Faculdade de Direito da Universidade Nova de Lisboa

OS NOVOS DESAFIOS À PROTEÇÃO DE DADOS PESSOAIS NO INÍCIO DO SÉCULO XXI:
A CRIAÇÃO DE PERFIS, A INTELIGÊNCIA AMBIENTE E A SINGULARIZAÇÃO

Mestrado em Direito na área de Ciências Jurídico-Forenses
Dissertação orientada pela Professora Doutora Filipa Calvão

Graça Pacheco Costa

Julho 2013

Quero agradecer à Professora Doutora Filipa Calvão, orientadora desta dissertação, por toda a atenção, disponibilidade...

Não posso deixar de agradecer ao Mestre João Paulo Ribeiro pela preciosa ajuda na compreensão de conceitos técnicos na área da Informática.

Agradeço ainda à minha família e aos meus amigos, por todo o apoio e carinho.

RESUMO

A proteção de dados pessoais é um direito fundamental que enfrenta novos desafios no início do século XXI. As problemáticas que se suscitam são particularmente potenciadas pelas inovações tecnológicas. De entre essas novas problemáticas, destaca-se a criação de perfis, a inteligência ambiente e a singularização. As soluções para estes desafios deverão assentar na prevenção, no direito ao esquecimento, nas tecnologias de potenciação da privacidade, na transparência das relações e na sensibilização e capacitação dos titulares dos dados.

Palavras-Chave: proteção de dados pessoais; direitos fundamentais, privacidade

Abstract

Data protection is a fundamental right which faces new challenges at the beginning of the XXI century. The problems raised by these challenges are particularly potentiated by technological developments. Profiling, ambient intelligence and single out are highlighted by this subject. The solutions must focus on prevention, the right to be forgotten, privacy enhancing technologies, transparency and on data subjects' awareness and empowerment.

Keywords: data protection; fundamental rights; privacy

ABREVIATURAS E SIGLAS

AmI – *Ambient Intelligence* (inteligência ambiente)

CEDH - Convenção Europeia dos Direitos do Homem

CF. – Confrontar

CNPD – Comissão Nacional de Proteção de Dados

CNUDC – Convenção das Nações Unidas sobre os Direitos da Criança

CRP – Constituição da República Portuguesa

Diretiva da Privacidade Eletrónica – Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, alterada pela Diretiva 2009/136/CE, de 18 de dezembro

Diretiva 95/46/CE / Diretiva de Proteção de Dados - 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 dos dados pessoais e à livre circulação desses dados

DUDH - Declaração Universal dos Direitos Humanos

Endereço de IP/ IP – *Internet Protocol Adress*

GPS – *Global Positioning System* (Sistema de Posicionamento Global ou georreferenciação)

Grupo de Trabalho do Artigo 29.º - Grupo de Trabalho sobre a Protecção das Pessoas Singulares no que diz respeito ao Tratamento de Dados Pessoais

LPD – Lei de Proteção de Dados (Lei n.º 67/98, de 26 de outubro)

NLP – *Natural Language Processing* (processamento da linguagem natural)

OCDE/OECD – Organização para a Cooperação e Desenvolvimento Económico

P./PP. – Página/Páginas

PET – *Privacy Enhancing Tecnologies* (tecnologias de potenciação da privacidade)

RFID – *Radio frequency Identification* (identificação por radiofrequência)

SS. – seguintes

TEDH - Tribunal Europeu dos Direitos do Homem

VOL. - Volume

VS. - Versus

INTRODUÇÃO

O ser humano caracteriza-se pela comunicação, sociabilidade e criatividade, resultando desta tríplice aliança o desenvolvimento na área das tecnologias da informação e da comunicação.

Na procura de respostas às suas necessidades, a humanidade tem quebrado barreiras no espaço e no tempo, sendo hoje a comunicação da informação mais rápida, em maior quantidade e a um preço mais reduzido do que nunca. É neste plano que se reconhece que a necessidade de comunicação, aliada às constantes evoluções informáticas, tem motivado a acentuação da dependência tecnológica no Homem no século XXI.

Mas, se é verdade que uma sociedade sem comunicação e sem informação não é uma sociedade livre, não é menos verdade que a comunicação e a informação têm de obedecer a garantias de segurança e de fiabilidade. A inviolabilidade da correspondência sublinha precisamente essas garantias, no quadro da liberdade de expressão, de informação e de comunicação social.

Verifica-se, portanto, que o direito à vida privada não é incompatível com a sociabilização, assim como o não é com a vida pública. O ser humano, nas suas múltiplas vicissitudes, necessita tanto de um espaço que promova a interação social, como de um outro que fomente a reflexão, a intimidade e o recolhimento.

É da conjugação da vida pública com a vida privada que resulta o crescimento de cada um enquanto pessoa e, logo, da sociedade como um todo.

Diga-se que o respeito pela vida privada nada tem que ver com esconder ou enganar, tratando-se antes de um campo de cogitação e de introspeção, na esteira da promoção do livre desenvolvimento da personalidade de cada indivíduo.

É, por isso, essencial a proteção deste espaço de reserva da intimidade da vida privada, enquanto garante do direito ao livre desenvolvimento da personalidade, do direito à identidade e enquanto manifestação do princípio da dignidade humana.

O direito à reserva da intimidade da vida privada, pese embora seja um direito fundamental, é uma conquista frágil nos nossos dias. São inúmeras as violações de dados pessoais, estando a mais recente polémica relacionada com o acesso ilegítimo pela agência norte-americana *NSA - National Security Agency* aos registos de

chamadas telefónicas e ao conteúdo do correio eletrónico de milhões de cidadãos em todo o mundo.

Com efeito, é necessário reforçar o papel da proteção de dados pessoais, que assume uma posição de destaque na tutela da privacidade e da reserva da intimidade da vida privada.

No fundo, a proteção de dados pessoais é um dos pilares da consagração de vários direitos fundamentais, designadamente do direito à identidade, do direito à imagem, do direito ao livre desenvolvimento da personalidade, do direito à igualdade, do direito à liberdade e, claro está, do direito à vida privada.

Assim, impõe-se que seja dada visibilidade à proteção de dados pessoais, uma vez que a sua ação nunca foi tão necessária como agora.

Como se sabe, as inovações tecnológicas sempre fizeram parte das sociedades humanas e contribuíram em grande medida para o progresso civilizacional. Veja-se a invenção da escrita, da imprensa, da máquina fotográfica, da máquina de filmar, etc., cujo impacto na sociedade veio trazer novos desafios à proteção de dados pessoais, permitindo uma eventual eternização da passagem de um ser humano pelo nosso planeta.

Em todo o caso, e com o devido distanciamento histórico – que só o tempo permite – reconhecemos o enorme valor de todos estes progressos tecnológicos e quase ousamos dizer que a Internet desempenhou o mesmo efeito impulsionador na "sociedade da informação"[1].

Nessa perspetiva, cremos que a tecnologia deve estar ao serviço da humanidade, sendo as suas vantagens de tal modo inestimáveis que não devem ser poupados esforços na sua difusão pelo mundo. Contudo, apesar de não perfilharmos a visão fatalista de que o uso da tecnologia implica necessariamente a devassa da vida privada, acreditamos que as mais recentes inovações tecnológicas conglobam novos desafios à proteção de dados pessoais e, nessa medida, requerem a sensibilização de todos os intervenientes, nomeadamente dos seus utilizadores.

---

[1] Sobre este tema veja-se ALMEIDA, Reginaldo Rodrigues, *Sociedade Bit: Da Sociedade da Informação à Sociedade do Conhecimento*, 2.ª Edição, Quid Juris Sociedade Editora, 2004

Essa é também uma das razões que motivou a realização deste trabalho, que se espera venha a contribuir para a consciencialização da sociedade em geral e, em particular, dos utilizadores de meios eletrónicos.

De facto, as exigências da sociedade têm vindo a ser alvo de modificações ao longo do último século, pese embora a necessidade de proteção dos cidadãos ante a intromissão na sua vida privada seja a mesma que se colocava anteriormente, como o demostra o artigo de Warren e Brandeis sobre o direito à privacidade[2], redigido em 1890.

Neste sentido, as atuais preocupações que iremos tecer nada têm de novo na sua génese, relativamente às inquietações de então, salvo no que respeita ao seu grau e escalabilidade.

Com efeito, o fenómeno da globalização – como se constata da universalidade da própria terminologia informática[3] – potencia os efeitos da desproteção dos titulares dos dados.

Assim, atendendo às diferenças no impacto das modernas tecnologias na reserva da intimidade da vida privada e ao reflexo da globalização nos fluxos da informação, vimos avançar com algumas possíveis soluções para mitigar os riscos de violações de dados pessoais.

Importa sublinhar que este trabalho propõe uma análise jurídica sobre esta problemática, pese embora sejam tratados vários aspetos da área das Tecnologias da Informação e da Comunicação, uma vez que a realidade tecnológica obriga à decomposição de alguns conceitos relacionados com a computação e com a inteligência ambiente.

Assim, após uma breve contextualização da proteção de dados pessoais no campo dos direitos fundamentais, analisaremos a definição do conceito de dados

---

[2] WARREN, Samuel, BRANDEIS, Louis, "The Right to Privacy", in *Harvard Law Review*, n.º 5, vol. 4, dezembro, 1890.

[3] Apesar de a linguagem informática ser maioritariamente na língua inglesa, na realização deste trabalho tentámos, sempre que possível, adotar uma tradução em língua portuguesa. Advertimos, porém, que as traduções foram realizadas pela própria autora, pelo que as citações serão também escritas na sua língua original.

pessoais, os princípios estruturantes desta temática e veremos a importância da proteção de dados pessoais na plena concretização do direito à identidade.

Não faltam exemplos de problemáticas que atualmente se apresentam à proteção de dados pessoais, nomeadamente a computação em nuvem (*cloud computing*), a governação eletrónica (*e-government*), os *cookies*, os sistemas biométricos, etc. Todavia, para melhor podermos estudar as questões que cada uma suscita e para que não nos percamos na sua análise, optámos por delimitar o âmbito deste estudo a três desafios, a saber: a criação de perfis, a inteligência ambiente e a singularização. A escolha destes três temas prendeu-se com a sua atualidade e com o leque de problemáticas que suscitam no campo da proteção de dados.

Nesse sentido, este trabalho debruçar-se-á sobre esses três novos desafios, que entendemos serem merecedores de maior destaque, pelos riscos que aportam no quadro desta temática.

Por fim, avançaremos algumas possíveis soluções para as problemáticas que a matéria da proteção de dados suscita, em especial para os três desafios que nos propusemos analisar.

I. PROTEÇÃO DE DADOS PESSOAIS

Versando este trabalho sobre os novos desafios à proteção de dados pessoais no início do século XXI, importa delimitar o objeto do estudo no campo dos direitos fundamentais, relacionando-se particularmente com o direito ao livre desenvolvimento da personalidade, com o direito à reserva da intimidade da vida privada e com o direito à identidade pessoal.

Antes de prosseguirmos para a análise do regime jurídico da proteção de dados pessoais, cumpre tecer algumas considerações sobre o enquadramento constitucional desta matéria. Seguidamente, desenvolveremos algumas reflexões sobre o próprio conceito de dados pessoais, imprescindível para a compreensão do objeto deste estudo. Oportunamente, será ainda feita uma referência específica ao direito fundamental à identidade pessoal, por estar intimamente relacionado com o direito à proteção de dados e por se tratar de um direito particularmente posto em causa pelos novos desafios à proteção de dados pessoais que aqui iremos abordar.

i. A PROTEÇÃO DE DADOS PESSOAIS NO PLANO CONSTITUCIONAL

Porque constantes da Lei Fundamental, os direitos nela consagrados adquirem a designação de direitos fundamentais e são a expressão dos princípios axiológicos basilares de uma determinada sociedade, refletindo o seu estádio de evolução.[4]

Segundo Jorge Miranda, «[s]*omente há direitos fundamentais (…) quando o Estado e a pessoa, a autoridade e a liberdade se distinguem e até, em maior ou menor medida, se contrapõe*»[5].

---

[4] Sobre a evolução histórica do direito à reserva da vida privada, veja-se JIMÉNEZ, Luis, "Evolución histórica y conceptual del derecho a la vida privada", in *Revista de Los Tribunales Agrarios*, Segunda Época, n.º 42, año IV, Mayo-Agosto de 2007.

[5] MIRANDA, Jorge, *Manual de Direito Constitucional*, 3.ª Edição, Coimbra Editora, 2000, Tomo IV, p. 12.

Refere o mesmo autor que *«... a evolução e as vicissitudes dos direitos fundamentais, seja numa linha de alargamento e aprofundamento, seja numa linha de retração ou de obnubilação, acompanham o processo histórico, as lutas sociais e os contrastes de regimes políticos – bem como o progresso científico, técnico e económico»*[6].

Neste contexto, importa referir um conceito afim ao dos direitos fundamentais e que é o conceito de «direitos de personalidade», intrínseco à própria natureza humana e emanação dessa mesma personalidade humana.

Contudo, não obstante alguma coincidência, o conceito de direitos fundamentais não é sobreponível em absoluto ao conceito de direitos de personalidade.

Nessa medida, são vários os exemplos de direitos de personalidade, designadamente o direito ao desenvolvimento da personalidade, ao bom nome e reputação, à imagem, à palavra (cf. artigo 26.º da Constituição de República Portuguesa - CRP), certas garantias relativas à informática (cf. artigo 35.º da CRP), à reserva sobre a intimidade da vida privada (cf. artigo 80.º do Código Civil).

Ademais, pode dizer-se que os artigos 70.º a 81.º do Código Civil – sob a epígrafe «Direitos de Personalidade» - assumem a natureza de direitos fundamentais, quer por força da cláusula aberta prevista no n.º 1 do artigo 16.º da CRP, quer por decorrência do próprio princípio da dignidade humana.

Aliás, o artigo 1.º da CRP ao reconhecer, em primeiro lugar, a dignidade humana como valor logicamente anterior à própria ideia de Estado de Direito democrático, atribui a acentuação tónica da sua construção ao ser humano. Por outras palavras, será no respeito pela dignidade da pessoa humana que o texto constitucional assentará.

Suportando esta perspetiva, são inúmeros os exemplos na Constituição que constituem expressão direta do postulado básico da dignidade da pessoa humana.

Deste modo, a título exemplificativo, atentemos no artigo 26.º da Lei Fundamental[7], cuja epígrafe é «Outros direitos pessoais». Este dispositivo constitui a

---

[6] Ibidem, p. 27.

[7] Artigo 26.º da CRP:

enunciação do direito geral de personalidade e é, naturalmente, uma consagração do princípio pela dignidade humana.

Nas palavras de Rui Medeiros, «[p]*or ser expressão direta do postulado básico do respeito pela dignidade humana, o princípio consagrado neste artigo 26.º constitui uma "pedra angular" na demarcação dos limites ao exercício dos outros direitos fundamentais*».[8]

Refira-se que a Constituição da República Portuguesa concretiza e densifica o conteúdo do direito ao desenvolvimento da personalidade em vários momentos, contrariamente a outras leis fundamentais de outros ordenamentos jurídicos. A título de comparação, veja-se a Constituição alemã, que radica no n.º 1 do seu artigo 2.º todos os direitos fundamentais não especificados.

Porém, ainda que não adquira a dimensão estruturante que o Direito Alemão atribui ao n.º 1 do artigo 2.º da Lei Fundamental alemã – artigo que consagra o direito ao livre desenvolvimento da personalidade – o n.º 1 do artigo 26.º assume particular relevância, no que concerne à dignidade humana.[9]

De facto, o artigo 26.º da CRP tipifica alguns direitos de personalidade, concretizando o princípio fundamental de respeito pela dignidade humana. Contudo, o

---

1. 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.
2. A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.
3. A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica.
4. 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.

[8] MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Coimbra Editora, 2005, p. 283.

[9] Veja-se inclusivamente o regime processual privilegiado que a Constituição estabelece no n.º 5 do artigo 20.º, para a tutela dos direitos, liberdades e garantias, nos quais se integram os direitos previstos no artigo 26.º da CRP.

direito geral de personalidade compreende vários direitos e, portanto, estende-se para além dos direitos consagrados neste dispositivo legal.

Aliás, alguns dos direitos de personalidade encontram-se em áreas sobreponíveis, reforçando-se a sua aplicação pela coincidência das temáticas, de que são exemplo o direito ao desenvolvimento da personalidade e o direito à reserva da intimidade da vida privada, já que ambos os direitos são reflexo um do outro e pressupõem a sua existência conjunta.

Do mesmo modo, o direito à não discriminação é uma decorrência do princípio da igualdade, constitucionalmente consagrado no artigo 13.º da Lei Fundamental, pelo que a sua tutela está também duplamente reforçada.

Na verdade, os direitos de personalidade entrecruzam-se, sendo difícil determinar fronteiras claras entre estes direitos. Exemplificando, o direito ao desenvolvimento da personalidade pressupõe necessariamente a existência dos restantes direitos elencados no n.º 1 do artigo 26.º da CRP.

Assim, por maioria de razão, é manifesta a relevância destes direitos e, logo, o seu acolhimento constitucional. Porém, de entre os vários direitos de personalidade supra abordados, pode dizer-se que o direito à reserva da intimidade da vida privada será um dos direitos previstos no artigo 26.º com maior alcance prático. Ainda que a definição da intimidade da vida privada seja delineada por cada indivíduo, a doutrina tem considerado existirem três graus: a *esfera íntima*, a esfera *privada* e a *esfera social*[10].

Esta teoria foi primeiramente desenhada pela jurisprudência[11] e, posteriormente, pela doutrina alemãs, que – a par de uma esfera pública – definiram três esferas de maior reserva, a saber, a esfera pessoal, a privada e a íntima. O conteúdo de cada uma destas segmentações prende-se com o grau de intimidade que cada indivíduo

---

[10] MIRANDA, Jorge e MEDEIROS, Rui, Constituição Portuguesa Anotada, Coimbra Editora, 2005, p. 290.

[11] SCHWABE, Jürgen, *Jurisprudencia del Tribunal Constitucional Federal Alemán - Extratos de las Sentencias Más Relevantes*, Konrad-Adenauer – Stiftung e V., 2009.

atribui aos comportamentos e ações que desenvolve, na sua relação com a sociedade e com o mundo[12].

Contudo, segundo Rui Medeiros, é de rejeitar esta teoria, dada a sua rigidez conceptual, já que a teoria mais não é que a aplicação à reserva da intimidade da vida privada do regime das restrições aos direitos, liberdades e garantias, previsto nos n.ºs 2 e 3 do artigo 18.º da CRP.

Na verdade, diga-se que também o Tribunal Constitucional, em Portugal, tem tido um papel importante na concretização do direito à reserva da intimidade da vida privada, seja na área da videovigilância, seja na problemática da obtenção de prova em processo penal, na violação do segredo bancário, etc.

Ainda que muitas vezes conceptuais, as teorias avançadas pela jurisprudência e doutrina tendem a permitir uma reflexão mais estruturada, a partir da qual podem delinear-se, porventura, inúmeras exceções. Todavia, entendemos que a organização lógica desta divisão das várias esferas da reserva da intimidade da vida privada pode ser útil para a compreensão das problemáticas que se lhe apresentam.

Debrucemo-nos, agora, sobre o n.º 2 do artigo 26.º da CRP, que vem remeter para a lei o estabelecimento de garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.

Um dos diplomas legais que materializa esta imposição constitucional é a Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados - LPD), dispondo o seu artigo 2.º que o tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.

O entendimento subjacente a este diploma espelha que a efetiva garantia contra a obtenção e utilização abusivas de informações relativas ao indivíduo e à família se traduz na observância dos princípios da finalidade, da legalidade, da necessidade, da

---

[12] Sobre o direito à reserva da intimidade da vida privada, e com particular enfoque no ciberespaço, cf. FARINHO, Domingos Soares, *Intimidade da Vida Privada e Media no Ciberespaço*, Almedina, 2006, p. 43 e ss.

adequação, da proporcionalidade em sentido estrito e da não discriminação, enquanto decorrência do princípio da igualdade.

Sobre esta questão, veremos adiante o enquadramento legal e os princípios estruturantes que enformam os tratamentos de dados pessoais.

Regressando à análise do artigo 26.º da CRP, verifica-se que o n.º 3 deste artigo vem sublinhar a defesa da dignidade humana, colocando algumas reservas quanto à utilização de tecnologias e à experimentação científica. Esta preocupação do legislador constitucional deve-se aos abusos cometidos no passado – designadamente durante a II Guerra Mundial – ao abrigo da ciência e de outros discursos legitimadores, assim como à incerteza e incompreensão do caminho a trilhar num século marcadamente caraterizado pela revolução tecnológica. Recorde-se que o século XX assistiu à chegada do homem à lua, à criação do telemóvel, dos computadores e da Internet e à descodificação do ADN humano, e que o assoberbamento de tão rápidos avanços tecnológicos – muitas vezes aliado a um generalizado desconhecimento científico – foi tão admirável quanto temível.

Neste contexto, foram tanto preocupações éticas, quanto respeitantes à dignidade humana, que sensibilizaram o legislador, levando-o a consagrar constitucionalmente determinadas garantias.

Nessa senda, o artigo 35.º da CRP[13] vem também debruçar-se sobre a utilização da informática, sempre com vista à defesa da dignidade humana. Analisemos, por isso, o seu texto.

---

[13] Artigo 35º

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 previstos na 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 a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo

Em primeiro lugar, cumpre referir que a Constituição da República Portuguesa de 1976 foi a primeira a consagrar o direito à privacidade, na sua vertente de proteção dos dados pessoais informatizados, de entre o catálogo de direitos, liberdades e garantias, pelo que aqui se presta a devida homenagem à sensibilidade do legislador constituinte para estas matérias[14]. Feita esta justa homenagem, analisemos o teor do artigo 35.º da CRP na sua atual redação.

A título de enquadramento jurídico, importa esclarecer que a lei a que os n.ºs 1, 2, 6 e 7 deste artigo se reportam é a Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados – LPD).

O n.º 1 daquele artigo prevê os direitos de acesso, de retificação, de atualização e de informação, que são densificados nos artigos 10.º e 11.º da LPD. Trata-se de direitos da maior importância, na medida em que permitem ao titular dos dados um controlo efetivo da informação que lhe respeita.

Do mesmo modo, a definição do conceito de dados pessoais e as condições dos tratamentos de dados são desenvolvidas na LPD, a qual cria a Comissão Nacional de Protecção de Dados, nos termos do n.º 2 do artigo 35.º da CRP.

Na alínea a) do artigo 3.º da mesma lei, define-se como dado pessoal 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»), considerando identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação

---

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 lei o 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.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

[14] VARGES GOMES, Mário, *Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência*, Centroatantico.pt, 2006, p. 27.

ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

Paralelamente, a mesma lei distingue, dentro da classificação genérica de dados pessoais, uma categoria de dados à qual atribui uma proteção acrescida: os dados pessoais sensíveis (cf. artigo 7.º da LPD). Nesta categoria de dados incluem-se os 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 (cf. n.º 1 do artigo 7.º da LPD)[15]. Neste âmbito, veja-se a preocupação do legislador em sublinhar a exigência de garantias de não discriminação quanto ao tratamento de dados sensíveis.

Simultaneamente, o n.º 3 do artigo 35.º da CRP vem também elencar os dados que, pela sua natureza, merecem uma proteção reforçada. Inserem-se nesta categoria de dados, aqueles relativos a suspeitas de atividades ilícitas, infrações penais e contraordenações.

Relativamente à entidade administrativa independente constitucionalmente prevista, atualmente sob a designação de Comissão Nacional de Protecção de Dados (CNPD), cumpre destacar a sua ação meritória face às múltiplas solicitações e exigências técnicas com que se confronta, constituindo um indubitável bastião da defesa da dignidade humana.

Esta entidade administrativa independente, tem como atribuições controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, assim como tem uma função consultiva, no que respeita a quaisquer disposições legais e instrumentos jurídicos em preparação em instituições comunitárias ou internacionais, relativos ao tratamento de dados pessoais.

---

[15] O n.º 1 do artigo 7.º da LPD proíbe o tratamento de dados sensíveis, dispondo o n.º 2 do mesmo artigo as situações excecionais em que aquele tratamento pode ter lugar, por força de lei, mediante autorização da Comissão Nacional de Proteção de Dados ou com o consentimento do titular (desde que garantidas condições de não discriminação e medidas de segurança adequadas).

A CNPD não só é um garante da proteção de dados pessoais, como vê a sua missão efetivada pelos poderes de investigação e de inquérito, bem como de autoridade, que lhe são legalmente atribuídos. (cf. o n.º 2 do artigo 22.º da LPD).

Salientamos que as constantes alterações legislativas e tecnológicas obrigam a CNPD a desdobrar-se em várias frentes de defesa, desde a videovigilância ao controlo de trabalhadores por sistemas biométricos, da georreferenciação à constituição de biobancos, etc., obrigando esta entidade a reinventar-se, quer pela permanente exigência de atualização tecnológica, quer pelo esforço de estabelecer medidas preventivas numa área em constante mudança, sendo-lhe exigida uma incessante versatilidade para a cabal defesa dos direitos fundamentais.

Regressando à análise do artigo 35.º da CRP, o seu n.º 4 estabelece a proibição do acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. Estes casos estão dispersos em vários diplomas legais, sendo de sublinhar que, dado o seu caráter absolutamente excecional, todas as situações deviam ser fruto de uma ponderação minuciosa do legislador.

Ora, sendo terceiro todo aquele que não é o próprio titular dos dados, torna-se clara a restrição do acesso aos dados pessoais. E, note-se, não falamos apenas de dados sensíveis, mas de quaisquer dados pessoais.

Mesmo o responsável pelo tratamento de dados terá algumas limitações de acesso aos dados pessoais que trata, de acordo com os princípios norteadores da proteção de dados. Exemplificativamente, veja-se o caso das entidades empregadoras que, embora possuam serviços de medicina no trabalho, não podem aceder aos dados de saúde dos trabalhadores, que são de acesso exclusivo pelo médico do trabalho, pelas autoridades competentes e, naturalmente, pelo próprio titular[16].

Já a proibição constante do n.º 5 do artigo 35.º encontra a sua *ratio* no livre desenvolvimento da personalidade, impossibilitando que a articulação de várias

---

[16] Cf. Deliberação N.º 840/2010 da CNPD aplicável aos tratamentos de dados no âmbito da gestão da informação dos serviços de segurança e saúde no trabalho.

Veja-se ainda a Lei n.º 102/2009, de 10 de setembro, que estabelece o regime jurídico da promoção da segurança e saúde no trabalho.

fontes de informação permita a completa identificação e monitorização da vida de um indivíduo. A rastreabilidade da vida de um sujeito nas suas várias dimensões constituiria uma devassa na sua vida privada e intimidade.

De facto, a autodeterminação implica uma liberdade de ação que terá de ser incondicional, não sujeita a pressões externas e fiel à consciência do sujeito. O indivíduo só poderá desenvolver-se livre e plenamente se possuir um espaço de intimidade, no qual se possa descobrir e que seja propício à geração de ideias próprias, num ambiente que predisponha a essa reflexão introspetiva.

Continuando a análise do artigo 35.º, o seu n.º 6 aborda a temática dos fluxos transfronteiriços de dados. Na verdade a era tecnológica trouxe novas problemáticas a esta questão, uma vez que a circulação da informação foi potenciada, tornando-se pouco controlável. Seja pela rapidez das comunicações e interconexões de dados, seja pela maior centralização e descentralização da informação, seja pela possibilidade do seu cruzamento em quantidade, assistimos hoje a novos desafios, no que respeita à proteção de dados pessoais.

Acresce que os vários ordenamentos jurídicos não oferecem as mesmas garantias à proteção de dados, pelo que a circulação da informação por diferentes países poderá implicar uma perda significativa de direitos.

Por fim, não deixa de ser curioso que o último número do artigo 35.º da CRP, cuja epígrafe é a «Utilização da Informática», venha atribuir aos dados pessoais constantes de ficheiros manuais idêntica proteção aos ficheiros informatizados.

Pese embora tenha sido o tratamento de dados pessoais automatizados a despertar a atenção do legislador para a necessidade da sua especial proteção, a consciência de que os ficheiros manuais suscitavam problemas semelhantes mereceu também abrigo constitucional.

Assim, o legislador constituinte optou por focar a atenção nos ficheiros automatizados, estendendo as suas medidas de segurança *mutatis mutandis* aos ficheiros manuais.

Em suma, o artigo 35.º da CRP vem destacar tanto a vertente negativa do direito à proteção de dados pessoais («*the right to be let alone*»[17]), como a sua vertente positiva. Citando Catarina Sarmento e Castro, «[o] *direito consagrado no artigo 35.º 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. (…) Mas é mais. 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*»[18].

Feita esta análise sumária do enquadramento jurídico-constitucional da matéria de proteção de dados pessoais, importa agora perceber o que constituem dados pessoais.

---

[17] Cf. WARREN, Samuel, BRANDEIS, Louis, "The Right to Privacy", in *Harvard Law Review*, n.º 5, vol. 4, dezembro, 1890.

[18] CASTRO, Catarina Sarmento, "O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro" in *Comunicação no VIII Congresso Ibero-americano de Direito Constitucional*, Sevilha, 2003.

ii. O conceito de Dados Pessoais

Pese embora o conceito de dados pessoais esteja definido pela lei, parecem existir situações de fronteira, cujo enquadramento se reveste de alguma complexidade.

De facto, não é desejável que a proteção atribuída aos dados pessoais seja estendida a outros dados, para que não se imponham regras muito restritivas ao tratamento de dados não pessoais. Lembremos que a ideia subjacente à proteção de dados pessoais reside na proteção de direitos fundamentais, como o direito à intimidade da reserva da vida privada, o direito à identidade e o direito ao livre desenvolvimento da personalidade.

Contudo, é igualmente nociva a ideia de desproteção de verdadeiros dados pessoais. Em causa estão valores fundamentais reconhecidos constitucionalmente e, portanto, não pode a legislação descurar a sua proteção.

Vejamos, por isso as definições do conceito de dados pessoais, espelhadas em diferentes diplomas legais.

A alínea a) do artigo 2.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, estabelece como dado pessoal «*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*».

A Lei n.º 67/98, de 26 de outubro – que transpõe para a ordem jurídica portuguesa a Diretiva 95/46/CE, relativa à proteção das pessoas singulares, no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados – é particularmente fiel ao texto daquela Diretiva.

As semelhanças entre o texto da Diretiva 95/46/CE e da Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados – LPD), são evidentes ao longo de todo o diploma, não sendo a definição do conceito de dados pessoais exceção a esta regra[19].

Em ambos os diplomas, tanto o legislador comunitário como o legislador nacional pretenderam conferir uma noção alargada ao conceito de dados pessoais, aspirando abranger todas as informações que identifiquem ou possam identificar um determinado indivíduo. De facto, esta abordagem deliberadamente flexível do legislador permite, hoje em dia, a inclusão neste conceito de dados que não eram previsíveis à data da sua redação, como por exemplo o endereço de correio eletrónico.

Por um lado, não quis o legislador comunitário contemplar todos os dados, mas apenas aqueles que identifiquem ou permitam identificar uma pessoa. Por outro, pretende também evitar restrições indevidas na interpretação do conceito de dados pessoais.

Aliás, uma vez que falamos de interpretação do conceito de dados pessoais, atente-se que o artigo 29.º da Diretiva 95/46/CE veio estabelecer a criação de um grupo de trabalho de caráter consultivo e independente, composto por um representante da autoridade ou autoridades de controlo designadas por cada Estado-Membro, por um representante da autoridade ou autoridades criadas para as instituições e organismos comunitários, bem como por um representante da Comissão.

Dando resposta a esse imperativo normativo, foi criado o Grupo de Trabalho sobre a Protecção das Pessoas Singulares no que diz respeito ao Tratamento de Dados Pessoais (Grupo de Trabalho do Artigo 29.º), com vista a uniformizar a aplicação das normas jurídicas nacionais dos vários ordenamentos jurídicos comunitários quanto a este tema.

---

[19] Cf. alínea a) do n.º 3 da LPD: *«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»); 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»*.

Nesse sentido, veio o referido Grupo de Trabalho delimitar o âmbito do conceito de dados pessoais no Parecer n.º 4/2007, adotado em 20 de junho, que merece a nossa análise, com vista a melhor compreender a *ratio* dos legisladores comunitário e nacional. Assim, aquele Grupo de Trabalho decompôs a definição de dados pessoais em quatro elementos: 1) «*qualquer informação*», 2) «*relativa a*», 3) «*identificada ou identificável[pessoa singular]*» e 4) «*pessoa singular*».

1) PRIMEIRO ELEMENTO: «*QUALQUER INFORMAÇÃO*»

Vejamos, em primeiro lugar, qual o conteúdo da informação que identifica ou permite identificar um indivíduo. Tal como denunciado pela expressão *qualquer informação*, a amplitude dada ao conceito de dados pessoais é generosa. Assim, quer estejamos face a dados de identificação (como por exemplo o nome, morada, número de telefone, fotografia, etc.), quer a dados biométricos (como a impressão digital, padrões de retina, geometria da mão, etc.), quer a dados sobre as relações laborais ou de comportamento económico e social, desde que se identifique ou se possa identificar o indivíduo em causa, estamos perante dados pessoais.

Por conseguinte, a legislação não limita as categorias de dados, pelo que independentemente da natureza ou do conteúdo da informação, ou mesmo do suporte em que é tratada – sendo esta última parte apenas taxativamente consagrada pelo legislador nacional, apesar de ir ao encontro do espírito da lei da Diretiva 95/46/CE – sempre que essa informação identifique ou permita identificar um indivíduo, consideramo-la um dado pessoal.

Ademais, os dados pessoais não estão circunscritos a informações objetivas, como a cor do cabelo ou a estatura de uma pessoa, abarcando também informações subjetivas, como opiniões, preferências e comportamentos.

No que concerne ao conteúdo, cumpre fazer a distinção entre dados pessoais *lato sensu* e dados pessoais sensíveis, cuja natureza obriga a uma reserva e proteção acrescidas. O n.º 1 do artigo 8.º da Diretiva 95/46/CE descreve como dados sensíveis *aqueles que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual*. Já o n.º 1 do artigo 7.º da LPD, compreende nesta categoria os dados 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.

Comparando os dois preceitos, conclui-se que o legislador nacional foi mais abrangente no elenco dos dados sensíveis, na medida em que incluiu neste naipe os dados referentes à «vida privada».

Este é um ponto-chave na diferença entre a previsão normativa nacional e comunitária, e que se reflete na aplicação fáctica das duas disposições. Senão, vejamos. Enquanto a definição comunitária de dados sensíveis se circunscreve aos elementos taxativamente elencados no já referido n.º 1 do artigo 8.º da Diretiva de Proteção de Dados, a LPD vem aumentar o campo de aplicação dos dados sensíveis, na medida em que acolhe o conceito indeterminado de *dados da vida privada*, alargando significativamente o leque de dados sensíveis em Portugal[20].

Assim, em Portugal, os cidadãos beneficiam de um regime potencialmente mais protetor no que concerne aos dados pessoais sensíveis, já que incluiu nesta categoria todos os dados que respeitem à vida privada.

Como se sabe, a transposição da Diretiva de Proteção pelos vários Estados-Membros veio permitir alguma liberdade aos legisladores nacionais, o que, do ponto de vista da harmonização legislativa comunitária, não é forçosamente benéfico. Contudo, se o conceito comunitário de dados pessoais sensíveis é amplo – ainda que circunscrito aos temas supra referidos – entre nós, o legislador nacional veio prever uma maior amplitude.

Regressando à análise da definição geral de «dados pessoais», sublinha-se que a informação não tem de ser verdadeira, para que seja vista como um dado pessoal, nomeadamente, porque a legislação confere aos titulares dos dados o direito de retificação (cf. alínea d) do artigo 6.º da Diretiva 95/46/CE, alínea d) do artigo 11.º da LPD e n.º 1 do artigo 35.º da CRP).

---

[20] Refira-se que o primeiro instrumento jurídico a consagrar o direito ao respeito pela vida provada foi a Declaração Universal dos Direitos do Homem (1948), pese embora não tivesse caráter vinculativo. Dois anos mais tarde, em 1950, a Convenção Europeia dos Direitos do Homem veio dispor no n.º 1 do artigo 8.º que «*Toda a pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência*», afigurando-se como o primeiro diploma jurídico vinculativo a consagrar este direito.

2) SEGUNDO ELEMENTO: *«RELATIVA A»*

Por outro lado, nos termos do Parecer n.º 4/2007 do Grupo de Trabalho do Artigo 29.º, a informação pode considerar-se «relativa a uma pessoa» quando é sobre essa pessoa. Se existem situações em que é clara a relação entre a informação e a pessoa, outras há em que a mesma não é patente. Ilustrando com dois exemplos, o processo clínico de um doente e a matrícula de um veículo automóvel são, no nosso entendimento, ambos dados pessoais, porque relativos a uma pessoa. Se no primeiro caso não se levantam problemas, já no segundo – porque primeiramente relacionado com um objeto e não diretamente com uma pessoa – poder-se-iam suscitar algumas dúvidas[21].

Voltando à questão da identificação de dados «relativos a uma pessoa», o já mencionado Parecer n.º 4/2007 do Grupo de Trabalho de Protecção de Dados do Artigo 29.º considera que podemos aferir a presença deste aspeto em função de um elemento de *conteúdo*, ou de *finalidade* ou de *resultado*.

Deste modo, é dito no referido Parecer que o elemento de conteúdo figura sempre que a informação é sobre uma pessoa, independentemente do objetivo do responsável pelo tratamento, ou de um terceiro, ou do impacto dessa informação na pessoa em causa.

Já o elemento de finalidade, como o próprio nome indica, surge quando os dados são utilizados com a finalidade de avaliar, tratar de determinada forma ou influenciar o estatuto ou o comportamento de uma pessoa.

Por último, refere o Grupo de Trabalho do Artigo 29.º que o elemento de resultado está implícito quando os dados relativos a uma pessoa tenham um impacto nos seus direitos e interesses. Não se exige que o resultado potencial tenha um grande impacto, bastando que o indivíduo possa ser tratado de forma diferente de outras pessoas como resultado do tratamento desses dados.

---

[21] Porém, não se colocam hoje dúvidas quanto à caraterização da matrícula como um dado pessoal, pelo que permite a identificação indireta do proprietário ou utilizador do veículo.

3) TERCEIRO ELEMENTO: «*IDENTIFICADA OU IDENTIFICÁVEL* [PESSOA SINGULAR]»

Um outro aspeto do conceito de dados pessoais prende-se com o facto de a informação se reportar a uma pessoa identificada ou identificável. Considera-se identificada a pessoa que é diferenciada de todas as outras, enquanto que será identificável aquela que, apesar de ainda não ter sido identificada, pode vir a sê-lo.

São os dados pessoais que permitem identificar ou tornar identificável uma pessoa, seja porque se referem ao aspeto exterior (por exemplo, a cor dos olhos, o género ou a raça), seja porque evidenciam uma característica própria, mas não imediatamente visível (como o nome ou a data de nascimento).

Assim, podemos classificar os dados pessoais como diretos ou indiretos. Os dados pessoais diretos permitem, por si só, identificar imediatamente o titular dos dados. Já os dados indiretos apenas identificam um determinado cidadão quando combinados com outros dados. No caso dos dados pessoais indiretos, será sempre necessário recorrer-se a informação paralela e complementar para se descobrir a identidade de um sujeito. A título de exemplo, vejamos o n.º do Cartão do Cidadão – que é um dado pessoal, na medida em que se reporta a um indivíduo – que, para a maioria das pessoas, não corresponderá imediatamente a um concreto indivíduo. Contudo, a consulta do Registo Civil permitirá a identificação indireta do sujeito em causa, pelo que o n.º do Cartão do Cidadão é um dado pessoal.

A informação apenas adquire a designação de dado pessoal quando, num caso concreto, permite a identificação de um sujeito. De facto, os dados pessoais não têm de identificar nominativamente o indivíduo em causa, bastando que o distingam ou possam distingui-lo dos demais. A identificação dependerá, portanto, das circunstâncias do caso concreto.

Deste modo, pese embora o nome seja o identificador mais comum, nem sempre permite a identificação imediata de uma pessoa. Exemplificando, se cinco das crianças de uma sala de aula se chamarem Maria, o professor não poderá distingui-las apenas pelo primeiro nome.

Por outro lado, poderá não ser necessário o nome para identificar concretamente uma pessoa. Por exemplo, o n.º de telemóvel identifica o seu utilizador, sem que tenha sido recolhido o seu nome. Do mesmo modo, se numa prova de equitação apenas estiver inscrita uma mulher, bastará o género para que a mesma seja identificada.

O Tribunal de Justiça da União Europeia veio confirmar este facto, ao afirmar que a possibilidade de identificar uma pessoa não implica necessariamente a capacidade para descobrir o seu nome[22].

Relativamente aos dados que se reportam a pessoas identificadas, não é problemático reconhecê-los imediatamente como dados pessoais. Diferentemente, no que respeita a dados de pessoas identificáveis, nem sempre é tão axiomática a sua catalogação.

Nestes casos, o cidadão não é identificado de forma imediata, mas mediatamente. Por outras palavras, os dados em questão são relativos a uma pessoa e, pese embora o indivíduo não tenha sido identificado, é possível identificá-lo.

Todavia, a possibilidade eventual de identificar um cidadão pode não ser suficiente para qualificar um dado como pessoal. A consideração de uma pessoa como *identificável* está sujeita à condição de o indivíduo ser identificado através da utilização de meios razoáveis.

Assim, a identificabilidade é condicional ao emprego de meios suscetíveis de serem razoavelmente utilizados para identificar o titular dos dados, quer pelo responsável pelo tratamento, quer por outra pessoa, nos termos do considerando 26 da Diretiva 95/46/CE.

A razoabilidade dos meios não se limita ao mero custo económico da identificação, mas contempla também o esforço necessário para a aquisição dessa informação e os riscos envolvidos. Tratando-se de um conceito indeterminado, terá de ser aferido em função da tecnologia e da sua previsível evolução.

Nesta matéria, tendo os avanços tecnológicos assumido um ritmo que ultrapassou as expectativas mais otimistas, deverão ser cautelosas as medidas de segurança e as obrigações que impendem sobre os responsáveis pelo tratamento, sob pena de a proteção de dados pessoais ser ineficaz.

---

[22] Cf. Acórdão do Tribunal de Justiça da União Europeia C-101/2001 de 6.11.2003 (Lindqvist), ponto 27: *«… a referência a várias pessoas, numa página da Internet e a sua identificação pelo nome ou por outros meios, designadamente a indicação do número de telefone ou de informação relativa às suas condições de trabalho e tempos livres constitui tratamento de dados pessoais […] no sentido […] da Diretiva 95/46/CE*».

É com esta preocupação em mente, que devemos ser prudentes, antevendo que determinados dados – ainda que presentemente não identifiquem os seus titulares – sejam reconduzíveis a um único indivíduo. Neste caso, a sua futura relação com dados pessoais poderá levar à identificação desse indivíduo, pelo que esse conjunto de dados agregados que se reportem a um mesmo indivíduo deve ser considerado como um dado identificável[23].

No caso da identificação indireta, os elementos que identificam, ou permitem identificar um indivíduo, não têm de estar na posse do responsável pelo tratamento. Desde que o responsável ou um terceiro consigam identificar a referida pessoa através de um conjunto de meios razoáveis, estamos no campo dos dados pessoais.

No Parecer n.º 4/2007, o Grupo de Trabalho do Artigo 29.º alerta para duas limitações a ter em consideração na correta interpretação do conceito de dados pessoais.

Primeiramente, aponta que a flexibilidade, que o conceito legal de dados pessoais permite, terá de encontrar o seu equilíbrio à luz da razoabilidade da utilização dos meios que possibilitem tornar a pessoa identificável numa pessoa identificada.

Em segundo lugar, adverte para a forma como os dados são tratados, dado que o tratamento eletrónico dos dados importa um «*maior risco de acesso fácil aos dados pessoais*», tal como alude o considerando 27 da Diretiva 95/46/CE.

Nesse sentido, o supra mencionado Parecer do Grupo de Trabalho do Artigo 29.º alerta que «*[a]s Autoridades Nacionais de Supervisão da Proteção de Dados desempenham um papel essencial nesta área, no âmbito da sua missão de controlo da aplicação da legislação de proteção de dados, que inclui assegurar a interpretação das disposições legais e dar orientações concretas aos responsáveis pelo tratamento e às pessoas em causa*».

4) QUARTO ELEMENTO: «*PESSOA SINGULAR*»

Até agora, debruçámo-nos sobre à análise das diferentes partes da definição de dados pessoais, constantes da Diretiva 95/46/CE, quanto ao conteúdo da

[23] Abordaremos melhor esta questão no capítulo relativo à singularização dos cidadãos (*Single out*).

informação, quanto à sua relação com o indivíduo e quanto às características de identificação e de identificabilidade.

Passemos, agora, ao estudo do último aspeto da definição comunitária de dados pessoais, que consiste no sujeito da norma: o indivíduo.

Como vimos, refere o texto da alínea a) do artigo 2.º da Diretiva 95/46/CE que dados pessoais correspondem a *qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular*[24] *identificada ou identificável.* Todavia, o conceito de pessoa singular terá de ser interpretado na esteira do espírito que o legislador comunitário faz transparecer em todo o corpo da Diretiva.

Se, por um lado, o legislador comunitário é claro no n.º 1 do artigo 1.º daquela Diretiva em delimitar a aplicação da mesma a pessoas singulares, traçando como objeto da Diretiva a proteção das liberdades e dos direitos fundamentais das pessoas singulares – nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais – por outro, tal não significa que se excluam liminarmente as pessoas coletivas da aplicação deste corpo legal.

Sendo a finalidade última deste diploma a proteção dos dados pessoais – de tal modo que, independentemente do seu conteúdo, a informação relativa a uma pessoa que a torne identificada ou identificável encontra abrigo legal – não seria juridicamente correto restringir a aplicação da lei às pessoas singulares.

Não queremos com isto dizer que as pessoas coletivas, em regra, se encontram ao abrigo da Diretiva 95/46/CE – dado que inclusivamente o argumento literal vem elucidar que as pessoas coletivas não são as destinatárias da norma – mas tão somente que, quando em causa estejam dados que identifiquem ou permitam identificar um indivíduo (leia-se uma pessoa singular), estamos no campo dos dados pessoais, ainda que se reportem a uma pessoa coletiva.

Por outras palavras, os dados pessoais não deixam de sê-lo, ainda que sejam também dados de pessoas coletivas. Recorrendo a um exemplo para melhor esclarecer esta ideia, se o nome de uma pessoa coletiva incorpora o nome dos seus

---

[24] Sublinhado nosso.

sócios (pessoas singulares), identificando-os, não é pelo facto de se tratar do nome de uma pessoa coletiva que os dados em causa deixam de merecer a proteção garantida aos dados pessoais.

iii. Princípios da Proteção de Dados Pessoais

Analisado o enquadramento jurídico da proteção de dados e o conceito de dados pessoais, cumpre agora refletir sobre os princípios gerais e as exigências que emolduram o seu regime.

De facto, os princípios que norteiam a proteção de dados pessoais estão dispersos em várias normas. Nesse sentido, analisaremos os princípios enunciados na Diretiva 95/46/CE e na LPD, e que respeitam sobretudo à qualidade dos dados, assim como os princípios constantes das orientações da Organização para a Cooperação e Desenvolvimento Económico (OCDE), que, apesar de não serem vinculativas, se repercutiram em vários diplomas, nomeadamente naquela Diretiva e consequentemente nas leis nacionais que a transpuseram.

Um dos princípios basilares da proteção de dados é, sem dúvida, o princípio da legalidade, que se concretiza quer na exigência de licitude do tratamento de dados (cf. alínea a) do n.º 1 do artigo 6.º da Diretiva de Proteção de Dados e a alínea a) do n.º 1 do artigo 5.º da LPD), quer na definição do âmbito de aplicação da Lei de Proteção de Dados (cf. n.º 1 do artigo 4.º da LPD).

Essencial é ainda que o tratamento de dados pessoais obedeça a um padrão ético de conduta entre as partes envolvidas numa relação jurídica (princípio da boa fé).

Um outro princípio de primordial destaque é o princípio da proporcionalidade, nos termos da alínea c) do n.º 1 do artigo 5.º da LPD e da alínea c) do n.º 1 do artigo 6.º da Diretiva 95/46/CE, sublinhando a necessidade de observância dos subprincípios da adequação, da necessidade e do não excesso do tratamento de dados.

Rege ainda esta temática o princípio da finalidade, consagrado na alínea b) do n.º 1 do artigo 5.º da LPD e na alínea b) do n.º 1 do artigo 6.º da Diretiva 95/46/CE, que impõe que os dados pessoais não sejam tratados de modo incompatível com a finalidade que deu origem à sua recolha primitiva. Este princípio irá demarcar as condições do tratamento de dados, a par do princípio da proporcionalidade e do princípio da legalidade.

Outro dos timbres do regime geral da proteção de dados é a transparência dos tratamentos de dados pessoais, que decorre tanto do artigo 2.º da LPD, como de outras obrigações e princípios – designadamente do princípio da finalidade – sendo espelhada na obrigação de o responsável pelo tratamento garantir o direito de informação e de acesso aos titulares dos dados, sem demoras ou custos excessivos.

Assinale-se ainda a necessidade de exatidão e atualidade dos dados – evidenciando a importância da qualidade dos dados, que é também cara à matéria da proteção de dados – cuja obrigação vem prevista na alínea d) do n.º 1 da LPD e na alínea d) do n.º 1 do artigo 6.º da Diretiva de Proteção de Dados. Assim, os tratamentos de dados pessoais deverão ser completos, exatos e atualizados.

Já no que respeita à conservação dos dados pessoais, determina-se que os mesmos sejam conservados unicamente durante o período necessário para a prossecução das finalidades da recolha ou do tratamento (cf. alínea e) do n.º 1 do artigo 5.º da LPD e alínea e) do n.º 1 da Diretiva de Proteção de Dados).

De outra banda, as Orientações da OCDE[25], no que respeita à proteção da privacidade e fluxos transfronteiriços de dados, vêm estabelecer oito princípios fundamentais: o princípio da limitação da recolha de dados, o princípio da qualidade dos dados, o princípio da definição da finalidade, o princípio da limitação da utilização dos dados, o princípio das garantias de segurança, o princípio da abertura, o princípio da participação do indivíduo e o princípio da responsabilização.

Debrucemo-nos, então, sobre o conteúdo de cada um dos princípios delineados pela OCDE.

Balizando a recolha de dados pessoais quer pelo princípio da necessidade, quer pelo princípio da minimização do risco, a OCDE refere que os tratamentos de dados deverão circunscrever-se aos dados estritamente necessários à sua finalidade. Deste modo, os tratamentos de dados pessoais têm de conter a preocupação *ab initio* de

---

[25] Estas Orientações (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* – 1980) constituem o primeiro documento de cariz internacional que define princípios sobre a privacidade. Graças à linguagem tecnologicamente neutra e ao caráter geral destes princípios, eles mantiveram-se inalterados até hoje. Aliás, têm sido adotados por vários países com sistemas jurídicos muito distintos, destacando-se ainda a sua aplicação em países que não são membros da OCDE.

não recolher dados acessórios ou irrelevantes, diminuindo-se o impacto de possíveis violações das normas de proteção de dados (princípio da limitação da recolha).

Cumpre lembrar que os tratamentos de dados pessoais devem ser relevantes para a finalidade que lhes deu causa e, nessa medida, ser atuais, completos e exatos (princípio da qualidade dos dados).

As orientações da OCDE sublinham, uma vez mais, a relevância do princípio da definição da finalidade, cujo conteúdo é muito próximo daquele vazado no princípio da finalidade da Diretiva 95/46/CE e da LPD.

Aliás, estas orientações vão mais longe ao consagrar expressamente uma concretização deste princípio, dado que – para além de proibirem a utilização dos dados para finalidades distintas daquela que esteve subjacente à sua recolha – não permitem que os dados sejam tratados para finalidades não especificadas nesse momento, ainda que com aquela compatíveis (princípio da limitação da utilização). Este princípio inclui, no entanto, exceções a esta regra, desde que legitimadas pelo consentimento do titular ou por força da lei.

Aquelas orientações impõem ainda que sejam adotados mecanismos de segurança contra potenciais riscos, tais como a perda ou o acesso, a destruição, o uso, a modificação ou a divulgação de forma não autorizada (princípio das garantias de segurança).

Outra das exigências impostas pela OCDE prende-se com a transparência dos tratamentos de dados, pela obrigação de informar sobre a sua existência, sobre a sua finalidade e sobre a identidade do responsável pelo tratamento e a sua localização (princípio da abertura).

Por outro lado, aquelas orientações fazem recair sobre o próprio titular dos dados o direito de obter junto do responsável pelo tratamento a confirmação de um tratamento sobre os seus dados pessoais, bem como a informação que este detenha sobre ele, num prazo e de maneira razoáveis, sem custos excessivos e de forma compreensível (princípio da participação do indivíduo). No fundo, trata-se da consagração do direito de acesso e de retificação dos dados, previsto também no artigo 11.º da LPD.

Por fim, o princípio da responsabilização faz impender sobre o responsável pelo tratamento a obrigação de observar os princípios de proteção de dados e encontra-se

também plasmado no n.º 3 do artigo 5.º da LPD e do n.º 2 do artigo 6.º da Diretiva 95/46/CE.

Uma vez analisados os princípios estruturantes do regime da proteção de dados pessoais, lembremos que, por maioria de razão, igualmente se aplicam os princípios que enformam os direitos fundamentais.

E, falando em direitos fundamentais, merece ser destacado o direito à identidade, para pôr em evidência a conexão deste direito com o direito à proteção de dados e a relevância dessa afinidade nos dias de hoje.

iv. A PROTEÇÃO DE DADOS PESSOAIS COMO EXPRESSÃO DO DIREITO À IDENTIDADE

De facto, o direito à identidade é um direito fundamental, cuja amplitude se interliga com o direito à proteção de dados.

Ora, o direito à identidade é caraterizado não só pela imagem que temos de nós mesmos, mas também pela imagem que projetamos da nossa individualidade nos outros. Assim, a incorreta representação de uma pessoa diminui a sua identidade, pela deturpação do seu ser e existir.

O conceito de direito à identidade tem vindo a evoluir historicamente, sendo sobretudo marcado pela sua transformação ao longo dos tempos. Enquanto direito, tem alargado a sua extensão com o crescente progresso tecnológico, por forma a incluir o maior número de elementos que representem um indivíduo, apresentando hoje um grau de complexidade que passaremos a analisar.

Até ao século XX, a proteção da identidade pessoal não se encontrava plasmada como um direito. De facto, até à Idade Média, o indivíduo era pertença de um grupo ou família, não se autonomizando a sua identidade da comunidade na qual se inseria. A partir do século XVI, com o desenvolvimento do aparelho estadual, bem como da centralização administrativa, os Estados sentiram a necessidade de individualizar os seus cidadãos para melhor governarem. Deste modo, a identidade pessoal começou a ser vista como uma necessidade para a coleta de impostos, para a aplicação da lei, para o redimensionamento das cidades, etc.[26] . A solução passou por criar um conjunto de critérios que permitisse a identificação de cada indivíduo. Os registos administrativos deveriam descrever algumas características pessoais de um sujeito – designadamente o nome, a filiação, a nacionalidade, a residência, a data de nascimento e o género – resultando a identificação de um sujeito do conjunto de documentos oficiais constantes daqueles registos[27].

---

[26] Veja-se ANDRADE, Norberto N.G., "Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization", in *Computers, Privacy and Data Protection: an element of Choice*, Bruxelas, Springer, 2011, pp. 66-70.

[27] Ibidem, p. 71.

Neste modelo, o direito à identidade reportava-se unicamente à visão de um indivíduo sob a perspetiva do seu Estado. Assim, apenas era contemplada a materialização em papel da identidade de alguém, à luz da representação pelas autoridades estaduais, não sendo atendido o conjunto de elementos intrínsecos à onticidade de cada indivíduo.

Apesar das limitações apontadas, esta noção de identidade representou um importante avanço na construção do direito à identidade, na medida em que consagrava o direito legal à individualização dos cidadãos ante os demais sujeitos – pese embora de um modo meramente superficial e institucional.

Já nos séculos XIX e XX, a Revolução Industrial e a consequente transformação social, a evolução da imprensa e o aparecimento da fotografia implicaram novas ameaças com especial impacto sobre os direitos de personalidade. Com o advento dos cartões de identidade em suporte de papel, que permitiam a individualização e identificação de uma pessoa, os cidadãos começaram a correlacionar-se com os seus próprios sinais distintivos. Ora, todo este contexto veio promover uma nova conceção jurídica da identidade, que esteve na origem da atribuição dos direitos de personalidade, direitos conferidos à nascença[28].

Os direitos de personalidade vieram salvaguardar a dignidade humana, protegendo juridicamente os interesses e valores intrinsecamente relacionados com a pessoa humana, como vimos supra. Assim, o direito à identidade, enquanto direito de personalidade, foi consagrado em vários sistemas jurídicos, evidenciando-se como uma decorrência autónoma da personalidade humana e digna de proteção legal.

Esta construção jurídica foi suportada e desenvolvida pela doutrina e jurisprudência, mais recentemente sublinhando as *nuances* do desdobramento dos direitos de personalidade nos direitos à identidade pessoal, à reserva da intimidade da vida privada e à proteção de dados.

Destaque-se que, graças ao tónus idiossincrático do ser humano, o direito à identidade pessoal adquire autonomia dentro dos direitos de personalidade. Apesar deste direito ter sido inicialmente consagrado como um direito negativo, impondo a

---

[28] Ibidem, pp. 66-70.

terceiros obrigações de não agir, atualmente o direito à identidade ganhou um novo significado – abrangendo não apenas o nome, a naturalidade, a data de nascimento, etc., mas também os dados biométricos, a voz, a história de vida, a reputação, etc. – exigindo a sua configuração também como um direito positivo[29].

De início, os direitos de personalidade foram inseridos no ramo de Direito Privado, como o espelham vários códigos civis nos ordenamentos jurídicos europeus. Todavia, no decurso do chamado *movimento de constitucionalização do Direito Privado*, os direitos de personalidade foram elevados a direitos fundamentais[30].

Hodiernamente, além de ser constitucionalmente protegido (cf. n.º 1 do artigo 26.º da CRP), o direito à identidade pessoal está expressamente consagrado no Direito Público Internacional, sob a alçada dos direitos humanos. É disso exemplo a previsão do direito à identidade no artigo 8.º da Convenção das Nações Unidas sobre os Direitos da Criança (CNUDC)[31] que, por sua vez, é inspirada na Declaração Universal dos Direitos Humanos (DUDH). Veja-se que o artigo 8.º da CNUDC salienta a relação entre a identidade, a nacionalidade, a família e o nome, fazendo uma ponte entre o primitivo conceito de identidade – o qual se limitava aos critérios estadualmente definidos – e o atual, mais abrangente e aberto a outras caraterísticas individuais.

Assinalamos, ainda, que o reconhecimento dos direitos de personalidade – como o direito à identidade pessoal – tanto constitucionalmente, como pela via dos direitos

---

[29] Ibidem, p. 71.

[30] Ibidem.

[31] Cf Artigo 8.º da Convenção sobre os Direitos da Criança, adotada pela Assembleia Geral nas Nações Unidas em 20 de Novembro de 1989 e ratificada por Portugal em 21 de Setembro de 1990:

> 1. Os Estados Partes comprometem-se a respeitar o direito da criança e a preservar a sua identidade, incluindo a nacionalidade, o nome e relações familiares, nos termos da lei, sem ingerência ilegal.
>
> 2. No caso de uma criança ser ilegalmente privada de todos os elementos constitutivos da sua identidade ou de alguns deles, os Estados Partes devem assegurar-lhe assistência e proteção adequadas, de forma que a sua identidade seja restabelecida o mais rapidamente possível.

humanos, constitui uma importante proteção do indivíduo nos vários sistemas jurídicos, potenciando ainda o desenvolvimento de novas construções teóricas sobre esses direitos.

A jurisprudência italiana apresenta um caso de referência a este respeito[32] [33]. O Tribunal Constitucional italiano autonomizou claramente o direito à identidade pessoal dentro do quadro dos direitos de personalidade, configurando-o como o direito de cada um aparecer e ser representado na vida social, especialmente nos meios de comunicação social, de modo coincidente com a sua identidade pessoal. Nesta aceção, assinalam-se duas novidades: por um lado, o conceito de um indivíduo ser idealmente representado de acordo com a sua identidade real e, por outro, o relevo dado à vertente social do direito à identidade pessoal.

O conceito de representação da identidade real como a projeção do indivíduo na sociedade, aporta a esta temática um aperfeiçoamento qualitativo, na medida em que a identidade é concebida como um feixe de caraterísticas intrínsecas de alguém – compreendendo não só o seu registo documental, mas também os valores e ideais que defende – explanadas na sua relação com a sociedade, e que não podem ser distorcidas ou erradamente representadas[34]. Esta perspetiva compreende quer quem nós somos para nós mesmos, quer como somos representados para e pelos outros.

Na tentativa de encontrar o verdadeiro «*ego*», a jurisprudência italiana tenta conciliar a visão intrínseca do ser à sua visão extrínseca, identificando esta última

---

[32] A este propósito cf. Pretura Roma 6-5-1974 (Pangrazi e Silvetti vs. Comitato Referendum). Trata-se de um caso paradigmático na construção do direito à identidade em Itália e que, em suma, decide a favor de um casal, cuja imagem a trabalhar no campo foi utilizada numa propaganda anti-divórcio, aquando do referendo do divórcio em Itália, com o intuito de invocar o espírito da família tradicional. Contudo, além da fotografia ter sido utilizada sem o consentimento dos titulares, veio a apurar-se que os seus dois protagonistas não eram, na verdade, casados e que, aliás, eram a favor do divórcio.

[33] Sobre este e outros casos jurisprudenciais sobre o direito à identidade, Cf ZENO-ZENCOVICH, Vincenzo, *Identità Personale,* Estrato dal Digesto, IV Edizione, vol. IX Civile, UTET, 1993.

[34] Veja-se ANDRADE, Norberto .N.G., "Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization", in *Computers, Privacy and Data Protection: an element of Choice*, Bruxelas, Springer, 2011, pp. 72-74.

com a representação do indivíduo nos meios de comunicação social. Não obstante, a crítica que se aponta a este entendimento assenta no facto de a representação externa de um sujeito ser bem mais abrangente que a sua mediatização.

Simultaneamente, o Tribunal Constitucional italiano reforçou dois traços distintivos do direito à identidade, ao evidenciar o seu caráter conceptualmente autónomo relativamente aos demais direitos de personalidade e a sua plasticidade – decorrente tanto da complexidade de um direito em constante transformação, como da indeterminabilidade apriorística de antecipar todas as possíveis violações. Ademais, é precisamente a elasticidade deste direito que permite a sua adaptação a novas situações, nomeadamente àquelas trazidas pelo progresso tecnológico.

Ainda no campo da densificação do direito à identidade pessoal pela jurisprudência, importa destrinçar a solução jurídica preconizada pelo TEDH daquela apresentada pelo Tribunal Constitucional italiano. Apesar de ambos os tribunais defenderem o direito à identidade, relacionando-o com o contexto social, enquanto o Tribunal Constitucional italiano envereda por uma análise em que as relações sociais são a tela onde se projeta o indivíduo, para o TEDH a sociedade colabora na criação e desenvolvimento da identidade pessoal. Assim, o TEDH sublinha no direito à identidade não apenas a sua expressão como um direito negativo, mas sobretudo como um direito positivo, que exige da sociedade um papel formador no livre desenvolvimento da personalidade individual[35]. Este tribunal entende que o direito à identidade decorre do direito à vida privada (cf. artigo 8.º da CEDH), dado a CEDH ser lacunar quanto à previsão específica daquele direito[36].

Deste modo, na perspetiva dos direitos humanos – e contrastando com a visão da identidade baseada em elementos ditados pelo Estado – o direito à identidade constrói-se a partir do indivíduo, que determina quais os elementos que o particularizam. Neste enquadramento, não é o Estado que individualiza os cidadãos segundo critérios próprios, mas antes a pessoa que, no exercício dos seus direitos, traça a sua história de vida, individualizando-se. Naturalmente que a identidade passa

[35] Ibidem, pp. 74-79.

[36] Nesse sentido veja-se o Acórdão P.G. e J.H. vs United Kingdom ECHR 2001 IX.

por conhecer as suas origens, data de nascimento, etc., mas, mais do que uma análise estática, trata-se de um processo em criação ao longo da vida.

Aliás, a sociedade deve estar sensível à necessidade de garantir um quadro educativo e legal que promova o livre desenvolvimento da personalidade humana (na vertente positiva do direito à identidade), não bastando reconhecer o direito à identidade pela abstenção de comportamentos com o mesmo incompatíveis (vertente negativa).

Por outro lado, tal como a revolução industrial marcou profundamente a perceção do direito à identidade, também o progresso tecnológico a que atualmente assistimos tem um profundo impacto na potenciação de violações da identidade. Quase podemos dizer que os avanços tecnológicos obrigam a uma reflexão sobre os direitos de personalidade.

Contudo, se, por um lado, a tecnologia apresenta novos perigos para a identidade, por outro, permite uma expansão da própria identidade. A Internet das Coisas (também apelidada de inteligência ambiente[37]) trará, uma vez mais, novos desafios à proteção dos direitos de personalidade, dado que estaremos rodeados de objetos que

---

[37] AARTS, Emile, WICHERT, Reiner, "Ambient Intelligence", in BULLINGER, Hans-Jörg et al., *Technology Guide: Principles, Applications, Trends*, Springer, 2009, p. 244: *«A inteligência ambiente caracteriza-se pela sensibilidade e adaptação de ambientes eletrónicos, que respondem às ações de pessoas e de objetos, atendendo às suas necessidades. Esta abordagem inclui a globalidade do meio circundante – incluindo cada objeto físico – e associa-o com a interação humana. Desta opção por uma interação mais extensa e mais intuitiva, é expectável uma melhoria da eficiência, um aumento da creatividade e um maior bem-estar pessoal» («Ambient Intelligence (AmI) is about sensitive, adaptive electronic environments that respond to the actions of persons and objects and cater for their needs. This approach includes the entire environment – including each single physical object – and associates it with human interaction. The option of extended and more intuitive interaction is expected to result in enhanced efficiency, increased creativity and greater personal well-being»)*.

A Internet das Coisas é utilizada como um sinónimo de inteligência ambiente, como também o é a computação omnipresente (*pervasive computing*). A diferença terminológica assenta sobretudo nos aspetos que cada um destes conceitos destacar. Para melhor compreensão cf. CAS, Johann, "Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contraditions", in GUTWIRTH, Serge, et al., *Computers, Privacy and Data Protection: an element of choice*, Springer, 2011, pp. 139-169.

responderão às necessidades dos indivíduos de uma forma invisível, com base na criação de perfis automáticos.

Tal como descrito por Norberto Andrade, a Internet das Coisas «*...vai caraterizar-se, por um lado, pela sua invisibilidade, discrição e impercetibilidade e, por outro, pela sua sensibilidade, interatividade e capacidade de resposta à pessoa humana*»[38].

Para esse efeito, a inteligência ambiente implicará o recurso a sensores e outros dispositivos de monitorização, como a identificação por radiofrequência (*Radio Frequency Identification - RFID*), para que os utilizadores possam interagir com o mundo físico em que vivem.

Assim, a identificação de cada um de nós será mais minuciosa, quer para que a Internet das Coisas cumpra o seu objetivo de procurar responder às necessidades individuais de cada pessoa, quer porque serão registados dados pessoais nunca antes analisados.

Segundo Norberto Andrade, «*O cenário da inteligência ambiente traz consigo importantes transformações no modo como a identidade de uma pessoa é captada, representada e disseminada, decorrentes de um sem número de novas características e tendências presentes neste panorama*»[39].

Para este autor, a quantidade de dados pessoais criados, recolhidos e comunicados será francamente aumentada, tanto mais que a contínua digitalização da informação pessoal é um pressuposto do funcionamento da Internet das Coisas[40]. Seja pela recolha da informação através de dispositivos eletrónicos, sejam os próprios titulares dos dados a facultar a informação, a verdade é que serão criados, analisados

---

[38] Cf. ANDRADE, Norberto .N.G., "Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization", in *Computers, Privacy and Data Protection: an element of Choice*, Bruxelas, Springer, 2011, p. 80 *"The AmI will thus be characterized, on the one hand, by its invisibility, discretion and unobtrusiveness and, on the other, by its sensitivity, interaction and responsiveness to the human person".*

[39] Ibidem, p. 81 *"The AmI scenario will carry a number of important transformations to the way a person's identity is captured, represented and disseminated. Such important changes will derive from a number of new characteristics and tendencies present in the future world of AmI*".

[40] Ibidem.

e tratados mais dados pessoais sobre um indivíduo, e inclusivamente serão tratados dados nunca antes analisados.

Cada indivíduo poderá definir a sua identidade em inúmeras formas no mundo virtual. Contudo, isso não significa que a desmultiplicação da identidade impeça um conhecimento profundo daquele ser uno. Por outras palavras, a Internet das Coisas permitirá a cada um a criação de diversos avatares, de acordo com a segurança, conveniência ou mesmo com a finalidade do tratamento de dados. Porém, esses desdobramentos de personalidade não são incompatíveis com a sua recondução a um mesmo indivíduo, pelo que o somatório das várias facetas de uma pessoa no mundo virtual poderá ser facilmente reconduzido a uma mesma pessoa, cuja identidade – que tanto se queria ocultar no seu todo – acaba por ser intimamente revelada.

Neste plano, a inteligência ambiente implica o conhecimento das pessoas e, consequentemente, a sua identificação. Para isso, a criação de perfis terá de ser de tal modo específica que garanta a acuidade da análise de um sujeito, do seu comportamento e relacionamento com o mundo que o rodeia. A monitorização subjacente à caraterização de um sujeito será, por isso, constante e de considerável grau de sofisticação. Não é por acaso, que a inteligência ambiente também é denominada como computação omnipresente (*pervasive computing*).

Por último, Norberto Andrade adverte para a possível confusão entre o mundo físico e o mundo virtual. A identidade de cada sujeito será tanto mais interligada na Internet das Coisas, quão mais dispersa se encontrar[41]. É esta ubiquidade da informação que permitirá traçar um perfil de cada indivíduo com detalhe, estando fora do controlo do próprio titular dos dados.

Se presentemente já não assistimos ao binómio um indivíduo/uma identidade, parece que no contexto da inteligência ambiente a projeção de um indivíduo em várias identidades tenderá a aumentar. Por outro lado, a complexidade do fenómeno da identidade poderá conduzir a que uma mesma identidade seja partilhada por várias

[41] Ibidem.

pessoas, como por exemplo o caso em que vários autores escrevem sob um mesmo pseudónimo num *blog*.

Um dos receios desta multiplicidade de desdobramentos da identidade reporta-se à influência da inteligência ambiente na própria construção do indivíduo. Estando a identidade em constante construção, e encontrando-se o indivíduo em contínua relação com a Internet das Coisas, até que ponto não será nociva a influência da leitura que a inteligência ambiente retira da representação permanente do indivíduo no meio em que se insere?

Nesse sentido, o direito à identidade terá obrigatoriamente que se compadecer com um direito a várias identidades, seja pela fragmentaridade da identidade, seja pela multiplicidade de identidades de um indivíduo.

Recorrendo a um exemplo para melhor clarificar esta ideia, um indivíduo esquizofrénico não deixa de ter uma única identidade, apesar da sua personalidade ser composta por várias subidentidades. O mesmo se passa com um indivíduo que assuma diferentes avatares no mundo digital, ou mesmo o mero desdobramento de uma mesma pessoa no mundo físico e no mundo virtual. Do nosso ponto de vista, a segmentação da personalidade não implica a desagregação da individualidade. A coesão da multiplicidade de egos de um mesmo indivíduo é conciliável com um conceito uno de identidade, tanto mais que, facticamente, a própria tecnologia permite quer a radialização do indivíduo (designadamente no mundo digital), quer a sua unificação, sobretudo pela análise conjugada da inteligência ambiente.

O direito ao esquecimento[42] assume também relevo na problemática da identidade. Se, como vimos, a identidade é um processo em constante formação – quer pelo crescimento, amadurecimento, pela aprendizagem, etc. – cabe ao indivíduo a faculdade de adequar a sua representação no mundo face à sua evolução pessoal.

---

[42] A Comissão Europeia destaca a clarificação do direito ao esquecimento como «*o direito de as pessoas impedirem a continuação do tratamento dos respetivos dados e de os mesmos serem apagados quando deixarem de ser necessários para fins legítimos*». Cf. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – "Uma abordagem global da proteção de dados pessoais na União Europeia" COM(2010) 609 final, versão portuguesa, p. 8.

Contrariamente aos demais direitos de personalidade, o direito à identidade é flexível e mutável, acompanhando precisamente a transformação pessoal do indivíduo.

Assim, a necessidade de retificar a evolução de cada um exige que sejam eliminados dados do passado, quando já não se identifiquem com a realidade presente de um indivíduo. A capacidade de apagar rastos eletrónicos do passado pode ser essencial para a reconstrução da personalidade presente, designadamente enquanto expressão do livre desenvolvimento da personalidade e da possibilidade de começar de novo.

Naturalmente que o direito ao esquecimento tem de ser contrabalançado com o próprio direito à memória. Também no que respeita à identidade se condena o abuso de direito, de modo a que alguém, cujo comportamento passado se afigurou altamente censurável pela sociedade, não possa invocar o direito ao esquecimento como forma de garantir a repetição do mesmo comportamento reprovável.

Importa, portanto, contextualizar o direito ao esquecimento não apenas no quadro do direito à proteção de dados, mas também do direito à identidade – ainda que ambos os direitos se encontrem intimamente ligados.

Em conclusão, o direito à identidade terá de adaptar-se às novas realidades impostas pela tecnologia, designadamente a inteligência ambiente. Deste modo, a reconceptualização deste direito passa pela compreensão da multiplicidade de subidentidades de um mesmo indivíduo, assim como da unificação de *alter egos* decorrentes da associação de vários sujeitos.

Como bem afirma Norberto Andrade, *«[e]mbora seja a tarefa de cada um de nós maximizar os benefícios da tecnologia na construção e afirmação das nossas identidades pessoais, cabe à lei incluir tais potencialidades tecnológicas dentro de uma estrutura "amiga da identidade". Um quadro jurídico que permita que cada um tenha a liberdade de construir, desconstruir e reconstruir a sua própria identidade»*[43].

---

[43] Cf. ANDRADE, Norberto .N.G., "Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization", in *Computers, Privacy and Data Protection: an element of Choice*, Bruxelas, Springer, 2011, p. 95: "*While it is up to us to maximize the benefits of technology in the construction and affirmation of our personal identities, it is up to law to enclose such technological*

II. NOVOS DESAFIOS À PROTEÇÃO DE DADOS PESSOAIS NO SÉCULO XXI

Feito o enquadramento jurídico da matéria da proteção de dados pessoais, e em particular a sua especial relação com o direito ao livre desenvolvimento da personalidade, com o direito à reserva da intimidade da vida privada e, sobretudo, com o direito à identidade, centremo-nos agora no cerne deste trabalho e na análise dos desafios à proteção de dados a que nos propusemos.

Nos últimos anos, assistimos a profundas revoluções tecnológicas e de intercomunicação social, como a difusão da Internet, a informatização das bases de dados e o seu possível amalgamento, a democratização dos telemóveis, o aparecimento de redes sociais em linha (*online*) e estamos prestes a avistar a chegada da Internet das Coisas.

Do ponto de vista da proteção de dados, muitas outras mudanças marcaram o início deste século, como o aparecimento da computação em nuvem (*cloud computing*), a governação eletrónica (*e-government*), os *cookies*, os sistemas biométricos, a consolidação do correio eletrónico como meio de comunicação, as alterações de comportamento social, etc.

Por impraticabilidade e por falta de audácia, não pretendemos neste estudo abordar todas as temáticas relacionadas com os desafios à proteção de dados pessoais no início do século XXI.

Aliás, entendemos que cada uma destas temáticas, por si só, é merecedora de uma reflexão autónoma, sendo as problemáticas por elas invocadas dignas de estudo. Assim, apenas as referimos aqui, a título exemplificativo.

Outrossim, debruçar-nos-emos sobre três aspetos que julgamos de particular importância, mormente a criação de perfis, o advento da inteligência ambiente e a singularização (s*ingle out*) dos indivíduos.

---

potentialities within an identity-friendly framework. A legal framework that enables every human person to freely construct, de-construct and re-construct their own identities".

i. A CRIAÇÃO DE PERFIS

A criação de perfis (*profiling*) remonta ao início da vida e resulta da observação e análise racional da realidade. O ser humano, como qualquer ser vivo, necessita de conhecer o meio no qual se movimenta para poder adaptar-se aos seus condicionalismos.

Este exercício de adaptação exige o conhecimento prévio das características ambientais e dos comportamentos que nos rodeiam, sendo o processo de aprendizagem construído a partir da sistematização dessa informação. Como afirmam Humberto Maturana e Francisco Varela, *«… a chave para a compreensão da fenomenologia biológica é a compreensão da organização do indivíduo*»[44].

Contudo, de entre o vasto volume de informação com que somos confrontados, apenas uma parte é relevante. A destrinça da informação relevante da informação acessória, ou mesmo da informação irrelevante, caracteriza a operação de mineração de dados (*data mining)*.

Deste modo, após o reconhecimento de um padrão – pela observação e pelo teste – não é difícil a construção de um perfil. Uma vez construído o perfil, a fase seguinte é a aplicação do mesmo e, consequentemente, a adoção de uma conduta face aos comportamentos nele traçados.

Todavia, não é este tipo de criação de perfis (*profiling)* intuitivo e instintivo que coloca em causa a proteção de dados pessoais. Vejamos, então, o raciocínio que está por detrás da criação de perfis e quais as suas implicações no mundo hodierno.

Se, por um lado, a necessidade de adaptação requer dos indivíduos uma enorme atenção no processamento da informação que adquirem, por outro, o reconhecimento de padrões nem sempre é benéfico ou inócuo.

Mas se traçar perfis é algo tão natural ao ser humano, porquê limitar essa sua capacidade?

---

[44] MATURANA, Humberto, VARELA, Francisco, *Autopoiesis and Cognition – The Organization of the Living*, D. Reidel Publishing Company, 1980, p. 116 "… *the key to the understanding of the biological phenomenology is the understanding of the organization of the individual*".

Aqui, o cerne da questão reconduz-se ao momento em que a criação de perfis passa a ser um tratamento de dados pessoais, prendendo-se a resposta com o método e com as finalidades empregues. A liberdade de agir obriga a um conhecimento das circunstâncias, para que possamos tomar decisões conscientes e informadas, pelo que restringir essa capacidade de análise seria limitar a autonomia do ser humano, que está intimamente ligada à possibilidade de escolher e de atuar de acordo com a sua própria vontade. Contudo, essa escolha deverá ser livre e esclarecida, ou seja, fruto da reflexão do próprio sujeito, que alcança todas ou grande parte das possíveis consequências dos seus atos.

Ora, a problemática da proteção de dados pessoais relacionada com a análise perfilística encontra-se apenas no campo da automatização da criação de perfis[45].

Deste modo, suscitam-se sobretudo problemas quando a criação e aplicação de perfis não têm intervenção humana, recorrendo-se a *softwares* programados para a análise de dados e para a extração de ligações – aparentemente encobertas – de comportamentos humanos, desconhecendo o sujeito em causa tanto a própria criação do perfil, como o impacto da aplicação desse perfil a si mesmo.

Assim, do ponto de vista da proteção de dados, a maior preocupação nesta matéria reside na construção de perfis para utilização massiva através de mecanismos automatizados, que permitam a discriminação de pessoas.

Dediquemos, por isso, alguma atenção ao processo de criação de um perfil. Na elaboração e aplicação de um perfil podemos distinguir três fases: a observação da realidade (*data warehousing*), a correlação entre múltiplas variáveis, estabelecendo um padrão (*data mining*), e a aplicação do perfil criado a outros indivíduos[46].

---

[45] Cf. HILDEBRANDT, Mireille, *Profiling and the Rule of Law*, DOI 10.1007/s12394-008-0003-1, Spinger, publicado on-line a 19 de dezembro de 2008.

[46] Cf. Opinião do Comité Consultivo da Convenção para a Proteção de Indivíduos, no que respeita ao processamento automático de dados pessoais (*Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*), DINANT, Jean-Marc, LAZARO, Christophe, POULLET, Yves, LEFVER, Nathalie e ROUVROY, Antoinette, *Application of Convention 108 to the profiling mechanism – Some ideas for the future work of the consultative committee (T-PD)*, Strasbourg, 11.01.2008.

Porém, note-se que nem todas as fases implicam necessariamente um tratamento de dados pessoais, senão vejamos.

1) A OBSERVAÇÃO DA REALIDADE (*DATA WAREHOUSING*)

Na primeira fase, pretende-se acumular o máximo de informação, incluindo dados anónimos e/ou dados pessoais. Em regra, mesmo que os dados sejam pessoais, eles serão posteriormente anonimizados, já que o objetivo é agregar o maior número de informação possível para posterior análise estatística. Cumpre sublinhar que a mera consulta de dados pessoais configura ela mesma um tratamento de dados pessoais, de acordo com a alínea b) do artigo 3.º da LPD. Assim, a própria operação de anonimização será um tratamento de dados pessoais, na medida em que implica a consulta de dados que identificam ou permitem identificar um indivíduo.

A revolução tecnológica que marcou o final do século XX e o início do século XXI – aliada à tentação de conservar dados, com potencial utilidade futura, pese embora o seu interesse nesse momento não seja ainda manifesto – facilita a recolha de dados para este primeiro estádio.

Com esse intuito, a cada minuto são recolhidos dados nominativos, dados codificados e dados anónimos para as mais diversas finalidades, muitas das vezes sem que o próprio titular disso se aperceba.

A Internet das Coisas[47] trará novos desafios à proteção de dados pessoais, ao conectar o mundo físico (*offline)* à Internet. A potencial recolha de uma vasta quantidade de informação, que *per se* não é sensível, mas que, quando agregada, tem enorme relevância do ponto de vista da reserva da intimidade da vida privada, parece ser merecedora da proteção atribuída aos dados pessoais. Contudo, esse será um tema abordado mais adiante.

2) A CORRELAÇÃO ENTRE MÚLTIPLAS VARIÁVEIS, ESTABELECENDO UM PADRÃO (*DATA MINING*)

---

[47] Cf. A Internet das coisas ou Web 3.0 é considerada a próxima era tecnológica da Internet, e pauta-se por uma maior interação entre o utilizador e o mundo que o rodeia através de dispositivos tecnológicos. Assim, o mundo real (*offline*) passará a estar ligado ao mundo virtual (*on-line*).

Relativamente à segunda fase, as operações em causa prendem-se com a aplicação de métodos estatísticos, que estabeleçam uma relação (ou a falta de relação) entre as variáveis em estudo, ainda que com alguma margem de erro. Através desta operação, os indivíduos serão catalogados de acordo com as características que possuem e serão deduzidas outras características implicitamente. Os diferentes agrupamentos possíveis da mesma informação geram um conhecimento novo, fornecendo «… *respostas a perguntas que não sabíamos perguntar …*»[48].

Destaque-se que este género de análise assentará fundamentalmente em dois métodos: no método descritivo e no método preditivo[49].

Contudo, terá de ser feita a destrinça entre a mera análise estatística e a criação de perfis – ainda que esta última possa incluir a primeira. Enquanto que a finalidade do processamento estatístico da informação reside na compreensão de fenómenos, através da sua quantificação, para a futura tomada de decisões, já a criação de perfis implica a identificação do critério individual mais adequado a uma dada situação, de um modo qualitativo, criando um conhecimento novo[50].

De facto, o mundo burocrático no qual vivemos alimenta-se de informação, seja ela de grande ou diminuta importância. O Estado não é infalível e podemos mesmo dizer que, em certa medida, é graças a alguma ineficiência dos Estados que não existem maiores atentados à privacidade, mesmo em Estados de Direito democráticos.

O mesmo se diga em relação ao setor privado. O armazenamento de informação, da mais variada ordem, é demasiado tentador para um burocrata, cuja função é tomar decisões baseadas em factos ou em suposições que serão inferidas da análise da realidade. Daí que quanto mais informação se reunir, melhor se conhecerá o mundo.

---

[48] ZARSKY, Tal, "Mine your own business! Making the case for the implications of the data mining of personal information in the forum of public opinion", in *Yale Journal of Law and Technology*, 5, 2002-2003, p. 6 "*Data mining provides its users with answers to questions they did not know to ask*".

[49] Ibidem, p. 9.

[50] Ibidem.

Mas, se a informação é importante e valiosa, não menos relevante é o contexto dessa informação. Nesse sentido, as operações de relacionamento, nomeadamente pelo cruzamento e comparação de várias fontes, dão uma nova vida à informação. Do mesmo modo, a descontextualização pode causar inúmeras imprecisões, graças às impressões erradas em que se baseia.

A operação de mineração de dados *(Data mining)* permite depurar a informação recolhida, tornando a mera informação em *conhecimento*, sendo o processo através do qual se retira a informação relevante, separando-a da informação acessória.

Esta operação de filtragem da informação permite o reconhecimento de padrões, através da análise de quantidades massivas de informação. Isto significa que quando são confrontadas diferentes bases de dados, encontram-se relacionamentos mais facilmente.

Atente-se que os processos de *mineração de dados* não têm de recorrer a informação secreta. De facto, eles podem utilizar apenas informação que já se encontra disponível na Internet. Porém, ao relacionar diferentes tipos de informação ou diferentes abordagens sobre uma mesma realidade, a análise revela informação nova, que vivia na sombra de outros dados já conhecidos.

Diferentemente, a análise estatística não é um fim em si mesma, e os seus resultados serão sempre analisados de forma agregada, pelo que nenhuma decisão terá consequências diretas e pessoalizadas num indivíduo concreto. Os dados estatísticos são um auxílio na tomada de decisões, mas não implicam a tomada de decisão em si mesma. Ainda que a análise estatística parta de dados pessoais, o seu fim último não será reconverter os dados agregados a um específico indivíduo.

O mesmo não poderá ser dito relativamente à criação de perfis, cuja finalidade é a aplicação do perfil traçado aos cidadãos que potencialmente nele se enquadrem, pelo que se pretende uma individualização.

As recentes inovações tecnológicas albergaram novas metodologias de análise e de estatística. Graças à chamada inteligência artificial, os computadores conseguem extrair informação diferente sobre dados já conhecidos, explorando relações multifatoriais e em grande escala – dado que a informação pode ser proveniente das mais diversas fontes. E, sublinhe-se, quão maior a sofisticação tecnológica, maior o refinamento da informação apurada.

Por último, reitera-se que a análise dos comportamentos humanos será sempre apetecível quer para o setor público, quer para o setor privado – sendo particularmente cara ao marketing e às atividades de gestão de risco – já que compreender como funciona e o que move o ser humano é um bem de inestimável valor para os agentes no mercado.

3) A APLICAÇÃO DO PERFIL CRIADO A OUTROS INDIVÍDUOS

Uma vez traçado o perfil, o mesmo será aplicado aos indivíduos, inferindo-se determinados comportamentos ou notas distintivas. Geralmente, a criação de perfis (*profiling)* está apenas associada a esta última operação, mas – ainda que os efeitos da criação do perfil sejam mais evidentes nesta derradeira fase – a verdade é que este processo se inicia desde a compilação dos dados e engloba igualmente o relacionamento dos fatores em análise, como *supra* referido.

Deste modo, após a análise dos comportamentos de um grupo de indivíduos e do seu estudo mais detalhado, com vista a compreender as relações entre as suas ações, conclui-se que existe um padrão de comportamento.

Parece, então, inequívoco afirmar que os detentores dessa informação irão utilizar o padrão de comportamento daquela amostra de pessoas como regra de comportamento de todos os indivíduos, tomando a parte pelo todo, adaptando a sua oferta de serviços, as suas campanhas de publicidade ou mesmo a sua relação com potenciais clientes, face àquela dedução[51].

Atente-se que o maior risco desta estereotipagem reside na redução do indivíduo ao perfil criado por meio de um processo automatizado, e que influenciará processos de decisão aos quais será sujeito, sem que as suas singularidades sejam atendidas. A criação de um perfil implica que o indivíduo seja tratado à luz das características

[51] As instituições bancárias, sobretudo na análise do risco de incumprimento aquando da concessão de crédito, recorrem muitas vezes a perfis de clientes para avaliarem o grau de "propensão" para o cumprimento de um determinado cliente.

inferidas da análise dos comportamentos de outros sujeitos, e não dos seus próprios comportamentos[52].

Do exposto, depreende-se que a aplicação do perfil não assenta unicamente nas caraterísticas de um determinado indivíduo, mas na associação das suas características pessoais (por exemplo a sua idade, género e nacionalidade) a uma ideia preconcebida – que resultou da análise de um determinado padrão de comportamento de um grupo, que apresenta as mesmas características. Aqui, as idiossincrasias da pessoa escrutinada não são relevadas, circunscrevendo-se a identificação do sujeito aos aspetos que o interessado na criação de perfis aponta como mais importantes. Nestes termos, não são atendidos os traços distintivos individuais que extravasem os elementos pré-determinados, sendo o indivíduo reduzido a um perfil.

Foi também esta a preocupação do legislador ao consagrar a Convenção n.º 108 do Conselho da Europa, em 28 de janeiro de 1981, cuja finalidade é garantir o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito (cf. artigo 1.º desta Convenção). Contudo, no texto desta Convenção não encontramos nenhuma norma que expressamente proíba a tomada de decisões, cujo suporte seja unicamente um *tratamento automatizado de dados.*

Diferentemente, o n.º 1 do artigo 15.º da Diretiva 95/46/CE é claro ao dispor que *«os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento».* Do mesmo modo, o n.º 1 do artigo 13.º da LPD refere que *«qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza*

---

[52] Cf. os ilustrativos exemplos referidos em ZARSKY, Tal, "Mine your own business! Making the case for the implications of the data mining of personal information in the forum of public opinion", in *Yale Journal of Law and Technology*, 5, 2002-2003, p. 18 e ss.

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»*[53].

Todavia, tal como descrito na Diretiva 95/46/CE e na LPD, a regra que estabelece a proibição de tomadas de decisão baseadas exclusivamente num tratamento automatizado de dados está sujeita a determinadas condições e, ainda assim, comporta exceções.

Relativamente às condições, a referida proibição apenas abarca as tomadas de decisão com base num tratamento exclusivamente automatizado com a finalidade de avaliar determinados aspetos da personalidade do titular dos dados, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedor ou o seu comportamento, como supra visto. Por outro lado, exige aquele normativo que a decisão em questão produza efeitos na esfera jurídica do titular dos dados ou que o afete *de forma significativa*. Ainda que estes conceitos indeterminados careçam de interpretação jurídica, cuja amplitude é considerável, trata-se de requisitos cuja observância é obrigatória.

De outra banda, no que respeita às exceções, o n.º 2 do artigo 13.º da LPD dispõe que uma pessoa pode ficar sujeita a uma decisão tomada nos termos do n.º 1, desde que tal ocorra no âmbito da celebração ou da execução de um contrato, e sob condição de o seu pedido de celebração ou execução do contrato ter sido satisfeito, ou de existirem medidas adequadas que garantam a defesa dos seus interesses legítimos, designadamente o seu direito de representação e expressão.

Complementarmente, o direito de acesso, previsto na alínea c) do n.º 1 do artigo 11.º da LPD, dispõe que o titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos, *o conhecimento da lógica subjacente ao tratamento*

[53] Destaque a negrito nosso.

automatizado dos dados que lhe digam respeito. Idêntica previsão normativa resulta da alínea a) do artigo 12.º da Diretiva 95/46/CE.

Deste modo, conforme havíamos já adiantado, é patente a preocupação dos legisladores nacional e comunitário com esta questão. A falta de envolvimento do indivíduo nas decisões que o afetam mereceu a melhor atenção normativa, assumindo a criação de perfis (*profiling)* um lugar de destaque. Efetivamente, a tomada de decisões com base em projeções, inferências e prognósticos encontra o seu suporte unicamente no mundo virtual, não podendo os decisores aceitar meras ilações como se de uma realidade objetiva se tratasse.

Por outro lado, a criação de perfis afeta quer os indivíduos cujos dados são utilizados para a construção de padrões de comportamento, quer os indivíduos a quem os perfis criados serão futuramente aplicados.

Ora, são inúmeras as discriminações a que os cidadãos poderão estar sujeitos devido à segmentação do mercado, ou a outras compartimentações. Porém, aquelas serão ainda mais nefastas quando o titular dos dados desconheça que está a ser alvo dessa discriminação, razão pela qual os legisladores comunitário e nacional consagraram expressamente o direito de o titular dos dados afetado conhecer a lógica subjacente ao tratamento de dados a que é sujeito[54].

É sabido que a informação representa poder. Todavia, sendo patente a assimetria de poder entre os criadores de perfis e os cidadãos, cumpre ao Direito proteger a parte mais desfavorecida. Assim, aos respetivos titulares não deverá apenas ser facultado o mero acesso aos seus dados pessoais, mas também à logica que está por detrás da recolha desses dados.

Se um indivíduo ignora que está a ser catalogado dentro de um perfil, desconhece que poderá ser seduzido a adotar determinados comportamentos, que – de outra forma – não adotaria. Num primeiro plano, tão nocivo quanto o acesso indevido aos dados de um indivíduo, será a sua utilização perversa para manipular as suas escolhas. Deste modo, a proteção de dados pessoais tem de agir em duas frentes: por

[54] Cf. alínea c) do n.º 1 do artigo 11.º da LPD e alínea a) do artigo 12.º da Diretiva 95/46/CE.

um lado, garantir que não haja acessos indevidos aos dados pessoais e, por outro, obstaculizar o desvio da finalidade que esteve na origem da recolha dos dados.

Destarte, a aplicação de um perfil, por força da estereotipagem, pode ser uma limitação à liberdade dos cidadãos e inclusivamente uma restrição na construção da sua identidade.

Recorde-se que o direito à reserva da intimidade da vida privada, *maxime* à privacidade, não deve ser visto apenas da perspetiva da proteção de dados pessoais. De facto, a privacidade é um direito fundamental, que está na base da liberdade de ação e da própria construção da identidade. Assim, a liberdade negativa (liberdade para não ser sujeito a determinadas restrições) é tão fundamental quanto a liberdade positiva (liberdade para agir), e ambas terão de ser defendidas juridicamente. Então, vejamos. Quando um consumidor recebe *marketing* comercial na sua caixa postal, desconhecendo que essa informação lhe foi enviada devido à sua estereotipagem dentro de um perfil, a sua liberdade de escolha ficará cerceada, sem que o próprio disso tenha consciência.

Por outro lado, a aplicação de perfis na área da segurança é igualmente perniciosa. Se for demonstrado estatisticamente que a criminalidade nos centros comerciais é cometida por indivíduos do sexo masculino, entre os dezasseis e os trinta anos de idade, isso não legitimará que seja vedada a entrada aos sujeitos que se enquadrem nesse perfil. Daqui se retira que a relação entre a privacidade e a segurança tem de ser vista com um olhar renovado, já que não são antónimos, nem são negociáveis, podendo inclusivamente a perda da primeira implicar a diminuição da segunda. Do mesmo modo que um Estado de Direito democrático falha a sua missão se não acautelar a segurança dos seus cidadãos, incumprirá igualmente os seus deveres se não garantir também a sua privacidade e liberdade[55].

---

[55] E porque os exemplos reais permitem mais facilmente compreender a realidade em estudo, não pode deixar de se aludir ao recente "*Caso Snowden*", em que um trabalhador da Agência de Segurança Interna Norte Americana (NSA) divulgou os programas de vigilância daquela instituição, e que consistiam na leitura de mensagens de correio eletrónico e de chamadas telefónicas de cidadãos em todo o mundo, sem obedecerem a critérios de legalidade.

É neste sentido que o compromisso entre a segurança e a privacidade tem de ser revisto, tanto mais que a tradicional proteção de dados não é eficaz no que concerne à Internet das Coisas ou a outras tecnologias de informação. Por essa razão, terá de ser repensado o papel das entidades reguladoras, assim como a necessidade de legislação que regule estas matérias. Ainda que conscientes da dificuldade de legislar temas em constante evolução tecnológica, o paradigma da proteção de dados terá de ser outro, de modo a abraçar também a criação de perfis.

Não pode deixar de se referir que existem fenómenos sociais, que contribuem em larga medida para a recolha massiva de informações sobre os cidadãos, em particular, as redes sociais eletrónicas.

De facto, vivemos num mundo de vigilância, de vigilantes e, sobretudo, de vigiados. A monitorização de que somos alvo, seja através de câmaras de videovigilância, seja por aparelhos de GPS, seja de rastreabilidade de IP's, conduz-nos a uma cultura de suspeição e de desconfiança. Porém, é de sublinhar que essa constante vigilância parece ser justificada, mais do que por razões de segurança, pelo comportamento voluntário dos próprios cidadãos.

A desconfiança implícita no relacionamento com desconhecidos não tem sido impeditiva de uma grande exposição do indivíduo à sociedade em que se insere. E, efetivamente, se a doutrina cartesiana defendia a máxima «*cogito, ergo sum*», o mundo da «pós-modernidade líquida»[56] parece optar por um outro aforismo, no qual *quem não consta do mundo virtual não existe no mundo real*.

Atente-se na exposição a que muitos cibernautas incautos se prestam, atualizando ao minuto a sua localização e mostrando fotografias de momentos de suposta intimidade, quando, se por imposição legal tivessem de se revelar desse modo, engrossariam certamente o número de manifestantes de uma revolução pela liberdade.

Constata-se que os cidadãos ainda não sabem o que pretendem das novas tecnologias, nem parecem saber proteger-se dos seus riscos. Naturalmente que cada um de nós terá diferentes perspetivas sobre o que considera privado. Contudo, existirá

---

[56] Cf. BAUMAN, Zygmunt, *Amor Líquido - Sobre a fragilidade dos laços humanos,* Relógio d'Água, 2008.

um núcleo irredutível no conceito de esfera privada que será comum a todos e ao qual associamos o conceito de reserva da intimidade da vida privada.

Porém, a proteção da reserva da intimidade da vida privada não tem merecido a mesma atenção por todos os cidadãos. Se, em teoria, todos pretendemos que respeitem a nossa privacidade, na prática o exemplo é outro. O valor que o cidadão médio atribui à sua privacidade é muito baixo, avaliando a percentagem significativa de pessoas que regateia o preço dos seus dados pessoais a troco de um bem de reduzido valor (como, por exemplo, uma caneta) ou de pequenas melhorias na prestação de serviços.

Nessa medida, terá de ser sublinhado que os maiores defensores da nossa privacidade somos nós próprios, pelo que a gestão da informação que pretendemos partilhar com o mundo deve ser ponderada e comedida. Não se defende uma autocensura, mas uma reflexão prévia sobre as possíveis consequências de um uso indevido da informação que se pretende divulgar.

Relativamente às restantes dimensões da vida privada que não se circunscrevam àquele núcleo, insiste-se que terão de ser os próprios titulares dos dados a decidir o que consideram privado, e não uma autoridade pública em seu nome.

É também nesta medida que a privacidade está intimamente ligada à autonomia do ser humano, já que, para ser livre, o indivíduo não pode estar sujeito a interferências externas, dentro do circunstancialismo possível. O livre desenvolvimento da pessoa humana exige um espaço de reflexão e de reserva tipicamente privado. Nesse sentido, devemos controlar a influência que os outros têm em nós mesmos, para que estejamos conscientes de seguir as nossas preferências, e não as ideias impostas por terceiros.

Mas regressemos ao tema da exposição dos cidadãos através das redes sociais e atentemos no caso particular dos menores. Se, por um lado, é verdade que os mais jovens parecem estar mais predispostos a interagir por intermédio das tecnologias da informação e da comunicação, por outro, essa apetência natural nem sempre se reveste de uma maior precaução e prudência.

Assim, pese embora os mais jovens estejam, à partida, tecnicamente mais habilitados para protegerem a sua identidade no mundo eletrónico (nomeadamente por saberem alterar as configurações dos *softwares* e por utilizarem com destreza as

ferramentas informáticas), são também eles os mais sujeitos aos riscos de violações de dados pessoais, pela frequência e pela dimensão da sua exposição nos meios tecnológicos.

Atente-se que para os mais novos, cuja existência desde cedo se reflete na Internet, será possível reconstruir a sua vida desde tenra idade. Aqui, traga-se à colação a responsabilidade parental, tanto pelo comportamento que os pais adotam na gestão da sua própria presença em linha (*on-line*), como pela própria exposição dos seus filhos nas redes sociais. Uma vez mais, a acentuação tónica terá de recair sobre a sensibilização de todos os utilizadores, sendo a responsabilização dos agentes um primeiro passo para a consciencialização da necessidade de autoproteção dos dados pessoais de cada um.

Destaca-se, desde logo, que as redes sociais – contrariamente a outras formas de interação eletrónica – estimulam os seus utilizadores a revelarem a sua verdadeira identidade, quer pela publicação de fotografias, quer pela autenticação mediante o nome e endereço eletrónico[57].

Parece, então, inequívoco afirmar que é a própria autenticação que impõe, desde o início, um tratamento de dados, assim como é um garante da confiança na recolha da informação, que se presume verdadeira[58].

Porém, qual o papel da proteção de dados pessoais, quando são os próprios titulares dos dados que procuram a sua exposição?

Entendemos que, face ao crescimento exponencial das redes sociais – nomeadamente pela adesão massiva dos utilizadores e pela franca expansão em todo

---

[57] A título de exemplo, a «Declaração de Direitos e Responsabilidades» do *Facebook* indica no Ponto 4: «*Os utilizadores do Facebook fornecem o seu nome e dados verdadeiros e precisamos da tua ajuda para que assim continue a ser. Eis alguns compromissos que assumes para connosco relativamente ao registo e à manutenção da segurança da tua conta: 1. Não fornecerás qualquer informação pessoal falsa no Facebook. (…)2. Não criarás mais do que uma conta pessoal (…)7. Manterás a tua informação de contacto correta e atualizada».*

[58] Cf. ZARSKY, Tal, "Law and Online Social Networks: Mapping the Challenges and Promises of User-generated Information Flows", in *Fordham Intellectual Property, Media and Entertainment Law Journal*, volume 18, livro 3, 2008, p. 778 e ss.

o mundo – deveria ser dada prioridade no estudo desta temática, com vista a auxiliar os reguladores, os legisladores, os responsáveis pelo tratamento e os utilizadores destas redes.

Do exposto, resulta que a tecnologia não altera os princípios e regras de uma sociedade, mas sim os meios e as condições da interação social.

Ora, um dos problemas clássicos da proteção de dados pessoais reside na tangibilidade dos benefícios ao fazer uma concessão na privacidade, face à intangibilidade dos potenciais custos. Surge, assim, o dilema: ou protegemos a nossa privacidade, ou beneficiamos das vantagens do mundo eletrónico, mas não podemos ter ambos – pelo menos, não plenamente.

É para esta questão que os utilizadores deverão ser sensibilizados, sendo fundamental a educação para a sociabilização em linha (*online*). Esta problemática é de tal modo extensa e complexa, que merece um estudo próprio e aprofundado. Atendendo à limitação de tempo e à extensão deste estudo, não podemos dedicar-lhe a atenção merecida, mas não podíamos deixar de tecer alguns considerandos, dada a sua importância enquanto desafio à proteção de dados no século XXI e à sua especial relação com a criação de perfis, como fonte de recolha massiva de dados pessoais disponibilizados pelos seus utilizadores.

ii. A INTELIGÊNCIA AMBIENTE

Atentemos agora num outro desafio que a tecnologia apresenta à proteção de dados pessoais.

«As t*ecnologias de computação ubíqua têm o potencial de fornecer níveis anteriormente inconcebíveis de apoio para as atividades humanas em diferentes áreas da vida, através de sistemas que funcionam discretamente em segundo plano, com base em tecnologia embutida em ambientes e artefactos no dia-a-dia*»[59]. Assim é vista a Internet das Coisas por Johann Cas.

Estamos prestes a assistir a uma revolução tecnológica, cujos riscos e benefícios têm escapado ao debate público. De facto, pese embora haja já exemplos claros de utilização da informática de forma intrusiva – como a localização por georreferenciação (*Global Positioning Systems - GPS*) através de radiofrequência (RFID) através dos telemóveis ou de outros aparelhos – não tem sido destacada a mudança de paradigma que terá lugar muito em breve.

A inteligência ambiente define-se por um ambiente, no qual, através das tecnologias de informação e de computação, os objetos estão sensíveis à interação com as pessoas, uma vez que estão equipados com sensores e aparelhos que permitem identificar as necessidades dos seus utilizadores e responder melhor às mesmas.

Para a concretização desta tecnologia, é necessária uma infra-estrutura que suporte a interoperacionalidade entre objetos e entre estes e os seus utilizadores, assim, como a permanente recolha de informação sobre essa interatividade. Assim, todos os objetos terão de estar interligados entre si através de nanotecnologia, encontrando-se a computação integrada no ambiente.

---

[59] CAS, Johann, *Computers, Privacy and Data Protection: an element of Choice*, Bruxelas, Springer, 2011, p. 140 "*Ubiquitous computing technologies have the potential to provide previously inconceivable levels of support for human activities in different spheres of life by systems working unobtrusively in the background, based on technology embedded in everyday environments and artifacts*".

Como bem ilustram Kieron O'Hara e Nigel Shadbolt «*As nossas casas albergam muitos dispositivos pequenos, relativamente estúpidos, relativamente impotentes, embutidos nos bens de consumo. Tais dispositivos, ligados entre si, podem criar um comportamento surpreendentemente inteligente e flexível, para reduzir os custos de aquecimento e danos ambientais, ou para aplicar recursos de forma inteligente para poupar dinheiro. Cinco minutos antes do despertador tocar, poderia ser enviada uma mensagem para a chaleira se ligar, e para o assento da sanita e o toalheiro aquecerem. Ativando o chuveiro, poderia ligar-se a torradeira. A máquina de café poderia sentir quando o café tinha sido servido e, em seguida, enviar uma mensagem para a ignição do carro. No carro, o cinto de segurança poderia dizer à porta da garagem para se abrir, enquanto a porta da garagem desligaria o aquecimento central*»[60].

A contrapartida de uma tal assistência personalizada seria a constante monitorização das ações dos utilizadores dos equipamentos domésticos. E seria um preço justo a pagar?

Atualmente, salvo raras exceções, os titulares dos dados detêm o controlo sobre os seus dados pessoais, ou consentem na utilização dos mesmos por terceiros, com vista a uma determinada finalidade. A inteligência ambiente irá inverter esta regra, dado que a cada momento serão monitorizados os comportamentos de todos os indivíduos, sem que seja solicitada autorização aos titulares para esse tratamento de dados.

Consequentemente, a inteligência ambiente apresenta novos desafios à privacidade e à proteção de dados pessoais.

---

[60] O'HARA, Kieron e SHADBOLT, Nigel, *The Spy in the coffee machine: the end of privacy as we know it*, Oxford, OneWorld, 2008, pp. 8-9: "*Our homes are host to many small, relatively stupid, relatively powerless computing devices, embedded in household goods. Such gadgets, linked together, can create surprisingly intelligent and flexible behavior, to keep heating costs and environmental damage down, or to deploy resources intelligently to save money. Five minutes before it goes off, the alarm clock could send a message to the kettle to switch on, and the toilet seat and towel rail to warm up. Activating the shower might start the toaster. The coffee machine might sense when coffee had been poured and then send a message to the car ignition. In the car the seat belt might tell the garage door to open, while the garage door turns the central heating down*".

De facto, a Internet das Coisas assenta em regras que são inconciliáveis com muitos dos princípios norteadores da proteção de dados pessoais. Num sistema em que a recolha de dados será constante e cuja quantidade de dados pessoais recolhidos será vastíssima, a inteligência ambiente parece estar em clara contradição com o princípio da minimização do risco, vindo mesmo a potenciar os riscos, quer pela quantidade, quer pela qualidade dos dados tratados.

Do mesmo modo, a finalidade para a qual os dados são tratados não é determinada no momento da sua recolha, pelo menos, não de forma definida. Note-se que a solicitação do consentimento dos titulares para autorizarem um desvio da finalidade será impraticável, uma vez que, a cada instante, o titular teria de dar ou negar o consentimento para os constantes tratamentos de dados que estariam a ocorrer. Assim, fica demonstrada a fragilidade da aplicação do princípio da finalidade.

Analisemos, então, os desafios que a inteligência ambiente comporta.

Cumpre frisar, desde o início, a desigualdade de posições entre o próprio titular dos dados e os responsáveis pelo tratamento, já que a informação que os segundos deterão sobre o primeiro, bem como o conhecimento sobre o próprio funcionamento do sistema, desequilibrará a relação de forças entre ambas as partes.

Assim, não só o cidadão estará a ser constantemente monitorizado por aparelhos informáticos, como não terá qualquer possibilidade de reagir contra esse permanente controlo dos seus comportamentos. Se atualmente muitos dos cidadãos optam por não aderir a determinados tratamentos de dados – com as consequentes desvantagens que esse apartamento implica – no futuro, o direito de escolha será francamente cerceado, uma vez que a monitorização pelos objetos quotidianos poderá vir a ser a única opção disponível.

Ademais, não apenas a recolha, mas também o armazenamento e a comunicação de dados escaparão ao controlo do titular dos dados.

Note-se ainda que a finalidade da inteligência ambiente exige um conhecimento profundo de cada indivíduo, de modo a conseguir satisfazer as suas necessidades. Com esse escopo, atendendo à quantidade de informação recolhida e ao tipo de dados em causa, os responsáveis pelo tratamento poderão conhecer um determinado indivíduo melhor do que ele mesmo.

Assim, a difusão de tecnologia capaz de recolher dados pessoais a cada instante é por isso essencial para o cabal cumprimento da finalidade a que se propõe a inteligência ambiente. Ao reconduzir a um único indivíduo os dados decorrentes da sua interação com o mundo que o rodeia, todos os dados parecem elevar-se à categoria de dados pessoais, na medida em que, no seu conjunto, identificam ou permitem identificar um sujeito.

Neste contexto, os dados outrora considerados triviais – como a frequência cardíaca ou o número de vezes que alguém abre o frigorífico – deixarão de o ser, pela aplicação de processos de criação de perfis (*profiling)* e de mineração dos dados. O relacionamento de dados insignificantes dar-lhes-á um novo significado, sendo a soma das partes reveladora, *in extreminis,* da vida privada de cada indivíduo, já que a informação será reconduzida a um mesmo sujeito.

Sublinha-se que é precisamente o contexto que parece conferir o estatuto de dados pessoais à informação recolhida no quadro da inteligência ambiente. Por exemplo, o número de vezes e a que horas o interruptor da luz da entrada de um prédio é acionado não pode ser visto como um dado pessoal, na medida em que não se pode reconverter aquela informação a um determinado indivíduo. Situação diferente será aquela em que o interruptor é acionado pela impressão digital ou por um cartão pessoal, ficando o detentor da informação na posse do número de vezes que um indivíduo entrou no prédio e a que horas, e que são claramente dados da vida privada.

Neste exemplo, a utilização de dados biométricos implicaria sempre um tratamento de dados pessoais. Contudo, se fosse recolhido o número de vezes que o interruptor da luz de cada uma das frações de um prédio é acionado, bem como a hora, não estaríamos ante uma informação de natureza sensível, porque respeitante à vida privada dos moradores de cada fração? Note-se que nos casos em que os moradores habitem a fração sozinhos, é claro o relacionamento entre os seus horários em casa e os do funcionamento do interruptor da luz. Nos casos de coabitação, os titulares dos dados seriam, ainda assim, identificáveis.

É pelas razões supra expostas que o conceito de dados pessoais carece de uma redefinição, na medida em que presentemente não contempla os dados triviais que se

reportam a uma pessoa singularizada, e que estarão na base da inteligência ambiente.

Na verdade, a inteligência ambiente ainda não está em total operacionalização, pelo que a crítica que ora se tece não visa uma alteração legislativa imediata, mas antes a sensibilização do legislador para a mudança tecnológica que estamos prestes a assistir.

Se, por um lado, não se pretende fechar as portas à evolução tecnológica, por outro, não se deixam de antever semelhanças entre esta «Sociedade Panóptica»[61] e a obra orwellinana "1984"[62].

Sublinha-se que a vigilância decorrente da utilização de sensores, sistemas de identificação por radiofrequência, câmaras de videovigilância, etc., que serão responsáveis pela quantidade massiva de dados a processar, é especialmente minuciosa. Mas mais do que a quantidade, será a qualidade da informação que deverá preocupar os agentes envolvidos nesta transformação tecnológica.

Recorde-se que a monitorização não será exclusiva nem do setor privado, nem do público, partilhando ambos uma vasta informação sobre os cidadãos. Se, por um lado, os Estados serão mais capazes de tomar decisões que vão ao encontro das necessidades detetadas pelos seus cidadãos, por outro, as empresas conseguirão dirigir os seus produtos para os indivíduos que realmente estão interessados neles.

Quanto a estes aspetos, nada a apontar. O que acontece, simultaneamente, é que os mesmos Estados e empresas estarão dotados de um conhecimento que extravasa em larga escala os seus propósitos. Ademais, poderá ser utilizada essa informação de um modo maquiavélico, criando nos cidadãos e consumidores as necessidades que os aparelhos público e privado entendam por convenientes.

Esta deturpação da informação é tanto mais grave, quanto maior a perversidade que lhe está associada. A utilização abusiva da informação gerada pela inteligência ambiente será sempre censurável, mas a possibilidade de implantação de falsas necessidades nos próprios utilizadores constitui claramente um abuso de poder.

---

[61] Cf. BENTHAM, Jeremy, *A Plan of Management for a Panopticon Penitentiary-House*, T. Payne, 1791.

[62] Sugerimos a leitura de ORWELL, George, *1984,* Penguin Books, 2008.

Vejamos outro aspeto igualmente relacionado com a qualidade dos dados. Dado que a inteligência ambiente está em permanente contacto com os comportamentos dos indivíduos, poderia parecer que a qualidade da informação, tão minuciosamente recolhida, seria o mais fidedigna possível. Porém, este silogismo parte de premissas erradas. Não podemos afirmar: *se a informação é mais completa; a informação completa é rigorosa; logo, a informação é rigorosa*. De facto, a informação tratada sobre um determinado indivíduo será, à partida, mais completa, mas não necessariamente mais rigorosa. Atente-se que, para além da recolha da informação, a inteligência ambiente assenta na aplicação de perfis previamente criados com base em informação anteriormente recolhida, da qual se extraíram determinados padrões. Assim, a interpretação da informação recolhida, baseada em ideias pré-concebidas, pode deturpar a leitura do processamento automático dos dados, deturpando a sua análise.

Não se quer aqui afirmar, que a aplicação de perfis seja, por norma, fundada em pressupostos errados. Muitas das vezes, a acuidade da criação e aplicação de um determinado perfil será inquestionável, como também o é a sua margem de erro.

Outra característica a salientar na inteligência ambiente respeita à já abordada memória eletrónica. A contínua expansão da capacidade de armazenamento da informação e a diminuição dos custos que essa conservação de dados acarreta, parecem tornar ilimitada a memória eletrónica, com os consequentes riscos e vantagens para a identidade e para a privacidade dos seus utilizadores. Se a memória é, sem dúvida, o motor da evolução da humanidade, não é menos verdade que é imperioso saber conciliá-la com a proteção de dados pessoais. A conservação de dados pessoais pode, inclusivamente, ultrapassar a longevidade dos seus próprios titulares, criando problemas quanto à aplicabilidade dos direitos de personalidade, nomeadamente o direito à imagem *post mortem*.

De facto, o impacto deste perpétuo armazenamento da informação não pode ainda ser quantificado, mas não deixam de ser evidentes os potenciais riscos de uma eternização da presença de um indivíduo no mundo.

Veja-se, ainda, que o recurso a pseudónimos na Internet das Coisas será pouco eficaz, já que a informação – com elevado grau de pormenor – será reconvertível a um mesmo indivíduo[63]. Por esta razão, como supra visto, os dados recolhidos pela inteligência ambiente parecem forçosamente tornar-se dados pessoais, ainda que atualmente não sejam qualificados desse modo.

Em igual medida, o anonimato será uma utopia na Internet das Coisas. Tal como agora consideramos que a matrícula de um carro é um dado pessoal, a relação do indivíduo com os seus objetos do quotidiano virá a ser, por maioria de razão, igualmente considerada.

Uma vez que neste estudo já enunciámos os princípios basilares da proteção de dados pessoais, vejamos agora em que aspetos a inteligência ambiente não se compagina com muitos deles.

De facto, a Internet das Coisas assenta na recolha generalizada de informação a cada instante, de modo a proporcionar aos titulares dos dados a resposta para as suas necessidades individuais. Mesmo que apenas uma pequena parte desta informação fosse conservada, o princípio da necessidade perde a sua métrica, já que os dados são recolhidos massivamente, encontrando-se invertida a regra da minimização do risco. Com a inteligência ambiente, a regra passa a ser a da potenciação do risco, já que se recolhem, por um lado, dados nunca antes recolhidos e, por outro, porque a recolha da informação é incessante e sob vários meios.

Ainda que se advogue que a recolha pressuporá o consentimento dos titulares dos dados, na verdade, será impraticável a sua solicitação constante, pelo que não se aceita esta solução. Nem mesmo o interesse público será suficiente para legitimar uma recolha tão abrangente de dados pessoais, tanto mais que a Internet das Coisas não procura ir ao encontro do interesse público, mas sim dos interesses individuais de cada pessoa.

---

[63] LOUKIDES, Grigorius, et al., "The disclosure of diagnosis codes can breach research participants' privacy", in Journal of *American Medical. Informatics Association*, 17, 2010, pp. 322-327, Doi: 10.1136/jamia.2009.002725.

Aliás, além da impraticabilidade de a cada momento estar a consentir num tratamento de dados pessoais, coloca-se a questão da efetiva liberdade do consentimento, uma vez que o não consentimento implicará a exclusão da prestação de um serviço ou da oferta de um produto.

Relativamente ao princípio da qualidade dos dados, quer na sua vertente próxima do princípio da finalidade, quer como decorrência da exatidão e da atualidade da informação, são manifestas as implicações da inteligência ambiente.

De uma banda, a recolha de dados será de tal modo abrangente que nem sempre terá diretamente que ver com a finalidade do tratamento de dados naquele preciso momento. Contudo, dada a natureza difusa da Internet das Coisas, poderá ser indiretamente útil para outro tratamento de dados subsequente, ou mesmo para inferir idiossincrasias do sujeito, com vista a melhor caracterizá-lo.

De outra banda, a exigência de exatidão fica igualmente posta em causa, dado que a recolha de muita informação não significa necessariamente informação com acuidade e qualidade. Ademais, tratando-se a Internet das Coisas de um paradigma tecnológico que assenta igualmente na construção de perfis de utilizadores, a incorreta catalogação de um indivíduo poderá ser prejudicial, causando situações de discriminação injustificadas.

O princípio da definição da finalidade não escapa ileso a esta revolução tecnológica, pois a própria Internet das Coisas tem uma finalidade de difícil definição e que não é única. O que se pretende é uma recolha generalizada da informação, permitindo construir uma imagem dos utilizadores tão fiel à realidade quanto possível, de modo a que possam ser prestados serviços e oferecidos produtos que vão ao encontro das suas necessidades. Deste modo, torna-se praticamente impossível aferir da proporcionalidade, assim como determinar a observância do princípio da minimização do risco.

O princípio da limitação da utilização está intimamente relacionado com o princípio da finalidade, pelo que a inteligência ambiente, ao pretender deixar em aberto várias utilidades para a recolha da informação, não é conciliável com a aplicação daquele princípio. A aplicação deste princípio limitaria as potencialidades daquela tecnologia no seu âmago.

Já no que respeita aos restantes princípios delineados pela OCDE, e que se caraterizam por atribuírem o ênfase à vertente procedimental, existem igualmente incongruências com a sua aplicação na Internet das Coisas.

Atentemos no princípio das garantias de segurança, que obriga à aplicação de medidas técnicas de segurança contra os riscos e contra o acesso, perda, destruição, uso, modificação ou divulgação de dados de forma não autorizada. Para uma recolha tão abrangente de informação terá de destacar-se a criação de um sistema estruturado e hierarquizado de medidas de segurança que garantam uma efetiva proteção dos dados. A complexidade de um sistema desta natureza poderá ser vista como um desafio. Contudo, o simples facto de os dados serem recolhidos através da Internet – rede consabidamente insegura aos dias de hoje – não oferece a proteção que se deseja. Quando falamos de dados sensíveis, que requerem medidas de segurança acrescidas, a desproteção é ainda mais evidente.

O princípio da abertura exige que o responsável pelo tratamento faculte todas as informações relativas ao tratamento de dados, para que os titulares dos dados estejam plenamente conscientes desse tratamento de dados. De facto, sem a consciencialização das implicações de um tratamento de dados, os titulares dos dados não poderão prestar um consentimento livre e informado. O conhecimento do processamento da informação e das condições do tratamento de dados é, portanto, vital para a escolha do titular dos dados. Assim, impõe-se transparência nas várias fases do tratamento de dados, mitigando o desequilíbrio de informação entre o responsável pelo tratamento e o titular dos dados na Internet das Coisas.

Nessa sequência, o princípio da participação individual ganha novo ânimo, dado que para a verdadeira participação do indivíduo no tratamento de dados, quer colaborando na fase da recolha da informação, quer fiscalizando se o tratamento se encontra em conformidade com as diretrizes de proteção de dados, terá de existir uma verdadeira capacitação do sujeito. Não se pretende que a todos os indivíduos seja exigido um nível de conhecimentos informáticos de excelência, mas – e em completa sintonia com o princípio da abertura – que os utilizadores sejam capazes de criteriosamente analisar as vantagens e desvantagens de um tratamento de dados. Para tanto, os titulares dos dados terão de estar habilitados para conhecer os termos do tratamento de dados, assim como a lógica que lhe está subjacente.

Todavia, dada a natureza ubíqua da Internet das Coisas, assegurar o princípio da responsabilização será uma tarefa complicada. Aliás, o problema coloca-se logo na definição dos intervenientes no tratamento de dados pessoais, já que a definição de «responsável pelo tratamento» não será um exercício fácil. A nova vaga de tratamentos de dados pessoais exige, nessa medida, uma redefinição dos papéis do responsável pelo tratamento e das entidades subcontratadas. Assim, a radialização da recolha da informação e a sua comunicação a várias entidades imporá o redimensionamento da definição da responsabilidade dos intervenientes no tratamento de dados pessoais, inclusivamente do próprio titular dos dados.

iii. A SINGULARIZAÇÃO (*SINGLE OUT*)

Como supra visto, a inteligência ambiente vai permitir a recolha de dados pessoais muito detalhados sobre os seus utilizadores. Todavia, esta tecnologia potenciará um outro desafio à proteção de dados pessoais, que consiste na singularização dos indivíduos.

Ora, a singularização de uma pessoa consiste no seu imediato destacamento das demais, sem que, todavia, seja imediatamente identificado esse sujeito. Por outras palavras, estamos ante uma situação de singularização quando conseguimos agregar informações de vária ordem sobre um mesmo indivíduo, sem que o tenhamos identificado no momento da recolha desses dados.

De facto, é a minúcia dos dados recolhidos – quer pela sua quantidade, quer pela sua qualidade, quer por ambas – que permite a singularização dos indivíduos. Todavia, em que medida falamos da singularização como um dos desafios à proteção de dados pessoais no século XXI?

Sucede que as tecnologias que temos vindo a abordar – nomeadamente a criação de perfis e a inteligência ambiente – vieram potenciar a capacidade de singularização dos indivíduos que, nesse prisma, se apresenta como um dos novos desafios à proteção de dados pessoais.

Ora, recuemos à análise do conceito de dados pessoais. Como vimos, um dos critérios para a consideração de um dado como pessoal prende-se com a possibilidade de um sujeito ser identificado através do emprego de meios razoáveis.

Assim, atendendo à facilidade em correlacionar dados – designadamente pelo amalgamento de bases de dados – e ao seu baixo custo[64], podemos dizer que os meios necessários para identificar um indivíduo singularizado não serão excessivos, nem desproporcionados.

Assim, a singularização é já um primeiro passo na identificabilidade dos sujeitos a que respeitam os dados compilados. De resto, é possível reconverter muitos dos

[64] Veja-se a Lei de Moore, segundo a qual o número de transístores dos chips teria um aumento de 60%, pelo mesmo custo, a cada período de 18 meses.

dados que singularizam pessoas à categoria de dados pessoais, quando eles tornem o seu sujeito identificável. Porém, nem sempre os dados que singularizam indivíduos implicam que o seu titular seja identificável no momento da recolha. E é sobretudo relativamente a este tipo de dados que singularizam, mas que não identificam, nem permitem identificar o seu titular no momento da recolha, cuja proteção suscita maiores dificuldades.

Acresce que, apesar de a Internet das Coisas vir enfatizar a faculdade de singularização de uma pessoa – como supra analisado – a verdade é que, hoje em dia, já existem diversos mecanismos de singularização dos indivíduos, designadamente os dados de geolocalização.

Estando a utilização dos telemóveis tão banalizada nos nossos dias, com particular destaque para a crescente utilização dos chamados *smartphones*, importa analisar o impacto que estas tecnologias podem ter na privacidade.

Nesse sentido, e com especial atenção para a faculdade destes dispositivos móveis possuírem sistemas de geolocalização, quer através de identificação por radiofrequência (RFID), quer pela captação de rede móvel – que obriga à identificação da antena de emissão de sinal mais próxima – não é difícil identificar os locais mais frequentados por cada portador de um desses aparelhos.

Mesmo sem conhecer a identidade desses cidadãos, a sua individualização na multidão é clara, para quem aceder aos seus dados de geolocalização[65]. Deste modo, mesmo sem saber quem é aquele indivíduo, acede-se a informação de caráter sensível, no âmbito da sua vida privada, nomeadamente os seus trajetos e o tempo de permanência em cada local.

---

[65] Neste sentido, veja-se o estudo desenvolvido por Yves-Alexandre de Montjoye et al., no qual se determinou a singularização de 95% da amostra em análise a partir dos quatro pontos de localização mais frequentes: MONTJOYE, Yves-Alexandre, HIDALGO, César A., VERLEYSEN, Michel, BLONDEL, Vincent, "Unique in the Crowd: The privacy bounds of human mobility", Scientific Reports 3, Article number: 1376, doi:10.1038/srep01376, 2013 e disponível em: http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html.

Consequentemente, acreditamos que é mais intrusivo na privacidade dos cidadãos a recolha de dados que os singularizem do que de alguns dados pessoais que os identifiquem, como por exemplo o nome ou o género.

Contudo, cumpre aqui realçar que, à data da legislação vigente, não podemos nem incluir este tipo de informação no conceito de dados pessoais, nem existe legitimidade para a extensão do regime da proteção de dados à informação que singularize indivíduos. Efetivamente, por não identificarem, nem permitirem identificar uma pessoa no momento da recolha dos dados, não podemos incluir os dados que singularizam um indivíduo no conceito de dados pessoais nos termos da alínea a) do artigo 3.º da LPD.

Porém, porque as razões que conduziram à proteção de dados pessoais se afiguram análogas às que agora se levantam face aos dados que singularizam indivíduos, acreditamos que estes dados são merecedores de idêntico regime.

Não obstante a identidade de cada um ser composta pelo nome, género, nacionalidade, etc. entendemos que é muito mais do que isso. Assim, informações sobre os locais mais frequentados por uma pessoa, sobre os hábitos de consumo e sobre as preferências pessoais têm de ser vistas claramente como dados da vida privada e incluem-se no conjunto de características que nos definem, que nos individualizam e, logo, que nos podem identificar.

É por essa razão que os dados que singularizam, destacando alguém dos demais e permitindo a sua eventual discriminação, devem ser considerados no catálogo de dados pessoais.

Ademais, veja-se que este tipo de dados tende a ser de natureza sensível, contrariamente à categoria genérica de dados pessoais. Não temos dúvidas que as implicações e potenciais discriminações que poderão advir do tratamento dos dados pessoais como o nome ou a idade são menos lesivas que as do tratamento de informação sobre os gostos, preferências e geolocalização de um indivíduo concreto, ainda que não seja conhecida a sua identidade nesse momento.

É indubitável que, a partir do momento em que seja estabelecida uma relação entre a identificação de um indivíduo e a informação agregada sobre o mesmo, estamos perante dados pessoais e já não se suscitam os problemas de aplicação do regime da proteção de dados.

Ora, a problemática coloca-se a montante, já que – reconhecendo que a atual tecnologia permite a associação de informações de várias fontes num curto espaço de tempo e sem grandes esforços através do cruzamento de bases de dados, logo, com emprego de meios razoáveis – é realista admitir que os dados que singularizam indivíduos podem rapidamente tornar-se dados pessoais.

De harmonia com o exposto, atendendo à sua especial propensão para se tornarem dados pessoais, não se compreende a não inclusão dos dados que singularizam pessoas naquela categoria, tanto mais que podem muito facilmente transformar-se em dados pessoais *sensíveis*, sendo esta desproteção mais gritante.

Ademais, dispondo a legislação portuguesa de uma clara abertura quanto à integração de dados da vida privada na categoria de dados sensíveis, não se alcança a razão para afastar a aplicação do regime de proteção de dados pessoais destes *quasi* dados pessoais – como o são os dados que singularizam pessoas.

Esta desproteção legislativa, não encontra abrigo na *ratio legis* da legislação de proteção de dados, tendo-se já o Grupo de Trabalho do Artigo 29.º pronunciado no sentido de incluir no conceito de dado pessoal a informação que singularize um indivíduo e que permita o seu tratamento diferenciado.

Na Opinião n.º 08/2012, adotada a 5 de outubro, o Grupo de Trabalho do Artigo 29.º veio sugerir a seguinte redação do Recital 23 da proposta do Regulamento de Proteção de Dados: *«[o]s princípios de proteção devem ser aplicados a qualquer informação que respeite a uma pessoa identificada ou identificável* ***e a qualquer informação que permita que uma pessoa natural seja singularizada e tratada de modo diferente****»*[66].

Contudo, não é fácil a definição dos dados que podem singularizar alguém. De facto, não pode existir uma catalogação fechada de dados que singularizem um indivíduo, já que essa singularização resulta, muitas das vezes, da conjugação de dados de várias fontes.

---

[66] O texto a negrito reporta-se à proposta de texto daquele Grupo de Trabalhos face à redação do Regulamento proposta pela Comissão Europeia.

Assim, a análise dos dados que permitem a singularização terá de ser sempre casuística, pese embora o IP, os dados de geolocalização e os dados de consumos sejam, inequivocamente, dados que permitem a singularização.

Entendemos, pelas razões supra expostas, que é premente a necessidade de estender o regime de proteção de dados pessoais a esta categoria de *quasi* dados pessoais, que singularizem os seus titulares e, nessa medida, são reveladores da sua vida privada, pese embora não os identifiquem no momento da recolha dos dados.

III. SOLUÇÕES PARA OS NOVOS DESAFIOS QUE SE COLOCAM À PROTEÇÃO DE DADOS PESSOAIS NO SÉCULO XXI

Traçadas algumas das problemáticas que a evolução tecnológica suscita no século XXI, e uma vez que se pretende que esta análise seja construtiva, importa agora debruçarmo-nos sobre as soluções que deverão ser atendidas na aplicação de uma tão profunda revolução no tratamento de dados pessoais.

Note-se que cada um dos aspetos supra enunciados vê o seu risco potenciado, quando relacionados, pelo que o risco de singularização aumenta pelo cruzamento de várias bases de dados e pela recolha difusa de informação através da inteligência ambiente, assim como a criação de perfis tenderá a ser ainda mais detalhada, graças à informação constante das redes sociais e mediante a inteligência ambiente.

Sumamente, as propostas que se avançarão nas próximas linhas não constituem a única resposta a esses desafios – designadamente no que concerne à Internet das Coisas – nem podem ser vistas como absolutamente infalíveis. Todavia, acreditamos que poderão minorar os efeitos negativos que se adivinham, sobretudo com a generalização da inteligência ambiente.

i. ADEQUAÇÃO NORMATIVA

A resposta para os desafios que se apresentam à proteção de dados pessoais no século XXI não se prende com profundas alterações legislativas. Como referido anteriormente, a legislação de proteção de dados tem tido um caráter tecnologicamente neutro, permitindo a sua permanente atualidade. Contudo, dadas as especificidades muitas vezes trazidas pela evolução tecnológica, será conveniente regulamentar alguns aspetos mais específicos – tomando o exemplo da Diretiva de

Privacidade Eletrónica[67] – bem como densificar determinados princípios da proteção de dados, para uma maior harmonização na prática[68], dado que o seu caráter genérico nem sempre permite antever a sua concretização prática, no que toca às novas tecnologias.

Não pretendemos neste estudo substituir-nos ao papel do legislador. Todavia, avançamos algumas propostas para a maior eficácia da proteção de dados pessoais no plano normativo[69].

Neste quadro, ousamos propor o alargamento da notificação geral obrigatória, em caso de violação de dados pessoais[70]. Esta ideia não é absolutamente inédita, uma vez que foi já preconizada para as situações de violação de dados pessoais no setor das comunicações eletrónicas, nos termos do artigo 4.º da Diretiva da Privacidade Eletrónica. Por conseguinte, este alargamento a todas as violações de dados pessoais, independentemente do setor onde ocorressem, permitiria aos titulares dos dados

---

[67] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, alterada pela Diretiva 2009/136/CE, de 18 de dezembro.

[68]A Comissão Europeia tem-se revelado atenta à matéria de proteção de dados pessoais e, nesse sentido, emitiu em 2010 uma Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, intitulada «Uma abordagem global da proteção de dados pessoais na União Europeia» – Bruxelas, 4.11.2010, COM(2010) 609 final.

[69] No plano do reforço normativo, salienta-se que o artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE), alterado pelo Tratado de Lisboa que entrou em vigor em dezembro de 2009, também vem declarar o direito à proteção de dados pessoais, atribuindo à União Europeia meios adicionais para garantir este direito fundamental. Por outro lado, este último Tratado conferiu à Carta dos Direitos Fundamentais da União Europeia efeito jurídico vinculativo, consagrando nos artigos 7.º e 8.º o respeito pela vida privada e familiar e a proteção de dados pessoais, respetivamente.

[70] Ademais, o considerando 59 da Diretiva 2009/136/CE, que altera a Diretiva da Privacidade Eletrónica (Diretiva 2002/58/CE) refere que «*Este interesse generalizado por parte dos utilizadores em serem notificados não se limita, claramente, ao setor das comunicações eletrónicas, pelo que a comunicação obrigatória e explícita das exigências aplicáveis a todos os setores deverá ser introduzida a nível comunitário com caráter prioritário*».

conhecer e reagir prontamente, minimizando algumas das consequências que adviriam dessa violação[71].

Por outro lado, não deixamos de alertar, uma vez mais, para a necessidade de proteção de uma categoria de dados que, pese embora ainda não possam ser qualificados como dados pessoais – na medida em que não identificam, nem permitem identificar os seus titulares no momento da recolha – podem facilmente tornar-se dados pessoais sensíveis. Falamos dos dados que singularizam os seus titulares e que resultam, sobretudo, da recolha de informação através de dispositivos eletrónicos, como os dados de georreferenciação ou dados de consumo.

Assim, e em consonância com as considerações tecidas pelo Grupo de Trabalhos do Artigo 29.º, aplaude-se a extensão do conceito de dados pessoais, de modo a incluir os dados que singularizam os seus titulares e que podem ser suscetíveis de criar situações de discriminação.

Aliás, defende a Comissão Europeia que «*… devido aos desenvolvimentos tecnológicos e sociais, é 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*»[72].

Esta preocupação da Comissão vem ao encontro do que se pretende defender com este estudo, ou seja, que o conceito de proteção de dados pessoais seja alargado – sem que se contradiga a sua definição primitiva, vertida no artigo 3.º da LPD e na alínea a) do artigo 2.º da Diretiva de Proteção de Dados – de modo a incluir dados recolhidos através de várias fontes e que no seu conjunto singularizam os seus titulares (pese embora ainda não os identifiquem, nem permitam identificar no momento da sua recolha), revelando informações da sua vida privada, e que permitam a sua discriminação.

---

[71] A este respeito, veja-se também PURSER, Steve, "The Role of Security Breach Notifications in Improving Cyber Security", *Nação e Defesa*, n.º 133 – 5.ª Série, 2012, pp. 147-153.

[72] Cf. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – "Uma abordagem global da proteção de dados pessoais na União Europeia" COM(2010) 609 final, versão portuguesa, p. 10.

Também cumpre destacar a necessidade de melhor regular a criação de perfis, tendo o Parlamento Europeu já referido «*... que a recolha, análise, troca, e utilização abusiva de dados e o risco da "criação de perfis", estimulados pelos desenvolvimentos técnicos, atingiram proporções sem precedentes e, por conseguinte, requerem normas rigorosas de proteção de dados, como a legislação aplicável e a definição das responsabilidades de todas as partes interessadas no que se refere à aplicação da legislação da UE em matéria de dados*»[73].

Na mesma Resolução, o Parlamento Europeu «*[l]embra que a criação de perfis constitui uma tendência significativa no mundo digital, dada também a importância crescente das redes sociais e de modelos empresariais Internet integrados*» e exorta a Comissão «*... a incluir disposições sobre a criação de perfis, definindo claramente as expressões "perfil" e "criação de perfis"*»[74].

Estas preocupações refletem o entendimento do Grupo de Trabalho do Artigo 29.º, na medida em que a criação de perfis pode não implicar *ab initio* a identificação dos titulares dos dados. Contudo, pela análise emparelhada de diversas fontes de informação não identificável, poderá ser possível a concreta singularização de uma pessoa e, eventualmente, a sua consequente identificação.

Voltando às nossas soluções no plano normativo, não pode deixar de se referir que a harmonização da legislação dos vários ordenamentos jurídicos comunitários se apresenta como um imperativo para a efetiva proteção de dados pessoais dos seus cidadãos.

Esta harmonização não deverá limitar-se aos aspetos mais polémicos, devendo garantir-se uma harmonização plena. É nessa senda que a Diretiva de Proteção de Dados, que implica a sua transposição para os ordenamentos jurídicos internos, abre

---

[73] Em resposta à Comunicação da Comissão Europeia supra mencionada, o Parlamento Europeu emitiu uma Resolução, em 6 de julho de 2011, sobre uma abordagem global da proteção de dados pessoais na União Europeia, na qual espelha em grande medida o entendimento da Comissão Europeia, mas acrescenta algumas nuances. Cf. Considerando H. da Resolução do Parlamento Europeu, de 6 de julho de 2011 sobre uma abordagem global da proteção de dados pessoais na União Europeia (2011/2025(INI)).

[74] Ibidem, ponto 18.

caminho a alguma discricionariedade e, consequentemente, a divergências entre as normas de proteção de dados dos vários Estados-Membros.

Sucede que estas divergências, como a Comissão Europeia bem o reconhece, «*... são fonte de insegurança jurídica não só para os responsáveis pelo tratamento de dados, mas também para as pessoas em causa, podendo assim distorcer o nível de proteção equivalente que a diretiva visa alcançar*»[75].

No entanto, sublinhamos que se encontra em elaboração o Regulamento de Proteção de Dados, que virá substituir a Diretiva 95/46/CE, colmatando esta e outras questões, como a simplificação dos procedimentos de notificação de tratamentos de dados pessoais.

Contudo, os desafios comunitários não se restringem à harmonização legislativa interna. Por um lado, a aplicação da lei no espaço carece de clarificação, já que a globalização e as tecnologias de comunicação trouxeram novos problemas quanto ao fluxo dos dados.

Por outro lado, a definição do papel de responsável pelo tratamento e de subcontratante não é tão clara quanto outrora foi, muito devido a esses fenómenos da globalização e das tecnologias de comunicação, pelo que se exige uma redefinição daqueles conceitos. Assim, os responsáveis pelo tratamento e os subcontratantes devem ver as suas obrigações reforçadas, designadamente pela eventual introdução do princípio de responsabilização (*accountability principle*) e pela criação de regimes de certificação da União Europeia para a proteção de dados.

Relativamente aos fluxos de dados, uma vez que o nível de proteção adequada de um país terceiro é aferido por cada Estado-Membro, o reconhecimento desse estatuto não é uniforme. Por conseguinte, verificam-se situações em que um país terceiro é considerado por alguns Estados-Membro como tendo proteção adequada, mas não por outros[76].

---

[75] Ibidem, p. 11.

[76] A Comissão Europeia vem defender o aperfeiçoamento dos atuais mecanismos, quer pela celebração de novos acordos internacionais, quer pela harmonização dos parâmetros de «proteção adequada» de países terceiros. Cf. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité

Ora, uma das soluções para colmatar esta multiplicidade de critérios passa por promover a adoção de princípios universais em todo o mundo. E, já que a União Europeia tem tomado a dianteira na proteção de dados pessoais, deverá continuar a trilhar esse caminho. Dado que a globalização das empresas potencia o tratamento de dados dos cidadãos europeus ao abrigo de ordenamentos jurídicos terceiros, e sem as garantias exigidas pelas normas comunitárias, é premente um esforço diplomático, no sentido de harmonizar, a nível global, os princípios de proteção de dados[77].

Do mesmo modo, um quadro institucional mais forte, ajudará na aplicação das regras e princípios de proteção de dados[78].

Por último, terá de ser analisada a eficácia do regime sancionatório atual, com vista a encontrar-se um equilíbrio entre a prevenção geral e a prevenção especial[79].

Económico e Social Europeu e ao Comité das Regiões – "Uma abordagem global da proteção de dados pessoais na União Europeia" COM(2010) 609 final, versão portuguesa.

[77] É disso exemplo o facto de o Uruguai ratificar este ano a Convenção n.º 108 do Conselho da Europa em 1981, cuja finalidade é garantir o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito, sendo o primeiro país não europeu a ratificar aquele instrumento.

[78] Segundo a Comissão Europeia, *«… o papel das autoridades de proteção de dados é essencial para a aplicação das normas nesta matéria. São guardiãs independentes dos direitos e liberdades fundamentais no tocante à proteção de dados pessoais, com os quais as pessoas contam para a proteção dos respetivos dados e para a licitude das operações de tratamento»* - Cf. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – "Uma abordagem global da proteção de dados pessoais na União Europeia" COM(2010) 609 final, versão portuguesa, p. 19. Ainda com vista a uma maior uniformização de critérios e à harmonização normativa, considera a Comissão Europeia que *«… as autoridades de proteção de dados devem reforçar a cooperação entre si e coordenar melhor as atividades que desenvolvem»* (Ibidem) e não podíamos estar mais de acordo.

[79] A Comissão Europeia vem determinar que *«… para assegurar a aplicação das normas de proteção de dados, é essencial ter disposições eficazes em matéria de recursos e sanções …", pelo que irá "… ponderar a possibilidade de ampliar os poderes para instaurar ações nos tribunais nacionais às autoridades nacionais de proteção de dados e às associações da sociedade civil, bem como a outras associações que representem os interesses das pessoas a que os dados se referem».* Ibidem, p. 10.

ii. DIREITO AO ESQUECIMENTO

Em primeiro lugar, terá de ser dado destaque à autonomização do direito ao esquecimento. Não vemos este direito como uma manifestação do direito de oposição ou como uma decorrência necessária do princípio da finalidade, mas como um direito próprio e autónomo.

Pelo disposto, e sobretudo com as atuais possibilidades de fácil reprodução e cópia da informação, a eternização da passagem de cada um – quer no mundo físico, quer no mundo virtual – obriga a um maior enfoque na total destruição dos dados pessoais.

O direito ao esquecimento, já abordado por Samuel Warren e Louis Brandeis[80] em 1890, não perdeu a sua atualidade. Pelo contrário, é hoje mais importante reforçar o seu exercício, na medida em que os meios tecnológicos de eternização e de disseminação da informação são mais hábeis e possuem uma maior capacidade de armazenamento.

Cremos que a quantidade de informação que a tecnologia permite hoje armazenar é tão fascinante, quanto aterradora.

Por um lado, os computadores vieram otimizar as capacidades humanas, constatando-se que, nalguns casos, a obra superou o próprio criador[81].

Por outro, a tecnologia desenhou novas e inéditas potencialidades, designadamente a possibilidade de não esquecer, já que a gigantesca capacidade de armazenamento (e em constante multiplicação) aliada à fácil transmissão da informação e aos baixos custos que as mesmas implicam, possibilitam a conservação de dados – permita-se o exagero – *ad eternum*.

Os limites da memória são contornados pelo recurso aos suportes informáticos, que expandem as capacidades humanas naturais. Contudo, se – numa primeira

---

[80] WARREN, Samuel, BRANDEIS, Louis, "The Right to Privacy", in *Harvard Law Review*, n.º 5, vol. 4, dezembro, 1890.

[81] Veja-se as capacidades para prever jogadas de xadrez pelos computadores, ou mesmo a rapidez de cálculo matemático dos *softwares* atuais.

análise – a memória eterna pode ser benéfica, a capacidade de esquecimento também o é. Ser humano é ser capaz de selecionar a informação importante, que é útil e/ou significativa, daquela que é acessória e dispensável. Ao sermos gestores da nossa memória e ao criarmos as nossas próprias memórias, individualizamo-nos.

De outra banda, na ausência de controlo da qualidade dos dados, bem como da sua circulação, o próprio titular não está apto a defender-se de eventuais erros. A memória virtual será tão capaz de atraiçoar os utilizadores, quanto a memória humana. Ademais, a memória virtual será construída por múltiplos factos, cuja importância terá de ser hierarquizada, porquanto não terão todos a mesma relevância. Nessa aferição, apenas o julgamento humano pode ter em consideração as circunstâncias casuísticas de cada evento, memória ou episódio.

Porém, a memória digital limita-se a compilar toda a informação que encontra sobre um determinado indivíduo, tornando impossível a análise de todas as referências associadas a uma mesma pessoa (pelo menos, de acordo com as capacidades humanas!).

Não obstante, qual a utilidade da compilação de toda a informação relacionada com um mesmo indivíduo que circula na Internet?

De facto, a sua análise humana e minuciosa será praticamente impossível. No entanto, contrariamente às limitações humanas, a informática poderá ler todos os dados que foram agrupados sobre um determinado sujeito e retirar conclusões baseadas em operações de mineração dos dados (*data mining)*.

Analisemos, então, os riscos destas operações, já que poderão partir de pressupostos errados.

Graças à falta de controlo e à rápida circulação da informação, podemos encontrar na Internet um mesmo facto relacionado com um indivíduo em diversas fontes, sem que o mesmo seja verdadeiro. A disseminação do erro é também mais imediata na era virtual, já que a velocidade a que a informação circula e a impossibilidade de rastrear quem acedeu à mesma, propende a eternizar os erros.

Assim, ainda que estes venham a ser corrigidos, não se pode garantir que não tenha sido criada nova informação baseada naqueles erros[82].

Logo, podemos dizer que os meios digitais são tão vulneráveis a falsificações, censura, subjetividade e repressão – como qualquer outro meio de comunicação – já que sendo a fonte impura, não se pode esperar que o conhecimento que daí advenha seja impoluto.

Ora, é por todas as razões supra expostas que alguns autores acreditam que a era da privacidade tem (ou teve) um fim anunciado[83], porquanto a recolha de informação em suporte digital jamais será destruída.

Porém, outros há que, temendo a revolução da memória eletrónica (*e-memory*), defendem um prazo de validade para os ficheiros digitais[84]. Neste caso, os ficheiros informáticos estariam programados desde a sua conceção para a autodestruição automática, findo um período predeterminado.

De facto, a imortalidade que muitos buscam pode facilmente ser alcançada na Internet – não carecendo de mérito, de demérito ou mesmo de qualquer proatividade - sendo um mero reflexo da existência no mundo tecnológico, e cujas consequências não são mensuráveis, nem podem ser antevistas.

Ainda assim, atrevemo-nos a alertar para a problemática da reificação do indivíduo nos meios tecnológicos, através dos múltiplos dados pessoais disseminados em sistemas informatizados. A representação do indivíduo na era digital permite a autonomização da sua própria existência através da repercussão desta nos meios tecnológicos. Por outras palavras, o indivíduo deixa de ser identificado por aquilo que, de facto, ele é e passa a ser associado à representação dos seus interesses e

---

[82] Vejam-se os casos de imprecisões em artigos na Wikipedia – cujo trabalho meritório não se pretende aqui desvalorizar - e que, mesmo que venham a ser detetados e retificados, ainda antes da sua correção já deram origem a uma miríade de reproduções do erro inicial, pela consulta constante dessa informação pelos utilizadores.

[83] Sobre este tema, BELL, Gordon e GEMMEL, J., *Total Recall: How the E-Memory Revolution will change everything,* New York, Dutton, 2009.

[84] Consultar também MAYER-SCHÖNBERGER, *Delete: The virtue of forgetting in the digital age*, Princeton, Princeton University Press, 2009.

comportamentos, de acordo com a documentação existente nos suportes digitalizados.

Deste modo, o risco de se reduzir alguém a um conjunto de representações difusas nos suportes tecnológicos potencia a descontextualização da informação. Consequentemente, a coisificação do ser humano, baseada na mera representação da sua ação no mundo virtual, peca tanto por defeito como por excesso.

Veja-se que a recondução de uma pessoa ao seu rasto digital encontra-se enfermada pelos mesmos vícios que a assunção do todo pela parte. A dedução não poderá ser holística, dado que se baseia em informações parciais, cuja análise não permite compreender a totalidade da realidade. Mais, o reflexo da representação de um sujeito poderá mesmo não corresponder à realidade. Senão, vejamos. Por analogia, recorrendo à imagética das figuras chinesas, nem sempre pela sombra conseguimos perceber a realidade fáctica. Do mesmo modo, a representação de um indivíduo poderá nada ter que ver com a sua essência real, pelo que as inferências baseadas no seu rasto digital poderão dar causa a discriminações injustificadas.

Conforme já havíamos desenvolvido, entendemos que a autodeterminação do ser humano implica que o mesmo se relacione no mundo que o rodeia de modo livre e múltiplo. Assim, o ser humano encontra a sua individualidade na fragmentaridade e unicidade que o caracterizam. A regulamentação comunitária não é alheia a esta temática, pelo que a proteção de dados pessoais vai no sentido de abranger as multifacetadas expressões do indivíduo, quer estejam sob a forma de representação informática ou noutro suporte.

Todavia, com o intuito de evitar a possível descontextualização da informação, o legislador parece ter incumbido o titular dos dados da verificação da informação, ao conceder-lhe os direitos de acesso, de informação, de oposição, de atualização, etc. Esta capacitação (*empowerment*) do próprio titular – que é o maior interessado em proteger os seus próprios dados – foi a técnica que o legislador entendeu mais conveniente para garantir uma efetiva proteção. Nesse sentido, o ónus de verificar a acuidade da informação é simultaneamente um direito do titular dos dados. Contudo, este direito só pode ser plenamente exercido se o titular dos dados estiver consciente da sua ação e do reflexo dos seus comportamentos no mundo.

Adicionalmente, o próprio princípio da finalidade vem estabelecer que os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades (cf. alínea b) do n.º 1 do artigo 5.º da LPD). Embora este princípio esteja intimamente ligado ao direito ao esquecimento – vindo mesmo a fortalecê-lo – por si só, ele não esgota aquele direito.

Ora, de acordo com o princípio da finalidade, os dados serão tratados apenas para a finalidade indicada aquando da sua recolha, mas nada se diz quanto à necessidade de serem eliminados findo um determinado período de tempo. A finalidade pode continuar a existir, mas o titular dos dados poderá não querer que os seus dados pessoais sejam continuamente tratados. É por esta razão que os tratamentos de dados pessoais consagram um período máximo de conservação dos dados, atendendo aos princípios da finalidade e da necessidade, casuisticamente, e com vista a garantir o direito ao esquecimento.

Por seu turno, o princípio da proporcionalidade determina que os dados pessoais sejam adequados, pertinentes e não excessivos, relativamente às finalidades para que são recolhidos e posteriormente tratados (cf. alínea c) do n.º 1 do artigo 5.º da LPD). Aqui, pese embora o princípio da proporcionalidade seja visto à luz dos dados pessoais recolhidos, nada impede que o mesmo se aplique ao tempo de conservação da informação.

Decerto, sopesado num critério de adequação, pertinência e não excesso, o prazo de conservação dos dados pessoais terá de ser determinado em função da finalidade, da necessidade e na esteira do princípio da minimização do risco, sendo nesta ponderação de diferentes fatores que o direito ao se materializa.

iii. PREVENÇÃO

De facto, por toda a fundamentação supra exposta, a tónica da proteção de dados pessoais deverá incidir sobre a prevenção. Assim, o regime de proteção deverá fundear-se tanto na concretização dos princípios que norteiam a proteção de dados – em particular do princípio da minimização do risco, do princípio da necessidade e atendendo ao prazo de conservação dos dados – como na adoção de medidas técnicas assentes na privacidade por defeito (*privacy by default*) – seja na vertente da privacidade por desenho (*privacy by design*), seja na da privacidade por redesenho (*privacy by redesign*) – e, ainda, na própria capacitação e sensibilização dos titulares dos dados.

Dir-se-á que a proteção deve ser prevista durante todo o ciclo de vida da informação e os processos de tratamentos de dados devem, preferencialmente por defeito, garantir a máxima proteção dos dados pessoais.

No que respeita à criação de perfis e à singularização dos indivíduos, entendemos que a limitação na recolha – observando, em particular, o princípio da minimização do risco – poderá ser importante na prevenção de futuras violações dos direitos dos titulares dos dados.

Ainda que conscientes da dificuldade da aplicação deste princípio no contexto da inteligência ambiente, se a recolha da informação for restrita *ab initio*, os riscos de violação de proteção de dados a que estará sujeita serão proporcionalmente menores.

Nesse sentido, a minimização dos riscos encontrará um importante aliado nos criadores de *software*, na medida em que a configuração dos sistemas de recolha de dados deverá ter em conta a proteção dos cidadãos. Por conseguinte, a privacidade por defeito obrigará a que os sistemas sejam pensados, desde origem, para proteger os titulares dos dados. Por outro lado, os sistemas previamente criados sem essa preocupação deverão ser reformulados, com vista a uma reconfiguração mais garantística da proteção de dados pessoais (privacidade por redesenho).

De harmonia com este entendimento, os tratamentos de dados partirão de um pressuposto de segurança, minimizando os riscos de violação dos princípios da proteção de dados pessoais. Sublinhe-se que a adoção de medidas de proteção de

dados pessoais desde a conceção de tratamentos de dados não é incompatível com a capacitação dos titulares dos dados. Pelo contrário, trata-se de um reforço da sua proteção que complementa a segurança da informação. Assim, eleva-se o critério mínimo de proteção de dados, podendo as definições da programação ser posteriormente alteradas pelo utilizador, quer para um regime mais securitário, quer para um sistema mais aberto.

iv. TECNOLOGIAS DE POTENCIAÇÃO DA PRIVACIDADE

É importante que a tecnologia seja vista como uma ferramenta, e não como um problema ou como uma solução. Neste prisma, o seu uso implica riscos, que têm de ser acautelados, e exige que sejam tomadas medidas de segurança.

Com efeito, não deixamos de sublinhar que o utilizador é a peça chave neste sistema. Todavia, ainda que sejam implementadas medidas de salvaguarda da proteção da privacidade por defeito (privacidade por desenho) e assumindo que o utilizador está recetivo a aprender o sistema e a utilizá-lo corretamente, tal não impedirá que ocorram erros. Logo, as tecnologias de potenciação da privacidade (*PET - Privacy Enhancing Technologies*) têm de ser omnipresentes e operáveis por qualquer utilizador, independentemente do seu grau de especialização na área da informática, da sua sensibilidade para a computação e da sua recetividade às novas tecnologias.

Daqui se depreende que os riscos se mantêm, ainda que sejam significativamente reduzidos. Como diz Kieron O'Hara: «*... tentativas de queixa contra (...) a intrusão são normalmente acolhidas pela surpreendente falsa resposta que "se se mantiver dentro da lei, não tem nada a recear". A resposta que seria correta, mas de certo modo menos persuasiva, seria: "se se mantiver dentro da lei, e o governo se mantiver dentro da lei, e os seus funcionários se mantiverem dentro da lei, e o computador que contem a base de dados não errar, e se o sistema tiver sido cuidadosamente desenhado de acordo com os princípios de engenharia de* software *e mantido de modo adequado, e se o governo não poupar nos esforços, e se todos os dados forem cuidadosamente inseridos, e se a polícia for adequadamente treinada para usar o sistema, e se o sistema não for alvo de* hacking*, e se a sua identidade não for roubada, e se o* hardware *funcionar bem, não tem nada a temer"*» [85].

---

[85] O'HARA, Kieron e STEVENS, David, *inequality.com:Power, Poverty and the Digital Divide*, Oxford, Oneworld, 2006, p. 251-252 *"Attempts to complain about (…) intrusion are standardly met by the stunning false reply that 'if you keep within the law, you have nothing to fear'. A response that would be correct, but somewhat less persuasive, would be 'if you keep within the law, and the government keeps within the law, and its employees keep within the law, and the computer holding the database doesn't screw up, and the system is carefully designed according to well-understood software engineering principles and maintained*

Na verdade, constata-se que as violações de privacidade ocorrem, na sua maioria, acidentalmente, e não intencionalmente[86].

Daqui também decorre que, se a informação não for classificada como confidencial, não poderá ser tratada em conformidade com as exigências dessa classificação. Assim, compete também ao utilizador garantir, através das ferramentas e da linguagem ao seu dispor, que a informação que lhe respeita é tratada de forma adequada.

Uma vez mais se note o facto de os computadores não compreenderem as motivações humanas constituir uma importante proteção à privacidade. Veja-se que a linguagem digital não consegue distinguir o humor, a ironia, as figuras de estilo, etc., pelo que não deteta a diferença entre um texto laudatório e um texto crítico, que utilizem as mesmas palavras. Assim, atualmente a linguagem humana não permite uma leitura mecanizada e, portanto, os computadores não compreendem o texto de uma página na Internet.

Todavia, o desenvolvimento da tecnologia parece não ter barreiras. Aliás, um dos graves erros do passado prende-se com a assunção de que a tecnologia pode ser definida e limitada previamente, quando, inversamente, a ciência da computação tem demonstrado que a tecnologia está em constante evolução e que é rápido o progresso tecnológico – e, muitas vezes, o consequente recuo da proteção dos dados pessoais. Prova disso é o chamado processamento da linguagem natural (*Natural Language Processing* - NLP), técnica de leitura de textos e de extração de informação que permite aos computadores mais avançados criar hipóteses sobre o conteúdo da informação com treino de operadores humanos e baseando-se em exemplos massivos de informação. Os benefícios da NLP são notórios, mas, por outro lado, abrem-se portas a uma visibilidade da informação outrora opaca.

---

properly, and the government doesn't scrimp on the outlay, and all the data are entered carefully, and the police are adequately trained to use the system, and the system isn't hacked into, and your identity isn't stolen, and the local hardware functions well, you have nothing to fear".

[86] Cf. PATRÃO, Bernardo, "Como manter um segredo … secreto", in *Nação e Defesa*, n.º 133, 5.ª Série, 2012, pp. 196-209.

Tal como no mundo real, existem espaços de maior e de menor reserva de intimidade na Internet, como o demonstra a leitura de correio eletrónico de terceiros, que configura uma violação da correspondência, na medida em que é uma situação análoga ao correio postal. Com efeito, evidenciamos que as preocupações e as regras são em tudo idênticas no mundo real e no mundo virtual.

Continuando a exemplificação, para a maioria, a casa será o lugar de privacidade por excelência, no qual cada indivíduo retira maior proveito da sua autonomia, um espaço físico que fica associado a uma maior reserva da intimidade. De igual modo, há zonas de maior privacidade no ciberespaço, ainda que não haja uma demarcação territorial física – e, reforçando o exemplo de há pouco, o conteúdo de uma mensagem de correio eletrónico é privado, pese embora circule numa rede (a Internet) que é pública.

Neste enquadramento, a *World Wide Web*, ainda que inicialmente criada como uma ferramenta para ajudar cientistas na partilha de documentos e de informações, é hoje utilizada pelos inúmeros navegadores para compras, operações bancárias, encontros com amigos, para namorar, para fazer apostas, para entretenimento, etc. As vantagens desta rede são inúmeras, mas a passagem do mundo real para o mundo virtual acarreta uma maior desproteção dos indivíduos, já que torna possível a vigilância remota, que pode ser realizada com ou sem o conhecimento do titular dos dados. Por isso, assegurar a privacidade em sistemas intrusivos não é de submenos importância, desempenhando as tecnologias de potenciação da privacidade um papel essencial no aumento da proteção da reserva da vida privada[87].

[87] Com esta ideia em mente e consciente de que apenas se poderá garantir uma proteção efetiva se se conhecer profundamente a realidade a proteger, a Comissão Europeia propõe um estudo do impacto real das novas tecnologias da proteção de dados dos cidadãos na Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – "Uma abordagem global da proteção de dados pessoais na União Europeia" COM(2010) 609 final, versão portuguesa.

V. TRANSPARÊNCIA E CAPACITAÇÃO/SENSIBILIZAÇÃO DOS TITULARES DOS DADOS

A transparência não deverá ser unicamente vista como uma exigência dos responsáveis pelo tratamento garantirem o direito de informação e de acesso, mas como uma característica de todo o tratamento de dados.

Note-se que, desde a recolha até à destruição dos dados pessoais, tanto o responsável como o titular dos dados devem agir de modo transparente e honesto. Porém, como já vimos, a transparência não tem pautado a generalidade dos tratamentos de dados pessoais, sobretudo aqueles que se prendem com a criação de perfis e com a inteligência ambiente.

Alertamos, por isso, que a necessidade de informar os titulares dos dados é crucial para a eficácia da proteção dos dados. Nesse sentido, todos os agentes envolvidos no tratamento de dados, desde o próprio titular aos responsáveis pelo tratamento, às entidades subcontratantes para o processamento da informação, aos trabalhadores destas entidades, aos administradores de sistemas, etc. têm de estar sensibilizados para os riscos e problemáticas associados aos tratamentos de dados pessoais.

Uma vez que a perda de confiança dos utilizadores na Internet ou nos agentes envolvidos nos tratamentos de dados implicaria um retrocesso de décadas no atual estádio de desenvolvimento, não se pode fazer perigar a confiança dos utilizadores, nem criar falsas sensações de segurança na utilização da rede e na sua expansão para a inteligência ambiente.

Ainda que a complexidade das interações entre os indivíduos e a tecnologia dificultem a responsabilização dos agentes envolvidos, os responsáveis pelo tratamento não podem furtar-se às suas obrigações. Coloca-se, então, a questão sobre se o tradicional conceito de responsável pelo tratamento consegue abarcar todas as facetas que se lhe exigem. Como supra visto, acreditamos que sim, dado que a lei adotou uma definição ampla e tecnologicamente intemporal, sem prejuízo de os responsáveis pelo tratamento e os subcontratantes verem as suas obrigações reforçadas face aos novos desafios tecnológicos. Todavia, o próprio titular dos dados

terá de desempenhar um papel mais ativo na proteção dos seus dados pessoais[88] e também dos dados de terceiros[89].

Para que a pedra de toque em todo o regime da proteção de dados pessoais seja a transparência, o consentimento pelo titular dos dados deverá ser o suporte de legitimidade no tratamento de dados com recurso a tecnologias de informação. Naturalmente, esse consentimento só poderá ser válido se observar os requisitos necessários à sua compreensão pelos titulares dos dados, devendo o mesmo ser específico, informado, expresso e livre[90].

E, aqui, sublinha-se a necessidade de sensibilização dos cidadãos para estas matérias[91], para que os indivíduos tenham mais controlo sobre a sua informação pessoal disponível em linha (*online)*, de modo a utilizarem a Internet de forma responsável.

---

[88] A Comissão Europeia sublinha também a importância do aumento do controlo sobre os próprios dados pessoais, designadamente, quer pela limitação da atuação do responsável pelo tratamento dos dados às finalidades a atingir (refletindo o Princípio da Finalidade e o Princípio da Minimização dos Dados), quer pelo controlo efetivo das pessoas sobre os dados que lhes respeitam. Este controlo efetivo assume uma dificuldade acrescida no que concerne aos serviços em linha, nomeadamente, nas redes sociais. Contudo, a Comissão defende o melhoramento das condições para o exercício efetivo do direito de acesso, retificação, supressão e bloqueamento dos dados. Ibidem.

[89] Assim, designadamente na utilização de redes sociais, o titular dos dados deverá ponderar sobre a informação que divulga sobre si na Internet, procurar informar-se sobre os riscos e sobre as condições do tratamento de dados em causa e definir medidas de proteção. Naturalmente, deverá ainda respeitar a privacidade dos outros utilizadores, não divulgando dados sensíveis de terceiros, nem informações pessoais sem o seu consentimento.

[90] Indica a Comissão Europeia que «*[a]s condições de base para que exista transparência (…) são particularmente importantes num ambiente em linha, no qual muitas vezes os avisos de privacidade são pouco claros, de difícil acesso, pouco transparentes e nem sempre em conformidade com as normas em vigor*». Cf. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – "Uma abordagem global da proteção de dados pessoais na União Europeia" COM(2010) 609 final, versão portuguesa, p. 6.

[91] Os resultados de um inquérito do Eurobarómetro de 2008 demonstram que a maioria dos cidadãos dos Estados-Membros consideram baixa a sensibilização para a proteção de dados pessoais. Cf. Flash Eurobarómetro n.º 225 – Proteção de Dados na União Europeia: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

A preocupação das instituições europeias na sensibilização dos utilizadores das novas tecnologias é patente, tanto mais que foi expressamente reconhecida como uma área prioritária pelo Grupo Europeu de Ética para as Ciências e Novas Tecnologias da Comissão Europeia no seu Parecer n.º 26, de 22 de fevereiro de 2012[92].

No quadro da educação dos titulares dos dados para a proteção dos seus dados pessoais, cumpre destacar a especial necessidade de criar programas direcionados para as crianças e jovens. De acordo com o Diretor Executivo de uma das mais populares redes sociais, o maior número de utilizadores daquela rede tem menos de vinte e cinco anos[93]. Quer isto dizer que os mais jovens não só estão mais predispostos à interação através da Internet e das novas tecnologias, como também mais vulneráveis aos seus riscos. Por estas razões, deve existir uma preocupação acrescida de literacia digital nas faixas etárias mais jovens, promovendo desde cedo uma saudável utilização dos meios informáticos e a consciencialização dos benefícios e perigos que os mesmos envolvem.

---

[92] European Group on Ethics in Science and New Technologies to the European Commission: Opinion n.º 26 - Ethics of Information and Communication Technologies, Brussels, 22 February 2012

[93] STROSS, Randall, "When everyone is a friend, is anything private?", in *The New York Times*, 7 de março de 2009, disponível em http://www.nytimes.com/2009/03/08/business/08digi.html :«*Facebook says it is the world's largest social network, with 175 million members. But in the United States, most members are still relatively young; Facebook offers advertisers a target of 54.4 million members of all ages. But if an advertiser wants to narrow its target audience to those 25 or older, the number drops to 28.8 million. Narrow it to those 30 or older, and Facebook has 20.3 million to offer».*

CONCLUSÕES

- A proteção de dados pessoais é uma manifestação do direito à dignidade, do direito à identidade e do direito à reserva da vida privada, pelo que se enquadra no campo dos direitos fundamentais. Assim, atendendo à sensibilidade dos direitos em questão, deve este tema ser objeto de uma reflexão mais profunda.

- A identidade é um processo em criação ao longo da vida, pelo que o direito à identidade acompanha esse processo evolutivo do livre desenvolvimento da personalidade, contrabalançando o direito à memória e o direito ao esquecimento. Aliás, o direito à identidade pessoal, marcadamente plurisemântico e mutável, exige especial abrigo à luz da proteção de dados pessoais, dado que as novas tecnologias permitem uma ímpar multiplicação, fragmentação e desconstrução da identidade.

- As possibilidades tecnológicas atuais e as que se avizinham – nomeadamente a criação de perfis, a inteligência ambiente e a singularização – aportam novas problemáticas à proteção de dados pessoais.

- A criação de perfis através da utilização massiva de mecanismos automatizados, potencia o risco de redução do indivíduo ao perfil criado por meio de um processo automatizado, e pode influenciar processos de decisão aos quais será sujeito, sem que as suas singularidades sejam atendidas. Assim, um sujeito poderá ser alvo de discriminação, ao ser tratado à luz das características inferidas da análise dos comportamentos de outros sujeitos e não da sua própria conduta.

- A inteligência ambiente implicará uma monitorização constante de todas as tarefas quotidianas, pelo que a sua intrusão na reserva da vida privada não poderia ser maior. Contudo, esta problemática não tem sido abordada com o devido destaque, inexistindo estudos sobre o impacto desta tecnologia na vida dos cidadãos ou relativos à sua opinião sobre este grau de invasão na sua esfera de reserva da vida privada.

- A singularização (*single out*) é outro dos desafios que se coloca à proteção de dados pessoais. É, por isso, necessário considerar uma revisão do conceito de dados pessoais, de modo a que a *ratio legis* que fundamentou os preceitos legais que definem este conceito não seja desatendida face às novas possibilidades tecnológicas de identificação.

- Reconhece-se que o alargamento da noção de dados pessoais deverá ser cirúrgico, de modo a que não se estenda o regime da proteção de dados pessoais ilegitimamente. O alargamento indiscriminado seria tão nocivo quanto a desproteção de verdadeiros dados pessoais.

- As redes sociais são um exemplo onde a capacitação dos titulares dos dados, que são os maiores interessados em proteger os seus dados pessoais, é fundamental para reduzir os riscos associados a violações de proteção de dados. Para o efeito, deve ser dada prioridade à educação para a sociabilização em linha (*on-line*), em particular dos menores.

- A possibilidade de rápida disseminação de informação incorreta sobre uma pessoa, a elevada e crescente capacidade de armazenamento de informação e a evolução da identidade, enquanto expressão do livre desenvolvimento da personalidade, aportam ao direito ao esquecimento um novo significado no atual contexto tecnológico.

- A solução para todos estes problemas terá de assentar na prevenção, nas tecnologias de potenciação da privacidade, na transparência das relações, na sensibilização e na capacitação dos titulares dos dados.

- Paralelamente, deve também ser equacionado o impacto das novas tecnologias na proteção de dados a nível comunitário, deve ser reforçada a vertente de proteção de dados no mercado interno, devem ser melhorados os termos das transferências de dados internacionais, deve privilegiar-se um quadro institucional mais firme para a aplicação efetiva das normas de proteção de dados e a coerência do quadro normativo que rege a proteção de dados.

BIBLIOGRAFIA

AARTS, Emile, WICHERT, Reiner, "Ambient Intelligence", in BULLINGER, Hans-Jörg et al., *Technology Guide: Principles, Applications, Trends*, Springer, 2009, pp. 244-249

ALMEIDA, Reginaldo Rodrigues, *Sociedade Bit: Da Sociedade da Informação à Sociedade do Conhecimento*, 2.ª Edição, Quid Juris Sociedade Editora, 2004

BAUMAN, Zygmunt, *Amor Líquido – Sobre a fragilidade dos laços humanos,* Relógio d'Água, 2008

BELL, Gordon e GEMMEL, J., *Total Recall: How the E-Memory Revolution will change everything,* New York, Dutton, 2009

BENTHAM, Jeremy, *A Plan of Management for a Panopticon Penitentiary-House*, T. Payne, 1791

CANOTILHO, José Gomes, *Direito Constitucional e Teoria da Constituição*, 5.ª Edição, Almedina, 2002

CANOTILHO, José Gomes e MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, 4.ª Edição revista, volume I, Coimbra Editora, 2007

CAS, Johann, "Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contraditions", in GUTWIRTH, Serge, et al., *Computers, Privacy and Data Protection: an element of choice*, Springer, 2011, pp. 139-169

CASTELLS, Manuel, *O Poder da Identidade*, 2.ª edição, Fundação Calouste Gulbenkian

CASTRO, Catarina Sarmento, "O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro" in *Comunicação no VIII Congresso Ibero-americano de Direito Constitucional*, Sevilha, 2003

DONEDA, Danilo, "A proteção dos dados pessoais como um direito fundamental" in *Espaço Jurídico*, volume 12, n.º 2, julho/dezembro, Unoesc, 2008, pp. 91-108

ECO, Humberto, *Como se faz uma Tese em Ciências Humanas,* 17.ª Edição, Editorial Presença, 2011

FARINHO, Domingos Soares, *Intimidade da Vida Privada e Media no Ciberespaço*, Almedina, 2006

GOLDMAN, Eric, "Data Mining and Attention Consumption", in *Santa Clara Law Digital Commons*, 2005, disponível em: http://digitalcommons.law.scu.edu/facpubs/618 (consultado em 14/07/2013)

GOMES, Mário Varges, *O Código da Privacidade e da Proteção de Dados Pessoais na Lei e na Jurisprudência*, Centroatlantico.pt, 2006

GUTWIRTH, Serge, et al., Computers, *Privacy and Data Protection: an element of choice*, Springer, 2011

GUTWIRTH, Serge, et al., *Data Protection in a Profiled World*, Springer, 2010

HILDEBRANDT, Mireille, *Profiling and the Rule of Law*, DOI 10.1007/s12394-008-0003-1, Spinger, publicado on-line a 19 de dezembro de 2008

JIMÉNEZ, Luis, "Evolución histórica y conceptual del derecho a la vida privada", in *Revista de Los Tribunales Agrarios*, Segunda Época, n.º 42, IV, maio-agosto, 2007, disponível em http://www.tribunalesagrarios.gob.mx/images/stories/Publicaciones/REVISTA_Tribunales-Agrarios/rev42_5.pdf (consultado em 14/07/2013)

LOCORATOLO, Beatrice e LANDOLFI, Francesco, *Privacy e Diritto D'Acesso nella Publica Amministrazione*, 4.ª Edição, Grupo Editoriale Simone, 2011

LOUKIDES, Grigorius, et al., "The disclosure of diagnosis codes can breach research participants' privacy", in *Journal of American Medical Informatics Association*, 17, 2010, pp. 322-327, Doi: 10.1136/jamia.2009.002725

MARTINS, Ives et al., *Direito à Privacidade*, Idéias e Letras e Centro de Extensão Universitária, 2005

MARTINS, António Lourenço, MARQUES, José Garcia e DIAS, Pedro Simões, *Cyberlaw em Portugal – O direito das tecnologias da informação e comunicação*, Centroatlantico.pt, 2004

MATURANA, Humberto, VARELA, Francisco, *Autopoiesis and Cognition – The Organization of the Living*, D. Reidel Publishing Company, 1980

MAYER-SCHÖNBERGER, *Delete: The virtue of forgetting in the digital age*, Princeton, Princeton University Press, 2009

MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Coimbra Editora, 2005

MIRANDA, Jorge, *Manual de Direito Constitucional*, 3.ª Edição, Coimbra Editora, 2000, Tomo IV

MONTJOYE, Yves-Alexandre, HIDALGO, César A., VERLEYSEN, Michel, BLONDEL, Vincent, "Unique in the Crowd: The privacy bounds of human mobility", Scientific Reports 3, Article number: 1376, doi:10.1038/srep01376, 2013 e disponível em: http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html (consultado em 14/07/2013)

NEETHLING, J., POTGIETER, J. M. e VISSER, P.J., *Neethling's Law of Personality*, Durban, Butterworths, 1996

NOVAIS, Jorge Reis, *Os Princípios Constitucionais Estruturantes da República Portuguesa,* Coimbra Editora, 2004

O'HARA, Kieron e SHADBOLT, Nigel, *The Spy in the coffee machine: the end of privacy as we know it*, Oxford, OneWorld, 2008

O'HARA, Kieron e STEVENS, David, *inequality.com:Power,Poverty and the Digital Divide*, Oxford, Oneworld, 2006

OLIVEIRA ASCENSÃO, José de, *Estudos sobre Direito da Internet e da Sociedadeda Informação*, Almedina, 2001

ORWELL, George, *1984,* Penguin Books, 2008

PATRÃO, Bernardo, "Como manter um segredo … secreto", in *Nação e Defesa*, n.º 133, 5.ª Série, 2012

PECES-BARBA, Gregorio, *Educación para la Ciudadania y Derechos Humanos*, Epasa, 2007

PURSER, Steve, "The Role of Security Breach Notifications in Improving Cyber Security", in *Nação e Defesa*, n.º 133 – 5.ª Série, 2012, pp. 147-153

SILVA, Hugo Lança, *Monitorização da Internet, onde fica o direito à privacidade*, Verbo jurídico, 2006

STROSS, Randall, "When everyone is a friend, is anything private?", in *The New York Times*, 7 de março de 2009, disponível em http://www.nytimes.com/2009/03/08/business/08digi.html (consultado em 14/07/2013)

SWEENEY, Latanya, "k-anonymity: a model for protecting privacy", in International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, n.º 10 (5), 2002, pp. 557-570

TEH, Jeanette, "Privacy wars in cyberspace: an examination of the legal and business tensions in information privacy", in *Yale Journal of Law and Technology*, 4, 2001-2002

VARGES GOMES, Mário, *Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência*, Centroatantico.pt, 2006

VAZ, Ana, "Segurança da Informação, Proteção da Privacidade e dos Dados Pessoais", in *Nação e Defesa*, n.º 117 - 3.ª Série, 2007, pp. 35-63

WARREN, Samuel, BRANDEIS, Louis, "The Right to Privacy", in *Harvard Law Review*, n.º 5, vol. 4, dezembro, 1890

ZARSKY, Tal, "Mine your own business! Making the case for the implications of the data mining of personal information in the forum of public opinion", in *Yale Journal of Law and Technology*, 5, 2002-2003

ZARSKY, Tal, “Law and Online Social Networks: Mapping the Challenges and Promises of User-generated Information Flows”, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, volume 18, livro 3, 2008

LEGISLAÇÃO

- Nacional

Código Civil

Constituição da República Portuguesa

Lei n.º 102/2009, de 10 de setembro, que estabelece o regime jurídico da promoção da segurança e saúde no trabalho

Lei n.º 67/98, de 26 de outubro, que transpõe para a ordem jurídica Portuguesa 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 dos dados pessoais e à livre circulação desses dados

- Internacional

Carta dos Direitos Fundamentais da União Europeia, proclamada no Tratado de Nice, a 7 de dezembro e, novamente, em Lisboa, em dezembro de 2007

Convenção das Nações Unidas sobre os Direitos da Criança, adotada pela Assembleia Geral nas Nações Unidas em 20 de novembro de 1989

Convenção Europeia de Proteção dos Direitos do Homem e das Liberdades Fundamentais, adotada pelo Conselho da Europa e proclamada em Roma a 4 de maio de 1950, aprovada para ratificação pela Lei n.º 65/78, de 13 de outubro

Convenção n.º 108 do Conselho da Europa, para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, aberta à assinatura dos Estados Membros do Conselho da Europa em 28 de Janeiro de 1981

Declaração Universal dos Direitos Humanos adotada e proclamada pela Assembleia Geral das Nações Unidas na sua Resolução 217-A (III), de 10 de dezembro de 1948

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, alterada pela Diretiva 2009/136/CE, de 18 de dezembro

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 dos dados pessoais e à livre circulação desses dados

Pacto Internacional sobre Direitos Civis e Políticos, adotado e aberto à assinatura, ratificação e adesão pela resolução 2200A (XXI) da Assembleia Geral das Nações Unidas, de 16 de dezembro de 1966, aprovado para ratificação em Portugal, pela Lei n.º 29/78, de 12 de junho

Tratado de Lisboa, que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de Dezembro de 2007

ÍNDICE