilitate the transition through a traditional society that coexists with an information society, to a single society whose citizen have accepted and adopted the fusion of physical and digital realities. In this future society, people will still be able to control and manage distance from others with new tools provided by ambient intelligence space technologies".

[600] "Por exemplo, o lugar de acesso sem fios em um parque por redes Wi-Fi é um território informacional, distinto do espaço físico parque e do espaço eletrônico internet. Ao acessar a internet por essa rede Wi-Fi, o usuário está em um território informacional imbricado no território físico (e político, cultura, imaginário, etc.) do parque, e no espaço das redes telemáticas. O território informacional cria um lugar, dependente dos espaços físico e eletrônico a que ele se vincula (...)". Cf. Lemos, André. (2008). Mídias locativas e territórios informacionais. In L. Santaelle, P. Arantes (Eds.), *Estéticas tecnológicas. Novos modos de sentir* (pp. 207-230). São Paulo: EDUC, p.221. Disponível em: http://geografias.net.br/pdf/Midia_Locativa_e_Territorios_Informacionais.pdf consultado a 10 de outubro em 2014.

[601] Beslay, L., Hakala, H. (2007), *op. cit.,* p. 71: "a temporary defined space that can be used to limit the information coming into and leaving the bubble in the digital domain. It constitutes a digitization of the definition of personal space described by the psychologist Robert Sommer as a soap bubble. The vision of the bubble is defined to gather together all the interfaces, formats and agreements etc. needed for the management of personal, group and public data and informational interactions".

digitais podem ser vistas como fronteiras dos territórios informacionais, enquanto zonas de controlo que podem limitar a entrada e a saída da informação, que podem servir para garantir a privacidade, a segurança e a proteção de dados pessoais no mundo de computação ubíqua, no qual muitas vezes os dados pessoais são recolhidos e usados sem conhecimento dos utilizadores, uma vez que os limites entre os espaços privados e públicos têm sido eletronicamente esbatidos, deixando de ser claros.

De acordo com Barbara Dessala e Ioannis Maghiros o território digital deve ser pensado em vários níveis, com permeabilidades diferenciadas[602]. Os autores apontam para três tipos de territórios digitais: primário ou pessoal, secundário ou de grupo e, por último, público, que são classificados de acordo com o número de pessoas e o nível de controlo que estas exercem sobre o determinado território digital.

O território digital primário (ou pessoal) diz respeito ao espaço pessoal digital de uma pessoa que engloba todas as identidades digitais existentes, bem como todos os dados pessoais em formato digital, incluindo todos os dados que são gerados durante a sua atividade *online*[603]. Dentro deste "espaço" o indivíduo pode exercer controlo total sobre o seu território digital e decidir por si próprio se e que quantidade da sua informação pessoal pretende revelar, para quem e com que finalidade.

Por sua vez, o território digital secundário (ou de grupo) é de acesso público (que pode ser utilizado por duas ou mais pessoas) e os seus utilizadores possuem um certo grau de controlo sobre o mesmo, mas é mais limitado comparativamente ao do controlo existente no território digital primário ou pessoal[604]. Este tipo de território digital diz respeito a grupos de pessoas que compartilham os meus interesses e propósitos, sendo um exemplo muito caraterístico uma casa baseada na tecnologia de AmI[605]. Um exemplo representativo deste tipo de território digital é um ambiente doméstico, onde uma família pode partilhar vários nós de acesso físico, espaço de armazenamento, ferramentas digitais e onde os eventos podem ocorrer

---

[602] Daskala B., Maghiros I. (2007). *D1gital TerritOries Towards the Protection of Public and Private Space in a Digital and Ambient Intelligence Environment.* EUR - Scientific and Technical Research Reports. Luxembourg: Office for Official Publications of the European Communities, p.16. Disponível em: http://ftp.jrc.es/EURdoc/eur22765en.pdf consultado a 9 de outubro de 2014.

[603] Daskala B., Maghiros I. (2007), *op. cit.,* p. 16.

[604] *Idem, ibidem.*

[605] *Idem,* p. 17.

dentro de um sistema fechado[606]. A duração da existência deste território digital não é fixa; ela varia de situação para situação e depende do tipo de interesses e propósitos em comum que mantém os indivíduos juntos. No caso de ambiente doméstico: ele pode consistir inicialmente, por exemplo, de uma família de cinco membros (dois pais, duas crianças e um avô), mas cuja situação pode mudar quando as crianças crescem e saem de casa ou quando o avô é transferido para um lar de idosos.

Quanto aos territórios digitais públicos, praticamente qualquer pessoa tem acesso livre, exercendo um baixo nível de controlo sobre os mesmos. Representam um tipo de "bens comuns" no espaço digital, enquanto territórios livres, abertos a membros da sociedade em geral[607]. No espaço físico este tipo de território poderia representar, por exemplo, um centro comercial, uma rua ou um parque, enquanto que no espaço digital, este território pode ser representado por um fórum *online*, uma rede social (*Facebook; Twitter*) ou um *site* que permite que seus utilizadores carreguem e compartilhem vídeos em formato digital (por exemplo, *YouTube*). É preciso sublinhar que os três tipos de territórios digitais descritos em cima podem coexistir para o mesmo serviço ou aplicação.

A tecnologia baseada na computação ubíqua, especificamente nos ambientes inteligentes, potencia a violação de fronteiras dos territórios digitais por onde os dados pessoais circulam. As margens invisíveis dos territórios digitais devem ser controladas pelos próprios utilizadores, garantindo o nível de privacidade e anonimato desejado. Só assim é possível evitar formas de controlo, monitorização e vigilância indesejadas[608].

O conceito de território digital poderá ser implementado como proteção dos direitos fundamentais, visto como uma extensão da casa/domicílio que seguiria o indivíduo no ciberespaço como uma bolha invisível e inconetável, oferecendo aos utilizadores o poder de determinar as fronteiras, bem como opacidade ou transparência da sua bolha[609]. Um conjunto de normas legais poderá ser previsto para este fim, incluindo garantias processuais similares às

---

[606] *Idem, ibidem.*

[607] *Idem,* pp. 17-18.

[608] *Idem*, p. 18.

[609] Beslay, L., Hakala, H. (2007), *op. cit.,* p. 71*:* "This private digital space can be considered as an extension of the home that would ''follow'' the individual in cyberspace, like an unlinkable and invisible bubble. The user would have the ability to determine the borders of his digital territory."

aplicáveis ao domicílio, por exemplo requerendo um mandado de busca devidamente autorizado[610].

O território digital pode servir de instrumento para delimitar, de forma dinâmica e flexível, as fronteiras entre o espaço público e privado[611]. Além disso, o conceito de território digital pode ajudar na promoção da conscientização das pessoas em relação à privacidade e aos riscos de segurança existentes no mundo digital, indicando as práticas de segurança que os utilizadores teriam de seguir, a fim de proteger seus dados pessoais. Neste contexto, poderia ser utilizado no desenvolvimento de produtos ou serviços baseado em AmI, aumentando o nível de segurança e privacidade[612]. A lei deve proteger o espaço digital privado contra intervenções indesejadas e despercebidas por parte de terceiros (das partes privadas ou das entidades públicas). Soluções técnicas como tecnologias de reforço de privacidade e tecnologias de reforço de transparência, que serão discutidos mais detalhadamente no ponto seguinte, devem ser encorajadas e, se possível, impostas legalmente[613].

3.3.5. Reforço da segurança e controlo sobre dados pessoais através do recurso à tecnologia

O artigo 17.º da Diretiva 95/46/CE, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [614] estabelece a obrigação do responsável pelo tratamento dos dados de pôr em prática medidas técnicas e organizativas adequadas para garantir um nível de proteção

[610] De Hert, P., *et al.* (2009), *op. cit.,* p. 442: "If such virtual private digital territories are to become effective, they must be legally defined and protected. The law should protect against unwanted and unnoticed (surreptitious) interventions by private parties or public actors, just like it ensures the inviolability of the home. A set of legal rules could be envisaged to that end, including procedural safeguards similar to those applicable to the home, e.g. requiring a duly authorized search warrant".

[611] Daskala B., Maghiros I. (2007), *op. cit.,* pp. 7-8.

[612] *Idem*, p. 8.

[613] De Hert, P., *et al.* (2009), *op. cit.,* pp. 441-442.

[614] Diretiva 95/46/CE, artigo 17.º: "Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito. Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger." A mesma previsão está nos artigos 14.º e 15.º da LPDP.

adequado tendo em conta a natureza dos dados e os riscos representados pelo seu tratamento[615]. Ao mesmo tempo a Convenção 108, no seu artigo 7.º determina que "para a proteção dos dados de caráter pessoal registados em ficheiros automatizados devem ser tomadas medidas de segurança apropriadas contra a destruição, acidental ou não autorizada, e a perda acidental e também contra o acesso, a modificação ou a difusão não autorizados." A utilização de tecnologia que contribui para o cumprimento da legislação, em especial as regras de proteção de dados, já está prevista em certa medida na Diretiva 2002/58/CE de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónica[616].

Nos termos do artigo 14.º da Lei n.º 67/98, de 26 de outubro, a garantia da segurança de dados é uma obrigação legal do responsável pelo tratamento de dados pessoais que lhe impõe a adoção de mecanismos de garantia preventivos, devendo proteger os dados contra a sua destruição, acidental ou ilícita, bem como contra a sua perda acidental, ou contra erros e irregularidades, i.e., a garantia da segurança traduz-se na salvaguarda da informação, mas também na manutenção da sua integridade, através da adoção de medidas que impeçam a alteração dos dados, que permitam detetar disfuncionalidades e corrigi-las.

A segurança também obriga os responsáveis pelos tratamentos a medidas adequadas para impedir a difusão ou o acesso não autorizados de dados pessoais, garantindo, assim, a sua confidencialidade[617].

Contudo, a lei por si só não é capaz dar respostas exaustivas para os desafios normativos e regulamentares que dizem respeito à privacidade e à segurança de dados num contexto de ambientes inteligentes. Com efeito, os preceitos legais para serem eficientes devem estar incorporados na própria tecnologia.

---

[615] Foram também estabelecidas normas nacionais e internacionais para o tratamento de dados. Como exemplo disso pode ser apontado "O Rótulo Europeu de Proteção da Privacidade" (EuroPriSe), que é um projeto eTEN (Redes Transeuropeias de Telecomunicações) da UE que explorou a possibilidade de certificar certos produtos, especialmente *software*, que cumpram a legislação europeia sobre proteção de dados. A Agência Europeia para a Segurança das Redes e da Informação (ENISA) foi criada pelo Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, com o objetivo de reforçar a capacidade da UE, dos Estados-Membros da UE e da comunidade empresarial para evitar, gerir e resolver problemas de segurança das redes e da informação. A referida agência pública regularmente análises sobre as atuais ameaças à segurança e conselhos sobre a resposta a dar às mesmas. *Vide* em: http://europa.eu/legislation_summaries/information_society/internet/l24153_pt.htm

[616] Considerando 46 e n.º 3 do artigo 14.º da Diretiva 2002/58/CE de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).

[617] Castro, Catarina Sarmento e. (2005), *op. cit.,* p. 267.

No Parecer sobre a promoção da confiança na sociedade da informação através do reforço de proteção de dados e da privacidade, a Autoridade Europeia para a Proteção de Dados (AEPD) defende a ideia de integração da proteção de privacidade em soluções tecnológicas da conceção de novos produtos e serviços que realizam o tratamento de dados pessoais, conferindo responsabilidades acrescidas das organizações que processam os dados e para a autodefesa dos utilizadores – conceito conhecido como privacidade desde a conceção[618]. A AEPD entende que é pertinente conceber e desenvolver as TIC de forma que respeitem a privacidade e a proteção dos dados ao longo de todo o ciclo de vida da tecnologia, desde a fase inicial de conceção, até à sua instalação, utilização e eliminação finais[619].

Segundo o Parecer supra referido a privacidade desde a conceção pode implicar diversas ações, consoante o caso ou a aplicação em concreto[620]. Assim, em alguns casos, pode exigir a eliminação ou redução dos dados pessoais ou a prevenção de um tratamento desnecessário. Noutros casos, pode indicar instrumentos para aumentar o controlo das pessoas sobre os seus dados pessoais que podem ser incorporados na arquitetura dos sistemas de informação e comunicação, ou nas estruturas organizativas das entidades que tratam dados pessoais.

A Diretiva 95/46/CE, de 24 de outubro de 1995 relativa à proteção de dados não prevê uma exigência explícita de privacidade desde a conceção, mas contém disposições que, de forma indireta, podem exigir a aplicação deste princípio em diversas situações, nomeadamente, o artigo 17.º determina que os responsáveis pelo tratamento devem pôr em prática medidas técnicas e organizativas adequadas para prevenir o tratamento ilícito dos dados[621]. As disposições da diretiva abrangem o princípio da privacidade desde a conceção de forma muito genérica e visam principalmente os responsáveis pelo tratamento e a forma como tratam os dados

---

[618] Em inglês "*Privacy by design*" - Privacidade desde a conceção. Autoridade Europeia para a Proteção de Dados, *Parecer sobre a promoção da confiança na sociedade da informação através do reforço da proteção dos dados e da privacidade*, (2010/C280/01), de 16 de outubro de 2010, p.2. Disponível em:http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:PT:PDF consultado a 13 de março de 2014.

[619] *Idem*, p.3.

[620] *Idem*, pp.3-4.

[621] O artigo 17.º dispõe o seguinte: "Os Estados-membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito". O considerando 46 complementa esta disposição afirmando: "Considerando que a proteção dos direitos e liberdades das pessoas em causa relativamente ao tratamento de dados pessoais exige que sejam tomadas medidas técnicas e organizacionais adequadas tanto aquando da conceção do sistema de tratamento como da realização do próprio tratamento, a fim de manter em especial a segurança e impedir assim qualquer tratamento não autorizado".

pessoais, não exigem explicitamente que as tecnologias da informação e das comunicações cumpram os requisitos de privacidade e proteção de dados, o que também envolveria os concetores e os fabricantes das TIC.

Por sua vez, a Diretiva 2002/58/CE de 12 de julho de 2002 relativa à privacidade e às comunicações eletrónicas é mais explícita. O artigo 14.º, n.º 3 dispõe o seguinte: "Caso seja necessário, poderão ser adotadas medidas para garantir que o equipamento terminal seja construído de uma forma compatível com o direito de os utilizadores protegerem e controlarem a utilização dos seus dados pessoais, em conformidade com o disposto na Diretiva 1999/5/CE e na Decisão 87/95/CEE do Conselho, de 22 de dezembro de 1986, relativa à normalização no domínio das tecnologias da informação e das telecomunicações".

Não obstante as supracitadas disposições das duas diretivas serem úteis para a promoção da privacidade desde a conceção, na prática não são suficientes para garantir a incorporação da privacidade nas TIC, uma vez que a lei não exige de forma suficientemente precisa e expressa que estas últimas sejam concebidas de acordo com o princípio de privacidade desde a conceção.

Ademais, as autoridades responsáveis pela proteção de dados não possuem competências suficientes para garantir a incorporação desse princípio, o que gera ineficácia, por exemplo, as autoridades responsáveis pela proteção dos dados podem ter condições para impor sanções por ausência de resposta aos pedidos de acesso apresentados por pessoas singulares e possuir as competências necessárias para exigir a aplicação de medidas que impeçam o tratamento ilícito dos dados[622].

Segundo a AEPD, a inclusão do princípio da privacidade desde a conceção, de forma inequívoca e explícita relativo à proteção de dados tornaria o dito princípio mais forte, mais explícito, e imporia a sua aplicação efetiva, além de que conferiria maior legitimidade às autoridades responsáveis pela aplicação da lei para exigirem a sua aplicação na prática[623]. Isto é particularmente necessário tendo em conta os aspetos acima descritos, não só pela importância do princípio em si mesmo como instrumento para favorecer a confiança, mas também como

[622] Autoridade Europeia para a Proteção de Dados, *Parecer sobre a promoção da confiança na sociedade da informação através do reforço da proteção dos dados e da privacidade*, *op. cit.,* pp. 5-6.

[623] *Idem*, p.6.

incentivo para as partes interessadas implementarem a privacidade desde a conceção e reforçarem as garantias previstas no quadro jurídico existente.

Da mesma forma, o Grupo de Trabalho do Artigo 29.º na seu Parecer 168 "O futuro da privacidade, contribuição conjunta para a consulta da Comissão Europeia sobre o quadro jurídico relativo ao direito fundamental à proteção dos dados pessoais" defende a importância da introdução do princípio de privacidade desde a conceção como primado geral no quadro jurídico relativo à proteção de dados, nomeadamente na Diretiva relativa à proteção de dados, afirmando que: "Este princípio deve ser vinculativo para os concetores das tecnologias e para os seus produtores, bem como para os responsáveis pelo tratamento que têm de decidir sobre a aquisição e a utilização das TIC. Eles devem ser obrigados a ter a proteção tecnológica dos dados em conta logo na fase de planeamento dos procedimentos e sistemas das tecnologias da informação. Os fornecedores desses sistemas ou serviços, bem como os responsáveis pelo tratamento, devem demonstrar que tomaram todas as medidas necessárias para cumprir estes requisitos"[624].

Consciente do problema, Viviane Reding, comissária europeia de Justiça, no seu discurso em 16 de março de 2011 no Parlamento Europeu[625] introduziu um novo conceito - privacidade por defeito[626], realçando a preocupação com a necessidade de existência do efetivo controlo do titular sobre os seus dados e com a exigência do consentimento explícito através de mecanismos confiáveis para a obtenção do mesmo.

---

[624] "This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements". - Grupo de Proteção de Dados Pessoais do Artigo 29.°, *Parecer 168 do sobre o futuro da privacidade, contribuição conjunta para a consulta da Comissão Europeia sobre o quadro jurídico relativo ao direito fundamental à proteção dos dados pessoais* (*art.° 29 WP and WP on Police and Justice, Future of Privacy, Joint Contribution to the consultation of the European Commission on the legal framework for the fundamental light to protético of personal data*), (02356/09/EN WP 168), adotado em 1 de dezembro de 2009, p.13. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf consultado a 13 de março de 2014.

[625] Reding, Viviane. (16 de março de 2011), *op. cit.*

[626] "*Privacy by default"* em inglês. Consiste na responsabilidade de fabricantes e fornecedores de tecnologias TIC destinadas a tratar dados pessoais, de as conceber com garantias de proteção dos dados e da privacidade já incorporadas. Privacidade por defeito exige que os parâmetros da privacidade sejam desenhados e incorporados na conceção de arquitetura de sistemas para serem facilmente encontrados e manipulados pelo utilizador, garantindo que o titular de dados possa dar o seu consentimento com todo o conhecimento de causa. *Vide* Autoridade Europeia para a Proteção de Dados, *Parecer sobre a promoção da confiança na sociedade da informação através do reforço da proteção dos dados e da privacidade*, *op. cit.,* pp.5, 12.

Enquanto uma solução para todas estas preocupações, o novo Regulamento Geral de Proteção de Dados estabelece expressamente no seu artigo 23.º as obrigações do responsável pelo tratamento, decorrentes dos princípios de proteção de dados desde a conceção e de proteção de dados por defeito. O Considerando 61 do RGPD enuncia que "a proteção dos direitos e liberdades dos titulares dos dados relativamente ao tratamento dos seus dados pessoais exige a tomada de medidas técnicas e organizacionais adequadas, tanto no momento da conceção como no momento da execução do tratamento, para assegurar o cumprimento dos requisitos do presente regulamento. A fim de assegurar e comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deve adotar regras internas e aplicar medidas apropriadas que devem respeitar, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito".

O princípio da proteção de dados desde a conceção obriga a que a proteção de dados seja inserida em todo o ciclo de vida da tecnologia, desde a fase inicial de conceção, até à sua instalação, utilização e eliminação finais[627]. Nos termos do artigo 23.º, n.º 1, segunda parte do RGPD, a proteção dos dados desde a conceção deve ter em conta a gestão completa do ciclo de vida dos dados pessoais, desde a recolha, passando pelo tratamento, até à eliminação, centrando-se sistematicamente em garantias processuais abrangentes respeitantes à precisão, confidencialidade, integridade, segurança física e eliminação dos dados pessoais. Sempre que o responsável pelo tratamento tiver levado a cabo uma avaliação de impacto na proteção de dados nos termos do artigo 33.º, os resultados da referida avaliação são tidos em conta para efeitos de desenvolvimento destas medidas e procedimentos.

O princípio da proteção de dados por defeito exige que as definições de privacidade aplicáveis a serviços e a produtos cumpram, por defeito, os princípios gerais da proteção de dados, tais como a minimização dos dados e a limitação das finalidades[628]. Privacidade por defeito pode impedir a coleção, exibição, ou compartilhamento de quaisquer dados pessoais sem consentimento explícito do seu titular, bem como a utilização de dados para quaisquer outros fins que não os especificados originalmente. O artigo 23.º n.º2.º do RGPD obriga o responsável pelo tratamento de dados a garantir, por defeito, que apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento e, especialmente, que não

[627] Considerando 61 do RGPD.

[628] *Idem, ibidem.*

são recolhidos ou divulgados para além do mínimo necessário para essas finalidades, tanto em termos da quantidade de dados, como da duração da sua conservação.

Contudo, apesar desta previsão, ainda falta especificar mais concretamente os critérios técnicos e as exigências aplicáveis às medidas e aos mecanismos adequados para proteção dos direitos e liberdades dos titulares de dados, em especial quanto à proteção de dados desde a conceção aplicáveis ao conjunto de setores, produtos e serviços.

Reconhecendo a necessidade de adaptar as salvaguardas existentes para a proteção de dados e da vida privada aos novos desafios e tendo em conta o princípio da privacidade desde a conceção, uma tecnologia como a dos AmI pode ser, igualmente, equilibrada através da utilização de tecnologias de proteção da privacidade ou PETs[629] que "designam um sistema coerente de medidas no domínio das TIC que protegem a privacidade, suprimindo ou restringindo os dados de carácter pessoal ou evitando o tratamento inútil e/ou não desejado desses dados sem, no entanto, diminuir a funcionalidade do sistema de informação".[630] Leenes e Koops reconhecem o potencial desses PETs para fazer cumprir a lei de proteção de dados e privacidade[631]. O recurso a este tipo de tecnologia visa não apenas limitar a quantidade de dados recolhidos ao mínimo necessário, bem como contribui para garantir que as violações dos direitos individuais em matéria de proteção de dados e privacidade sejam não só proibidas e sujeitas a sanções, mas também mais difíceis do ponto de vista técnico[632].

Como complemento às tecnologias de proteção da privacidade, que visam controlar a disseminação de dados, podem ser igualmente apresentadas tecnologias indutoras de

---

[629] PET- *"privacy enhancing technology"* (em inglês) - tecnologias de proteção da privacidade. "As PET's contêm conjuntos de mecanismos que permitem aos utilizadores apagar os vestígios pessoais das suas mensagens ou ações na internet de modo a que não se possa associar um dado conteúdo a um utilizador (mesmo que esse utilizador seja mesmo anónimo). As duas principais tecnologias que integram a categoria agora analisada são o anonimous remailing e o anonimous surfing. No primeiro caso estamos perante uma forma de envio de e-mails sem revelação de identidade, através da encriptação de dados considerados pessoais; no segundo caso permite-se ao utilizador evitar que o host-computer com que entra em contacto possa recolher informações sobre o seu computador, programas de navegação, endereço IP e últimos websites visitados." *Vide* Farinho, Domingos Soares. (2006), *op. cit.*, p. 75.

[630] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu e ao Conselho relativa à promoção da proteção de dados através de tecnologias de proteção da privacidade,* (COM (2007) 228 final), de 2 de maio de 2007, p.3. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0228 consultado a 13 de outubro de 2013.

[631] Leenes, R., Koops, B. J. (2005). 'Code': Privacy's Death or Saviour?. *International Review of Law Computers & Technology*, *19*(3), 329-340, pp.335-337. DOI: 10.1080/13600860500348572.

[632] Winn, J. K. (2009). Technical standards as data protection regulation. In Serge Gutwirth, *et al.* (Eds.), *Reinventing Data Protection? Reinventing Data Protection?* (pp. 191-206), Países Baixos: Springer, pp.199-200.

transparência (TETs)[633] cujo principal objetivo consiste em contribuir para a troca de informações e para a sua gestão. Um exemplo é o das chamadas "políticas pegajosas" que seguem os dados assim que disseminados[634], fornecendo aos responsáveis pelo tratamento de dados e aos controladores indicações relativamente à política de privacidade que se aplica aos dados em causa[635]. Estas políticas facilitariam a auditoria e a fiscalização da legalidade do processamento de dados pelos sujeitos que fazem o controlo do tratamento de dados, permitindo a deteção e denúncia de abusos e fornecendo, por sua vez, ao titular de dados em causa os meios adequados para apresentar reclamações e queixas, bem como provar a responsabilidade em caso de dano[636]. Os agentes inteligentes de *software* poderiam ajudar a pessoa em causa para gerir seus dados[637]. É curioso observar que a tecnologia, portadora de um vasto número de perigos, pode ser considerada como uma parte da solução dos problemas a incorporar os princípios legais relativos aos direitos à privacidade e à proteção de dados.

Tanto quanto possível, a arquitetura das aplicações e dos sistemas baseados nos AmI deverá ser concebida de tal modo que só sejam recolhidos os dados pessoais que forem estritamente necessários para atingir os fins em vista. Caso não sejam necessários, ou apenas o sejam numa fase inicial do tratamento, os dados pessoais não deverão ser recolhidos ou deverão ser convertidos em dados anónimos o mais rapidamente possível. Importa pois ponderar, não só se é necessário recolher os dados, mas também se há necessidade de os conservar nos diversos sistemas.

A conservação de dados pessoais deve ficar sujeita a prazos que todos os intervenientes da cadeia de serviços terão de respeitar, e que deverão ser diferenciados consoante o tipo de

---

[633] "*Transparency Enhancing Technologies"* em inglês. *Vide* Hildebrandt, M., Koops, E.J. (2010). The challenges of ambient law and legal protection in the profiling era. *Modern Law Review*, *73*(3), 428-460, pp.449-450. Disponível em: https://pure.uvt.nl/portal/files/1248058/Koops_The_Challenges_of_Ambient_Law_100712.pdf consultado a 9 de maio de 2013.

[634] De Hert, P., *et al.* (2009), *op. cit.*, p. 441: "Advancements in information technology itself could provide important factual means of transparency. Complementary to privacy-enhancing technologies (PETs), which aim at controlling the dissemination of data, transparency-enhancing technologies (TETs) could contribute to information exchange and management".

[635] Mont, M. C., Pearson, S., Bramhall, P. (2003). *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. Technical Report HPL N.º 2003-49.* Reino Unido: HP Laboratories Bristol, pp.8-9. Disponível em: http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf consultado a 15 de junho de 2014.

[636] "As a retrospective measure, auditing enables the detection and reporting of abuses, which in turn provides the data subject the wherewithal to launch liability and damages claims. In addition, audits serve the data protection authorities for whom there is an urgent need to strengthen and internationally harmonize their powers, especially in light of the transnational or "beyond borders" character of the AmI world."- Wright, D., *et al.* (2009), *op. cit.,* p. 82.

[637] *Idem*, p. 18.

dados e os fins para os quais foram recolhidos[638]. Assim, quando já não seja necessário conservar os dados pessoais para atingir os fins para os quais foram recolhidos ou tratados, os dados devem ser anonimizados, ou seja, modificados de forma a impedir que sejam relacionados com uma pessoa identificada ou identificável, ou totalmente apagados.

A arquitetura dos sistemas e os procedimentos de intercâmbio de dados nos AmI deverão ser concebidos para tratar o mínimo possível de dados pessoais. Para o efeito, devem ser tidas em conta todas as etapas de recolha, transmissão, tratamento e todos os intervenientes da cadeia de prestação de serviços dos AmI. Alguns dados podem ser trocados e tratados anonimamente, ao passo que outros, mesmo que sejam trocados sem identificação, podem ser relacionados com dados respeitantes a pessoas identificadas, constituindo assim dados pessoais na aceção da alínea a), do artigo 2.º, da Diretiva 95/46/UE.

Os principais objetivos de proteção da privacidade durante a recolha de dados consistem em impedir o cruzamento e a correlação entre os diversos tipos de dados capturados sobre o mesmo utilizador e podem ser alcançados através da cuidadosa seleção de *hardware* que irá permitir a captação do mínimo de dados necessários para determinado fim, bem como através do aumento de recursos e da inteligência de *software* (para permitir que os dados possam ser processados em tempo real) e através da destruição de dados logo que possível.

A interoperabilidade das aplicações e dos sistemas é também um elemento essencial para que a implantação dos AmI seja bem-sucedida. Toda e qualquer interligação das bases de dados deve ser efetuada na observância dos princípios da proteção de dados e das garantias de segurança. As especificações técnicas a definir com vista à conceção de interfaces deverão assegurar a exatidão de dados obtidos graças à interligação de aplicações e sistemas. Dado que a interoperabilidade dos sistemas virá a facilitar a interligação das bases de dados e a correspondência entre dados para outros fins, toda e qualquer interligação deve ser efetuada na plena observância do princípio da limitação enunciado no n.º 1, alínea b), do artigo 6.º, da Diretiva 95/46/CE.

---

[638] Por exemplo, a conservação dos dados de tráfego e dados de localização tratados para efeitos da oferta de serviços de comunicações eletrónicas publicamente disponíveis em redes de comunicações públicas rege-se pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais à proteção da privacidade no sector das comunicações eletrónicas.

Contudo, as tecnologias de vigilância e as amplas possibilidades de perfis aumentam ainda mais a disponibilidade e intercâmbio de dados entre vários sistemas e dispositivos (e, consequentemente, entre as diferentes esferas da vida da pessoa), enquanto a interoperabilidade implica uma disponibilidade ilimitada de dados pessoais[639]. Por isso, é crucial que as aplicações dos AmI sejam concebidas de modo a impedir a posterior utilização de dados para fins diferentes dos que levaram à sua recolha. É necessário incorporar no sistema proteções de segurança adequadas para impedir a utilização abusiva, a divulgação ou o acesso não autorizados, ou quaisquer efeitos secundários dos dispositivos. Devem, por exemplo, ser instaladas proteções suficientes para impedir o acesso de terceiros não autorizados aos dispositivos e a utilização destes dispositivos para identificar e localizar pessoas. Quanto à licitude da própria interligação, é um aspeto a analisar caso a caso, tendo em conta a natureza de dados disponibilizados e trocados através dos sistemas, bem como as suas finalidades originais.

A transparência dos sistemas e o acesso ao conhecimento gerado, nomeadamente a perfis, poderão permitir aos indivíduos estar conscientes de erros, compreender o porquê das certas ações empreendidas pelo AmI e contestar se sentirem que as decisões por estes tomadas são demasiado onerosas. A transparência é uma condição imprescindível para que as pessoas possam exercer o controlo sobre os seus próprios dados e garantir a proteção efetiva dos mesmos. O regime legal vigente relativamente ao tratamento de dados pessoais requer que os titulares dos dados sejam informados acerca da maneira como os processos de recolha e processamento de dados são efetuados – artigo 10.º da Diretiva 95/46/CE[640].

Porém, estes requisitos em relação à transparência do processamento de dados não serão facilmente preenchidos num contexto dos AmI, uma vez que a invisibilidade de terminais dos sistemas dos ambientes inteligentes e a inclusão de modelos de serviços descentralizados são de facto incompatíveis com o princípio da transparência, na medida em não permite ao

[639] De Hert, P., *et al.* (2009), *op. cit.*, p. 439: *"Moreover, surveillance technologies and extensive profiling possibilities further increase the availability and exchange of data between various systems and devices (and, consequently, between different spheres of one's life)."*

[640] Artigo 10.º: "Os Estados-membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento a que os dados se destinam; c) Outras informações, tais como: - os destinatários ou categorias de destinatários dos dados, - o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder, - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos."

titular de dados ter uma visão compreensiva de como os seus dados são processados, nem ter consciência das implicações daí decorrentes.

Deve existir um princípio de transparência explícito que exija que qualquer informação ou comunicação destinada ao público ou ao titular de dados seja de fácil acesso e compreensão, e formulada numa linguagem clara e simples. O responsável pelo tratamento deve aplicar regras transparentes e de fácil acesso relativamente ao tratamento de dados pessoais e ao exercício dos direitos pelos titulares de dados[641].

Na técnica de mineração de dados, amplamente empregue nos sistemas de AmI, os dados muitas vezes são registados sem o consentimento inequívoco, ou até mesmo sem o conhecimento, do titular dos dados. Aliás, ainda não está claro o que significa consentimento inequívoco no contexto de AmI, e como o mesmo deve ser expresso, especialmente quando está em causa a construção de perfis: como pode alguém dar um consentimento informado quando o âmbito e a finalidade da recolha de dados não são exatos? Tal facto aponta para a necessidade de desenvolver e clarificar ao nível da UE as modalidades e padrões mais concretos aplicáveis ao consentimento para que seja considerado informado e válido neste tipo de situações[642]. Para além disso, a própria opacidade dos sistemas do AmI torna mais difícil as pessoas estarem cientes dos respetivos direitos e darem um consentimento informado para tratamento dos seus dados.

Atualmente, o Regulamento Geral de proteção de Dados, recentemente aprovado pelo Parlamento Europeu, já contempla várias destas soluções. Contudo, mesmo com o novo quadro regulamentar em matéria de proteção de dados que está ser introduzido na EU, o atual regime europeu de proteção de dados deve ser atualizado e melhorado face às novas tecnologias, nomeadamente as disposições existentes em matéria de informações a fornecer ao titular de dados[643].

[641] Tal exigência já se encontra prevista no artigo 11.º do RGPD.

[642] Wright, D., *et al.* (2009), *op. cit.,* p. 83.

[643] Artigos 10.º e 11.º da Diretiva 95/46/CE.

3.4 Considerações finais

Da análise do sistema jurídico ocidental ficou claro que a privacidade é protegida, principalmente por disposições explícitas, tanto em tratados internacionais de direitos humanos como nas constituições nacionais, sendo um direito de personalidade que encontra os seus fundamentos na proteção da dignidade da pessoa humana, na proteção da individualidade e na autonomia de cada um. Por sua vez, a proteção de dados projeta-se como um direito autónomo, cuja tutela possui fundamento constitucional e assume a feição de um direito fundamental.

Com o desenvolvimento da nova sociedade tecnológica, introdução das tecnologias de AmI, e sobretudo com o aumento exponencial da recolha, armazenamento e a divulgação de dados pessoais, torna-se pertinente defender a privacidade e o direito à autodeterminação informativa dos cidadãos, fornecendo tanto proteção contra utilizações abusivas das suas informações, como garantias de que suas escolhas sobre a utilização de seus próprios dados serão livres e transparentes.

Foi possível concluir que apesar das inúmeras oportunidades oferecidas pela tecnologia dos AmI, existe um grande risco de os dados serem usados para tornar o indivíduo num objeto sob constante vigilância e monitorização, o que não é compatível com a verdadeira natureza da proteção de dados como direito fundamental, que é vista como expressão da liberdade pessoal e da dignidade.

O armazenamento, o processamento e a troca de dados pessoais pelas agências de segurança e pelas entidades governamentais, conjugados com a técnica de mineração de dados podem pôr em risco os princípios protetores do tratamento de dados pessoais, aproveitando os dados já recolhidos para diferentes finalidades e partilhando os mesmos com outras instituições sem o consentimento dos titulares.

Foram elencadas as medidas de caráter legislativo e ao mesmo tempo, chegou-se à conclusão de que o Direito deve também recorrer à ajuda da tecnologia para garantir que os mesmos instrumentos que servem para vigiar pessoas possam promover de forma eficiente a proteção adequada aos dados pessoais, criando, nomeadamente ferramentas de transparência.

No presente estado da investigação verificou-se que muitas das propostas apresentadas já se encontram contempladas no novo Regulamento Geral de Proteção de Dados, nomeadamente: o direito a ser esquecido, o princípio de transparência, reforçado pelas tecnologias indutoras de transparência, bem como a introdução dos mecanismos da proteção de dados desde a conceção e a proteção de dados por defeito. Contudo, ainda não foram resolvidas as questões relacionadas com a previsão legal de territórios digitais e o direito a identidades múltiplas, bem como persiste a necessidade de redefinir dados pessoais no contexto de AmI, entre outras. Concluiu-se que o vigente regime europeu em matéria de privacidade e proteção de dados pessoais deve ser reforçado no contexto da computação ubíqua através de uma conjugação do direito, da própria tecnologia e das partes interessadas no domínio das TIC.

Tal como a tecnologia, a forma como os dados pessoais são usados e partilhados está constantemente a mudar. Para o legislador, o desafio consiste em estabelecer um quadro normativo que resista à passagem do tempo, de modo que no final do processo de reforma, as normas de proteção de dados possam garantir, um elevado nível de proteção e segurança jurídica aos particulares, às administrações públicas e às empresas.

CONCLUSÃO

Finalizando a incursão pelo tema de ambientes inteligentes e suas repercussões na privacidade e proteção de dados pessoais resta-se sintetizar as seguintes conclusões:

i. O estudo desenvolvido e agora apresentado, permitiu esclarecer o conceito de ambientes inteligentes, assim como definir as suas principais caraterísticas, campos da aplicação e vantagens da sua implementação. Ao mesmo tempo foi possível concluir que o desenvolvimento de novas tecnologias, especialmente de ambientes inteligentes, apesar de proporcionar inúmeros benefícios, apresenta um enorme desafio para a privacidade, na medida em que fomenta o aumento da vigilância e da recolha invisível de dados pessoais.

ii. Pode-se argumentar que, atualmente, os Estados procuram um maior controlo das atividades particulares, em nome do interesse público da segurança e do bem-estar social, apostando em grande medida nos sistemas de vigilância baseados na tecnologia emergente de ambientes inteligentes que devido à opacidade do seu funcionamento acarretam o risco de um processamento indevido e não solicitado de dados pessoais.

iii. Hoje em dia, o direito à proteção de dados projeta-se como um direito autónomo cuja tutela possui fundamento constitucional e assume a feição de um direito fundamental, posto que se destina à proteção da pessoa perante interesses provenientes de uma multiplicidade de fontes, sejam aquelas situadas na esfera privada como na pública, muitos dos quais já foram vislumbrados neste trabalho. Contudo, ficou claro que a tecnologia, como muitas vezes acontece, está a evoluir mais rápidamente do que o processo de construção de políticas e legislação adequada. Face ao relatado, afirmamos, com elevado grau de certeza, que o atual regime europeu de privacidade e proteção de dados necessita de ser atualizado e melhorado face às novas tecnologias dos ambientes inteligentes.

iv. Neste contexto, destacamos a técnica de construção de perfis pessoais, a partir dos quais podem ser tomadas decisões a respeito dos cidadãos, afetando diretamente as suas vidas e influenciando o seu acesso a oportunidades sociais. Percebemos que crescem os riscos ao livre desenvolvimento da personalidade do

cidadão, na medida em que esses perfis, verdadeiros clones virtuais, representam informações fragmentadas e descontextualizadas, que podem ser utilizadas de modo a prejudicar a liberdade e as escolhas do indivíduo. Esses riscos, ampliados pela utilização da tecnologia de AmI, tornam imperativa a regulamentação jurídica da matéria.

v. Como verificamos, torna-se pertinente a criação de um quadro legal para limitar a vigilância tanto privada como governamental. Nesse sentido, propomos que seja desenvolvido um regime legal especificamente para territórios digitais enquanto uma importante salvaguarda da privacidade no mundo digital dos AmI. O conceito de território digital poderá ser implementado como proteção dos direitos fundamentais, visto como uma extensão da casa/domicílio que seguiria o indivíduo no ciberespaço como uma membrana invisível e inconectável, oferecendo aos utilizadores o poder de determinar as fronteiras, bem como opacidade ou transparência do seu território digital e protegê-lo contra interferência ilegal e abusiva.

vi. Chegamos à conclusão que o território digital pode servir de instrumento para delimitar de forma dinâmica e flexível as fronteiras entre o espaço público e privado. Além disso, o conceito do território digital pode ajudar na promoção da conscientização das pessoas em relação à privacidade e aos riscos de segurança existentes no mundo digital, indicando as práticas de segurança que os utilizadores teriam de seguir, a fim de proteger seus dados pessoais. Neste contexto, ele poderia ser utilizado no desenvolvimento de produtos ou serviços baseado em AmI, aumentando o nível de segurança e privacidade.

vii. O estudo desenvolvido permitiu demostrar que, no caso dos sistemas de AmI, as pessoas estão perante um ambiente cheio de vários sensores invisíveis, tornando difícil, se não impossível, para o utilizador ter conhecimento e controlar a recolha de dados, bem como alcançar o anonimato. O processamento dos dados através do recurso aos algoritmos de raciocínio inteligente, limitando o cruzamento de dados e o controlo de acesso aos dados recolhidos, parece ser uma das principais formas de proteção da privacidade em tais aplicações. Na nossa opinião, o uso de diferentes identidades com o mínimo de dados pessoais em cada aplicação poderá ajudar a prevenir a descoberta, a ligação/correlação entre

a identidade do utilizador e os seus dados pessoais, bem como entre as diferentes ações do mesmo utilizador.

viii. Percebemos, que atualmente, o direito ao anonimato, à privacidade e à confidencialidade das pessoas está em risco devido ao uso de novas tecnologias de informação e comunicação que atuam como um forte mecanismo de recolha massiva de informação pessoal. Assim, a possibilidade de agir anonimamente estará também em vias de extinção, uma vez que, tendencialmente, todos passamos a poder ser identificados, no sentido de conhecidos e reconhecidos.

ix. Concluiu-se que o uso cada vez maior das tecnologias baseadas nos ambientes inteligentes obriga a refletir sobre noção legal de dados pessoais do atual quadro jurídico da União Europeia e nos termos do recente Regulamento de Proteção de Dados e que, em ambos os casos, será inviável no futuro, devido a tecnologias de vigilância e amplas possibilidades de perfis em aumentar ainda mais a disponibilidade e cruzamento de dados entre vários sistemas e dispositivos e, consequentemente, entre as diferentes esferas da vida privada da pessoal. Mencionamos a possibilidade de passagem de proteção de dados pessoais para a proteção de dados *tout court* através de adaptação de uma nova geração de normas legais de proteção de dados, que não se baseariam apenas no critério de "identificabilidade."

x. Vimos que torna-se necessário rever as normas em vigor aplicáveis aos dados sensíveis, ponderar a eventual junção de outras categorias de dados, por exemplo de dados biométricos e clarificar ainda mais as condições para o tratamento destes dados. Existe necessidade de uma maior clarificação e harmonização das condições necessárias para o tratamento das diferentes categorias de dados sensíveis.

xi. Ademais, percebemos que o aumento de recolha e possibilidade de cruzamento dos dados pessoais vão esbater a distinção entre os dados sensíveis e não-sensíveis. O tratamento e o cruzamento de dados pouco relevantes, pode fornecer informações muito sensíveis, permitindo a elaboração do conhecimento sobre a pessoa em causa. Isso demonstra o potencial de algumas aplicações do ambiente inteligente vir alterar a natureza dos dados envolvidos. Verificamos que nenhuma lei prevê estas situações mesmo que a ligação possa ser usada para

conduzir à criação de perfis e monitorização, o que torna imprescindível a criação de novos instrumentos legais para os ambientes inteligentes, especialmente de normas dirigidas especificamente para a identificação por radiofrequências.

xii. A proposta de um direito a identidades múltiplas pretende chamar a atenção para a necessidade de adaptar o atual quadro jurídico para o mundo tecnológico, onde as identidades diferentes e simultâneas podem ser facilmente criadas e utilizadas. O direito a identidades múltiplas não só poderá servir aos interesses da privacidade do sujeito (mantendo os aspetos importantes da sua vida privada ocultos), mas também contribuirá para a minimização de divulgação de dados pessoais.

xiii. Tendo em conta o que foi dito anteriormente sobre a proliferação de dados no cenário dos ambientes inteligentes, a questão da admissibilidade de um direito a ser esquecido torna-se pertinente. Tradicionalmente ligado ao direito à privacidade, a questão do esquecimento também tem uma forte ligação ao direito à identidade. O direito a ser esquecido irá desenvolver um papel extremamente importante a permitir a um indivíduo reconstruir a sua identidade, conferindo possibilidade de ter partes da sua identidade apagada, impedindo que elas sejam disponíveis ao público.

xiv. Verificamos que torna-se necessário traçar normas específicas para regular o uso de agentes inteligentes de *software* no contexto dos AmI. A fim de beneficiar dos seus serviços, os utilizadores poderão delegar algum poder de controlo e de decisão a agentes que vão agir em nome do utilizador, aprendendo ao mesmo tempo sobre seus hábitos, gostos e preferências, como foi visto no caso dos Alvatares. Vimos que os níveis de autonomia de agentes podem variar e, em muitos casos, apesar de o agente tomar decisões por si, sem intervenção humana, o utilizador poderá ter uma maior ou menor capacidade de controlo sobre os parâmetros que influenciam o comportamento do agente. Poderão existir casos em que o agente, face à informação de que dispõe, poderá - no interesse do utilizador – ultrapassar claramente aquilo que o próprio utilizador poderá ter previsto, levando à perda do controlo e da autonomia do indivíduo, o que exige a construção de um quadro jurídico que regula esses agentes e que permitirá assegurar a sua confiabilidade e explorar todo o seu potencial.

xv. Concluímos que a transparência no contexto de AmI é uma condição imprescindível para que as pessoas possam exercer controlo sobre os seus próprios dados e garantir proteção efetiva dos mesmos. Deve existir um princípio de transparência explícito que exija que qualquer informação ou comunicação destinada ao público ou ao titular de dados seja de fácil acesso e compreensão, e formulada numa linguagem clara e simples.

xvi. Somos de opinião que a lei deve também procurar ajuda da tecnologia para garantir que os mesmos instrumentos que servem para vigiar pessoas possam promover de forma eficiente proteção adequada aos direitos e liberdades fundamentais dos indivíduos, criando, nomeadamente ferramentas de transparência. Uma tecnologia como a dos AmI poderá ser equilibrada através da utilização de tecnologias de proteção da privacidade ou PETs que protegem a privacidade, suprimindo ou restringindo o acesso a dados de caráter pessoal ou evitando o tratamento inútil e/ou não desejado desses dados.

xvii. A necessidade de existência do efetivo controlo do titular sobre os seus dados e a exigência do consentimento explícito pode ser satisfeita através da implementação do princípio de privacidade por defeito que exige que os parâmetros da privacidade sejam desenhados e incorporados na conceção de arquitetura de sistemas para serem facilmente encontrados e manipulados pelo utilizador, garantindo que o titular de dados possa dar o seu consentimento com todo o conhecimento de causa.

xviii. Privacidade por defeito pode impedir a recolha, exibição, ou compartilhamento de quaisquer dados pessoais sem consentimento explícito do seu titular, bem como a utilização de dados para quaisquer outros fins que não os especificados originalmente. Por sua vez, o recurso à privacidade desde a conceção vai permitir incorporação dos princípios legais na própria tecnologia, através da integração da proteção de privacidade em soluções tecnológicas da conceção de novos produtos e serviços que realizam o tratamento de dados pessoais.

xix. Como complemento às tecnologias de proteção da privacidade, que visam controlar a disseminação de dados, podem ser igualmente apresentadas tecnologias indutoras de transparência (TETs) cujo principal objetivo consiste em contribuir para a troca de informações e sua gestão. Um exemplo é o das

chamadas "políticas pegajosas" que fornecem aos responsáveis pelo tratamento de dados e aos controladores indicações relativamente à política de privacidade que se aplica aos dados em causa e facilitam a auditoria e fiscalização da legalidade do processamento de dados, permitindo a deteção e denúncia de abusos cometidos e, por outro lado, disponibilizando ao titular de dados em causa os meios adequados para apresentar reclamações e queixas, bem como provar a responsabilidade em caso de dano. Neste caso, os agentes inteligentes de *software* poderiam ajudar a pessoa em causa para gerenciar os seus dados.

xx. Verificamos que a fim de impedir o cruzamento e a correlação entre os diversos tipos de dados capturados sobre o mesmo utilizador**,** a arquitetura dos sistemas e os procedimentos de intercâmbio de dados nos AmI deverão ser concebidos para captação do mínimo de dados necessários para determinado fim e de modo a permitir que os dados possam ser processados em tempo real e destruídos logo que for possível.

xxi. Tendo em conta as alterações trazidas pelo Tratado de Lisboa e, em especial, a consagração pela Carta dos Direitos Fundamentais de novo direito fundamental à proteção de dados pessoais, e os próprios avanços tecnológicos e a globalização, a Comissão Europeia apresentou em 2010 uma reforma global que harmoniza, atualiza e moderniza os princípios estabelecidos na Diretiva 95/46/CE, de 24 de outubro e inclui uma comunicação que apresenta duas propostas legislativas: uma proposta de regulamento que define o quadro geral europeu para a proteção dos dados e uma proposta de diretiva relativa à proteção de dados pessoais para efeitos de prevenção, investigação, deteção e repressão de infrações penais e de atividades judiciárias conexas

xxii. Em 12 de março de 2014 o Parlamento Europeu aprovou a última versão do Regulamento Geral de Proteção de Dados que passou a contemplar várias soluções supra apresentadas e consagra novos princípios em matéria de proteção de dados: a transparência e a responsabilidade do responsável pelo tratamento de dados, bem como a proteção de dados desde a conceção e a proteção de dados por defeito. Aos responsáveis pelo tratamento e aos subcontratantes são atribuídas mais obrigações e os titulares de dados, além de

verem os seus direitos reforçados, têm agora direito ao esquecimento e à portabilidade de dados.

xxiii. Destacamos a introdução da distinção entre dados pessoais de diferentes categorias de titulares e entre diferentes categorias de dados, em função do seu nível de precisão e fiabilidade. Além disso, clarificam-se as condições de licitude do tratamento, que são taxativas, bem como os direitos do titular dos dados e as modalidades de exercício dos direitos, que são agora previstos de forma detalhada.

xxiv. No presente estádio da investigação verificamos que algumas das propostas apresentadas já se encontram contempladas na revisão da legislação atinente ao Regulamento Geral de Proteção de Dados, nomeadamente: o direito a ser esquecido, o princípio de transparência, reforçado pelas tecnologias indutoras de transparência, bem como a introdução dos mecanismos da proteção de dados desde a conceção e a proteção de dados por defeito.

xxv. Contudo, concluímos que, por foça de constante evolução tecnológica, as soluções apresentadas no RGPD não têm conseguido acompanhar os riscos decorrentes da utilização de AmI, uma vez que continuam por resolver as questões relacionadas com a previsão legal de territórios digitais e de direito a identidades múltiplas, bem como, continua a persistir a necessidade de repensar a definição de dados pessoais no contexto de AmI. Verificamos que continuam por esclarecer as condições do consentimento inequívoco no contexto de computação ubíqua. Não ficou explícito como vão ser cumpridos as exigências de um processamento transparente de dados nos sistemas de AmI. Ademais, continua a ser necessário traçar normas específicas para regular o uso de agentes inteligentes de *software* no contexto dos AmI.

xxvi. Face ao exposto concluímos que a realidade criada por ambientes inteligentes apresenta novos riscos. O direito à privacidade e protecção de dados pessoais está justamente incumbido de proporcionar respostas a tais riscos, fornecendo tanto proteção contra utilizações abusivas de suas informações como garantias de que suas escolhas sobre a utilização de seus próprios dados serão livres e transparentes. Na medida em que as tecnologias dos AmI se encontram em constante evolução, a aplicação das salvaguardas também deve ser considerada

como objeto de um processo dinâmico, isto é, diferentes e novas garantias legais devem ser adotadas a fim de lidar com o surgimento e evolução das novas ameaças à privacidade e aos dados pessoais, existindo, na nossa convicção, a necessidade de adoção de um quadro institucional mais firme e de um quadro normativo mais coerente.

xxvii. Assim, defendemos que, no nosso entender e face ao exposto, o quadro legal europeu da privacidade e proteção de dados deve ser reforçado no contexto de computação ubíqua através de uma conjugação do direito, da própria tecnologia e as partes interessadas no domínio das TIC, com o objetivo de dar uma resposta adequada aos desafios trazidos pelos ambientes inteligentes e para que eles se possam tornar uma história de sucesso em harmonia com os princípios democráticos, e não se transformar no pesadelo orwelliano.

BIBLIOGRAFIA

Aarts, E., Harwig R., Schuurmans M. (2002). Ambient Intelligence. In P. Denning (Eds.), *The Invisible Future: The Seamless Integration of Technology in Everyday Life* (pp. 235- 250). Nova Iorque: McGraw-Hill.

Aarts, E., Roovers, R. (2003). Embedded System Design Issues in Ambient Intelligence. In T. Basten, M. Geilen, & H. d. Groot (Eds.), *Ambient Intelligence: Impact on Embedded System Design* (pp. 11-29). Norwell, MA: Kluwer Academic Publishers. DOI: 10.1007/0-306-48706-3_2.

Agre, P. E., Rotenberg, M. (Eds.). (1998). *Technology and Privacy: The New Landscape*. Cambridge, MA: Mit Press.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002). A Survey on Sensor Networks. *Communications Magazine, IEEE*, *40*(8), 102-114.

Al-Alawi, Adel Ismail. (2006). WiFi Technology: Future Market Challenges & Opportunities. *Journal of Computer Science*, *2*, 13-18. Disponível em: http://thescipub.com/PDF/jcssp.2006.13.18.pdf consultado a 9 de março de 2014.

Alcañiz, M., Rey, B. (2005). New Technologies for Ambient Technology. In G. Riva *et al.* (Eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction* (pp.3-15). Amsterdão: IOS Press.

Andrade, F. (2008). *Da contratação eletrónica: em particular da contratação eletrónica inter-sistémica inteligente.* Dissertação de Doutoramento, Universidade do Minho, Braga, Portugal.

Andrade, F. (2012a). Comunicações eletrónicas e direitos humanos: o perigo do "homo conectus". In Mário Ferreira Monte, Paulo de Tarso Brandão (Coord.), *Direitos humanos e sua efetivação na era da transnacionalidade: debate luso-brasileiro* (pp. 207-226).Curitiba: Juruá Editora.

Andrade, F. (2012b). Consideração jurídica das assinaturas dinâmicas no ordenamento jurídico português. *In Memórias do XVI Congresso Ibero Americano de Derecho e Informática.* Quito.

Andrade, F., Carneiro, D., Novais, P. (2010). A Inteligência Artificial na resolução de conflitos em linha. *Scientia Ivridica, 59* (321), 137-164. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/19388/1/4%20-%202010b%20-%20Journal%20Scientia%20Ivridica.pdf consultado a 4 de março de 2013.

Andrade, F., Costa, A., Novais, P. (2011). Privacidade e proteção de dados nos cuidados de saúde de idosos. In *Memórias do XV Congresso Ibero Americano de Derecho e Informática*, de FIADI – Federacion IberoAmericano de Asociaciones de Derecho e Informática e Asociación Argentina de Informática Jurídica Tomo 1, Buenos Aires, Argentina: Publicación elDial.com e Biblioteca Jurídica Online. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/15197/1/2011%20-Congresso%20Direito%20Argentina.pdf consultado a 6 de abril de 2013.

Andrade, F., Novais, P., Carneiro, D., Zeleznikow, J., Neves, J. (2010). Using BATNAs and WATNAs in Online Dispute Resolution. In K. Nakakoji, Y. Murakami, E. Mc- Cready (Eds.), *New Frontiers in Artificial Intelligence* (Vol. 6284), (pp. 5–18). Berlim: Springer. DOI:10.1007/978-3-642-14888-0_2.

Andrade, José Carlos Vieira de. (2012). *Os direitos fundamentais na Constituição Portuguesa de 1976.* (5ª ed.). Coimbra: Almedina.

Andrade, Manuel da Costa. (2006). *Sobre as proibições de prova em processo penal*, 1.ª reimp., Coimbra: Coimbra Editora.

Andrade, Norberto Nuno Gomes de. (2011). Future Trends in the Regulation of Personal Identity and Legal Personality in the Context of Ambient Intelligence Environments: The Right to Multiple Identities and the Rise of the Alvatars. In Sam Muller, *et al.* (Eds.), *The Law of the Future and the Future of Law*, FICHL Publication Series n.°11, (pp. 567-585). Oslo: Torkel Opsahl Academic

EPublisher.

Augusto, J. C., Mcculagh, P. (2007). Ambient Intelligence: Concepts and Applications. *International Journal on Computer Science and Information Systems*, *4*(1), 1-28. Disponível em: http://www.comsis.org/archive.php?show=pprnst-4604 consultado a 19 de janeiro de 2012.

Augusto, J. C. (2010). Past, Present and Future of Ambient Intelligence and Smart Environments. In Joaquim Filipe, Ana Fred, Bernadette Sharp (Eds.), *Agents and Artificial Intelligence,* (pp. 3-15). Berlim: Springer. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.212.1516 consultado a 20 de janeiro de 2013.

Berlin, I. (1969). Two Concepts of Liberty. In Isaiah Berlin, *Four Essays on Liberty* (pp. 118-172). Oxford: Oxford University Press.

Beslay, L., & Hakala, H. (2007). Digital Territory: Bubbles. In Paul. T. Kidd (Ed.), *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society* (pp. 69-78). Nova Deli: Vision Book.

Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F., Rohs, M. (2005). Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In Werner Weber, Jan M. Rabaey and Emilie H.L. Aarts (Eds.), *Ambient Intelligence* (pp. 5-29). Berlim: Springer.

Bomsdorf, B. (2005). Adaptation of Learning Spaces: Supporting Ubiquitous Learning in Higher Distance Education. In Nigel Davies and Thomas Kirste and Heidrun Schumann (Eds.), *Dagstuhl Seminar Proceedings 05181, Mobile Computing and Ambient Intelligence: The Challenge of Multimedia* (pp.1-13). Leibniz:Internationales Begegnungs- und Forschungszentrum Center fur Informatik. Disponível em: http://drops.dagstuhl.de/opus/volltexte/2005/371/ consultado a 4 de março de 2013.

Brazier, F., Oskamp, A., Prins, C., Schellekens, M., & Wijngaards, N. (2003). Are Anonymous Agents Realistic? In A. Oskamp, E. Weitzenböck (Eds.), *Proceedings of the LEA 2003: The Law*

and Electronic Agents (pp. 69-79). Oslo: Unipub. Disponível em http://www.iids.org/publications/lea03_anonymity.pdf consultado a 3 de fevereiro de 2013.

Brazier, F., Oskamp, A., Prins, C., Schellekens, M., & Wijngaards, N. (2004). Anonymity and Software Agents: An Interdisciplinary Challenge. *Artificial Intelligence and Law*, *12*(1-2), 137-157. Disponível 2013 em:http://link.springer.com/article/10.1007/s10506-004-6488-5#page-1 consultado a 3 de fevereiro de 2013.

Brey, P. (2005). Freedom and Privacy in Ambient Intelligence. *Ethics and Information Technology*, *7* (3), 157-166. Disponível em: http://www.utwente.nl/gw/wijsb/organization/brey/Publicaties_Brey/Brey_2006_Freedom-Privacy_AI.pdf consultado a 1 de fevereiro de 2013.

Broek, G. Van den, Cavallo, F., Wehrmann, C. (Eds.). (2010). *AALIANCE Ambient Assisted Living Roadmap* (Vol. 6). Amsterdão: IOS Press.

Broekens, J., Jonker, C. M., Meyer, J. J. C. (2010). Affective Negotiation Support Systems. *Journal of Ambient Intelligence and Smart Environments*, *2*(2), 121-144.

Brown, H. J., Marriott, A. L. (1999). *ADR Principles and Practice*. Londres: Sweet & Maxwell.

Café, A., Carneiro, D., Novais, P., Andrade, F. (2010). Sistema de resolução *online* de conflitos para partilhas de bens – divórcios e heranças. In Luís Barbosa, Miguel Correia (Eds.), *INFORUM-2º Simpósio de Informática* (pp. 779-790). Braga:Inforum. Disponível em: http://inforum.org.pt/INForum2010/papers/sistemas-inteligentes/Paper064.pdf consultado a 5 de janeiro de 2013.

Canotilho, José Joaquim Gomes. (2000). *Direito constitucional e teoria da constituição* (4.ª ed.). Coimbra: Almedina.

Canotilho, José Joaquim Gomes, Moreira, Vital. (2007). *Constituição da República Portuguesa Anotada* (4ª ed. Revista), Volume 1º, Artigos 1º a 107º. Coimbra: Coimbra Editora.

Cardoso, G., Mendonça, S., Lima,T., Paisana,M. e Neves.M. (2014, janeiro). *A Internet em Portugal – Sociedade em Rede 2014.* Lisboa: Publicações OberCom- Observatório da Comunicação. Disponível em: http://www.obercom.pt/client/?newsId=548&fileName=internet_portugal_2014.pdf consultado a 2 de setembro de 2014.

Carneiro, D., Castillo, J. C., Novais, P., Fernandéz-Caballero, A., Neves, J. (2012). Multimodal Behavioral Analysis for Non-invasive Stress Detection. *Expert Systems with Applications*, *39*(18), 13376-13389. DOI: dx.doi.org/10.1016/j.eswa.2012.05.065.x.

Carneiro, D., Novais, P., Andrade, F., Zeleznikow, J., Neves, J. (2009). The Legal Precedent in Online Dispute Resolution. In Guido Governatori (Ed.), *Legal Knowledge and Information Systems, Jurix 2009: The Twenty Second Annual Conference* (pp. 47-52). Amsterdão: IOS Press. Disponível em: http://repositorium.sdum.uminho.pt/handle/1822/19082 consultado a 3 de março de 2013.

Carneiro, D., Novais, P., Andrade, F., Zeleznikow J., Neves, J. (2014). Online Dispute Resolution: An Artificial Intelligence Perspective. *Artificial Intelligence Review*, *4*(2), 211-240. DOI: 10.1007/s10462-011-9305-z.

Carneiro, D., Novais, P., Andrade, F., Neves, J. (2011). Retrieving Information in Online Dispute Resolution Platforms: A Hybrid Method. In Kevin D. Ashley & Tom M. van Engers (Eds.), *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Law* (pp. 224-228), University of Pittsburgh School of Law, Pittsburgh, Pennsylvania. Nova Iorque: ACM. Disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/14515/1/ICAIL11%20CNAN.pdf consultado a 2 de maio de 2013.

Carneiro, D., Novais, P., Andrade, F., Zeleznikow, J., Neves, J. (2010). Using Case-Based Reasoning to Support Alternative Dispute Resolution. In Andre Ponce de Leon F. de Carvalho, *et al.* (Eds.), *Distributed Computing and Artificial Intelligence*, (vol.79), (pp. 123-130). Berlim: Springer. DOI: 10.1007/978-3-642-14883-5_16.

Carneiro, D., Novais, P., Costa, R., Gomes, P., Neves, J. (2009). EMon: Embodied Monitorization. In M. Tscheligi, *et al.* (Eds.), *Ambient Intelligence* (Vol. 5859), (pp. 133-142). Berlim: Springer.

Carneiro, D., Novais, P., Machado, L., Analide, C., Costa, N., Neves, J. (2011, janeiro). Role Playing Games and Emotions in Dispute Resolution Environments. In Emilio Corchado, *et al.* (Eds.), *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011* (pp. 155-162). Berlim: Springer.

Carneiro, D., Novais, P., Neves, J. (2011). Toward Seamless Environments for Dispute Prevention and Resolution. In Paulo Novais, Davy Preuveneers, Juan M. Corchado (Eds.), *Ambient Intelligence-Software and Applications. 2nd International Symposium on Ambient Intelligence* (pp. 25-32). Berlim: Springer.

Carvalho, Orlando de. (1981). *Teoria geral do Direito Civil.* Coimbra: Centelha.

Čas, Johann. (2011). Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions. In Serge Gutwirth, *et al.* (Eds.), *Computers, Privacy and Data Protection an Element of Choice* (pp. 139-169). Londres: Springer.

Castro, Catarina Sarmento e. (2003, dezembro). O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro. In *VIII Congresso Ibero-Americano de Direito Constitucional*. Sevilha. Disponível em: http://www.estig.ipbeja.pt/~ac_direito/CatarinaCastro.pdf consultado a 5 de novembro de 2013.

Castro, Catarina Sarmento e. (2005). *Direito da informática, privacidade e dados pessoais.* Coimbra: Almedina.

Chagas, I. (1993). Aprendizagem não formal/formal das ciências: relações entre museus de ciência e escolas. *Revista de Educação*, *3* (1), 51-59. Disponível em: http://www.ie.ulisboa.pt/pls/portal/docs/1/298079.PDF consultado a 17 de dezembro de 2012.

Chang, K. H., Liu, S. Y., Chu, H. H., Hsu, J. Y. J., Chen, C., Lin, T. Y., Huang, P. (2006). The Diet-Aware Dining Table: Observing Dietary Behaviors Over a Tabletop Surface. In K. P. Fishkin, *et al.* (Eds.), *Proceedings of the International Conference on Pervasive computing. Lecture Notes in Computer Science* (Vol. 3968), (pp. 366-382). Berlim: Springer.

Cook, D. J., Youngblood, G. M., Jain, G. (2008). Algorithms for Smart Spaces. In A. Helal, M. Mokhtari and B. Abdulrazak (Eds.), *The Engineering Handbook of Smart Technology for Aging, Disability and Independence* (pp.783-800). Nova Jérsia: John Wiley & Sons. Disponível em: http://eecs.wsu.edu/~cook/pubs/adi07.pdf consultado a 9 de abril de 2013.

Cook, D. J., Augusto, J.C., Jakkula, V. R. (2009). Ambient Intelligence: Technologies, Applications and Opportunities. *Pervasive and Mobile Computing, 5* (4), 277-298. DOI:10.1016/j.pmcj.2009.04.001.

Correia, Luís Brito. (2000). *Direito da comunicação social* (Vol.I). Coimbra: Almedina.

Correia, Miguel J. A. Pupo. (2011). *Direito comercial, direito da empresa* (12ª ed. Revista e Atualizada). Lisboa: Ediforum.

Costa, Â., Castillo, J. C., Novais, P., Fernandéz-Caballero, A., Simoes, R. (2012). Sensor-driven Agenda for Intelligent Home Care of the Elderly. *Expert Systems with Applications*, *39*(15), 12192-12204.DOI:10.1016/j.eswa.2012.04.058.

Costa, Â., Novais, P., Corchado, J. M., Neves, J. (2012). Increased Performance and Better Patient Attendance in an Hospital with the Use of Smart Agendas. *Logic Journal of IGPL*, *20* (4), 689-698. DOI: 10.1093/jigpal/jzr021.

Costa, R., Carneiro, D., Novais, P., Lima, L., Machado, J., Marques, A., Neves, J. (2008). Ambient Assisted Living. In J. M. Corchado, D. Tapia, J. Bravo (Eds.), *Advances in Soft Computing, 3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008* (Vol. 51), (pp. 86-94). Berlim: Springer.

Costa, R., Novais, P., Lima, L., Carneiro, D., Samico, D., Oliveira, J., Machado, J., Neves. J. (2009). VirtualECare: Intelligent Assisted Living. In Dasun Weerasinghe (Ed.), *Electronic Healthcare* (pp. 138-144). Berlim: Springer.

Daskala B., Maghiros I. (2007). *D1gital Territ0ries Towards the Protection of Public and Private Space in a Digital and Ambient Intelligence Environment.* EUR - Scientific and Technical Research Reports. Luxembourg: Office for Official Publications of the European Communities. Disponível em: http://ftp.jrc.es/EURdoc/eur22765en.pdf consultado a 9 de outubro de 2014.

De Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., Fuster, G. G. (2009). Legal Safeguards for Privacy and Data Protection in Ambient Intelligence. *Personal and Ubiquitous Computing*, *13*(6), 435-444. DOI 10.1007/s00779-008-0211-6.

Delapierre, G., Grange, H., Chambaz, B., Destannes, L. (1983). Polymer-Based Capacitive Humidity Sensor: Characteristics and Experimental Results. *Sensors and Actuators*, *4*, 97-104.

Dey, A. K, Abowd, G. D. (2000). Towards a Better Understanding of Context and Context-Awareness. In *Workshop on the What, Who, Where, When, and How of Context-Awareness (CHI 2000)*. Haia, Países Baixos.Disponível em: https://smartech.gatech.edu/bitstream/handle/1853/3389/99-22.pdf;jsessionid=E9408D3271F7BA2980D7D8DD68E7A9E7.smart2?sequence=1 consultado a 2 de março de 2013.

Dias, Vera E. M. (2009). A responsabilidade dos prestadores de serviços em rede - as inovações do Decreto-Lei 7/2004. Relatório de Direito da Sociedade de Informação. In *Verbo Jurídico.* Disponível em: http://www.verbojuridico.com/doutrina/2011/veradias_responsabilidadeprestadoresservicosrede.pdf consultado a 9 de outubro de 2013.

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman, J. C. (2001). (Eds.). *Scenarios for Ambient Intelligence in 2010*, *ISTAG Final Report*. Sevilha: Institute for Prospective Technological Studies (IPTS). Disponível em:

http://www.ist.hu/doctar/fp5/istagscenarios2010.pdf consultado a 12 de março de 2014.

Farinho, Domingos Soares. (2006). *Intimidade da vida privada e media no ciberespaço*. Coimbra: Almedina.

Farringdon, J., Nashold, S. (2005). Continuous Body Monitoring. In Y. Cai (Ed.), *Ambient Intelligence for Scientific Discovery* (pp. 202-223). Berlim: Springer. DOI: 10.1007/978-3-540-32263-4_10.

Fox, D. (2009). The Right to Silence as Protecting Mental Control. *The Akron Law Review*, *42*, 763-801. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1617410 consultado a 2 de agosto de 2014.

Frada, M. Carneiro da. (2001). Vinho novo em odres velhos? A responsabilidade civil das «operadoras de internet» e a doutrina comum da imputação de danos. *Direito da Sociedade da Informação*, *2*, 7-32. Disponível em: http://www.apdi.pt/pdf/Vinho%20novo%20em%20odres%20velhos.pdf consultado a 6 de setembro de 2014.

Friedewald, M., Vildjiounaite, E., Punie, Y., Wright, D. (2006). The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues. In J. A Clark, *et al.* (Eds.), *Security in Pervasive Computing. Proceedings of the Third International Conference, SPC 2006, York, UK, April 18-21, 2006.* (pp. 119-133). Berlim, Heidelberg, Nova Iorque: Springer.

Friedewald, M., Vildjiounaite, E., Punie, Y., Wright, D. (2007). Privacy, Identity and Security in Ambient Intelligence: A Scenario Analysis. *Telematics and Informatics*, *24*(1), 15-29. Disponível em: http://friedewald-family.de/Publikationen/Telematics24.2007.15.pdf consultado a 9 de maio de 2013.

Friedman, R., Olekalns, M., Oh, S. H. (2007). Choosing Your Words Carefully: Managing'Face'During Online Dispute Resolution. In *IACM 20th Annual Conference 2007*

Meetings Paper. Budapeste, Hungria.Disponível em: http://ssrn.com/abstract=1111637 consultado a 11 de dezembro de 2012.

Gaggioli, Andrea. (2005). Optimal Experience in Ambient Intelligence. In G. Riva, *et al.* (Eds.), *Ambient Intelligence: The Evolution of Technology, Communication and Cognition Towards the Future of Human-Computer Interaction* (pp. 35-43). Amsterdão: IOS Press.

Galanxhi-Janaqi, H., Nah, F. F. H. (2004). U-commerce: Emerging Trends and Research Issues. *Industrial Management & Data Systems*, *104*(9), 744-755. DOI: dx.doi.org/10.1108/02635570410567739.

Gershman, A. (2002). Ubiquitous Commerce-always on, Always Aware, Always Pro-active. In *Proceedings of the 2002 Symposium on Applications and the Internet (SAINT 2002),* Nara, Japão (pp. 37-38). Washington, DC, EUA: IEEE Computer Society. DOI:10.1109/SAINT.2002.994443.

Goleman, D. (1995). *Emotional Intelligence.* Nova Iorque: Bantam Books.

Guerra, Amadeu. (2001). A lei da proteção de dados pessoais. In Alberto de Sá Mello, *et al.* (Eds.), *Direito da sociedade da informação* (Vol. 2). Coimbra: Coimbra Editora.

Gutwirth, S., De Hert, P. (2008). Regulating Profiling in a Democratic Constitutional State. In M. Hildebrandt, S. Gutwirth (Eds.), *Profiling the European Citizen*: *Cross Disciplinary Perspectives* (pp. 271-302). Dordrecht: Springer.

Hammond, A. M. G. (2003). How Do You Write "Yes"?: A Study on the Effectiveness of Online Dispute Resolution. *Conflict Resolution Quarterly*, *20*(3), 261-286. DOI: 10.1002/crq.25.

Heilmann, K., Kihanya, D., Light, A., Musembwa, P. (1995). *Intelligent Agents: A Technology and Business Application Analysis.* Berkeley: University of California.

Hildebrandt, M., Koops, E.J. (2010). The challenges of ambient law and legal protection in the profiling era. *Modern Law Review*, *73* (3), 428-460, pp.449-450. Disponível em:https://pure.uvt.nl/portal/files/1248058/Koops_The_Challenges_of_Ambient_Law_100712.pdf consultado a 9 de maio de 2013.

Hildebrandt, M. (2009). Profiling and AmI. In Kai Rannenberg, Denis Royer, Andre Deuker (Eds.), *The Future of Identity in the Information Society* (pp. 273-310). Berlim: Springer.

Hörnle, Julia. (2003). Online Dispute Resolution: The Emperor's New Clothes? *International Review of Law, Computers & Technology*, *17*(1), 27-37. DOI: 10.1080/1360086032000063093.

Hwang, G. J., Tsai, C. C., Yang, S. J. (2008). Criteria, Strategies and Research Issues of Context-Aware Ubiquitous Learning. *Educational Technology & Society*, *11* (2), 81-91. Disponível em: http://pdf.aminer.org/000/246/158/ubies_an_intelligent_expert_system_for_proactive_services_deploying_ubiquitous.pdf consultado a 2 de março de 2013.

Hwang, G. J., Yang, T. C., Tsai, C. C., Yang, S. J. (2009). A Context-Aware Ubiquitous Learning Environment for Conducting Complex Science Experiments. *Computers & Education*, *53*(2), 402-413. DOI: 10.1016/j.compedu.2009.02.016.

ISTAG - Information Society Technologies Advisory Group. (2005). Ambient Intelligence: From Vision to Reality. In G. Riva, *et al.* (Eds.), *Ambient Intelligence. The Evolution of Technology, Communication and Cognition Towards the Future of Human–Computer Interaction. Emerging Communication* (Vol. 6), (pp. 45-68). Amsterdão: IOS Press. Disponível em: http://www.neurovr.org/emerging/volume6.html consultado a 2 de fevereiro de 2013.

Jaquet-Chiffelle, D. O., Benoist, E., Haenni, R., Wenger, F., Zwingelberg, H. (2009). Virtual Persons and Identities. In K. Rannenberg, D. Royer, A. Deuker (Eds.), *The Future of Identity in the Information Society* (pp. 75-122). Berlim: Springer.

Jiawei, H., Kamber, M. (2001). *Data Mining: Concepts and Techniques.* São Francisco, EUA: Morgan Kaufmann.

Jones, P., Marsh, D. (1993). *Essentials of EDI Law: A Straightforward Legal Framework to Protect Your Business*. Ontário: Electronic Data Interchange Council of Canada.

Katsh, E. E., Katsh, M. E., Rifkin, J. (2001). *Online Dispute Resolution: Resolving Conflicts in Cyberspace*. São Francisco, EUA: Jossey-Bass Wiley Company.

Keegan, S., O'Hare, G. M., O'Grady, M. J. (2008). Easishop: Ambient Intelligence Assists Everyday Shopping. *Information Sciences*, *178* (3), 588-611. Disponível em: http://dl.acm.org/citation.cfm?id=1316219 consultado a 5 de janeiro de 2013.

Kolodner, J. L. (1992). An Introduction to Case-based Reasoning. *Artificial Intelligence Review*,*6* (1), 3-34. DOI: 10.1007/BF00155578.

Kosta, Eleni. (2013). *Consent in European Data Protection Law.* Países Baixos: Martinus Nijhoff Publisher.

Kourouthanassis, P., Roussos, G. (2003). Developing Consumer-friendly Pervasive Retail Systems. *IEEE Pervasive Computing*, *2*(2), 32-39. DOI: 10.1109/MPRV.2003.1203751

Kruger, D. (1998). *Access Denied? Preventing Information Exclusion* (Vol. 18). Londres: Demos.

Leenes, R., Koops, B. J. (2005). 'Code': Privacy's Death or Saviour?. *International Review of Law Computers & Technology*, *19*(3), 329-340. DOI: 10.1080/13600860500348572.

Leitão, Luís Menezes. (2001, janeiro). A responsabilidade civil na Internet. *Revista da Ordem dos Advogados, 61* (1)*,* 171-192.

Lemos, André. (2008). Mídias locativas e territórios informacionais. In L. Santaelle, P. Arantes (Eds.), *Estéticas tecnológicas. Novos modos de sentir* (pp. 207-230). São Paulo: EDUC.

Disponível em: http://geografias.net.br/pdf/Midia_Locativa_e_Territorios_Informacionais.pdf consultado a 10 de outubro em 2014.

Lemos, André. (2009). Mídias locativas e vigilância: sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais. In Rodrigo Firmino, Fernanda Bruno, Marta Kanashiro (Coord.), *Anais do evento "Vigilância, segurança e controle social na América Latina"* (pp. 621-648). Curitiba: Editora Universitária Champagnat, PUCPR. Disponível em*:* www2.pucpr.br/reol/index.php/SSSCLA?dd1=2696&dd99=pdf consultado a 9 de outubro de 2014.

Lewis, J. A., & Cuppari, M. (2009). Polygraph: The Truth Lies Within, *The Journal Psychiatry & Law*, *37*, 85-92.

Lieberman, H. (1998). Integrating User Interface Agents with Conventional Applications. *Knowledge-Based Systems*, *11* (1), 15-23. Disponível em: http://web.media.mit.edu/~lieber/Lieberary/Integrating-UI-Agents/Integrating-UI-Agents.html consultado a 5 de março de 2013.

Lin, K. J., Yu, T., Shih, C. Y. (2005). The Design of a Personal and Intelligent Pervasive-Commerce System Architecture. In *WMCS'05. The Second IEEE International Workshop on Mobile Commerce and Services, 2005.* (pp. 163-173). Munique, Alemanha: IEEE. DOI: 10.1109/WMCS.2005.25.

Lindwer, M., Marculescu, D., Basten, T., Zimmennann, R., Marculescu, R., Jung, S., Cantatore, E. (2003). Ambient Intelligence Visions and Achievements: Linking Abstract Ideas to Real-world Concepts. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition, 2003* (pp. 10-15). Munique, Alemanha: IEEE. DOI: 10.1109/DATE.2003.1253580.

Lodder, A., Thiessen, E. (2003). The Role of Artificial Intelligence in Online Dispute Resolution. In D.Choi, E.Katsh (Eds.), *Workshop on Online Dispute Resolution at the International Conference on Artificial Intelligence and Law.* Edimburgo, Reino Unido. Disponível em: http://www.mediate.com/Integrating/docs/lodder_thiessen.pdf consultado a 10 de março de 2013.

Lopes, J. M., Cabreiro, C. A. (2006). A emergência da prova digital na investigação da criminalidade informática. *Sub Júdice-Justiça e Sociedade*, *35*, 71-79.

Marques, José, A. S. Garcia, Martins, Lourenço. (2006). *Direito da informática*. (2ª ed.). Coimbra: Almedina.

Marques, J. A. G. (2004). Internet e privacidade. In Alberto de Sá e Melo, *et al.* (Eds.), *Direito da sociedade da informação*, (Vol.5), (pp. 23-64). Coimbra: Coimbra Editora.

McTear, M. F. (2000). Intelligent Interface Technology: From Theory to Reality? *Interacting with Computers*, *12*(4), 323-336. DOI: 10.1016/S0953-5438(99)00002-8.

Mikulecký, P. (2012, abril). Smart Environments for Smart Learning. In *DIVAI 2012 - 9th International Scientific Conference on Distance Learning in Applied Informatics* (pp. 213-222). Sturovo, Eslováquia. Disponível em: http://conferences.ukf.sk/public/conferences/1/divai2012_conference_proceedings.pdf consultado a 9 de janeiro de 2013.

McDermott-Wells, P. (2004). What is Bluetooth? *Potentials, IEEE, 23*(5), 33-35. DOI:10.1109/MP.2005.1368913.

Miranda, Jorge, Medeiros, Rui. (2010). *Constituição Portuguesa Anotada*. Tomo I (2ª ed.) Coimbra: Coimbra Editora.

Mont, M. C., Pearson, S., Bramhall, P. (2003). *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. Technical Report HPL N.º 2003-49.* Reino Unido: HP Laboratories Bristol. Disponível em: http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf consultado a 15 de junho de 2014.

Moreira, Teresa Alexandra Coelho. (2010). *A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação: contributo para um estudo dos limites do poder do controlo eletrónico do empregador.* Vila Nova de Gaia**:** Almedina.

Nabeth, Thierry. (2009). Identity of Identity. In K. Rannenberg, D. Royer, A. Deuker (Eds.), *The Future of Identity in the Information Society: Challenges and Opportunities* (pp. 19-69). Berlim, Londres: Springer.

Najafi, B., Aminian, K., Paraschiv-Ionescu, A., Leow, F., Bula, C. J. R., Robert P. (2003). Ambulatory System for Human Motion Analysis Using a Kinematic Sensor: Monitoring of Daily Physical Activity in the Elderly. *Biomedical Engineering, IEEE Transactions on*, *50*(6), 711-723. DOI: 10.1109/TBME.2003.812189.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, *17*(5), 559-596.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 101–158.

Novais, P. (2003). *Teoria dos processos de pré-negociação em ambientes de comércio Eletrónico*. Dissertação de Doutoramento, Departamento de Informática, Universidade do Minho, Braga, Portugal.

Novais, P., Carneiro, D., Gomes, M., Neves, J. (2012). Non-invasive Estimation of Stress in Conflict Resolution Environments. In Yves Demazeau, *et al.* (Eds.), *Advances on Practical Applications of Agents and Multi-Agent Systems* (pp. 153-159). Berlim: Springer.

Novais, P., Carneiro, D., Gomes, M., Neves, J. (2013). The Relationship Between Stress and Conflict Handling Style in an ODR Environment. In Yoichi Motomura, Alastair Butler, Daisuke Bekki (Eds.), *Lecture Notes in Computer Science, New Frontiers in Artificial Intelligence. JSAI-isAI 2012 Workshops, LENLS, JURISIN, AMBN, ISS, Revised Selected Papers,* 7859 (pp. 125-140). Berlim: Springer. DOI: 10.1007/978-3-642-39931-2_10.

Novais, P., Costa, R., Carneiro, D., Neves, J. (2010). Inter-organization Cooperation for Ambient Assisted Living. *Journal of Ambient Intelligence and Smart Environments*, *2*(2), 179-195. DOI: 10.3233/AIS-2010-0059.

O'Donoghue, J., Herbert, J. (2006). An Intelligent Data Management Reasoning Model Within a Pervasive Medical Environment. In J. C. Augusto, D. Shapiro (Eds.), *Proceedings of the 1st Workshop on Artificial Intelligence Techniques for Ambient Intelligence (AITAmI 2006)* (pp. 27-31). Riva del Garda, Itália. Disponível em: http://www.cs.ucc.ie/~herbert/pubs/AITAmI2006.pdf consultado a 19 de março de 2014.

Ogawa, M., Suzuki, R., Otake, S., Izutsu, T., Iwaya, T., Togawa, T. (2002). Long Term Remote Behavioral Monitoring of Elderly by Using Sensors Installed in Ordinary Houses. In *2nd Annual International IEEE-EMB Special Topic Conference on Microtechnologies in Medicine and Biology* (pp. 322-325). Madison, EUA: IEEE. DOI:10.1109/MMB.2002.1002339.

Pepetela. (2007). *O terrorista de Berkeley, Califórnia.* Lisboa: Dom Quixote de Portugal.

Peruginelli, G., Chiti, G. (2002). Artificial Intelligence in Alternative Dispute Resolution. In *Proceedings of the Workshop on the Law of Electronic Agents–LEA*. *Workshop on the Law of Electronic Agents* (pp. 97–104). Bolonha: CIRSFID.

Picard, R. W. (1997). *Affective Computing*. Cambridge, Massachusetts: MIT Press.

Pinto, P. M. (1993). O direito à reserva sobre a intimidade da vida privada. *Boletim da Faculdade de Direito da Universidade de Coimbra*, *69*, 479-586.

Pinto, P. M. (2000). A limitação voluntária do direito à reserva sobre a intimidade da vida privada. In Jorge Dias de Figueiredo *et al.* (Eds.), *Estudos em homenagem a Cunha Rodrigues* (Vol. 2), (pp. 527- 558). Coimbra: Coimbra Editora.

Pitkänen, O. (2003). Legal Challenges to Ubicommerce. In *UbiComp 2003 Adjunct Proceedings* (pp.16-19). Seattle, WA, EUA. Disponível em: http://www.dcs.bbk.ac.uk/~gr/u-commerce/ubicommerce.pdf consultado a 19 de janeiro de 2013.

Pollack, M. E. (2005). Intelligent Technology for an Aging Population: The Use of AI to Assist Elders with Cognitive Impairment. *AI Magazine*, *26* (2), 9-24. Disponível em: http://www.aaai.org/ojs/index.php/aimagazine/article/view/1810/1708 consultado a 3 de abril de 2014.

Poullet, Y. (2009). Data Protection Legislation: What is at Stake for our Society and Democracy? *Compute Law & Escurita Review*, *25* (3), 211-226. Disponível em: http://users.ecs.soton.ac.uk/pw6g08/notes/info2009/resource4.pdf consultado a 8 de dezembro de 2012.

Poullet, Y. (2010). About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In Serge Gutwirth, Yves Poullet, Paul De Hert (Eds.), *Data Protection in a Profiled World* (pp. 3-30). Paises Baixos: Springer.

Punie, Y. (2003). A Social and Technological View of Ambient Intelligence in Everyday Life: What Bends the Trend? *Reports for European Media, Technology and Everyday Life Research Network (EMTEL2).* Key Deliverable Work Package 2, Joint Research Centre. Sevilha: Institute for Prospective Technological Studies (IPTS). Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.4939&rep=rep1&type=pdf consultado a 16 de dezembro de 2012.

Punie, Y. (2005). The Future of Ambient Intelligence in Europe: The Need for More Everyday Life. *Communications and Strategies*, *57*(1), 141-165. Sevilha**:** Institute for Prospective Technological Studies (IPTS). Disponível em: http://www.idate.org/fic/revue_telech/410/CS57_PUNIE.pdf consultado a 2 de janeiro de 2013.

Qi, H., Iyengar, S. S., Chakrabarty, K. (2001). Multiresolution Data Integration Using Mobile Agents in Distributed Sensor Networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, *31*(3), 383-391. DOI:10.1109/5326.971666.

Quigley, Aaron J., Bodea, Florin. (2010). Face-to-Face Collaborative Interfaces. In A. Hamid, D. Ramón López-Cózar, J. C. Augusto (Eds.), *Human-Centric Interfaces for Ambient Intelligence* (pp.3-32). Amsterdão: Elsevier.

Raisinghani, M. S. *et al.* (2006). Ambient Intelligence: Changing Forms of Human-computer Interaction and their Social Implications. *Journal of Digital Information*, *5* (4).Disponível em: http://journals.tdl.org/jodi/index.php/jodi/article/view/149/147 consultado a 9 de março de 2014.

Rifkin, Janet. (2001). Online Dispute Resolution: Theory and Practice of the Fourth Party. *Conflict Resolution Quarterly*, *19*(1), 117-124. DOI: 10.1002/crq.3890190109.

Rodotà, S. (2009). Data Protection as a Fundamental Right. In Serge Gutwirth, *et al.* (Eds.), *Reinventing Data Protection?* (pp. 77-82). Paises Baixos: Springer.

Roussos, G., Moussouri, T. (2004). Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce. *Personal and Ubiquitous Computing*, *8* (6), 416-429. Disponível em: http://onemvweb.com/sources/sources/consumer_perception_commerce.pdf consultado a 4 de janeiro de 2013.

Rouvroy, A. (2008). Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence. *Studies in Ethics, Law, and Technology*, *2* (1), 1-51. DOI: 10.2202/1941-6008.1001. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 consultado a 9 de dezembro de 2012.

Rouvroy, A., Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In Serge Gutwirth *et al.* (Eds.), *Reinventing Data Protection?* (pp. 45-76). Paises Baixos: Springer.

Rule, C. (2003). *Online Dispute Resolution for Business: B2B, Ecommerce, Consumer, Employment, Insurance, and Other Commercial Conflicts*. São Francisco, EUA: Jossey-Bass Wiley Company.

Russell, S., Norvig, P. (1995). *Artificial Intelligence: A Modern Approach.* Nova Jérsia: Prentice-Hall, Englewood Cliffs.

Safaric, S., Malaric, K. (2006, junho). ZigBee Wireless Standard. In *Multimedia Signal Processing and Communications, 48th International Symposium ELMAR-2006* (pp. 259-262). Zadar, Croatia. DOI: 10.1109/ELMAR.2006.329562.

Saito, M. (2000, novembro). Expanding Welfare Concept and Assistive Technology. In *Proceedings of the IEEK Annual Fall Conference* (pp. 156-161). Ansan, Coreia do Sul. Disponível em: http://web.cecs.pdx.edu/~mperkows/Rehabilitation_Robots/Saito-paper.pdf consultado a 3 de abril de 2013

Santos, R. J. da Silva. (2010). *Sistema de apoio àoargumentação em grupo em ambientes inteligentes e ubíquos considerando aspetos emocionais e de personalidade*. Dissertação de Doutoramento, Universidade de Trás-os-Montes e Alto Douro, Vila Real, Portugal. Disponível em: http://hdl.handle.net/10348/2033 consultado a 19 de março de 2013.

Shekar, S., Nair, P., Helal, A. S. (2003, março). iGrocer: A Ubiquitous and Pervasive Smart Grocery Shopping System. In *Proceedings of the 2003 ACM Symposium on Applied Computing* (pp. 645-652). Nova Iorque, EUA: ACM. DOI: 10.1145/952532.952658.

Silva, Hugo Lança. (2005, dezembro). Os Internet Service Providers e o direito: são criminosos, são cúmplices, são parceiros da justiça, polícias ou juízes? In *Verbo Jurídico*. Disponível em: http://www.verbojuridico.com/doutrina/tecnologia/isp.pdf consultado a 6 de junho de 2014.

Silva, Hugo Lança. (2006, setembro). Monitorização da internet: onde fica o direito à privacidade? In *Verbo Jurídico.* Disponível em:

http://www.verbojuridico.com/doutrina/tecnologia/monitorizacaointernet.pdf consultado a 6 de setembro de 2013.

Spiekermann, S., Pallas, F. (2006). Technology Paternalism–Wider Implications of Ubiquitous Computing. *Poiesis & Praxis*, *4* (1), 6-18. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=761111 consultado a 6 de agosto de 2013.

Stanford, V. (2004). Biosignals Offer Potential for Direct Interfaces and Health Monitoring. *Pervasive Computing, 3* (1), 99-103. DOI: OI: 10.1109/MPRV.2004.1269140.

Stefanov, D. H., Bien, Z., Bang, W. C. (2004). The Smart House for Older Persons and Persons with Physical Disabilities: Structure, Technology Arrangements, and Perspectives. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, *12*(2), 228-250. Disponível em: http://www.schattauer.de/de/magazine/uebersicht/zeitschriften-a-z/imia-yearbook/imia-yearbook-2006/issue/special/manuscript/6806/download.html consultado a 5 de abril de 2013.

Steventon, A., Wright, S. (Eds.). (2010). *Intelligent Spaces: The Application of Pervasive ICT*. Londres: Springer.

Vardasca, R., Costa, A., Mendes, P. M., Novais, P., Simões, R. (2013). Information and Technology Implementation Issues in AAL Solutions. *International Journal of E-Health and Medical Communications (IJEHMC)*, *4*(2), 1-17. DOI:dx.doi.org/10.4018/jehmc.2013040101.

Vasconcelos, Pedro Pais de. (1999). Proteção de dados pessoais e direito à privacidade. In AA.VV., *Direito da sociedade da informação* (Vol.1), (pp. 241-253). Coimbra: Coimbra Editora.

Veiga, A., Rodrigues, B. S. (2007). A monitorização de dados pessoais de tráfego nas comunicações eletrónicas. *Raízes Jurídicas*, *3* (2), 59-110. Disponível em: http://www.estig.ipbeja.pt/~ac_direito/monitorizacao.pdf consultado a 5 de janeiro de 2014.

Vicente, Dário Moura. (2005). *Problemática internacional da sociedade da informação.* Coimbra: Almedina.

Vitaliano, P. P., Echeverria, D., Yi, J., Phillips, P. E., Young, H., Siegler, I. C. (2005). Psychophysiological Mediators of Caregiver Stress and Differential Cognitive Decline. *Psychology and Aging*, *20* (3), 402-411. Disponível em: http://faculty.washington.edu/pemp/pdfs/pemp2005-04.pdf consultado a 15 de maio de 2013.

Warren, S. D., Brandeis, L. D. (1890, dezembro). The Right to Privacy. *Harvard Law Review*, *4*(15), 193-220.

Weiser, M. (1999). The Computer for the 21st Century. *ACM SIGMOBILE Mobile Computing and Communications Review*, *3*(3), 3-11.

Weitzenboeck, E. M. (2001). Electronic Agents and the Formation of Contracts. *International Journal of Law and Information Technology*, *9*(3), 204-234. Disponível em:http://folk.uio.no/emilyw/documents/EMILY%20%20Version%2019%20August%20&%20source.pdf consultado a 2 de fevereiro de 2013.

Winn, J. K. (2009). Technical Standards as Data Protection Regulation. In Serge Gutwirth, *et al.* (Eds.), *Reinventing Data Protection?* (pp. 191-206). Paises Baixos: Springer.

Winters, N., Walker, K., Roussos, G. (2005, junho). Facilitating Learning in an Intelligent Environment. In *IEEE International Workshop on Intelligent Environments*, (pp. 74-79). Londres: Institute of Electrical Engineers. Disponível em: http://www.lkl.ac.uk/people/kevin/ie05.pdf consultado a 9 de janeiro de 2013.

Witten, I. H., Frank, E. (2005). *Data Mining: Practical Machine Learning Tools and Techniques*. São Francisco, EUA: Morgan Kaufmann.

Wolffenbuttel, R. F., Mahmoud, K. M., Regtien, P. P. (1990). Compliant Capacitive Wrist Sensor for Use in Industrial Robots. *Instrumentation and Measurement, IEEE Transactions on*, *39*(6), 991-997.

Woolf, B. P. (2009). *Building Intelligent Interactive Tutors: Student Centred Strategies for Revolutionizing E-learning.* Nova Jérsia: Elsevier.

Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M., Moscibroda, A. (2009). Privacy, Trust and Policy-Making: Challenges and Responses. *Computer Law & Security Review*, *25*(1), 69-83. DOI: 10.1016/j.clsr.2008.11.004.

Wright, D. (Ed.) (2006). *Safeguards in a World of Ambient Intelligence: Final Report*, *SWAMI Deliverable D4*. Karlsruhe: Fraunhofer Institute for Systems and Innovation Research. Disponível em: http://is.jrc.ec.europa.eu/pages/TFS/documents/SWAMID4-final.pdf consultado a 2 de fevereiro de 2013.

Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E., Punie, Y. (Eds.). (2008). *Safeguards in a World of Ambient Intelligence.* Dordrecht: Springer.

Pareceres, relatórios e outra documentação

Article 29 Data Protection Working Party, *Recommendation 3/97: Anonymity on the Internet,* (XV D /5022/97 final WP 6), adotado em 3 de dezembro de 1997. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf consultado a 15 de maio de 2013.

Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*,(10107/05/EN WP 105), de 19 de janeiro de 2005. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf consultado a 3 de abril de 2013.

Autoridade Europeia para a Proteção de Dados, *Parecer sobre a promoção da confiança na sociedade da informação através do reforço da proteção dos dados e da privacidade*, (2010/C280/01), de 16 de outubro de 2010. Disponível

em:http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:PT:PDF consultado a 13 de março de 2014.

CNPD, *Autorização n.º17/96*, in relatório da Comissão Nacional de Protecção de Dados, de 1996.

CNPD, *Autorização n.º45/96,* in relatório da Comissão Nacional de Protecção de Dados, de 1996.

CNPD, *Autorização n.º11/97,* in relatório da Comissão Nacional de Protecção de Dados, de 1997.

CNPD, *Autorização n.º51/99,* in relatório da Comissão Nacional de Protecção de Dados, de 1999.

CNPD, *Parecer 22/2001 acerca da comunicação a terceiros de dados pessoais contidos na Base de Dados do Recenseamento Eleitoral,* de 2001. Disponível em: http://www.cnpd.pt/bin/orientacoes/ACESSO-BDRE-2001.pdf consultado a 16 de fevereiro de 2013.

Comissão de Comunidades Europeias, *Envelhecer bem na sociedade da informação*, uma iniciativa i2010 Plano de Ação no domínio "Tecnologias da Informação e das Comunicações e Envelhecimento" (COM (2007) 332 final), de 14 de junho de 2007. Disponível em: http://europa.eu/legislation_summaries/information_society/strategies/l24292_pt.htm consultado a 8 de abril de 2014.

Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu e ao Conselho relativa à promoção da proteção de dados através de tecnologias de proteção da privacidade,* (COM (2007) 228 final), de 2 de maio de 2007. Disponível em: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0228 consultado a 13 de outubro de 2013.

Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma abordagem global da*

proteção de dados pessoais na União Europeia, (COM (2010) 0609 final), de 4 de novembro de 2010. Disponível em: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pt.pdf consultado a 13 de outubro de 2013.

Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Proteção da privacidade num mundo interligado; Um quadro europeu de proteção de dados para o século XXI*, (COM (2012) 9 final), de 25 de janeiro de 2012. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:PT:PDF consultado a 14 de outubro de 2013.

Comissão Temporária do Parlamento Europeu sobre o Sistema de Intercepção ECHELON, Relator: Gerhard Schmid, *Relatório sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON")*, (2001/2098 (INI)), de 11 de julho de 2001. Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=PT consultado a 8 de novembro de 2012.

Comité Económico e Social Europeu, *Parecer sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à resolução de litígios de consumo em linha (Regulamento ODR)*, (COM (2011) 794 final-2011/0374 (COD)), de 28 de março de 2012. Disponível em: https://toad.eesc.europa.eu/ViewDoc.aspx?doc=ces%5Cint%5Cint610%5CPT%5CR_CES96-2012_DT_PT.doc&docid=2819086 consultado 5 de abril de 2013.

Committee of Ministers*, Recommendation N.ºR (87) 15 and Explanatory Memorandum of the regulating the use of personal data in the police sector,* adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies. Disponível em: http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf consultado a 10 de outubro de 2014.

Conselho Europeu, *Programa de Estocolmo - uma Europa aberta e segura que sirva e proteja os cidadãos,* ((2010/C 115/01)), Jornal Oficial C115, de 4 de maio de 2010. Disponível em:

http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0034_pt.htm consultado a 26 de janeiro de 2013.

Grupo de Proteção de Dados do Artigo 29.º, *Parecer 9/2011 sobre a proposta revista da indústria relativa a um quadro para as avaliações do impacto das aplicações RFID na proteção da privacidade e dos dados,* (00327/11/PT WP180), adotado em 11 de fevereiro de 2011. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_pt.pdf consultado a 13 de março de 2014.

Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 1/2012 sobre as propostas de reforma em matéria de proteção de dados*, (00530/12/PT WP 191), adotado em 23 de março de 2013. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_pt.pdf consultado a 2 de fevereiro de 2013.

Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 168 do sobre o futuro da privacidade, contribuição conjunta para a consulta da Comissão Europeia sobre o quadro jurídico relativo ao direito fundamental à proteção dos dados pessoais* (*art.º 29 WP and WP on Police and Justice, Future of Privacy, Joint Contribution to the consultation of the European Commission on the legal framework for the fundamental light to protético of personal data*), (02356/09/EN WP 168), adotado em 1 de dezembro de 2009. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf consultado a 13 de março de 2014.

Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 2/2003 sobre a aplicação dos princípios de proteção de dados às listas Whois,* (10972/03/PT final WP 76), adotado em 13 de junho de 2003. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_pt.pdf consultado a 5 de novembro de 2013.

Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 3/1999 no que diz respeito ao tratamento de dados pessoais relativo a informação do sector público e proteção de dados*

pessoais. Contribuição para a consulta iniciada com o Livro Verde da Comissão Europeia intitulado "Informação do sector público: um recurso fundamental para a Europa", (COM (1998) 585 WP 20), adotado em 3 de maio de 1999. Disponível em:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp20pt.pdf consultado a 5 de novembro de 2013.

Grupo de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, (01248/07/PT WP136), adotado em 20 de junho de 2007. Disponível em: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf consultado a 13 de março de 2014.

Grupo de Trabalho de Proteção de Dados Pessoias do Artigo 29.º, *Parecer 15/2011 sobre a definição de consentimento,* (01197/11/PT WP187), adotado em 13 julho de 2011. Disponível em: http://www.gpdp. gov.mo/uploadfile/others/wp187_pt.pdf consultado a 12 de outubro de 2014.

Grupo de Trabalho de Proteção de Dados Pessoais do Artigo 29.º, *Parecer 2/2010 do sobre publicidade comportamental em linha,* (0909/10/PTWP171), adotado em 22 de junho de 2010. Disponível em:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf consultado a 13 de março de 2014.

Parlamento Europeu e Conselho Europeu, *Proposta de Diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados*, (COM (2012) 10 final), de 25 de janeiro de 2012. Disponível em:http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:PT:PDF consultado a 6 de junho de 2013.

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

(COM (2012) 11 final), de 25 de janeiro de 2012. Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf consultado a 15 de novembro de 2012.

Parlamento Europeu, *Resolução legislativa, sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,* (COM(2012)0011 –MC7 - 0025/2012 – 2012/0011(COD)), de 12 de março de 2014. Estrasburgo. Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=PT&ring=A7-2013-0402 consultado a 1 de abril de 2014.

Procuradoria-Geral da República – lGabinete Cibercrime, *A obtenção do endereço IP - súmula da jurisprudência recente. Nota Prática n.º 2/2013,* de 3 de abril de 2013. Disponível em: http://cibercrime.pgr.pt/documentos/2013_04_03%20nota%20pratica%20-%20jurispridencia%20sobre%20I.pdf consultado a 10 de outubro de 2014.

Jurisprudência

Acórdão da Relação de Évora de 22 de dezembro de 2012 no processo 72/11.2DFTR-4.E1. Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/050470526baad26f80257ada0044b126?OpenDocument consultado a 5 de setembro de 2014.

Acórdão da Relação de Évora de 7 de dezembro de 2012 no Processo n.º 315/11.2PBPTG-A.E1. Disponível em: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/6f0b16b32262478f80257abc00517327?OpenDocument consultado a 5 de setembro de 2014.

Acórdão da Relação de Lisboa de 22 de janeiro de 2013 no Processo n.º581/12.6PLSNT-A-L1-5. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7bd2dd8af10b34c380257b27003a5697?OpenDocument consultado a 5 de setembro de 2014.

Acórdão do Tribunal de Justiça da União Europeia (Grande Secção) de 8 de abril de 2014 nos Processos Apensos C-293/12 *(Digital Rights Ireland)* e C-594/12 *(Seitlinger)*. Disponível em em:http://curia.europa.eu/juris/document/document.jsf?docid=150642&text=&doclang=PT consultado a 20 de maio de 2014.

Acórdão do Tribunal de Justiça da União Europeia (Grande Secção) de 13 de maio de 2014 no Processo C-131/12. Coletânea geral, *Google Spain SL, Google Inc. contra Agência Espanhola de Proteção de Dados, Mario Costeja González.* Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd893c7971ed634404b9dbce9953fc6761.e34KaxiLc3qMb40Rch0SaxuNbxf0?text=&docid=152065&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=140038 consultado a 3 de junho de 2014.

Acórdão do Tribunal de Justiça da União Europeia de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, n.º 48. Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d54572c3c048834df2957684a99bb943cf.e34KaxiLc3eQc40LaxqMbN4ObhaKe0?text=&docid=115205&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=48954 consultado a 6 de dezembro de 2013.

Acórdão do Tribunal de Justiça da União Europeia de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, n.º 68. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=49163 consultado a 6 de dezembro de 2013.

Acórdão do Tribunal Europeu dos Direitos do Homem de 17 de julho de 2008, petição n.º 20511/03, *I. contra Finlândia.* Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87510#{"itemid":["001-87510"]} consultado a 5 de novembro de 2013.

Acórdão do Tribunal Europeu dos Direitos do Homem de 2 de dezembro de 2008, petição n.º 2872/02, *K.U. contra Finlândia.* Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]} consultado a 5 de novembro de 2013.

Acórdão do Tribunal Europeu dos Direitos do Homem de 2 de setembro de 2010, petição n.º 35623/05, *Uzun contra Alemanha.* Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-100293#{"itemid":["001-100293"]} consultado a 5 de novembro de 2013.

Acórdão do Tribunal Europeu dos Direitos do Homem de 3 de abril de 2007, petição n.º 62617/00, *Copland contra Reino Unido.* Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-79996#{"itemid":["001-79996"]} consultado a 5 de novembro de 2013.

Acórdão do Tribunal Europeu dos Direitos do Homem de 4 de dezembro de 2008, *S. e Marper contra Reino Unido* (pedidos n.ºs 30562/04 e 30566/04. ECHR 1581 (4 de dezembro de 2008). Disponível em: http://www.bailii.org/cgi-bin/markup.cgi?doc=/eu/cases/ECHR/2008/1581.html&query=title+ (+marper+) &method=boolean consultado a 28 de março de 2014.

Acórdão do Tribunal Europeu dos Direitos do Homem de 7 de fevereiro de 2012, *Von Hannover contra Alemanha (n.º 2)*, pedidos n.ºs 40660/08 e 60641/08. Disponível em: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109029#{"itemid":["001-109029"]} consultado a 6 de dezembro de 2013.

Acórdão *Lindqvist* do Tribunal de Justiça de 6 de novembro de 2003 proferido no âmbito do Processo C-101/01 de 6 de novembro de 2003, Coletânea da Jurisprudência 2003 I-12971. Disponível em: http://curia.europa.eu/juris/liste.jsf?language=pt&num=C-101/01 consultado a 3 de maio de 2013.

Artigos de imprensa

Euronews: SCI-Tech Innovation. (2012, 20 dezembro). A Machine Wich Can Read Your Mind. *Euronews*. Disponível em: http://www.euronews.com/2012/12/20/a-machine-which-can-read-your-mind/ consultado a 5 de janeiro de 2014.

Eveleth, Rose. (2014, 18 julho). Neuroscience: 'I Built a Brain Decoder'. *BBC.* Disponível em: http://www.bbc.com/future/story/20140717-i-can-read-your-mind consultado a 10 de agosto de 2014.

Gellman, Barton. (2014, julho 11). How 160,000 Intercepted Communications Led to Our Latest NSA Story. *Washington Post*. Disponível em http://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html consultado a 10 de agosto de 2014.

Kroft, Steve. (2014, 9 março). The Data Brokers Selling Your Personal Information. *CBSNEWS*. Disponível em: http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ consultado a 10 de agosto de 2014.

Lusa. (2013, 4 de dezembro). Cruzamento de dados descobre milhares de pessoas a enganar o Estado. *Expresso.* Disponível em:http://expresso.sapo.pt/cruzamento-de-dados-descobre-milhares-de-pessoas-a-enganaroestado=f844457#ixzz36n3WaWXb consultado a 10 de dezembro de 2013.

Reding, Viviane. (16 de março de 2011). Your Data, Your Rights: Safeguarding Your Privacy in a Connected World*. Press Releases Database of the European Commission*. Disponível em: http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm consultado a 9 de maio de 2013.

Snowden Edward. (2013, dezembro 25). Alternative Christmas Message 2013. *Channel 4 .* Disponível em: http://www.channel4.com/programmes/alternative-christmas-message consultado a 28 de dezembro de 2013.

Sítios web

Google. *Relatório de transparência*. Disponível em: https://www.google.com/transparencyreport/removals/europeprivacy/ consultado a 8 de dezembro de 2014.

Agência Europeia para a Segurança das Redes e da Informação (ENISA). Disponível em: http://europa.eu/legislation_summaries/information_society/internet/l24153_pt.htm consultado a 3 de outubro de 2014.

Assistência Médica Internacional - AMI. *Infoexclusão.* Disponível em: http://www.ami.org.pt/default.asp?id=p1p211p215p340p364&l=1 consultado a 3 de fevereiro de 2013.

Bluetooth Special Interest Group Member Website. Disponível em: https://www.bluetooth.org/ consultado a 6 de dezembro de 2012.

Comissão Europeia - Comunicado de Imprensa (2012, 25 de janeiro), *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses.* Disponível em: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en consultado a 9 de fevereiro de 2013.

ESHA - *Elizabeth Stewart Hands and Associates. The Oficial ESHA Nutrient Database Website.* Disponível em: http://www.esha.com/product/database consultado a 27 de outubro de 2013.

Ferenstein, Gregory. (2012, 27 agosto). *Brain Hacking Scientist Extract Personal Secrets With Commercial Hardware.* Disponível em: http://techcrunch.com/2012/08/27/brain-hacking-scientists-extract-personal-secrets-with-commercial-hardware/ consultado a 5 de janeiro de 2014.

Gholipour, Bahar. (2013, agosto 26). *Reading Minds: Brain Scans Create Pictures of What You See.* Disponível em: http://www.livescience.com/39175-brain-scans-read-letters.html consultado a 5 de janeiro de 2014.

Grupo de Trabalho do Artigo 29.º de Proteção de Dados Pessoais. Disponível em: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm consultado a 6 de fevereiro de 2013.

Gupta, Milon. (2002). *Walls with Ears and Brains. The Unobtrusive Intrusion of Ambient Intelligence.* Disponível em: http://archive.eurescom.eu/message/messageDec2002/A_bit_beyond.asp consultado a 3 de janeiro de 2013.

Infopédia Porto. *Porto Editora.* Disponível em: http://www.infopedia.pt/ consultado a 5 de dezembro de 2012.

Intel Proactive Health. Disponível em: http://www.intel.com/content/www/us/en/healthcare-it/healthcare-overview.html consultado a 19 de novembro de 2012.

ISTAG (*Information Society Technologies Advisory Group*). Disponível em: http://cordis.europa.eu/fp7/ict/istag/about_en.html consultado a 17 de novembro de 2012.

Lextec-Léxico. *Técnico do Português do Instituto de Camões.* (2009). Disponível em: http://www.instituto-camoes.pt/lextec/por/domain_7/definition/19662.html consultado a 9 de dezembro de 2012.

Police and Criminal Evidence Act. (1984). Disponível em: http://www.legislation.gov.uk/ukpga/1984/60/contents consultado a 25 de março de 2014.

SmartSettle – Online Negotiation System. Disponível em: http://www.smartsettle.com consultado a 14 de novembro de 2012.

TIARAC: Telemática e Inteligência Artificial na Resolução Alternativa de Conflitos. Grupo de Inteligência Artificial. Departamento de Informática da Universidade do Minho (Centro de Ciências e Tecnologias de Computação da Universidade do Minho). Braga, Portugal. Disponível em: http://islab.di.uminho.pt/tiarac/ consultado a 18 de novembro de 2012.

United Nations Commission on International Trade Law. Working Group III (Online Dispute Resolution), Twenty-Second Session, Vienna, (13-17 December 2010), *Online Dispute Resolution for Cross-border Electronic Commerce Transactions.* Disponível em: http://daccess-dds-ny.un.org/doc/UNDOC/LTD/V10/574/10/PDF/V1057410.pdf?OpenElement consultado a 2 de maio de 2013.

ZigBee Alliance. Disponível em: http://www.zigbee.org/ consultado a 6 de novembro de 2012.