UNIVERSIDADE AUTÓNOMA DE LISBOA

DEPARTAMENTO DE DIREITO

MESTRADO EM DIREITO

O TRATAMENTO DE DADOS PESSOAIS DE CLIENTES PARA MARKETING

Dissertação apresentada para a obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídico-Políticas

Orientadora: Professora Doutora Ana Roque

Candidata: Florbela da Graça Jorge da Silva Ribeiro

Abril

2017

Ao meu amor, Eduardo

Aos meus filhos do coração, Eduardo e Inês

À minha querida mãe, Maria Olinda

Agradecimento

A realização deste trabalho não teria sido possível sem o auxílio e estímulo de diversas pessoas. A minha gratidão e maior estima a todos aqueles que contribuíram para que esta tarefa se tornasse uma realidade.

Em primeiro lugar, à minha orientadora Professora Doutora Ana Roque, para quem não há agradecimentos que cheguem. Compreendeu os meus silêncios e as minhas angústias. Doutas e avisadas observações foram cruciais no aperfeiçoamento do trabalho e do meu próprio desenvolvimento pessoal assente na liberdade de ação concedida.

Em segundo lugar, não posso deixar de lembrar que a minha formação jurídica em muito dependeu da transmissão do saber de experiência feito, dos mais altos princípios da Justiça e do direito, e do conhecimento notável do meu Ilustre Patrono Dr. António Castelino e Alvim, que ainda hoje celebro com pequenas conquistas. Obrigado.

Não podendo nomear todas as pessoas, uma palavra de apreço à Professora Doutora Elionora Cardoso que muito contribuiu para a decisão de iniciar e concluir a dissertação na Universidade Autónoma de Lisboa, ao Senhor Procurador Jorge Costa pela sua inestimável amizade e motivação, à minha amiga Dr.ª Patrícia Machado e à minha colega Dr.ª Susana Garcia Romero, *data protection officer* da Wolters Kluwer España, pela sugestão de leituras sobre o tema da dissertação.

As minhas últimas palavras são para a minha família. Obrigado pelo apoio, o sossego, o carinho, a paciência e a compreensão nas horas mais difíceis. Não existem palavras, na Terra e no Céu, para agradecer o tempo que vos roubei. Um agradecimento especial ao Eduardo meu marido, meu amor, meu porto seguro.

«Ide pelo mundo inteiro, anunciai o evangelho a toda a criatura»
(Mc 16,15)

Resumo

O binómio consentimento do titular / finalidade do tratamento de dados pessoais alicerçados no princípio da transparência é a condição chave para o envio de comunicações comerciais não solicitadas. No contexto do marketing direto, o responsável pelo tratamento de dados deve garantir que todas as informações são claras e entendíveis pelos utilizadores dos serviços da sociedade de informação, dado que podem não entender a tecnologia que o suporta. Apenas as pessoas informadas estão em condições de prestar o seu consentimento ou exercer o seu direito incondicional de oposição à receção de comunicações não solicitadas.

Descritores: proteção de dados, consentimento, tratamento de dados pessoais, comunicações comerciais não solicitadas, marketing comportamental, marketing direto

Abstract

The binomial consent of the individual / purpose of the processing of personal data based on the principle of transparency is the key condition for sending unsolicited commercial communications. In the context of direct marketing, the data controller must ensure that all information is clear and understandable by information society service users as they may not understand the technology that supports it. Only the informed persons are able to give their consent or exercise their unconditional right to object the reception of unsolicited communications.

Keywords: data protection, consent, processing personal data, unsolicited commercial communications, behavioural marketing, direct marketing

Resumen

El binomio consentimiento del titular / finalidad del tratamiento de los datos personales fundado en el principio de la transparencia es la condición clave para el envío de comunicaciones comerciales no solicitadas. En el contexto del marketing directo, el responsable del tratamiento de los datos debe asegurarse de que toda la información es clara y comprensible para los usuarios de servicios de la sociedad de información, porque pueden no entender la tecnología que los soporta. Sólo las personas informadas son capaces de dar su consentimiento o ejercer su derecho incondicional de oposición a la recepción de comunicaciones comerciales no solicitadas.

Voces: protección de datos, consentimiento, tratamiento de datos personales, comunicaciones comerciales no solicitadas, marketing de comportamiento, marketing directo

ÍNDICE

Lista de Siglas e Abreviaturas:

Ac.	Acórdão
FRA	Agência dos Direitos Fundamentais da União Europeia
AEPD	Agencia Española de Protección de Datos (sigla oriunda do original em espanhol: Agência Espanhola de Proteção de dados)
Al) / al)	Alínea
AR	Assembleia da República
Art.º / art.º / Art.ºs / art.ºs	Artigo, artigo, Artigos, artigos
CADH	Convenção Americana dos Direitos Humanos
CC	Código Civil
CCTV	Closed-Circuit Television (sigla oriunda do original em inglês: Circuito Fechado de Televisão)
CDADC	Decreto-Lei n.º 63/85, de 14/03, que aprova o Código do Direito de Autor e dos Direitos Conexos
CdE	Conselho da Europa
CDFUE	Carta dos Direitos Fundamentais da União Europeia Comentada
CEDH	Convenção Europeia dos Direitos do Homem
CJ	Coletânea de Jurisprudência
CNPD	Comissão Nacional de Proteção de Dados
Código da Publicidade	DL n.º 330/90, de 23/10
COMISSÃO	Comissão Europeia / Comissão das Comunidades Europeias até 30/11/2009
Convenção 108	Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal
CRP	Constituição da República Portuguesa
Diretiva 2002/58/CE	Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12/07/2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)
Diretiva 97/7/CE	Diretiva 97/7/CE do Parlamento Europeu e do Conselho, de 20/05/1997, relativa à proteção dos consumidores em matéria de contratos à distância

Diretiva 97/66/CE	Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteçãoprotecção da privacidade no setor das telecomunicações
Diretiva 2006/24/CE	Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15/03/2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12/07/2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações (Diretiva relativa à privacidade e às comunicações eletrónicas).
Diretrizes sobre a Privacidade	Recomendação do Conselho da OCDE relativa às diretrizes que regem a proteção da privacidade e os fluxos transfronteiriços de dados pessoais, de 23/09/1980
DL	Decreto-Lei
DPR	Decreto do Presidente da República
DUDH	Declaração Universal dos Direitos do Homem
EEE	Espaço Económico Europeu
EOROC	Lei n.º 140/2015, de 07/09, Aprova o novo Estatuto da Ordem dos Revisores Oficiais de Contas
FEDMA	Federação Europeia de Marketing Direto e Interativo
GPS	Global Positioning System (sigla oriunda do original em inglês Sistema de Posicionamento Global)
GT29	Grupo de Trabalho do Artigo 29.º para a Proteção de Dados
HCI	Human-Computer Interaction (sigla oriunda do original em inglês: Interação Humana com o Computador)
IAm	Inteligência Ambiental
ID	Identidade (sigla oriunda do original em inglês: Identity)
IdC	Internet das Coisas
IP	Protocolo de Internet (sigla oriunda do original em inglês: Internet Protocol)
IWGDPT	International Working Group on Data Protection in Telecommunications
L	Lei

LADA	Lei n.º 46/2007, de 24/08, Regula o acesso aos documentos administrativos e a sua reutilização.
LPDP	Lei n.º 67/98, de 26/10, transpõe para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados
M2M	Máquina a Máquina (sigla oriunda do original em inglês: Machine-to-Machine)
N.º / n.º / N.ºs / n.ºs	Número / número
NFC	Near Field Communication (sigla oriunda do original em inglês: Comunicação por Campo de Proximidade)
OCDE	Organização de Cooperação e de Desenvolvimento Económicos
OEA	Organização dos Estados Americanos
P	Portaria
p.	Página / página / Páginas / páginas
PIDCP	Pacto Internacional de Direitos Civis e Políticos
PIN	Personal Identification Number (sigla oriunda do original em inglês: Número de Identificação Pessoal)
PNL	Programação Neurolinguística
pRPCE	Proposta de Regulamento do Parlamento Europeu e do Conselho, relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas), apresentada pela Comissão Europeia, de 10/01/2017.
RAR	Resolução da Assembleia da República
RD	Real Decreto
Regulamento (CE) n.º 45/2001	Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados
Res.	Resolução

RFID	Radio Frequency IDentification (sigla oriunda do original em inglês: Identificação por Radiofrequência)
RGPD	Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho de 27/04/2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)
segs.	Seguintes
SRS	Serviços de Redes Sociais
TC	Tribunal Constitucional
TCAS	Tribunal Central Administrativo do Sul
TEDH	Tribunal Europeu dos Direitos do Homem
TGUE	Tribunal Geral da União Europeia
TJUE	Tribunal de Justiça da União Europeia
TRP	Tribunal da Relação do Porto
TUE	Tratado da União Europeia
UE	União Europeia
WWW	World Wide Web (sigla oriunda do original em inglês: Rede mundial)

PARTE I – INTRODUÇÃO

CAPÍTULO I – INTRODUÇÃO

1-1. Apresentação da dissertação

As pessoas metamorfosearam-se em *bits* e *bytes* passando a viver num mundo misterioso chamado internet, e em função da magia tecnológica são classificados em distintas classes e vestidos à medida das necessidades da sociedade de informação. Na IAm flutuam dados que associados a uma pessoa passam a ter elevada relevância para os operadores económicos. Os Estados-Membros da UE para prosseguir com o mercado único assentam o seu relacionamento nas liberdades fundamentais essencialmente económicas pelo que é necessário articular o exercício das referidas liberdades com o direito fundamental à proteção de dados.

1-1.1. O objeto e estrutura da dissertação

O tema da dissertação tem como objeto a compreensão do estado de conhecimento do tratamento de dados pessoais de clientes para marketing, no sistema jurídico nacional, sem descurar a comparação constante das normas da UE, organizada em partes e capítulos, com a ordem seguinte:

1) Enquadrar o direito à proteção de dados no contexto tecnológico, cuja conceptualização é apresentada *in construhendo*: envolvendo o direito comparado sobretudo dos EUA e as organizações de que fazem parte os Estados do velho continente.
2) Determinar o que são dados pessoais e o tratamento de dados pessoais no ecossistema legal, com fundamento na jurisprudência, doutrina das organizações europeias e da mais eminente doutrina autoral. A análise e conceptualização dos conceitos do direito nacional não podem deixar de estarem enquadrados no direito da EU não só pela integração de Portugal na EU como pelos efeitos da globalização dos mercados.
3) Apresentar as especificidades do tratamento de dados pessoais para fins de marketing sustentado num conjunto de instrumentos que se reinventam a uma velocidade vertiginosa, num contexto de equilíbrio entre as liberdades económicas e o direito fundamental à proteção de dados.

1-1.2. O procedimento metodológico

A dissertação segue o método sistemático dado que procura analisar os princípios e as condições legítimas do tratamento de dados para fins de marketing (objeto da dissertação)

como um elemento do sistema jurídico do direito à proteção de dados pessoais em sintonia com as normas constitucionais, do direito da EU e das normas de direito internacional como a Convenção 108, a CDFUE e a CEDH.

Para demonstrar o alcance do tratamento de dados precisam-se os significados incorporados nos conceitos jurídicos que dão origem a ambiguidades de interpretação.

Assim, no âmbito do procedimento e na fase de recolha de fontes de informação (normas, jurisprudência e doutrina) recorre-se ao método histórico-comparativo e na fase de análise ao método dedutivo, para preenchimento do significado dos conceitos fundamentais, como por exemplo dados pessoais, de conteúdo variável atendendo ao momento histórico, ao contexto social, político, económico e de primordial importância o contexto tecnológico. As conclusões finais na atribuição de significados hão de ser concretizadas recorrendo a vários tipos de interpretação jurídica: (1) gramatical, lógico e linguístico; (2) teleológico e axiológico que procura explicar os fins e os valores que o tratamento de dados incorpora.

PARTE II – DISPOSIÇÕES GERAIS SOBRE A PROTEÇÃO DE DADOS PESSOAIS

CAPÍTULO II – CONTEXTO TECNOLÓGICO E O DIREITO À PROTEÇÃO DE DADOS

2-2. Contexto tecnológico

As tecnologias de informação e da comunicação são consideradas a maior ameaça à proteção de dados pessoais na medida em que impulsionam de forma elevada o processamento e a capacidade de armazenamento de dados, a vigilância omnipresente generalizada e a distribuição da informação a nível mundial em tempo real[1]. A utilização da internet permite que as pessoas criem fluxos de informação estáticos e dinâmicos[2] que à distância de um clique mudam para sempre os hábitos e as transações económico-sociais, evoluindo para o contexto de Inteligência Ambiental (IAm). A IAm vai além dos sensores que controlam a qualidade do ar, do sistema de aquecimento temperatura e da iluminação, detetores de fumos entre outros, na medida em que permite a interação de qualquer dispositivo eletrónico com os seus utilizadores porque é sensível às suas características e comportamentos. As pessoas vivem com coisas vestíveis e outros dispositivos eletrónicos incorporados em objetos que utilizam diariamente, distribuídas no espaço e interligados uns aos outros através de redes[3]. Estas ferramentas técnicas têm a capacidade de reconhecer características e interpretar o comportamento das pessoas, sendo aproveitadas pelos operadores económicos com o fim de antecipar as suas preferências para divulgar e prestar serviços personalizados[4].

---

[1] V. NISSENBAUM, Helen – *Privacy in Context, Technology, Policy, and Integrity of Social Life. Stanford, California : Stanford Law Books*, 2010. ISBN 978-0804752374 e PAYTON, Theresa M.; CLAYPOOLE, Theodore - *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*, Lanham (Maryland) [etc.] : Rowman & Littlefield, 2014. ISBN 978-1-4422-2545-9.

[2] LALANA, Ángel Daniel Oliver - *Código invisible y pequeño gran hermano: Nuevas condiciones de posibilidad del derecho de protección de datos*. [Em linha]. In *Revista de la Facultad de Derecho de la Universidad de la República*, n.º 22, p. 235-262, (jul. 2014). [Consult. 12 out. 2015]. Disponível em WWW <http://www.revistafacultadderecho.edu.uy/ojs-2.4.2/index.php/rfd/article/view/210>. ISSN 2301-0665.

[3] «A computação vestível refere-se a objetos do dia-a-dia e a vestuário… que incluem sensores destinados a ampliar as suas funcionalidades» que se distinguem das «coisas do eu quantificado concebidas para serem usadas em condições específicas com o fim de extraírem informações relevantes» de que são exemplos os «objetos que medem peso, pulso e outros indicadores de saúde» (V. GT29 - Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas [Em linha]. 1471/14/PT, WP 223. Brussels (Belgium), (26/09/2014). [Consult. 10 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_pt.pdf>, p. 6).

[4] Hoje em dia a domótica assume especial relevância porque é suscetível de monitorizar o domicílio profissional ou pessoal com transmissão de dados a fornecedores ou terceiros. O Laboratório dos Dispositivos Conectados na Universidade Brigham Young preparou um vídeo com o fim de explicar de como a vida das pessoas pode ser simplificada através da interligação com os objetos que utilizam diariamente, e está disponível em <https://www.youtube.com/watch?v=NjYTzvAVozo>.

2-2.1. Inteligência Ambiental

A IAm amplia a interação entre seres humanos e a informação digital através da utilização de três tipos de tecnologia fundamentais[5]:

a) Computação ubíqua[6], que é um paradigma tecnológico centrado na dispersão de componentes de hardware, com o fim integrar num único dispositivo eletrónico[7] a tecnologia de informação à distância[8], em qualquer lugar para apoiar as pessoas na realização de suas atividades e hábitos de forma simples, fácil e natural, desaparecendo amiudadamente a computação tradicional baseada no teclado, no rato e na unidade de exibição visual.

b) Comunicação ubíqua: as redes sem fios são a tecnologia dominante para a comunicação entre dispositivos que conhecemos como IdC[9]. Existem várias tecnologias envolvidas na IdC, tais como a RFID[10], NFC[11], M2M[12], bem como redes de sensores e atuadores sem

[5] V. BREY, Philip - *Freedom and Privacy in Ambient Intelligence. In Ethics and Information Technology* [Em linha]. Vol. 7, n.º 3 (set. 2005). p. 157-166. Dordrecht [etc.] : Springer Business Media Dordrecht. [Consult. 19 nov. 2015]. Disponível em WWW <https://link.springer.com/article/10.1007/s10676-006-0005-3> ISSN: 1572-8439.

[6] O conceito da computação ubíqua foi utilizado pela primeira vez em 1991 por Mark D. Weiser para expressar a sua visão do futuro dos computadores *«...[the] next generation computing environment in which each person is continually interacting with hundreds of nearby wirelessly connected computers. The point is to achieve the most effective kind of technology, that which is essentially invisible to the user … I call this future world Ubiquitous Computing*» (v. WEISER, Mark D. - *The Computer of the 21st Century. Scientific American*, Vol. 265, n.º 3, (set 1991), p. 78-89 [Em linha]. [Consult. 7 jul. 2015]. Disponível em WWW <http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf>. ISSN 1559-1662. p. 78.

[7] A al) b), do art.º 3.º, do DL n.º 192/2000, de 18/08 que estabelece o regime de livre circulação, colocação no mercado e colocação em serviço no território nacional dos equipamentos de rádio e equipamentos terminais de telecomunicações, bem como o regime da respetiva avaliação utiliza a expressão equipamento terminal de telecomunicações que define como «qualquer produto ou componente que torne possível a comunicação ou seja concebido para ser ligado, direta ou indiretamente, seja por que meio for, a interfaces de redes públicas de telecomunicações». O conceito é muito amplo e compreende os computadores, tabletes, telefones fixos, móveis e inteligentes, cartões com chip, equipamento com RFID incorporado, etc.

[8] A tendência é a miniaturização dos componentes de hardware (ao nível da molécula e com tendência para o uso universal (v. AUGUSTO, Juan C. [et al.] - *Intelligent Environments: a manifesto. Human-centric Computing and Information Sciences* [Em linha]. Vol. 3, n.º 12 (2013) [Consult. 19 nov. 2015]. Disponível em WWW <http://www.hcis-journal.com/content/3/1/12> ISSN: 2192-1962.) na ordem inversa ao aumento do software no que respeita ao processamento e desempenho na gestão da informação com maior confiança. Observa-se, igualmente, que a utilização dos dispositivos eletrónicos é cada vez menos complexa, de uso fácil e simples de experimentar, contribuindo para a captação de mais utilizadores.

[9] A Internet das Coisas (IdC) é um sistema de dispositivos interligados em que objetos, animais ou pessoas providos com um identificador único que têm a capacidade de transferir dados através de uma rede sem a necessidade interação humana ou interação humana-computador. Uma coisa, no contexto da IdC pode ser uma pessoa com um implante que monitoriza o batimento cardíaco, um animal com um chip localizador, um automóvel com sensores de velocidade, etc. A primeira coisa de IdC foi uma máquina de Coca-Cola colocada em *Carnegie Melon University* no início de 1980 à qual os programadores se ligavam através da Internet para verificar o estado da máquina e determinar a temperatura das bebidas. (Informação disponibilizada no seguinte endereço eletrónico <http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>)

[10] A RFID é uma tecnologia que permite a identificação e captação de dados de forma automática mediante a utilização de radiofrequências. Esta tecnologia tem como principal característica permitir associar um identificador único e outras informações remotamente através de dispositivos denominados etiquetas RFID (v. COMISSÃO EUROPEIA - Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Identificação por radiofrequências (RFID) na Europa:

fio[13], concebidas para registar, tratar, armazenar e transferir dados[14]. A combinação entre o uso simplificado e a sua capacidade de aceder a dados e informações aumentam a conectividade dos dispositivos entre si, com maior eficiência para os utilizadores e de forma cada vez mais impercetível.

c) Interface inteligente adaptada ao utilizador, isto é, o utilizador tem a perceção que os sistemas que se adaptam automaticamente às suas necessidades e preferências quando interage com eles. A interface inteligente caracteriza-se pela criação de perfis e pela consciência de contexto[15] [16] em tempo real devido ao uso generalizado das fontes de informação[17] e software de extração e sincronização eficiente de dados, baseado na web semântica[18].

2-2.2. Operadores económicos

O aumento progressivo da interação do utilizador com os sistemas da IAm alterou o paradigma da comunicação dos operadores económicos para alcançar maiores benefícios económico-financeiros. A alteração da estratégia de comunicação e respetivos canais de

---

rumo a um quadro político [Em linha]. COM(2007) 96 final. [Consult. 10 Dez. 2015]. Disponível em WWW <http://www.umic.pt/images/stories/publicacoes200710/com2007_0096pt01.pdf>).

[11] NFC refere-se à tecnologia que permite a troca de informações sem fio e de forma segura entre dispositivos compatíveis mediante uma simples aproximação entre eles, sem que o utilizador tenha de introduzir um login, clicar em botões ou realizar qualquer ação para estabelecer a ligação.

[12] M2M refere-se, geralmente, à IdC para uso industrial, comercial e aplicações comerciais. (v. LOUCHEZ, Alain - *The Internet of things: Machines, businesses, people, everything. In ITU News* [Em linha]. N.º 6. [2013?] Genéve : International Telecommunication Union, 2013. [Consult. 19 jan. 2016]. Disponível em WWW <https://itunews.itu.int/En/4291-The-Internet-of-things-Machines-businesses-people-everything-.note.aspx> e ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO - *Machine-to-machine communications: connecting billions of devices*. [Em linha]. DSTI/ICCP/CISP(2011)4/FINAL, OECD *Digital Economy Papers*, n.º 192, OECD Publishing (2012). [Consult. 12 Mar. 2016]. Disponível em WWW <http://www.oecd-library.org/docserver/download/5k9gsh2gp043.pdf?expires=1460899221&id=id&accname=guest&checksum=EB86294E2B573CC92443177E517D66AB>).

[13] Atuadores sem fio convertem informações ou energia proveniente de sensores em ação (medem características do nosso ambiente físico, como a pressão, calor e humidade) e transmitem-nas para outro mecanismo ou sistema sem intervenção humana.

[14] «A IdC implica geralmente o tratamento de dados que dizem respeito a pessoas singulares identificadas ou identificáveis qualificando-se, por conseguinte, como dados pessoais na aceção do art.º 2.º, da Diretiva Proteção de Dados da UE» (GT29, cit. 3, p. 4)

[15] A tecnologia, suportada por um conjunto de algoritmos inteligentes capazes de interpretar o comportamento dos utilizadores registado em sensores, tem a capacidade de criar perfis bem como situá-los no contexto geográfico e em consequência reconhecê-lo para prestar a informação que eventualmente seja necessária (por exemplo, um utilizador de nacionalidade portuguesa que tem um número elevado de transações realizadas através do seu cartão de crédito, num restaurante italiano, quando viaja para o Reino Unido, pode receber um alerta no dispositivo com os restaurantes italianos mais próximos do local onde se encontra). O registo da atividade dos utilizadores feito no passado é recuperado para a criação de perfis num contexto futuro. É interessante notar a diferença entre realidade virtual onde as pessoas entram no mundo do computador e a computação ubíqua em que é o computador que entra no mundo das pessoas (v. WEISER, cit. 6).

[16] V. AUGUSTO, cit. 8.

[17] Por exemplo, os sensores baseados na tecnologia HCI e os sistemas de CCTV, GPS, Bluetooth e RFID.

[18] Para maiores desenvolvimentos sobre a web semântica, sugere-se a consulta com extensa informação do seguinte endereço eletrónico: <http://www.w3.org/Consortium/>

comunicação dos operadores económicos foca-se na obtenção da confiança do utilizador com o objetivo direcionar o seu estilo de vida através do envolvimento e da criação de experiências, tais como formas de criar presença em linha (ou não) e respetiva ligação afetuosa por meio de mensagens personalizadas adaptadas ou mesmo antecipatórias às suas necessidades, na hora certa e no lugar certo. A confiança, do utilizador, é alcançada com recurso a técnicas de persuasão baseadas no conhecimento do seu comportamento e hábitos em linha e reconhecimento do seu contexto situacional.

A atividade económica pode conduzir a abusos na recolha de informação pessoal dos clientes[19] e ameaçar a privacidade e a proteção dos seus dados. O cliente, cujas transações

[19] O conceito de consumidor e cliente são utilizados com o mesmo significado para efeitos do presente texto. O conceito de consumidor utiliza-se para designar as pessoas que merecem ser protegidas por uma lei especial relacionada com a matéria do consumo. Contudo, nem todos os textos dos vários diplomas têm o mesmo significado ou proteção. O n.º 1, do art.º 2º, da L n.º 24/96, de 31/07, que estabelece o regime legal aplicável à defesa dos consumidores, define como consumidor «todo aquele a quem sejam fornecidos bens, prestados serviços ou transmitidos quaisquer direitos, destinados a uso não profissional, por pessoa que exerça com caráter profissional uma atividade económica que vise a obtenção de benefícios». A al) c) do art.º 3º, do DL n.º 24/2014, de 14/02, que transpõe a Diretiva n.º 2011/83/UE do Parlamento Europeu e do Conselho, de 25/10/2011, relativa aos direitos dos consumidores, que define consumidor como "a pessoa singular que atue com fins que não se integrem no âmbito da sua atividade comercial, industrial, artesanal ou profissional" e idêntico conceito aparece na al) a) do art.º 3º, do DL n.º 57/2008, de 26/03, que estabelece o regime aplicável às práticas comerciais desleais das empresas nas relações com os consumidores, ocorridas antes, durante ou após uma transação comercial relativa a um bem ou serviço. No âmbito do direito da EU, também, não existe um conceito único de consumidor, respondendo a necessidades setoriais em detrimento da coordenação e sistematização, por exemplo, o art.º 2º, da Diretiva 2011/83/UE, de 25/10, que altera a Diretiva 93/13/CEE e a Diretiva 1999/44/CE e que revoga a Diretiva 85/577/CEE e a Diretiva 97/7/CE, relativas aos direitos dos consumidores, define consumidor como «qualquer pessoa singular que, nos contratos abrangidos pela presente diretiva, atue com fins que não se incluam no âmbito da sua atividade comercial, industrial, artesanal ou profissional», ainda que no Considerando 17 refira que «a definição de consumidor deverá abranger as pessoas singulares que atuem fora do âmbito da sua atividade comercial, industrial, artesanal ou profissional. No entanto, no caso dos contratos com dupla finalidade, se o contrato for celebrado para fins relacionados em parte com a atividade comercial da pessoa e em parte à margem dessa atividade e se o objetivo da atividade for tão limitado que não seja predominante no contexto global do contrato, essa pessoa deverá ser igualmente considerada consumidor». Parece adequado que «não se vê, […] por que razão não deva merecer proteção como consumidor quem adquira bens ou serviços para uso profissional (v. g., porque distinguir quem compra um romance de quem compra um livro científico ou por que distinguir quem faz uma viagem turística de quem faz uma viagem por motivos profissionais). De resto, a L n.º 23/96, de 26/07 (com as alterações introduzidas pelas Leis n.ºs 12 e 24/2008, de 26/02 e 02/06, respetivamente), ao definir utente de serviços públicos essenciais não faz tal distinção e, por certo, utente é ainda um consumidor» (v. MIRANDA, Jorge - Artigo 60º (Direitos dos consumidores) In MIRANDA, Jorge; MEDEIROS, Rui, coord. - Constituição Portuguesa Anotada, Tomo I. 2.ª ed., Coimbra : Wolters Kluwer, 2010. ISBN 978-972-32-1822-0. p. 1172). O conceito de consumidor tem sido objeto de interpretação jurisprudencial em diferentes áreas do direito nacional e da EU em termos amplos e apenas para um setor em concreto, com tendência a excluir as pessoas coletivas. A título comparativo, o art.º 2º, do Código Brasileiro de Defesa do Consumidor (L n.º 8.078, de 11/09/1990) define consumidor como "toda a pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final" com fundamento exclusivamente de caráter económico (v. GRINOVER, Ada Pellegrini [et al.] - Código Brasileiro de Defesa do Consumidor, Comentado pelos autores do Anteprojeto, 6ª ed., Rio de Janeiro, Forense Universitária, 2000. ISBN 87-218-02-49-8) e em Espanha, o art.º 1º, do RD Legislativo 1/2007, de 16/11, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, «*son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. Son también consumidores a efectos de esta norma las personas jurídicas y las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial.*» (POMBO, Eugenio Llamas, coord. - *Ley General para la Defensa de los Consumidores y Usuários, Comentarios y Jurisprudencia*

(gratuitas ou onerosas) são realizadas em linha, tem de fornecer informação pessoal através do preenchimento de formulários para aceder ao produto ou serviço pretendido. A aceitação da política de privacidade, com o simples assinalar de uma cruz na quadrícula disponível, é na maioria das vezes feita de forma automática sem leitura prévia pelo cliente[20], para satisfação de necessidades instantâneas[21]. O cidadão médio utilizador da internet não está prevenido para a salvaguarda dos seus dados pessoais[22] desconhecendo até o destino e uso dos seus dados pessoais[23] e quando constata que a esfera da sua privacidade foi invadida, principalmente pela receção de correio não solicitado e com tendência a aumentar, assume uma atitude passiva e resignada[24].

O crescimento do comércio em linha, caracterizado pela rapidez, facilidade e baixo custo, beneficia as empresas que são encorajadas a registar a interação com os clientes devido aos custos reduzidos de processamento da informação recolhida e armazenada. O preço da diminuição da proteção de dados pessoais é o preço que os clientes pagam pela conveniência de fazerem transações em linha[25].

A proteção de dados pessoais é uma das questões fundamentais da era digital tendo em conta a relevância jurídica da natureza invasiva, omnipresente e invisível das tecnologias da IAm

---

de la Ley veinte años después. Las Rozas (Madrid) : La Ley-Actualidad, 2005. ISBN 84-9725-603-4).

[20] Em junho de 2014, foi realizada uma pesquisa organizada pelo Instituto de Pesquisa de Segurança Cibernética, com sede em Londres e apoiada pela EUROPOL, com o objetivo de destacar o desconhecimento público sobre as questões de segurança graves concomitante com o uso de Wi-Fi. O contrato, que descrevia os termos e condições, incluía a «cláusula de Herodes». Em pouco tempo, seis londrinos abdicaram dos seus primogénitos «pelo período da eternidade» para terem acesso a uma rede Wi-Fi por algumas horas, com um simples clique na quadrícula "Li e aceito", e sem ter tido conhecimento efetivo do seu conteúdo. A rede teve de ser desativada para evitar que as trinta e três pessoas, em espera, acedessem à rede, ainda que a cláusula fosse nula por ser contrária a todos os princípios de direito e justiça no que respeita à venda de crianças em troca de serviços gratuitos (v. FOX-BREWSTER, Tom - *Londoners give up eldest children in public Wi-Fi security horror show* [Em linha]. *The Guardian*, (29/09/2014) [Consult. 12 de out. 2015]. Disponível em WWW <https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause>).

[21] ARAYA, Agustin A. - *Questioning Ubiquitous Computing*. In HWANG, C. Jinshong; HWANG, Betty W. (Coord.) - *Proceedings of the 1995 ACM 23rd annual conference on Computer science*. [Em linha]. New York : ACM, 1995 [Consult. 22 nov. 2015]. Disponível em WWW <http://www.cc.gatech.edu/~keith/classes/ubicomplexity/pdfs/crit/araya-questio ning-ubicomp.pdf >. ISBN:0-89791-737-5. p.230-237

[22] COSTA, Francisco Bruto da, BRAVO, Rogério – Spam e Mail-Bomb subsídios para uma perspectiva penal. Lisboa : Quid Juris, 2005. ISBN 972-724-239-1. p.22

[23] Aconselha-se a leitura das políticas de privacidade dos serviços das redes sociais (Facebook, Linkedin, ...) para compreensão da falta de controlo do fluxo de dados dos perfis pelos próprios utilizadores no que respeita a visualização de anúncios publicitários do interesse de amigos e que supostamente, também, estariam interessados. Parece haver um certo entorpecimento por parte das pessoas quanto ao reconhecimento de que existem empresas capazes de os conhecer através da utilização das suas ferramentas tecnológicas ainda que independentes umas das outras. A empresa Google é o caso que melhor ilustra o anteriormente referido, na medida em que tem um motor de pesquisa, serviços de correio eletrónico e localização geográfica, serviços de publicidade e disponibilidade de notícias em linha, que recorrendo a tecnologias de hiperligação invisível, recolhe e retém informações de milhões de utilizadores.

[24] COSTA e BRAVO, cit. 22, p. 29.

[25] GUPTA, Jatinder N. D., SHARMA, Sushil K. - *Cyber Shopping and Privacy*. In FAZLOLLAHI, Bijan coord. - *Strategies for eCommerce Success*. Hershey, Pennsylvania : IRM Press, 2002. ISBN 1-931777-08-7. Cap. 1, p. 1-16.

utilizadas pelos operadores económicos para recolha e tratamento de dados pessoais[26].

A proposta de produtos e serviços selecionados pelas organizações dirigida a pessoas que teve o cuidado de identificar e analisar o seu comportamento em linha diminui a privacidade e a liberdade de escolha. Embora seja uma *conditio sine qua non* para a realização da visão da IAm[27], a construção de perfis[28] dos utilizadores em linha, baseados em modelos de mineração de dados[29] e algoritmos[30], pode dar origem a significados que as pessoas não têm de si próprias ou mesmo diferentes da sua identidade real e física[31] [32]. A criação de perfis individuais ou coletivos pode dar origem a riscos de discriminação[33] e estigmatização, direta ou indiretamente, do consumidor de produtos ou serviços[34], em razão, designadamente, do

[26] Como observa LANGHEINRICH: «*With a densely populated world of smart and intelligent but invisible communication and computation devices, no single part of our lives will per default be able to seclude itself from digitization. Everything we say, do, or even feel, could be digitized, stored, and retrieved anytime later*» (v. LANGHEINRICH, Marc - *Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems*. In ABOWD, Gregory D., BRUMITT, Barry, SHAFER, Steven, coord. *In Ubicomp 2001: Ubiquitous Computing - Lecture Notes In Computer Science, Proceedings of the 3rd international conference on Ubiquitous Computing, Atlanta, Georgia, USA* [Em linha]. Berlim [etc.]: Springer-Verlag Berlin Heidelberg New York, 2001. (Lecture Notes in Computer Science, Vol. 2201, p. 273-291). ISBN 978-3-540-45427-4, p 280.

[27] V. por todos a obra notável de HILDEBRANDT, Mireille, GUTWIRTH, Serge coord. – *Profiling the European Citizen Cross-Disciplinary Perspectives.* [S.l.] : Springer Science + Business Media B.V. 2008, ISBN 978-1-4020-6914-7.

[28] Um perfil, segundo Hildebrandt, resulta de um processo de descoberta automatizado de padrões dos dados armazenados em bases de dados, envolvendo diferentes tecnologias (RFID, biometria, sensores, limpeza de dados, agregação de dados e mineração de dados, entre outras) que quando interpretados podem ser usados para identificar ou representar um ser humano ou sujeito não-humano (individual ou em grupo). (HILDEBRANDT, GUTWIRTH, cit. 27.). Um operador económico pode, assim, construir uma base de dados de clientes organizada por hábitos de consumo comercial, estilo de vida, preferência em determinado contexto.

[29] A mineração de dados refere-se ao processo de análise de dados de uma base de dados, com recurso a técnicas de inteligência artificial, redes neurais e ferramentas estatísticas avançadas (tais como análise de cluster) para revelar tendências, padrões e estabelecer relações. O processo tem como objetivo a avaliação do risco e oportunidade para o exercício da atividade económica fundamentada nos comportamentos passados de um consumidor ou grupo de consumidores.

[30] Um algoritmo é constituído por uma série de funções que processam dados com a finalidade de extrair informações dos dados. (v. STEELE, Brian; CHANDLER, Jonh; REDDY, Swarna - *Algorithms for Data Science* [Em linha]. 1.ª ed., Cham : Springer International Publishing Switzerland, 2016. ISBN 978-3-319-45797-0. [Consult. 1 jan. 2017]. Disponível em WWW: < http://www.springer.com/in/ book/9783319457956> p. 11.

[31] HILDEBRANDT, GUTWIRTH, cit. 27.

[32] O tratamento de dados pessoais com recurso a processos automatizados é, por isso, uma atividade de risco. O risco consubstancia-se, essencialmente, na utilização indevida de dados pessoais ou com erros de representação sobre o seu titular, pelo que são necessários mecanismos de controlo sobre os próprios dados pessoais (v. HILDEBRANDT, GUTWIRTH, cit. 27.).

[33] O *status* profissional já foi discutido no TEDH embora não tivesse sido encontrada nenhuma violação ao art.º 14º, da CEDH (Ac. *Van Der Mussele v. Belgium*, do TEDH n.º 8.919/80, de 23/11/1983).

[34] Existem numerosas formas de classificação de sentimentos dos internautas com recurso a técnicas baseadas em PNL, para além do reconhecimento facial. A captura de dados (utilizando web *crawlers* e interfaces de aplicativos específicos em canais como blogs, pesquisa de mercado, relatórios, e-mails e redes sociais) sobre um documento disponível na internet é realizada para categorizar sentimentos positivos, negativos ou neutros sobre produtos ou serviços (V. KRISHNA, P. Radha - *Big Data Search and Mining*. In MOHANTY, Hrushikesha, CHENTHATI, Deepak, BHUYAN, Prachet, coord. Big Data A Primer [Em linha]. New Delhi [etc.]: Springer Índia, 2015. (*Studies in Big Data*, Vol. XI) [Consult. 12 ago. 2016]. Disponível em WWW <http://www. springer.com/gp/book/9788132224938> ISBN 978-81-322-2494-5. p 93-120.

sexo, raça, cor, língua, religião, política, origem nacional ou social[35], a pertença a uma minoria nacional, riqueza, nascimento, entre outros. Tem merecido preocupação o fenómeno das listas negras que incorporam registos de pessoas de determinadas bases de dados relacionada com determinados factos reprováveis socialmente e que lhe são desfavoráveis[36]. Atualmente assiste-se ao aumento de criação de ficheiros[37] com dados geridos por instituições de crédito e financeiras resultantes do incumprimento de um contrato de crédito ou da rescisão da convenção do uso de títulos de créditos (sobretudo do cheque) com vista à prevenção do sobre-endividamento do consumidor e cálculo do risco do credor e pela Administração Tributária com o fim de sancionar o devedor de tributos não só pela informação que é tornada pública e obter reprovação ética e social, mas, também, a inibição de contratar com pessoas coletivas de natureza pública ou de utilidade pública. Apesar destes ficheiros representarem um instrumento de desenvolvimento económico é indispensável que se procure o equilíbrio entre o direito à determinação informativa do cidadão/consumidor e os legítimos interesses comerciais das empresas[38] e da prossecução do bem público e dever dos cidadãos em geral.

A IAm apresenta desafios sem precedentes[39] que requerem desenvolvimentos tecnológicos e instrumentos reguladores que afiancem a segurança dos sistemas informáticos e a resolução dos problemas de acesso, recolha, retenção, autorização e consentimento para o tratamento dos dados pessoais, sem prejudicar os interesses dos operadores económicos na sociedade de informação[40].

---

[35] Discussão sobre tratamento de forma diferente não por ser diferente mas por causa dessa característica consubstanciada na origem social (Ac. *Olsson v. Sweden*, do TEDH n.º 10.465/83, de 24/03/1989).

[36] V. GT29 - Documento de trabalho sobre listas negras. [Em linha]. 11118/02/PT/final, WP 65. Brussels (Belgium), (03/10/2002). [Consult. 16 Fev. 2014]. Disponível em WWW <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_pt.pdf>

[37] Trata-se do fenómeno cada vez mais comum das chamadas "listas negras" difíceis de conceptualizar devido aos critérios específicos de cada tipo de lista negra em causa. As listas negras podem produzir «efeitos adversos e prejudiciais para as pessoas nelas incluídas e que podem ser discriminatórios contra um grupo de pessoas ao impedir-lhes o acesso a um serviço específico ou prejudicar a sua reputação» (v. GT29 cit. 36). As listas negras com maior relevância estão relacionadas com os ficheiros de devedores e serviços de informação de solvabilidade e crédito, os ficheiros relativos a infrações ou condenações penais e os ficheiros de deteção de fraudes, sobretudo no setor da atividade seguradora, que estão sujeitas a regimes legais com as restrições que têm sido consideradas oportunas. Existem outro tipo de listas negras relacionadas com a atividade laboral, nomeadamente com dados desfavoráveis sobre empregados ou candidatos a emprego, ou relativos a questões de saúde, comportamento social ou político ou negligência profissional, que são proibidas na maior parte dos Estados-Membros que proíbem o tratamento de dados sensíveis sem o consentimento explícito do seu titular, conforme previsto nos art.ºs 8º, 13º e 15º, da Diretiva 95/46/CE.

[38] CASTRO, Catarina Sarmento e - Direito da Informática, Privacidade e Dados Pessoais. 1ª ed, Coimbra : Almedina, 2005. ISBN 978-97-2402-424-0. p. 65 e seguintes.

[39] A preocupação com a proteção de dados tem sido sujeita a ampla reflexão na literatura, com particular relevância dos pareceres do Grupo de Trabalho do Artigo 29º e a os vários relatórios de pesquisa sobre ética, legal e social que levantam questões sobre o IAm.

[40] Segundo ASCENSÃO, José de Oliveira - Sociedade de Informação. in Direito da Sociedade da Informação,

2-2.3. Razão para proteger os dados pessoais

Seguindo o pensamento de Hoven existem essencialmente quatro tipos de razões morais e éticas para a proteção dos dados pessoais e respetivo controlo: a prevenção do dano relacionada com o uso indevido da informação pessoal por terceiro pode prejudicar o seu titular; a desigualdade informacional, na medida em que, os dados pessoais passaram a ser um ativo dos operadores económicos e os seus titulares não tem os mesmos meios de verificar de como são tratados ou transferidos; a discriminação sempre que os dados pessoais cedidos num determinado contexto (por exemplo, cuidados de saúde) pode mudar o seu significado quando utilizados noutro contexto (por exemplo, para propostas comerciais) e pode levar à discriminação ou situações desfavoráveis para o seu titular; a autonomia porque a falta de privacidade pode expor os titulares a determinadas forças externas que influenciam e limitam as suas escolhas.

2-2.4. O direito à proteção de dados

Nos últimos anos, a demanda pelos dados pessoais, o número crescente de fontes de recolha de dados, a complexidade das ferramentas de tratamento e análise de dados desequilibrou a balança do controlo da informação pessoal a favor das organizações dando origem à discussão sobre o âmbito do direito à proteção de dados pessoais e as crescentes medidas normativas. Num mundo em que as pessoas são cada vez mais transparentes e o mundo virtual cada vez mais opaco[41] a UE reconhece o direito à proteção de dados pessoais como um direito fundamental, em constante adaptação à evolução tecnológica e às alterações político-sociais[42],

---

Coimbra : Coimbra Editora, 1999. ISBN:972-32-0916-0. Vol. I, p. 163-184, p. 167 «Sociedade de Informação não é um conceito técnico: é um *slogan*. Melhor se falaria até em sociedade da comunicação, uma vez que o que se pretende impulsionar é a comunicação, e só num sentido muito lato se pode qualificar toda a mensagem como informação.»

[41] POULLET, Yves - *Data protection legislation: What is at stake for our society and democracy? In Computer Law and Security Review* [Em linha]. Vol. 25, n.º 3, (2009), p. 211–226. Amsterdam : Elsevier, 2009. [Consult. 11 jan. 2016]. Disponível em WWW <http://www.sciencedirect.com/science/article/pii/S0267364909000612>

[42] O exemplo dos atentados terroristas de 11/09/ 2011, em Nova Iorque, de 11/03/2004, em Madrid, 07/07/2005 em Londres, de 13/11/ 2015 em Paris, do massacre de Charlie Hebdo e das guerras no Afeganistão e no Iraque, para além dos esforços de prevenção e repressão do terrorismo internacional, tem impacto direto no direito à proteção dos dados pessoais. O governo dos EUA liderado por George Bush, após o 11/09 desencadeou políticas de vigilância e de mineração de dados pessoais com o objetivo de interpretar o comportamento, eventualmente suspeito, dos seus titulares sem autorização judicial com o fundamento de que se não tivessem nada a esconder não teriam nada a temer nem a sua privacidade e informação pessoais seriam afetadas. O argumento refletia o sentimento de grande parte da população culminando com o *Patriotic Act.* No Reino Unido iniciou-se a instalação de milhares CCTV nas cidades (cf. SOLOVE, Daniel J. - *A Brief History of Information Privacy Law* [Em linha]. *In Proskauer On Privacy, Pli* (07 feb. 2017). *GWU Law School Public Law Research Paper* n.º 215 [Consult. 14 Fev. 2017]. Disponível em WWW: <http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications>). Os cidadãos aceitam o constrangimento dos seus movimentos em troca de maior segurança. Contudo, e conforme leitura do Relatório do Relator Especial sobre a promoção e proteção dos direitos humanos e liberdades fundamentais na luta contra o terrorismo, Martin Scheinin, as

com a assinatura do Tratado de Lisboa.

O fluxo da informação[43] e as novas formas de interação social[44] criam ativos de informação pessoal muito valiosos, para as organizações com ou sem fins lucrativos pelo que as normas jurídicas de proteção terão de ser exequíveis num mundo digital onde é difícil rastrear a violação dos direitos[45] para além de criarem mecanismos de controlo, nomeadamente, através de entidades de supervisão. A UE, para prosseguir a sua missão, protege as pessoas singulares em relação ao tratamento dos seus dados pessoais harmonizando as normas de acordo com as exigências do comércio eletrónico num mercado que se quer cada vez mais unificado.

O debate atual em torno do equilíbrio relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos dados centra-se nos pilares

---

medidas que foram introduzidas de modo excecional alastraram-se a outros países e regiões do mundo. A limitação das garantias dos direitos e impacto negativo na proteção do direito à privacidade e aos dados pessoais levaram o Relator Especial a sugerir as melhores práticas internacionais através de um rigoroso conjunto de garantias legais e meios para considerar a avaliação da necessidade, proporcionalidade, razoabilidade das medidas de segurança contra o terrorismo (v. ORGANIZAÇÃO DAS NAÇÕES UNIDAS - *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin* [Em linha]. A/HRC/13/37, (28/12/2009) [Consult. 9 out. 2015] Disponível em WWW <http://www2. ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf.>, e Security Council resolution 1368 (2001) *Threats to international peace and security caused by terrorist acts* [Em linha]. S/RES/1368, (12/09/2001) [Consult. 9 out. 2015]. Disponível em WWW <http://www.refworld. org/docid/3c4e94557.html>, e CdE, *Guidelines of the Committee of Ministers to Members States on Human Rights and the Fight Against Terrorism adopted by the Committee of Ministers at its 804th meeting*. [Em linha]. (11/07/2002 [Consult. 12 mar. 2015]. Disponível em WWW <http://www.coe.int/t/dlapil/cahdi/Source/ Docs2002/H_2002_ 4E.pdf>),

[43] A internet é uma fonte de dados abertos (v. GT29 - Parecer 3/99 relativo a Informação do sector público e protecção de dados pessoais Contribuição para a consulta iniciada com o Livro Verde da Comissão Europeia intitulado "Informação do sector público: um recurso fundamental para a Europa" COM(1998) 585. [Em linha]. WP 20. Brussels (Belgium), (03/05/1999). [Consult. 14 fev. 2015]. Disponível em WWW<http://ec. europa.eu/justice/data-protection/article-29/documentation/opinion-ecommendation/files/1999/ wp20_en.pdf > e também, Parecer 5/2000 relativo ao uso de listas telefónicas públicas para serviços de pesquisa invertida ou multicritério (Listas invertidas) [Em linha]. 5058/00/ PT/FINAL, WP 33. Brussels (Belgium), (13/07/2000). [Consult. 14 fev. 2015]. Disponível em WWW <http: //ec.europa.eu/justice/data-protection/article-29/ documentation/opinion-recommendation/ files/2000/wp33_en.pdf>) e estando ao alcance de todos podem ser recolhidos sem qualquer interferência (Diretiva 95/46/CE e LPDP) e serem realizadas «todo o tipo de operações de tratamento de dados pessoais de um modo invisível para a pessoa em causa. Por outras palavras, o utilizador da Internet não tem consciência de que os seus dados pessoais foram recolhidos e tratados e de que podem ser usados com objetivos que lhe são desconhecidos. Não tem conhecimento desse facto, nem a liberdade de tomar decisões a esse respeito.» (v. GT29 - Recomendação 1/99 sobre o tratamento invisível e automatizado de dados pessoais na Internet realizado por software e hardware. [Em linha]. 5093/98/PT/final WP 17. Brussels (Belgium), (23/02/1999). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec. europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files /1999/wp17_en.pdf> p. 4.

[44] O IAm altera o modo de vida das pessoas. A necessidade de responder às exigências da vida pessoal e profissional num mundo em constante mudança exige flexibilidade nas rotinas diárias e a residência de cada um convocam a presença dos seus proprietários. As residências tornam-se inteligentes, interativas e passam a ser o centro da vida dos seus proprietários. A residência pessoal passa a suportar diversas funções ao nível da vida pessoal, da segurança, da independência, da aprendizagem e do trabalho; e passa igualmente a ser um novo espaço onde se facilita a comunicação e socialização para o exterior através da internet, como por exemplo viajar, praticar desporto, etc. e em ambiente controlado pela tecnologia (v. FRIEDEWALD, Michael, [et al.] - *Perspectives of ambient intelligence in the home environment* [Em linha]. *In Telematics and Informatics*, Vol. 22, n.º 3 (aug. 2005) p. 221-238. [S.l.] : Elsevier B.V. 2005. [Consult. 18 de jun. 2016]. Disponível em WWW <http://www. sciencedirect.com/science/article/pii/S0736585304000590> ISSN: 0736-5853.).

[45] LANGHEINRICH, cit. 26.

tradicionais da chamada quarta geração[46] da proteção de dados que do ponto de vista dos consumidores está relacionado, sobretudo, com o princípio do tratamento lícito, o princípio da limitação da finalidade e o consentimento livre, específico e informado[47].

2-2.5. Génese do direito à proteção de dados

A origem do direito à proteção de dados está intimamente relacionada com a necessidade de funcionalização do direito à privacidade[48]. O conceito de privacidade[49], tal como o entendemos hoje em dia, tem antecedentes históricos na desagregação da classe burguesa da sociedade feudal e estruturou-se para o reconhecimento de um direito à propriedade solitário e obstaculizar ingerências alheias na esfera íntima[50].

---

[46] A expressão *geração* para demonstrar a evolução histórica dos direitos fundamentais foi utilizada pela primeira vez por Karel Vazak, em 1979 (v. VAZAK, Karel – As Dimensões Internacionais dos Direitos do Homem – manual destinado ao ensino dos direitos do homem nas universidades. Lisboa : Editora Portuguesa de Livros Técnicos e Científicos / UNESCO, 1983.) e mais tarde adotada e consagrada por Noberto Bobbio, em 2004 (v. BOBBIO, Noberto - A Era dos Direitos [Em linha]. 7.ª Reimp. Trad. Carlos Nelson Coutinho, Rio de Janeiro: Elsevier, 2004. Título original L'età dei Diritti. [Consult. 20 ago. 2015]. Disponível em WWW <https:// direitoufma2010.files.wordpress.com/2010/05 /norberto-bobbio-a-era-dos-direitos.pdf> ISBN 10: 85-352-1561-1) No que respeita ao direito fundamental à proteção de dados, Viktor Mayer-Scönberger classificou a sua evolução em quatro gerações: a primeira geração, refletia o controlo da informação recolhida pelas administrações públicas e a sua reutilização através de mecanismos de concessão de autorizações; a segunda geração, a lei deixa de considerar apenas a evolução tecnológica para começar a criar mecanismos para proteger os cidadãos do uso indevido e abusivo por terceiros dos seus dados pessoais, tendo como expoente máximo exemplificativo a lei francesa de proteção de dados pessoais (Informatique et Libertées) de 1978; a terceira geração, preocupou-se em garantir a autodeterminação informativa do titular no processo de tratamento e utilização dos seus dados pessoais; e a quarta geração, no desenvolvimento de instrumentos que elevem o padrão coletivo de proteção, consoante o tipo de dados pessoais e respetivo contexto, hoje exemplificado pelas Diretivas 95/46/CE e 2000/58/CE (MANTELERO, Alessandro - *The Future of Consumer Data Protection in the E.U. Rethinking the Notice and Consent Paradigm in the New Era of Predictive Analytics. In Computer Law and Security Review* [Em linha]. Vol. 30, n.º 6, (dez. 2014), p. 643-660. Amsterdam : Elsevier, 2014. [Consult. 11 jan. 2016]. Disponível em WWW <http://www.sciencedirect. com/science/article/pii/S026736491400154X>).

[47] MANTELERO, cit. 46. p. 645.

[48] DONEDA, Danilo C. Maganhoto - Da privacidade à proteção de dados pessoais. Rio de Janeiro : Renovar, 2006. ISBN 85-7147-562-8.

[49] O direito à reserva da intimidade e familiar na nomenclatura constitucional (art.º 26º, n.º 1 da CRP) ou o direito à reserva sobre a intimidade da vida privada (epígrafe do art.º 80º, do CC) «é um valor relativamente recente, caracterizadamente urbano, e porventura até elitista» (conforme LOPES, Joaquim Seabra - A Proteção da Privacidade e dos Dados Pessoais na Sociedade da Informação: Tendências e Desafios numa Sociedade em Transição. in SILVA, Germano Marques da, coord. - Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa. Lisboa : Universidade Católica, 2002. ISBN 978-972-5400-44-9, p. 780). Parece que a pobreza e a privacidade estão intimamente e inversamente relacionadas (v. BENDICH, Albert M. - *Privacy, Poverty, and the Constitution* [Em linha]. *In California Law Review*, Vol. n.º 54, n.º 2, (1966). [Consult. 12 ago. 2016]. Disponível em WWW <http:// scholarship.law.berkeley. edu/californialawreview/vol48/iss3/1/>).

[50] V. RODOTÀ, Stefano – A vida na sociedade de vigilância, A privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda, Rio de Janeiro : Renovar, 2008. ISBN 978857147-688-2. Existem inúmeras teorias doutrinárias e jurisprudenciais para graduar e para delimitar os domínios da vida que se encontram abrangidos por uma reserva de intimidade. O tribunal constitucional tem recorrido à teoria das três esferas, com origem na doutrina alemã, para decidir sobre as questões relativas ao direito à reserva da vida privada e familiar. A teoria distingue: a esfera íntima que corresponde ao núcleo absolutamente protegido abrangendo informação que não deve estar disponíveis para terceiros; a esfera privada que pode variar de pessoa para pessoa admitindo critérios de proporcionalidade; e a esfera social cujos comportamento são suscetíveis de serem conhecidos pelo público. (v. MEDEIROS, Rui; CORTÊS, António – Artigo 26º (Outros direitos pessoais) In MIRANDA, Jorge;

O direito à privacidade, eminentemente patrimonial[51] e radicado no direito privado[52], foi defendido pela primeira vez por Warren e Brandeis num artigo publicado na HLR intitulado «*The righ to privacy*»[53] que expressam no «*right to be alone – the most comprehensive of rights, and the most valued by a free people*»[54], contra a difusão de notícias pela imprensa. Contudo, seria necessário esperar pela década dos anos sessenta do século XX para que os estudiosos do direito da *common law* definissem os danos[55] e as ameaças de natureza tecnológica[56].

A consagração do direito ao respeito pela vida privada, após ampla discussão internacional e tratamento ilícito da informação que deram origem a atos bárbaros[57] e perseguições[58], em todo o mundo surge no art.º 12º[59], da DUDH[6061], cujo teor foi reiterado no art.º 8º[62], da CEDH[63] e no art.º 17.º[64], do PIDCP [65].

MEDEIROS, Rui, coord. - Constituição Portuguesa Anotada, Tomo I. 2.ª ed., Coimbra : Wolters Kluwer Portugal, 2010. ISBN 978-972-32-1822-0. p. 603-632)

[51] DONEDA, cit. 48.

[52] PINHEIRO, Alexandre Sousa – *Privacy* e Proteção de dados pessoais: a construção dogmática do direito à identidade informacional. Lisboa : Associação Académica da Faculdade de Direito de Lisboa, 2015. 978-612-0002-60-5

[53] CASTRO, cit. 38, p. 17.

[54] O direito a estar só, «ou melhor, o direito a ser-se deixado em paz» (LOPES, cit 49, p. 782). O direito à privacidade conceptualizado por Warren e Brandeis só veio a ser reconhecido numa ação de responsabilidade civil pelo Supremo Tribunal da Geórgia conforme decisão no processo *Pavesich V. New England Life Insurance Co. Et Al*., em 1905 (v. PROSSER, William J. – *Privacy* [Em linha]. *In California Law Review*, Vol. n.º 48, n.º 3, (1960). [Consult. 12 Mar. 2016]. Disponível em WWW <http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1/>.

[55] A conceptualização dos danos e seus aspetos valorativos (v. PROSSER, cit. 54).

[56] A conceptualização do direito à privacidade com base na liberdade de escolha sobre as ações que seriam expostas para terceiros foi elaborada por Alain Westin, em 1969 (v. DONEDA, cit. 48.).

[57] Ocorridos sobretudo durante os regimes totalitários de que se destaca o regime nazi.

[58] Nos Estados Unidos e outros países da América Latina de que mereceu destaque o caso *Urteaga, Facundo Raúl vs. Estado Nacional - Estado Mayor Conjunto de las FF.AA. s/ amparo ley 16.986 - 15/10/1998 - Fallos: 321:2767*, do Supremo Tribunal da Argentina, que concedeu o acesso às informações pessoais do irmão do requerente que desapareceram, presumivelmente, durante a ditadura militar.

[59] «Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei».

[60] Aviso, de 09/03/1978, que autoriza a publicação do texto em inglês e a respetiva tradução em português da Declaração Universal dos Direitos do Homem, adotada e proclamada pela Assembleia Geral na sua Resolução 217A (III) de 10/12/1948.

[61] A IX Conferência Internacional Americana realizada em Bogotá criou a OEA que redigiu o primeiro documento internacional que declarou os direitos humanos: a Declaração Americana dos Direitos e Deveres do Homem aprovada em 1948, pois, a DUDH viria a ser aprovada mais tarde. No decorrer da III Conferência Interamericana Extraordinária, realizada em Buenos Aires, em 1967, a OEA viria a aprovar a CADH, com o nome oficial de Pacto de San José de Costa Rica.

[62] «1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.»

[63] A L n.º 65/78, de 13/10 aprovou, para ratificação, a Convenção Europeia dos Direitos do Homem, entrando

2-2.6. O papel do Conselho da Europa

O Conselho da Europa[66], com sede em Estrasburgo, foi criado a 05/08/1949, no final da II Grande Guerra e tem produzido uma série de instrumentos jurídicos, destacando-se com enorme relevância a CEDH. A fim de assegurar o respeito pelos compromissos, de forma concreta e efetiva[67], que resultam, para as Altas Partes Contratantes, da CEDH e dos seus Protocolos, foi criado o TEDH, o qual funciona a título permanente, conforme art.º 19º da CEDH.

O papel desempenhado pelo CdE e a jurisprudência emanada do TEDH inspiraram decisivamente os órgãos da União Europeia e dos Estados-Membros, na produção legislativa e jurisprudencial para a conceção e princípios do direito à proteção de dados pessoais.

2-2.6.1. O desenvolvimento legislativo

O CdE acreditando que as técnicas desenvolvidas na década de sessenta, tais como as escutas telefónicas, a vigilância dissimulada, o uso ilegítimo de inquéritos estatísticos para obter informações privadas, a publicidade subliminar e propaganda, em certos aspetos do desenvolvimento científico e tecnológico[68], eram uma ameaça para os direitos e liberdades das pessoas e, particular, ao direito à privacidade que é protegida pelo artigo 8º da CEDH, solicitou um estudo ao Comité de Ministros[69].

O estudo apresentado à Assembleia Parlamentar, por Karl Czernetz, referia que as garantias

---

em vigor na ordem jurídica portuguesa a 09/11/1978, com as modificações conforme as disposições dos Protocolos nºs 11 e 14. O nome oficial da Convenção é « Convenção para a proteção dos Direitos do Homem e das liberdades fundamentais». Refira-se, ainda que, o art.º 6º do Tratado da União Europeia estabelece que: «2. A União adere à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Essa adesão não altera as competências da União, tal como definidas nos Tratados. 3. Do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros.»

[64] «1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação. 2. Toda e qualquer pessoa têm direito à proteção da lei contra tais intervenções ou tais atentados.»

[65] Lei n.º 29/78, de 12/06, Aprovou, para ratificação, o Pacto Internacional sobre os Direitos Civis e Políticos com entrada em vigor na ordem jurídica portuguesa a 15/09/1978, que foi adotado e aberto à assinatura, ratificação e adesão pela resolução 2200A (XXI) da Assembleia Geral das Nações Unidas, de 16/12/1966.

[66] O CdE, considerado como a maior e mais antiga organização intergovernamental de caráter político, é constituído por todos os Estados-Membros da UE e 21 países da Europa Centro-Leste. Existe o estatuto de Estado Observador (Estados Unidos da América, Canadá, Santa Sé, Japão, Israel e México) e de Estado Convidado (quando está em fase de apreciação da aceitação da adesão).

[67] A Itália foi condenada por não ter garantido um advogado a um cidadão italiano após uma detenção ilegal na consequência de uma queixa à Comissão Europeia dos Direitos do Homem (Ac. *Artico v. Italy*, do TEDH n.º 6694/74, de 13/05/1980).

[68] Conforme leitura do Parágrafo 3º,da CdE *Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments (16th Sitting)* [Em linha]. (31/01/1968) [Consult. 12 mar. 2015]. Disponível em WWW <http://assembly.coe.int/ nw/xml/XRef/Xref-XML2HTML-en.asp? fileid=14546&lang =en>.

[69] LOPES, cit. 49, p. 780.

para a proteção dos dados pessoais era insuficientes, dando origem à Recomendação 509 (1968) sobre os Direitos do Homem e os desenvolvimentos científicos e tecnológicos modernos, adotada pela Assembleia a 31/01/1968. A partir desta Recomendação foram aprovadas várias Resoluções relativas à proteção de dados cujo caráter não vinculativo levou à preparação da denominada Convenção 108 do Conselho da Europa. A adoção das Resoluções (73) 22[70], a (73) 23[71] e a (74) 29[72] é considerada pela doutrina como início do movimento legislativo europeu[73] e fonte dos princípios ainda hoje vigentes, tais como o da qualidade dos dados e da adoção de medidas de segurança.

Diversos os países, neste contexto, procederam à regulamentação da proteção dos dados pessoais, de quais se destacam: a Alemanha[74], a Suécia[75], os Estados Unidos da América[76] e a

[70] CdE Resolution (73) 22 *of the Committee of Ministers to Members States on the protection of the privacy of individuals Vis-a-vis electronic data banks in the private sector* [Em linha]. (26/09/1973) [Consult. 12 mar. 2015]. Disponível em WWW <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830>.

[71] CdE *Resolution (73) 23 of the Committee of Ministers to Members States on harmonization measures in the field of legal data processing in the Member States of the Council Of Europe* [Em linha]. (26/09/1973) [Consult. 12 mar. 2015]. Disponível em WWW <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?.

[72] CdE *Resolution (74) 29 of the Committee of Ministers to Members States on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector* [Em linha]. (20/09/1974) [Consult. 12 mar. 2015]. Disponível em WWW <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51>.

[73] V. FUSTER, Gloria González - *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham [etc,] : *Springer International Publishing Switzerland*, 2014. (*Law, Governance and Technology Series*, Vol. XVI.) ISBN 978-3-319-05023-2.

[74] O Tribunal Constitucional Alemão, inspirado no *right to be alone*, começou a definir o direito à autodeterminação informativa, ao pronunciar-se sobre as garantias dos titulares quanto ao acesso aos seus dados pessoais e vida privada, a 16/07/1969, conforme decisão a *Mikrozensus-Entscheidung*. Surge, entretanto, a Lei adotada em 07/10/1970, sobre o tratamento e manipulação mecânica de dados na administração pública, no Land de Hessen inspirou a Lei Federal de proteção de dados, de 1977. Contudo estas leis não ofereceram as garantias suficientes aos cidadãos alemães. O Tribunal Constitucional Alemão foi de novo chamado a dirimir um conflito entre o Estado e os cidadãos que consideravam as respostas ao censo (desde situação profissional a práticas religiosas e políticas, bem como mecanismos de denúncia e procedimento contraordenacional para quem não respondesse) violavam a privacidade e o direito à autodeterminação informativa (RUARO, Regina Linden; RODRIGUEZ, Daniel Piñero; FINGER, Brunize - O direito à proteção de dados pessoais e a privacidade [Em linha]. In Revista da Faculdade de Direito – UFPR, n.º 53, Curitiba, 2011. [Consult. 16 set. 2015]. Disponível em WWW <http://revistas.ufpr.br/direito/article/download/30768/19876> ISSN 2236-7284. p. 45-66. A recolha de dados autorizada pela referida lei não oferecia as garantias de acordo com a finalidade do censo nem o anonimato. A Lei de Land de Hessen inspirou, igualmente, a Diretiva nº 95/46/CE ao incorporar dois aspetos originais da mesma: «…(i) a criação de entidades administrativas com competência para fiscalização em sede de proteção de dados, e (ii) o estabelecimento de que os tratamentos de dados pessoais dependiam essencialmente do consentimento ou de disposição legal» (PINHEIRO, cit. 52)

[75] A Lei Sueca de 11/05/1973, de âmbito nacional compreende o tratamento de dados pessoais no setor público e privado e cria uma autoridade nacional de proteção de dados (v. FUSTER, cit. 73).

[76] Nos EUA destacam-se o *Omnibus Crime and Control Act of 1968*, em consequência do caso *Katz v. United States*, 389U.S.347 (1967) onde o requerente alega uma expectativa razoável de privacidade quanto a escutas telefónicas, o *Fair Credit Reporting Act* de 1970 e o *Privacy Act* de 1974, que regulam parcialmente questões relativas à proteção de dados para instituições financeiras e administração pública. O *Privacy Act*, de 31/12/1974, tem como antecedente o Caso Watergate após ter sido demonstrado que qualquer um pode utilizar as novas tecnologias para invadir a privacidade de qualquer um.

França[77] [78]. Contudo, outros países seguiram caminhos diferentes na regulação do processamento de dados como Portugal[79], Espanha[80] e a Áustria[81] que lhe atribuíram dignidade constitucional.

2-2.6.2. O Tribunal Europeu dos Direitos do Homem

O TEDH ajudou à construção dos princípios da proteção de dados pessoais[82] e critérios de interpretação dos conceitos gerais plasmados no texto da CEDH[83], ao pronunciar-se sobre questões relacionadas com a distinção entre tratamento de dados pessoais que afetam a vida privada e os que não afetam a vida privada[84], processamento de dados com certas restrições sobre o segredo de correio e telecomunicações[85], o direito ao acesso a informação pessoal em ficheiros administrativos[86], a interceção de comunicações[87], dados indevidamente processados e armazenados pelos órgãos da Administração Pública em detrimento da pessoa em causa[88], reconhecimento da privacidade das atividades profissionais e comerciais estritamente ligadas

[77] *Loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978*, estabelecendo que os computadores devem servir os cidadãos. A discussão em França começa com a noção de Liberdade informática ou o bom uso da ciências e da tecnologia e não originariamente com a proteção de dados (v. FUSTER, cit. 73).

[78] V. CATE, Fred H. - *The EU Data Protection Directive, Information Privacy, and the Public Interest* [Em linha]. Indiana University Maurer School of Law. Paper 646, (1995) [Consult. 12 nov. 2015]. Disponível em WWW <http://www.repository.law.indiana.edu/facpub/646/>.

[79] Historicamente, Portugal foi o primeiro país a consagrar na Constituição, de 1976, e sucessivas revisões constitucionais, para alargar o âmbito da proteção das pessoas contra o tratamento informático de dados pessoais (V. VENÂNCIO, Pedro Dias - A previsão constitucional da utilização da informática. In Revista de Estudos Politécnicos Vol. 8, (2007), p. 243-264. [Consult. 19 out. 2015]. Disponível em WWW <http://www.scielo.mec.pt/pdf/tek/n8/v5n8a12.pdf>).

[80] O art.º 18.º da Constituição Espanhola, de 27/12/1978, com a seguinte redação: «*1. Se garantiza el derecho al honor, a la intimidad personal yfamiliar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*» (v. *Reino de España. Constitución Española* [Em linha]. *Boletín Oficial del Estado*, n.º 311, (29/12/1978), p. 29313-29424 [Consult. 11 out. 2015]. Disponível em WWW <https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229> e passando a ser reconhecido pela jurisprudência espanhola como um direito fundamental autónomo e independente diferenciando-o de outros nomeadamente do direito à intimidade (v. REINO DE ESPAÑA. *Tribunal Constitucional - Sentencia del Tribunal Constitucional* 292/2000, de 30/11. [Em linha]. *Boletín Oficial del Estado* n.º 4, (04/01/2001), p. 104-118 [Consult. 11 out. 2015]. Disponível em WWW <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332>.

[81] Lei Federal sobre a Proteção de Dados Pessoais de 1978.

[82] CASTRO, cit. 38, p. 71.

[83] O art.º 8º, da CEDH, não tem nenhuma referência expressa ao direito à proteção de dados, apenas garante o «direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência»

[84] Ac. *Pierre Herbecq and the Association Ligue des Droits de l'homme v. Belgium*, do TEDH apensos n.º 32200/96 e 32202/96, de 14/01/1998.

[85] Ac. *Klass and Others v. Germany*, do TEDH n.º 5029/71, de 06/09/1978.

[86] Ac. *Gaskin v. The United Kingdom*, do TEDH, nº 10454/83, de 07/07/1989.

[87] Ac. Malone v. *The United Kingdom*, do TEDH, n.º 8691/79, de 02/08/1984.

[88] Ac. *Leander v. Sweden*, do TEDH nº 9246/81, de 26/03/1987.

às esfera pessoal[89], para além de outras questões relacionadas com a manipulação da informação pessoal que serão citadas ao longo deste texto.

O trabalho desenvolvido pelo TEDH para a construção da proteção dos titulares de dados pessoais contra a recolha e tratamento de dados pessoais de forma injustificada, excessiva e desnecessária[90] teve um enorme impacto nas instituições europeias e nos Estados-Membros, bem como desencadeou várias iniciativas de consciencialização nas grandes multinacionais[91].

2-2.7. A proteção de dados nos instrumentos internacionais

A cooperação entre os Estados para a elaboração de instrumentos sobre o processamento de dados e informações sobre pessoas culminou na concretização de instrumentos internacionais muito relevantes.

A Recomendação do Conselho da OCDE[92] relativa às diretrizes que regem a proteção da privacidade e os fluxos transfronteiriços de dados pessoais, de 23/09/1980 (Diretrizes sobre a Privacidade)[93], teve a anuência dos países-membros para dar resposta às preocupações sobre a manipulação de dados pessoais pelos novos e automatizados meios de processamento de informações e para prosseguir os interesses comuns quanto ao respeito pelos direitos humanos e do mercado livre. As Diretrizes sobre a Privacidade definem conceitos fundamentais, estabelecem os princípios aplicáveis ao tratamento de dados pessoais e garantem a livre circulação de dados com respeito pelos princípios das Diretrizes, aplicáveis ao setor público e privado. Nos anos que se seguiram, a OCDE adotou outras linhas diretrizes para responder ao

---

[89] Ac. *Niemietz v. Germany*, do TEDH, nº 13710/88, de 16/12/1992.

[90] HERT, Paul De; GUTWIRTH; Serge - *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action.* in GUTWIRTH; Serge [et al.] - *Reinventing Data Protection?* [Em linha]. New York [etc.]: Springer Science + Business Media B.V. 2009. [Consult. 10 dez. 2014]. Disponível em WWW <https://link.springer.com/book /10.1007/978-1-4020-9498-9> ISBN 978-1-4020-9498-9. Cap. 1, p. 3-44.

[91] «*This consciousness is reflected by the new activism of the business community. The first into the field was Microsoft, which proposed a Charter for the digital identity. This was followed by a joint initiative by Microsoft, Google, Yahoo! and Vodafone who announced the publishing – by the end of the year – of a Charter for the protection of free speech on the Internet. In July, Microsoft presented its "Privacy Principles" and more recently, Google, having rejected a European Union proposal to block "dangerous" search terms ("bomb", "terrorism", "genocide" and the like), proposed the adoption of a global standard for privacy that would be supervised by a "Global Privacy Counsel" attached to the United Nations. It is apparent and widely recognized that there is an emergent need to protect fundamental rights, especially those concerning the freedom of expression and the protection of personal data. Safeguarding these rights cannot be left to private parties, since they will tend to offer guarantees that suit their interests*». (RODOTÁ, Stefano - *Data Protection as a Fundamental Right.* in GUTWIRTH; Serge; LEENES, Ronald; HERT, Paul De; - *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges* [Em linha]. Dordrecht : Springer Science+Business Media Dordrecht 2014. [Consult. 7 ago. 2016]. Disponível em WWW <http://www. springer.com/la/book/ 9789400775398> ISBN 978-94-007-7540-4. Cap. 3, p. 82.)

[92] A OECD é uma organização internacional, fundada em 1961, composta por 34 países para promover o desenvolvimento económico e comercial a nível mundial.

[93] Foi sujeita a alterações a 11/07/2013. As regras estabelecidas nas Diretrizes sobre a Privacidade não são vinculativas.

mercado digital[94].

Considerando desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de caráter pessoal suscetíveis de tratamento automatizado[95], foi adotada a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28/01/1981[96](2-2.6.1.). As instituições europeias na construção do direito à proteção dos dados pessoais verteram os princípios da Convenção 108, de forma aprimorada e com maior desenvolvimento no que respeita às garantias da sua concretização, na Diretiva 95/46/CE, na Diretiva 2002/58/CE, na Diretiva 2006/24/CE e no Regulamento (CE) n.º 45/2001 (2-2.7.1.).

A Resolução 45/95 da Assembleia-geral das Nações Unidas, relativa às Diretrizes para a regulamentação dos ficheiros informatizados de dados pessoais, adotada na 68 reunião plenária, da Assembleia-geral, a 14/12/1990, indica um conjunto de princípios sobre as garantias mínimas em matéria de proteção de dados (abrangendo os ficheiros informatizados públicos e privados, sem prejuízo de adaptações adequadas aos ficheiros manuais bem como a tomada de providências especiais e facultativas relativas aos ficheiros de pessoas coletivas) que devem estar previstas nas legislações nacionais. As diretrizes devem aplicar-se aos ficheiros de dados de caráter pessoal mantidos por organizações internacionais de caráter intergovernamental, sem prejuízo de algumas adaptações que possam ser necessárias para refletir algumas diferenças eventualmente existentes.

2-2.7.1. A Convenção 108 do Conselho da Europa

A Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, é o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados, tanto para

[94] A título de exemplo destacam-se os seguintes atos: *Guidelines for Cryptography Policy* [Em linha]. (27/03/1997) [Consult. 10 nov. 2015]. Disponível em WWW <http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm>, *Guidelines for Multinational Enterprises* [Em linha]. Ed.ª 2011, OECD Publishing. [Consult. 10 nov. 2015]. Disponível em WWW <http://www.oecd.org/daf/inv/mne/48004323.pdf>. ISBN ISBN 978-92-64-11528-6, *Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam* [Em linha]. (13/04/2006) [Consult. 10 nov. 2015]. Disponível em WWW <http://www.oecd.org/fr/sti/ieconomie/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm> e *Consumer Protection in E-commerce* [Em linha]. OECD Publishing, 2016 [Consult. 18 ago. 2015]. Disponível em WWW <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.

[95] Preâmbulo da Convenção 108.

[96] A Convenção 108, entrou em vigor na ordem jurídica portuguesa no dia 01/01/1994. Portugal aceitou a emenda introduzida a esta Convenção a 15/07/1999, que permite a adesão das Comunidades Europeias à Convenção. Entrou em vigor na ordem jurídica internacional no dia 01/01/1985, após ter sido ratificada por 5 países signatários.

o setor público como para o setor privado (art.º 3º, n.º 1, da Convenção 108), abrangendo os tratamentos de dados realizados pelas autoridades policiais e judiciárias. A Convenção 108 estabelece os princípios que devem ser obedecidos na recolha e no tratamento de dados de forma leal e lícita, registados para finalidades determinadas e legítimas, não podendo ser utilizados de modo incompatível com essas finalidades, adequados, pertinentes e não excessivos em relação às finalidades para as quais foram registados, exatos e conservados de forma que permitam a identificação das pessoas a que respeitam por um período que não exceda o tempo necessário às finalidades determinantes do seu registo (art.º 5º, da Convenção 108). A 08/11/2001 foi aberto à assinatura o Protocolo Adicional nº 1[97], que estabelece disposições sobre fluxos transfronteiriços de dados para Estados não signatários, os chamados países terceiros, e sobre a criação obrigatória de autoridades nacionais de controlo de proteção de dados, considerando que com o aumento do intercâmbio de dados pessoais através das fronteiras nacionais, é necessário garantir a proteção efetiva dos direitos humanos e das liberdades fundamentais, nomeadamente o direito à privacidade em relação a esses intercâmbios de dados pessoais (Paragrafo 4º do Preâmbulo do Protocolo Adicional nº 1).

O CdE emitiu, ainda, algumas recomendações dirigidas a diversos setores de atividade das quais destacamos a proteção de dados pessoais no marketing direto[98] e a definição de perfis em tratamento de dados pessoais[99].

2-2.8. O papel da União Europeia

A Comissão considerando a preocupação com o domínio das empresas americanas no mercado europeu dos computadores e processamento de dados, publicou uma comunicação ao Conselho, sobre a política comunitária no processamento de dados e a necessidade de adotar «medidas comuns para a proteção do cidadão»[100]. O debate foi aberto e após a apresentação de vários estudos, dos quais se destacam o Relatório elaborado pelo Lord Mansfield, em 1975,

[97] O DPR n.º 56/2006, de 20/06, Ratifica o Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, aberto à assinatura em Estrasburgo, em 08/11/2001 aprovado, para ratificação, pela RAR n.º 45/2006, de 20/06 de Junho, entrando em vigor na ordem jurídica portuguesa a 25/06/2006.

[98] V. CdE *Recommendation n.º R(85) 20 on the protection of personal data used for the purposes of direct marketing* [Em linha]. (25/10/1985) [Consult. 14 mar. 2015]. Disponível em WWW <https://search.coe.int/cm/ Pages/ result_details.aspx?ObjectID=09000016804bd336>

[99] V. CdE *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling* [Em linha]. (23/07/2010) [Consult. 12 mar. 2015]. Disponível em WWW <https://search.coe.int/cm/Pages/result_details. aspx?ObjectID=09000016805cdd00>.

[100] COMISSÃO EUROPEIA - *Community policy on data processing. Communication of the Commission to the Council.* [Em linha]. SEC (73) 4300 final, (21/11/1973) [Consult. 10 Dez. 2015]. Disponível em WWW <http://aei.pitt.edu/ view/eudocno/SEC_=2873=29_4300_final.html>

solicitado pela Comissão dos Assuntos Jurídicos[101], e o Relatório elaborado por Bayerl, em 1979[102], o Parlamento Europeu aprovou uma resolução sobre a proteção dos direitos do indivíduo em face do desenvolvimento do progresso técnico na área de processamento automático de dados (JOCE, C140/34, de 05/06/1979), recomendando a adoção de uma diretiva[103].

Considerando a Comissão que a Convenção 108 é adequada para introduzir à escala europeia um nível uniforme em matéria de proteção de dados, emite a Recomendação n.º 81/679/CEE de 29/07/1981, para que todos os Estados-Membros da Comunidade que assinem, durante o ano de 1981, e que ratifiquem, antes do final do ano de 1982, se ainda não o tiverem feito. Gorados todos os esforços, a Comissão apresenta diversas iniciativas, e em 27/07/1990 a Proposta de Diretiva do Conselho relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais[104], que viria a sofrer alterações e importantes contributos.

À margem do quadro institucional das Comunidades Europeias e no âmbito da cooperação intergovernamental de um número limitado de países[105], foi criado o Espaço Schengen, em 1985, para a supressão gradual dos controlos nas fronteiras comuns. O Acordo foi complementado, em 1990, pela Convenção de Aplicação do Acordo de Schengen[106], que estabeleceu os termos da supressão definitiva dos controlos nas fronteiras interna e medidas de implementação. A Convenção veio reforçar os controlos nas fronteiras externas, definir procedimentos para a emissão de vistos uniformes, criar o Sistema de Informação Schengen (SIS), intensificar a cooperação policial nas fronteiras internas e melhorar a luta contra

---

[101] V. PARLAMENTO EUROPEU - *Interim Report drawn on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing (Rapporteur: Lord Mansfield)* [Em linha]. *Working Documents* 1974-1975, Document 487/74, PE 39.608/fin, (19.feb.1975), p. 14. [Consult. 16 ago. 2016]. Disponível em WWW < http://aei.pitt.edu/ 65083/ 1/WD3126. pdf>.

[102] *Report drawn up on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of technical developments in data processing* (Rapporteur: Mr A. Bayerl) [Em linha]. *Working Documents 1979-1980, Document* 100/79 (04.may.1975), p. 3. [Consult. 16 ago. 2016]. Disponível em WWW <http://aei.pitt.edu/view/eusubjects/ H019.html>.

[103] V. FUSTER, cit. 73.

[104] Publicada no JOCE n.º C-277/3, de 05/11/1990.

[105] Alemanha, Bélgica, França, Países Baixos e Luxemburgo. Atualmente são signatários 30 países, incluindo todos os Estados-Membros da UE e três países que não são membros da UE (Islândia, Noruega e Suíça), Liechtenstein, Bulgária, Roménia e Chipre estão em fase de implementação do acordo. Alguns territórios dos Estados-Membros da EU signatários não estão abrangidos (por exemplo, no Reino Unido, Grécia, Itália, Alemanha).

[106] Foram aprovados para adesão pela RAR n.º 35/93, de 25/11 e ratificados pelo DPR n.º 55/93, de 25/11, entrando em vigor na ordem jurídica portuguesa a 01/03/1994, conforme a Declaração Comum Relativa ao art.º 139º da Convenção de Aplicação do Acordo de Schengen, contudo as disposições que não sejam relativas à criação, às atividades e à competência do Comité Executivo só serão aplicáveis a partir de 26/03/1995. Algumas disposições, nomeadamente as relacionadas com o mandato de detenção europeu e aos processos de entrega dos Estados-Membros do Protocolo de Adesão e o Acordo de Adesão foram sujeitas a alterações. Na L n.º 2/94, de 19/02, foram estabelecidos os mecanismos de controlo e fiscalização do Sistema de Informação Schengen.

condutas criminosas. A Convenção de Aplicação do Acordo de Schengen dedica o capítulo III à proteção dos dados pessoais e segurança de dados no âmbito do SIS, o que se traduziu num grande avanço para o reconhecimento do direito à proteção de dados pessoais.

2-2.8.1. O desenvolvimento legislativo na União Europeia

O Tratado de Maastricht[107], assinado em 07/02/1992 e com entrada em vigor a 01/11/1993, alterou os tratados europeus e instituiu a UE assente em três pilares as Comunidades Europeias (no âmbito das quais eram exercidas pelas instituições comunitárias as competências que eram objeto de transferência de soberania pelos Estados-Membros nos domínios visados pelo Tratado), a política externa e de segurança comum (PESC - regida pelas disposições do Título V do TUE) e a cooperação nos domínios da justiça e dos assuntos internos (JAI – conforme Título VI do Tratado), com o objetivo, entre outros, de preparar a união monetária. A união monetária dependia da instauração de um mercado interno onde era assegurada a livre circulação de mercadorias, pessoas, serviços e capitais que incluía a livre circulação de dados pessoais de um Estado para outro.

A Comissão consciente das diferenças dos sistemas jurídicos dos Estados-Membros da EU, dos obstáculos ao fluxo de dados transfronteiriços e das questões relacionadas com o processamento de dados pessoais tanto no setor privado como no setor público, prossegue a promoção da investigação e do estudo para a harmonização da proteção do processamento de dados e de um direito à proteção de dados. Por outro lado, o novo contexto político, delineado pelo Tratado de Maastricht, conjugado com o contexto tecnológico e os novos modelos de negócio obrigam as instituições europeias a tomar posição e a desencadear processos legislativos que se traduziram na publicação de vários atos normativos: a Diretiva 95/46/CE[108]/[109], Diretiva 97/7/CE[110], a Diretiva 97/66/CE[111], a Diretiva 2000/31/CE[112], a

[107] O Tratado de Maastricht foi alterado pelos: Tratado de Amesterdão (1997), Tratado de Nice (2001) e Lisboa (2009). Este Tratado foi igualmente alterado pelos seguintes Tratados de Adesão: Tratado de Adesão da Áustria, Finlândia e Suécia (1994), Tratado de Adesão de Chipre, da Eslováquia, da Eslovénia, da Estónia, da Letónia, da Lituânia, da Hungria, de Malta, da Polónia e da República Checa (2003), Tratado de Adesão da República da Bulgária e da Roménia (2005).

[108] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24/10/1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, com entrada em vigor em 13/12/1995, foi revogada pelo n.º 1 do art.º 94º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27/04/2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), apenas com efeitos a partir de 25/05/2018.

[109] «… tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais … A aproximação das legislações nacionais aplicáveis na matéria não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na União. Assim, … a harmonização das referidas legislações nacionais não se limita a uma harmonização mínima, mas conduz a uma harmonização que é, em princípio,

Diretiva 2002/58/CE[113], a Diretiva 2006/24/CE[114], a Decisão-Quadro 2008/977/JAI do Conselho[115] e o Regulamento (UE) n.º 611/2013[116].

Considerando que a Diretiva 95/46 CE parecia interpretar a noção de «livre circulação» como elemento mercado interno (proibindo os obstáculos à livre circulação de dados entre os Estados-Membros), no contexto do artigo 286º, do Tratado de Amesterdão[117], era necessário fixar o sentido do fluxo de dados entre as instituições e organismos comunitários, concretizado no Regulamento (CE) n.º 45/2001[118]. Por outro lado, a Comissão pode

---

completa», conforme Ac. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, do TJUE, apensos n.ºs C-468/10 e C-469/10, de 24/11/2011.

[110] Diretiva 97/7/CE do Parlamento Europeu e do Conselho, de 20/05/1997, relativa à proteção dos consumidores em matéria de contratos à distância, com entrada em vigor em 04/06/1997, foi revogada, com efeitos a partir de 13/06/2014, pela Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de Outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva 93/13/CEE do Conselho e a Diretiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Diretiva 85/577/CEE do Conselho e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho.

[111] Diretiva 97/66/CE do Parlamento Europeu e do Conselho, de 15/12/1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, com entrada em vigor em 19/02/1999, foi revogada com efeitos a partir de 31/10/2003, pela Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12/07/2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações (Diretiva relativa à privacidade e às comunicações eletrónicas).

[112] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico»), com entrada em vigor a 17/07/2000, foi alterada pela Diretiva 2009/22/CE do Parlamento Europeu e do Conselho, de 23/04/2009, relativa às ações inibitórias em matéria de proteção dos interesses dos consumidores (Versão codificada).

[113] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12/07/2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), com entrada em vigor em 31/07/2002, foi alterada pelas Diretivas 2006/24/CE de 15/03 e 2009/136/CE, de 25/11.

[114] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15/03/2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12/07/2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações (Diretiva relativa à privacidade e às comunicações eletrónicas), com entrada em vigor em 03/05/2006, foi declarada inválida pelo Ac. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources e Kärntner Landesregierung* e outros, do TJUE n.º C 293/12 e C 594/12, de 08/04/2014. A declaração de invalidade com fundamento de que a obrigação de conservação de dados gerados nas comunicações eletrónicas, como os dados de tráfego, localização ou de identificação dos utilizadores, era uma ingerência grave na vida privada, conforme os direitos garantidos pela Carta dos Direitos Fundamentais da União Europeia.

[115] Decisão-Quadro 2008/977/JAI do Conselho, de 27/11/2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, com entrado em vigor 19/01/2009 foi revogada, com efeitos a partir de 06/05/2018, pelo n.º 1 do artigo 59.º da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27/04/2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

[116] O Regulamento (UE) n.º 611/2013 da Comissão, de 24/06/2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas, com entrada em vigor a 25/08/2013.

[117] O Tratado de Amesterdão, que modificou o Tratado da União Europeia e os Tratados que instituem as Comunidades Europeias e certos atos afins, foi assinado em Amesterdão, em 02/10/1997, e entrou em vigor em 01/05/1999.

[118] Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18/12/2000, relativo à proteção das

considerar que um país terceiro em causa assegura um nível de proteção adequado dos direitos das pessoas singulares por força do seu direito interno, ou de compromissos internacionais que assumiu, não se aplicando nesse caso as limitações específicas sobre as transferências de dados para esse país (art.º 25º, n.º 6, da Diretiva 95/46 CE). A Comissão adotou diversas decisões de adequação, destacando-se a Decisão 520/2000/CE, de 26/07/2000 (designada por Decisão Porto Seguro) que regula as transferências de dados pessoais da UE para as empresas sedeadas nos EUA que tenham subscrito os princípios de privacidade do sistema «porto seguro», que se baseia em compromissos, bem como na autocertificação das empresas participantes. As regras são vinculativas aos assinantes que aceitem voluntariamente os acordos. A declaração de invalidade da Decisão 520/2000/CE, pelo TJUE[119], deu origem à Decisão de Execução (UE) 2016/1250[120] (2-2.9.).

2-2.8.2. A Carta dos Direitos Fundamentais da União Europeia

A CDFUE foi assinada e proclamada pelos presidentes do Parlamento Europeu, pelo Conselho da União Europeia e pela Comissão Europeia, em 07/12/2000, em Niza e incorpora os princípios da CEDH e os critérios jurisprudenciais do TEDH e do TJUE[121]. A segunda versão alterada da CDFUE foi proclamada a 12/12/2007, em Estrasburgo[122]. A CDFUE incorpora num único documento os direitos civis, políticos, económico e sociais dos cidadãos europeus e está dividida em seis secções: dignidade, liberdades, igualdade, solidariedade, cidadania e justiça. A CDFUE consagra explicitamente o direito à proteção de dados pessoais[123] como um direito fundamental, com caráter autónomo (art.º 8, nº 1, da CDFUE),

---

pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, com entrada em vigor em 01/02/2002.

[119] A Decisão 520/2000/CE foi retificada a 15/08/2000 e mais tarde declarada inválida pelo Ac. *Maximillian Schrems v. Data Protection Commissioner*, do TJUE n.º C-362/14, de 06/10/2015, na medida em que não existe uma lei geral sobre proteção de dados nos EUA, ou outras medidas de igual natureza que demonstrem que os EUA oferecem um nível adequado de proteção, semelhante à EU bem como as autoridades de aplicação da lei dos EUA não estão vinculadas aos seus princípios, podendo aceder aos dados sem qualquer fundamento legal ou garantias aos cidadãos europeus, para além de serem objeto de tratamentos incompatíveis e desproporcionais por parte destas autoridades.

[120] Decisão de Execução (UE) 2016/1250, da Comissão, de 12/07/2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

[121] A CDFUE refere-se, a este propósito, aos direitos que decorrem «das tradições constitucionais e das obrigações internacionais comuns aos Estados-Membros, do Tratado da União Europeia e dos Tratados comunitários, da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, das Cartas sociais aprovadas pela Comunidade e pelo Conselho da Europa, bem como da jurisprudência do Tribunal de Justiça das Comunidades Europeias e do Tribunal Europeu dos Direitos do Homem».

[122] A segunda versão da CDFUE foi assinada por Hans-Gert Pöttering, José Sócrates e José Manuel Durão Barroso, respetivamente, todos ex-presidentes do Parlamento Europeu, do Conselho da União Europeia e da Comissão Europeia.

[123] «Art.º 8.º Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal

indicando os princípios e regras a que fica sujeito (art.º 8, nº 2, da CDFUE), assegurando o seu cumprimento por uma autoridade independente (art.º 8, nº 3, da CDFUE).

Com a entrada em vigor do Tratado de Lisboa, em 01/12/2009, a CDFUE tem a mesma natureza vinculante dos tratados, ou seja direito primário, conforme declarado expressamente no art.º 6º do TUE[124] e reforçado pelo art.º 16º do TFUE[125] que atribui competências genéricas às instituições da EU para legislar sobre matérias relacionadas com a proteção de dados, sem distinguir entre matérias de direito civil, comercial e penal (com exceção para o Reino Unido e a Irlanda, nos termos do art.º 6-A, do Protocolo 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça).

Nos termos do art.º 51º, da CDFUE[126] aplica-se às instituições, órgãos e organismos da União, na observância do princípio da subsidiariedade, bem como aos Estados-Membros, ou seja aos seus atos legislativos e não legislativos, apenas podendo ser limitados por lei observando o princípio da proporcionalidade, se forem necessário e corresponderem efetivamente a objetivo de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros (art.º 52º, da CDFUE) [127].

---

que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.»

[124] Art.º 6º, do TUE: «1. A União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, em Estrasburgo, e que tem o mesmo valor jurídico que os Tratados. De forma alguma o disposto na Carta pode alargar as competências da União, tal como definidas nos Tratados. Os direitos, as liberdades e os princípios consagrados na Carta devem ser interpretados de acordo com as disposições gerais constantes do Título VII da Carta que regem a sua interpretação e aplicação e tendo na devida conta as anotações a que a Carta faz referência, que indicam as fontes dessas disposições. 2. A União adere à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Essa adesão não altera as competências da União, tal como definidas nos Tratados. 3. Do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros.»

[125] Art.º 16º do TFUE: «1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.º do Tratado da União Europeia.»

[126] O art.ºs 51º, da CDFUE, incorpora a jurisprudência que o TJUE vinha consolidando, em diverso acórdãos sobre a competência e dos quais se destacam: Ac. *Gestoras Pro Amnistía, Juan Mari Olano Olano e Julen Zelarain Errasti* v. Conselho da União Europeia, do TJUE nº C-354/04, de 27/02/2007 (parágrafo 51), Ac. *Segi, Araitz Zubimendi Izaga e Aritza Galarraga* v. Conselho da União Europeia, do TJUE, nº C-355/04, de 27/02/2007 (parágrafo 51), e Ac. *Advocaten voor de Wereld VZW v. Leden van de Ministerraad*, do TJUE n.º C-303/05, de 03/05/2007 (parágrafo 45).

[127] Quanto ao reconhecimento dos limites fundamentais indica-se, a título de exemplo, alguns acórdãos tanto do TJUE como do TEDH: Ac. J. *Nold Kohlen v*. Comissão das Comunidades Europeias, do TJUE, nº 4/73 de 14/05/1974 (parcialmente publicado), Ac. *Kjell Karlsson* e o., do TJUE n.º C-292/97, de 13/04/2000 e Ac.

2-2.8.3. O Tribunal de Justiça da União Europeia

O Tratado constitutivo das Comunidades Europeias não continham referências explícitas aos direitos fundamentais[128], pelo que o Tribunal de Justiça[129] segundo o art.º 31° do Tratado, considerava que só tinha que garantir o respeito do direito na interpretação e aplicação do Tratado e dos regulamentos de execução[130]. Contudo, «uma nova ordem de direito internacional»[131] foi iniciada e o Tribunal de Justiça ao reconhecer o direito comunitário, independente com precedência sobre a legislação dos Estados-Membros, tal como impõe obrigações aos particulares e lhes atribui direitos que entram na sua esfera jurídica[132]. A observância dos direitos fundamentais passa a ser garantida pelo Tribunal de Justiça que inspirado nas tradições constitucionais comuns aos Estados-Membros e nos instrumentos internacionais relativos à proteção dos direitos do homem, em que os Estados-Membros colaboraram ou a que aderiram[133] e não podendo haver medidas incompatíveis com o respeito pelos direitos fundamentais[134]. O TJUE começa a consolidar a doutrina no que diz respeito ao direito à vida privada[135] e amplia o controlo da conformidade da atuação das instituições comunitárias e dos seus Estados-Membros com o pedido de adesão formal da EU à CEDH[136]. O TEDH exerce, ainda que indiretamente, e como última instância o controlo das decisões do TJUE[137]. O TEDH tem proferido as suas decisões no sentido de que a jurisprudência de

---

Roquette Frères SA v. Directeur général de la concurrence, de la consommation et de la répression des fraude e Comissão das Comunidades Europeias, do TJUE, n.º C-94/00, de 22/10/2002, Ac *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy e Satamedia Oy*, do TJUE, nº C-73/07, de 16/12/2008 (parágrafos n.ºs 56, 61 e 62). Ac. *Mosley c. United Kingdom*, do TEDH, n.º 48009/08, de 10/05/2011 (parágrafos n.ºs 129 e 130), Ac. *Axel Springer AG v. Germany*, TEDH n.º 39954/08, de 07/02/2012 (Parágrafos n.ºs 90 e 91) e Ac. *Von Hannover v. Germany* (n.º 2) , do TEDH apensos n.ºs 40660/08 e 60641/08, de 07/02/2012 (Parágrafos n.ºs 118 e 124).

[128] V. FUSTER, cit. 73.

[129] O Tribunal de Justiça da União Europeia teve origem na instituição tímida prevista no Tratado de Paris (1951) que institui a Comunidade Europeia do Carvão e do Aço com papel reforçado no Tratado de Roma (1957) que instituiu a CEE e Euratom. Com a entrada em vigor do Tratado de Lisboa, o seu nome mudou de Tribunal de Justiça das Comunidades Europeias para Tribunal de Justiça da União Europeia. Desde 1989, existe uma arquitetura nova: a instituição é composta por dois órgãos o Tribunal de Justiça e o Tribunal Geral.

[130] Ac. *Friedrich Stork & Co*. v. Alta Autoridade da CECA, do TJUE n.º 1/58, de 04/02/1959 (parcialmente publicado).

[131] Ac. *Gend & Loos* v. Administração Fiscal, do TJUE, nº 26/62, de 05/02/1963 (parcialmente publicado).

[132] Ac. Costa v. ENEL, do TJUE, nº 6/64, de 15/07/1964 (parcialmente publicado).

[133] Ac. *Erich Stauder* v. Cidade de Ulm, do TJUE nº 29/69 de 12/11/1969 (parcialmente publicado) e Ac. J. *Nold Kohlen* v. Comissão das Comunidades Europeias, do TJUE, nº 4/73 de 14/05/1974 (parcialmente publicado).

[134] Ac. *Hubert Wachauf* v. República Federal da Alemanha, do TJUE, nº 5/88, de 13/07/1989 (parcialmente publicado).

[135] Parágrafos 17 e 23, do Ac. X v Comissão das Comunidades Europeias, do TJUE nº C-404/92, de 08/04/1992.

[136] Par. n.º 2/13, do TJUE, de 18/12/2014, emitido a pedido da Comissão Europeia, nos termos do art.º 218.°, n.º 11, TFUE, considerou que o projeto de acordo de adesão da EU à CEDH não é compatível com o art.º 6º, n.º 2, do TUE nem com o Protocolo (n.º 8) relativo à mesma disposição. Atualmente a EU e o CdE mantêm as negociações para a respetiva adesão.

[137] SOLÍS, David Ordóñez - *Privacidad y protección judicial de los datos personales*. 1.ª ed., Barcelona : Bosch, 2011. ISBN 978-84-9790-853-5.

ambos os tribunais é complementar[138] dado que a CEDH não exclui a transferência de competências para as organizações internacionais, sempre que os direitos garantidos continuem a ser reconhecidos porque a referida transferência não isenta a responsabilidade dos Estados-Membros[139] [140] e a proteção equivalente deve ser apreciada perante o interesse de cooperação internacional assumindo a CEDH o papel de um «instrumento constitucional da ordem pública europeia» no campo dos direitos humanos[141]. Mas só a partir da publicação das Diretivas supra referidas é que o Tribunal de Justiça começaria a resolver questões relacionadas com a interpretação, aplicação e cumprimento das disposições que regulam a proteção dos dados pessoais[142].

O TJUE começa por reconhecer o direito de acesso à identidade de um destinatário de bens para garantir o direito à defesa de determinados interesses perante os tribunais, desde que a sua utilização seja limitada e proporcional ao fim para o qual foram cedidos[143] ou tenha sido prestado o consentimento, como elemento essencial, para o tratamento de dados pessoais[144].

O TJUE proferiu acórdãos paradigmáticos na construção doutrinária do direito à proteção de dados pessoais e da privacidade na Internet[145], da proteção da vida privada e a divulgação de dados sobre os rendimentos de assalariados de determinadas entidades[146], do tratamento e circulação de dados pessoais de caráter fiscal[147], do tratamento e a transferência de dados contidos nos registos de identificação dos passageiros transferidos para o Serviço das Alfândegas e de Proteção das Fronteiras dos EUA[148], do tratamento geral de dados pessoais

---

[138] SOLÍS, cit. 137.

[139] Parágrafos 32 e 33, do Ac. *Matthews v. United Kingdom*, do TEDH n.º 24833/1994, de 18/02/1999 e Parágrafos 37 e 38 *Bernard Connolly* v. Comissão das Comunidades Europeias, do TJUE nº C-274/99, de 06/03/2001.

[140] V. CABALLERO, Susana Sanz - *Interferencias entre el Derecho Comunitario y el Convenio Europeo De Derechos Humanos (Luxemburgo versus Estrasburgo: ¿quién es la última instancia de los derechos fundamentales en Europa?). In Revista de Derecho Comunitario Europeo* [Em linha]. Año 8. n.º 17. (enero-abril 2004) p. 117-160. [Consult. 12 nov. 20165]. Disponível em WWW <https://dialnet.unirioja.es/ejemplar/93104> ISSN: 1989-5569.

[141] Parágrafos 154 a 156 e 165, do Ac. *Bosphorus v. Ireland*, do TEDH n.º 45036/98 de 24833/1994, de 30/06/2005.

[142] TAMM, Ditlev - *The History of the Court of Justice of the European Union Since its Origin* [Em linha]. *In Court of Justice of the European Union, Coord. - The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law*. 1ª ed. Hague : Springer, 2013. [Consult. 16 out. 2015]. Disponível em WWW <http://www.springer. com/la/book/9789067048965>. ISBN 978-90-6704-897-2. p. 9-35.

[143] AC. Adidas, do TJUE, nº C-223/98, de 14/10/1999 e Ac. Reino dos Países Baixos e *Gerard van der Wal* v. Comissão das Comunidades Europeias, do TJUE n.º C-174 e C-198/98 de 11/01/2000.

[144] Ac. Reino dos Países Baixos v Parlamento Europeu e Conselho da União Europeia do TJUE, nº C-377/98 de 09/10/2001.

[145] Ac. *Bodil Lindqvist*, do TJUE, nº C-101/01, de 06/11/2003.

[146] Ac. *Rechnungshof v. Österreichischer Rundfunk* e outros, do TJUE apensos n.ºs C-465/00, C-138/01 e C-139/01, de 20/05/2003.

[147] Ac *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy e Satamedia Oy*, do TJUE, nº C-73/07, de 16/12/2008.

[148] Ac. *Passenger Name Records*, do TJUE, apensos n.ºs C-465/00, C-138/01 e C-139/01, de 30/05/2006.

respeitantes a cidadãos nacionais de outro Estado-Membro[149], da publicação de dados de beneficiários de ajudas[150], do direito de acesso e à informação sobre os destinatários dos dados e prazo do seu exercício[151], da conservação e divulgação de determinados dados de tráfego[152], do consentimento dos titulares para a inclusão dos seus dados pessoais em lista acessível ao público em geral[153] ou que haja um interesse legítimo no seu tratamento[154].

2-2.9. A reforma da proteção de dados na União Europeia

A Comissão, em 25/01/2012, apresentou um pacote legislativo com fim de proceder à reforma da legislação relativa à proteção de dados da EU, que tinha sido concebida para um determinado contexto atualmente inexistente. A rápida evolução tecnológica e a globalização alteraram profundamente a forma como os dados são recolhidos, acessíveis e utilizados (Considerando 6, do RGPD). Esta evolução exige um quadro de proteção de dados mais sólido e coerente na União, de forma a superar a atual fragmentação no que respeita à aplicação e transposição da Diretiva 95/46/CE (Considerando 7 e 8, do RGPD). A reforma visa salvaguardar os dados pessoais na EU, harmonizando as diferentes leis em vigor em toda a UE, aumentando o controlo dos utilizadores sobre os seus próprios dados (Considerando 7, do RGPD) e reduzindo os custos e simplificando regras para as empresas no mercado único digital. Foram publicados os seguintes atos normativos em 27/04/2016, com entrada em vigor em 24/05/2016, mas cujos efeitos se produzem a partir do dia 25/05/2018:

a) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27/04/2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).
b) Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27/04/2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que

[149] Ac. *Heinz Huber v. Bundesrepublik Deutschland*, do TJUE, n.º C-524/06, de 16/12/2008.
[150] Ac. *Volker und Markus Schecke GbR e Hartmut Eifert v. Land Hessen*, do TJUE, apensos n.ºs C-92/09 e C-93/09, de 09/11/2010.
[151] Ac. *College van Burgemeester en Wethouders van Rotterdam v. M. E. E. Rijkeboer*, do TJUE, n.º C-553/07, de 07/05/2009.
[152] Ac. *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, TJUE, n.º C-275/06, de 29/01/2008.
[153] Ac. *Deutsche Telekom AG v. Bundesrepublik Deutschland*, do TJUE, nº C-543/09, de 05/05/2011.
[154] Ac. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, do TJUE, apensos n.ºs C-468/10 e C-469/10, de 24/11/2011.

revoga a Decisão-Quadro 2008/977/JAI do Conselho.

c) Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27/04/2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

Os atos normativos são muito extensos e de grande complexidade técnica pelo que exige aos Estados-Membros um grande esforço de adaptação ao novo paradigma da proteção de dados ao nível da formação e da reflexão. Para além da revisão de alguns conceitos foram introduzidos outros: introdução de um conceito de violação de dados pessoais[155], o tratamento desenvolvido da pseudonimização[156], o direito a ser esquecido[157], direito à portabilidade dos dados[158], princípios de proteção de dados desde a conceção e por defeito[159], avaliações de impacto sobre proteção de dados[160], o encarregado de proteção de dados[161], o mecanismo de balcão único[162] e a medida das sanções previstas[163].

Para além das medidas supra referidas, a Comissão negociou um importante acordo sobre a proteção de dados com os EUA com o objetivo de proteger os dados pessoais dos cidadãos europeus transferidos entre a EU e os EUA, consubstanciado na Decisão de Execução (UE) 2016/1250 da Comissão de 12/07/2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

O «Escudo de Proteção da Privacidade UE-EUA baseia-se num sistema de autocertificação através do qual as organizações dos EUA assumem o compromisso de estabelecer um conjunto de princípios de privacidade — os princípios do quadro do Escudo de Proteção da Privacidade UE-EUA, incluindo os princípios suplementares (em seguida designados em conjunto «os princípios») — emitidos pelo *Department of Commerce* dos EUA e constantes do anexo II da presente decisão. É aplicável simultaneamente aos responsáveis pelo tratamento e aos subcontratantes (agentes), com a especificidade de que os subcontratantes devem ser contratualmente obrigados a agir apenas mediante instruções do responsável

[155] Considerandos 73, 85 a 88, art.ºs 33º e 34º, do RGPD.
[156] Considerando 28, art.ºs 4, nº 5, 25º, 32º, n.º 1, a), e 40º, do RGPD.
[157] Considerandos 65, 66 e 156, e art.º 17º do RGPD.
[158] Considerandos 68, 73, 156, art.ºs 13º, n.º 2, al) b) e c) e 20º, do RGPD.
[159] Considerandos 78 e 108, art.ºs 25º e 47º, nº 2, al) d), do RGPD.
[160] Considerandos 77, 84, 89 a 94, art.ºs 35º, 36º, 57º, nº 1, al) e 67º, nº 1, al) a) do RGPD.
[161] Considerandos 77 e 97, art.ºs 13, n.º 1, al) b), 30º, n.º 1, al) a) e n.º 2, al) a), 33º, n.º 3, al) b), 35º, n.º 2, 36, n.º 3, al) d), 37º a 39º, 47º, nº 2, al) h) e 57º, n.º 3, do RGPD.
[162] Considerandos 127 e 128, do RGPD.
[163] Considerandos 11, 13, 19, 73, 148 a 150, 152 e art.º 84º, do RGPD.

europeu pelo tratamento e ajudar este último a responder aos pedidos das pessoas que exercem os seus direitos por força destes princípios»[164].

[164] Considerando 14, da Decisão de Execução (UE) 2016/1250.

CAPÍTULO III – O DIREITO À PROTEÇÃO DE DADOS NO CONTEXTO NACIONAL

2-3. A evolução da lei nacional

O primeiro diploma a garantir o acesso à informação pessoal foi publicado a 07/11/1872 e cujo decreto cria o registo criminal dada a importância do «conhecimento da capacidade e grau de confiança que podem inspirar os indivíduos com quem se contrata ou a quem se confiam valiosos interesses», no que respeita a condutas ilícitas[165]. O instituto da identificação civil só surgiria com a criação do bilhete de identidade («como valioso elemento de manutenção de ordem pública» e «um poderoso meio de repressão contra a criminalidade») pelo D n.º 4.837, de 25/09/1918, que regula o Arquivo de Identificação[166]. No decorrer do ano de 1973, foi aprovado um pacote legislativo relacionado com o registo de nacional de identificação e o tratamento de dados pessoais[167], e sucedem-se discussões parlamentares e constitucionais sobre tais matérias nos anos seguintes.

Portugal foi o primeiro país a reconhecer na lei constitucional[168] o direito à proteção de dados

[165] V. LOPES, cit. 49, p. 780.

[166] O instituto sofreu inúmeras alterações das quais destacamos as últimas alterações com a publicação dos seguintes diplomas: a L n.º 33/99, de 18/05, que regula a identificação civil e a emissão do bilhete de identidade de cidadão nacional, e a L n.º 7/2007, de 05/02 que cria o cartão de cidadão e rege a sua emissão e utilização.

[167] Trata-se da L n.º 2/73, de 10/02, que institui o Registo Nacional de Identificação, do DL n.º 555/73, de 26/02 (regulamenta a L n.º 2/73, de 10/02, que institui o Registo Nacional de Identificação, define as condições de funcionamento e utilização e reorganiza o Centro de Informática do Ministério de Justiça) e da L n.º 3/73, de 05/04, que promulga várias medidas respeitantes à proteção da intimidade da vida privada.

[168] A redação inicial do art.º 35 da CRP («Utilização da informática. 1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização. 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos.») sofreu inúmeras alterações não só devido à sua natureza mas, também, para adaptar o conteúdo às normas comunitárias e outros atos relacionados com tratados internacionais que foram entrando em vigor: (1) O art.º 27º, da LC n.º 1/82, de 30/09, que procede à primeira revisão da Constituição: 1 - No n.º 1 do artigo 35.º a expressão "registos mecanográficos" é substituída pela expressão "registos informáticos". 2 - É aditado ao artigo 35.º um novo n.º 2, com a seguinte redação: 2. São proibidos o acesso de terceiros a ficheiros com dados pessoais e a respetiva interconexão, bem como os fluxos de dados transfronteiras, salvo em casos excecionais previstos na lei. 3 - O n.º 2 do artigo 35.º passa a constituir o n.º 3 do mesmo artigo, sendo o seu texto substituído por: 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate do processamento de dados estatísticos não individualmente identificáveis. 4 - Ao artigo 35.º é aditado um n.º 4, com a seguinte redação: 4. A lei define o conceito de dados pessoais para efeitos de registo informático. 5 - O n.º 3 do artigo 35.º passa a constituir o n.º 5 do mesmo artigo. (2) O art.º 20º da LC n.º 1/89, de 08/07, que procede à segunda revisão da Constituição: 1 - O n.º 1 do artigo 35.º é substituído por: 1. Todos os cidadãos têm o direito de tomar conhecimento dos dados constantes de ficheiros ou registos informáticos a seu respeito e do fim a que se destinam, podendo exigir a sua retificação e atualização, sem prejuízo do disposto na lei sobre segredo de Estado e segredo de justiça. 2 - O n.º 2 do artigo 35.º é substituído por: 2. É proibido o acesso a ficheiros e registos informáticos para conhecimento de dados pessoais relativos a terceiros e respetiva interconexão, salvo em casos excecionais previstos na lei. 3 - O n.º 4 do artigo 35.º é substituído por: 4. A lei define o conceito de dados pessoais para efeitos de registo informático, bem como de bases e bancos de dados e

e a adotar[169] a L n.º 10/91, de 29/04, Lei da Proteção de Dados Pessoais face à Informática, referindo expressamente no art.º 1º que o processamento automatizado de dados seja transparente e no estrito respeito pela reserva da vida privada e familiar e pelos direitos, liberdades e garantias fundamentais do cidadão, e cujo principal objetivo era preparar Portugal para a assinatura da Convenção de Aplicação do Acordo de Schengen, em 1995[170]. A L n.º 10/91, de 29/04, seria revogada pelo art.º 51º, da LPDP, que transpõe a Diretiva 95/46/CE, assim como a L n.º 28/94, de 29/08, que aprovou as medidas de reforço da proteção de dados pessoais. A lei nacional, e desde logo a CRP, autonomiza o direito à proteção de dados (art.º 35, da CRP) do direito à reserva ou ao respeito pela vida privada (art.º 80º do CC e art.º 26º da CRP).

Posteriormente foram publicadas as seguintes normas pertinentes e relacionadas com o objeto

---

respetivas condições de acesso, constituição e utilização por entidades públicas e privadas. 4 - Ao artigo 35.º é aditado um novo n.º 6, com a seguinte redação: 6. A lei define o regime aplicável aos fluxos de dados transfronteiras, estabelecendo formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. (3) O art.º 18º, da LC n.º 1/97, de 20/09, que procede à quarta revisão constitucional: 1 — No n.º 1 do art.º 35º da Constituição a expressão «de tomar conhecimento dos dados constantes de ficheiros ou registos informáticos a seu respeito e do fim a que se destinam» é substituída por «de acesso aos dados informatizados que lhes digam respeito»; é aditada a expressão «e o direito de conhecer a finalidade a que se destinam, nos termos da lei», eliminando-se a parte final do preceito, que passa a ter a seguinte redação: «1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.» 2 — O n.º 2 do mesmo artigo passa a n.º 4, sendo eliminadas as seguintes expressões: «ficheiros e registos informáticos», «para conhecimento», «e respetiva interconexão», substituindo-se a expressão «relativos a» por «de», passando o preceito a ter a seguinte redação: «4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.» 3 — No n.º 3 do mesmo artigo elimina-se «ou» entre «fé religiosa» e «vida privada» e são aditadas as seguintes expressões: «e origem étnica» entre «vida privada» e «salvo»; «mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para» entre «salvo» e «processamento», passando o preceito a ter a seguinte redação: «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 mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.» 4 — O n.º 4 do mesmo artigo passa a n.º 2, com aditamento, in fine, da expressão «designadamente através de entidade administrativa independente» e a substituição de «para efeitos de registo informático bem como de bases e bancos de dados e respetivas condições de acesso, constituição e utilização por entidades públicas e privadas» por «bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção», passando a ter a seguinte redação: «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.» 5 — Na parte inicial do n.º 6 do mesmo artigo é aditada a expressão «A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei», bem como a expressão «e as» entre «transfronteiras» e «formas adequadas», sendo eliminada a expressão «a lei define», passando o preceito a ter a seguinte redação: «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.» 6 — É aditado um novo n.º 7 ao mesmo artigo, com a seguinte redação: «7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.»

[169] O TC antes da publicação da L n.º 10/91, de 29/04, considerou haver um incumprimento da Constituição por omissão de medidas legislativas previstas no n.º 4, do art.º 35º, da CRP, e necessária para tornar exequível a garantia constante do n.º 2 do mesmo artigo, ainda que não tenham faltado medidas legislativas nesse sentido (Ac. do TC, nº 182/89, de 01/02).

[170] V. FUSTER, cit. 73.

da presente dissertação:

a) DL n.º 7/2004, de 07/01[171], que transpõe para a ordem jurídica nacional a Diretiva n.º 2000/31/CE, de 08/06, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno, bem como o art.º 13º, Diretiva n.º 2002/58/CE;
b) L n.º 5/2004, de 10/02[172], que estabelece o regime jurídico aplicável às redes e serviços de comunicações eletrónicas e aos recursos e serviços conexos e define as competências da autoridade reguladora nacional neste domínio, no âmbito do processo de transposição das Diretivas n.ºs 2002/19/CE, 2002/20/CE e 2002/21/CE, todas do Parlamento Europeu e do Conselho, de 07/03[173], prevê a criação de uma base de dados de assinantes devedores de serviços de comunicações eletrónicas (art.º 46º, da L n.º 5/2004, de 10/02);
c) L n.º 41/2004, de 18/08, que transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, posteriormente alterada pela L n.º 46/2012, de 29/08, com as modificações determinadas pela Diretiva n.º 2009/136/CE; e,
d) L n.º 32/2008, de 17/07, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

2-3.1. O direito à proteção de dados e a doutrina nacional

Com a disponibilidade dos meios tecnológicos ao serviço da comunicação de dimensão global conjugado com os elementos informacionais, o direito à proteção de dados melhor seria designado pelo direito à identidade informacional absorvendo o direito à proteção de dados pessoais e eliminando insuficiências do conceito[174]. De facto, o regime jurídico consagrado tem por finalidade acautelar «intromissões abusivas na vida privada das pessoas através da recolha e tratamento de dados pessoais informatizados, muito embora a sua materialidade vá

[171] O diploma foi alterado pelo DL n.º 69/2009, de 10/03 e pela L n.º 46/2012, de 20/08.
[172] A L n.º 5/2004, de 10/02, conhecida pela Lei das Comunicações Eletrónicas (LCE) não pretende regular o tratamento de dados pessoais, contudo, prevê que as empresas que oferecem redes e serviços de comunicações eletrónicas estão sujeitas à obrigação da «proteção dos dados pessoais e da privacidade no domínio específico das comunicações eletrónicas, em conformidade com a legislação aplicável à proteção de dados pessoais e da privacidade», conforme al) h), n.º 1, do art.º 27, da LCE.
[173] As Diretivas n.ºs 2002/19/CE, 2002/20/CE e 2002/21/CE foram alteradas pela Diretiva n.º 2009/140/CE, do Parlamento Europeu e do Conselho, de 25/11, e das Diretivas n.ºs 2002/22/CE, do Parlamento Europeu e do Conselho, de 07/03, alterada pela Diretiva n.º 2009/136/CE, do Parlamento Europeu e do Conselho, de 25/11, e 2002/77/CE, da Comissão Europeia, de 16/09.
[174] V. PINHEIRO, cit. 52.

para além da tutela da esfera íntima de vida de cada um» … «relacionando-o de uma forma mais ampla com o princípio da dignidade da pessoa humana, do desenvolvimento da personalidade e da integridade pessoal»[175], o que se consubstancia no controlo de como a informação é recolhida, com que finalidade e abrangência de como é tratada e utilizada por terceiros[176]. E exemplo, do anteriormente referido, é que o objetivo da Diretiva 95/46/CE é «assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais» (art.º 1º da Diretiva 95/46/CE). (3-5.2.). Cremos, assim, que o bem jurídico protegido pelas normas do direito à proteção de dados pessoais é o direito à identidade informacional que consiste muito sumariamente no direito que assiste ao titular de controlar os seus dados pessoais e decidir que dados podem ser disponibilizados a terceiros bem como opor-se à sua recolha e utilização.

2-3.2. Âmbito de aplicação do regime do direito à proteção de dados[177]

O n.º 1, do art.º 4º, da LPDP, refere que a lei aplica-se ao tratamento de dados pessoais (2-4) por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados. O n.º 2, do art.º 4º, da LPDP, acrescenta que o tratamento de dados pessoais será efetuado (1) no âmbito das atividades de estabelecimento do responsável do tratamento situado em território português; (2) fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional; e (3) por responsável (com representante estabelecido em Portugal) que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia.

Assim, e de acordo, com a LPDP podemos extrair as seguintes conclusões que estão intimamente ligadas entre si:

a) A lei é aplicável aos dados pessoais de pessoas singulares;

---

[175] FARIA, Maria Paula Ribeiro de – Artigo 35º (Utilização da Informática). In MIRANDA, Jorge; MEDEIROS, Rui, coord. - Constituição Portuguesa Anotada, Tomo I. 2.ª ed., Coimbra : Wolters Kluwer Portugal, 2010. ISBN 978-972-32-1822-0. p. 786.

[176] Sobre o conteúdo e alcance do direito à proteção de dados em diversas correntes doutrinárias veja-se por todos a obra notável de PINHEIRO, cit. 52.

[177] Note-se que as diretivas da EU são aplicáveis diretamente na medida em que os Estados-Membros não podem invocar normas de direito interno para justificar a inobservância das obrigações nelas previstas, sobretudo quanto à consulta para interpretar ou integrar lacunas e suprir deficiências das normas internas (cf. LÓPEZ, Jordi Verdaguer; JANÉ, Mª Antonia Bergas – *Todo protección de datos. Valencia* : CISS, 2013. ISBN 978-84-9954-489-2).

b) O tratamento de dados não requer um suporte específico; e,
c) O âmbito territorial do direito à proteção de dados pessoais depende da localização do estabelecimento do responsável do tratamento de dados.
d) Necessidade de encontrar um nível de adequação do controlo da circulação de dados pessoais para países terceiros ou organizações internacionais.

2-3.2.1. Dados pessoais de pessoas singulares

A lei é aplicável aos dados pessoais, no sentido que é relativa a pessoas singulares identificadas ou identificáveis (al) a), do art.º 3º da LPDP, e art.ºs 1 e 2º, al) c), do nº 1 e n.º 6, do art.º 30º e art.º 33º, da Diretiva 95/46/CE[178]). De acordo com o Considerando 2, da Diretiva 95/46/CE, os sistemas de tratamento de dados estão ao serviço do Homem que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada (aliás já garantido pelo art.º 1º, da CEDH) e o Considerando 24 que refere expressamente que a legislação para a proteção das pessoas coletivas relativamente ao tratamento de dados que lhes dizem respeito não é afetada pela Diretiva 95/46/CE.

Contudo, a questão tem suscitado interpretações no sentido de conceder às pessoas coletivas os direitos e deveres compatíveis com a sua natureza, como por exemplo o tratamento de dados respeitantes a direitos fundamentais de que beneficiam como a liberdade de associação, liberdade de empresa, direito de propriedade, entre outros, que podem constar de bases de dados para tratamento[179]. Esta posição na doutrina é considerada adequada nos termos desta dissertação, acrescentando os seguintes argumentos: (1) as pessoas coletivas podem alcançar esta proteção interpretando de forma analógica a proteção dos interesses legítimos, previstos no art.º 8º da CDFUE, dentro do especial contexto do destinatários da normas jurídicas da EU no que respeita ao mercado único e direito da concorrência[180]; (2) existem algumas disposições da L n.º 41/2004, de 18/08 que são extensíveis às pessoas coletivas para especificar e complementar as disposições da LPDP (conforme os n.ºs 2 e 3, do art.º 1º), como por exemplo, as relativas às listas de assinantes e comunicações não solicitadas a pessoas coletivas (art.º 13º e segs.); e (3) a tendência jurisprudencial do TJUE, destacando-se com o

[178] O RGPD refere-se às pessoas singulares ao longo do texto.
[179] V. CANOTILHO, J.J. Gomes, MOREIRA, Vital - Constituição da República Portuguesa Anotada Vol. I. 4.ª ed. rev. e reimp., Coimbra : Coimbra Editora, 2014. ISBN 978-972-32-2286-9. p. 547-558.
[180] V. NANCLARES, José Martín y Pérez de – Artigo 8º (*Protección de datos de carácter personal*). In MARTÍN, Araceli Mangas e ALONSO, Luis N. González, coord. - *Carta de los Derechos Fundamentales de la Unión Europea - Comentario artículo por artículo*, 1.ª ed., Bilbao : Fundación BBVA, 2008. ISBN 978-84-96515-80-2. p. 223-243.

início da declaração da existência de um direito subjetivo das empresas à inviolabilidade do seu domicílio[181], no sentido do n.º 1, do art.º 8º da CEDH.

O alargamento da transposição da Diretiva 95/46/CE, pelos Estados-Membros, no que se refere ao âmbito de aplicação às pessoas coletivas é possível[182] desde que nenhuma outra disposição do direito da EU o impeça, valendo o mesmo princípio para as pessoas falecidas[183] (por exemplo, o segredo médico não finda com a morte do doente) e para os nascituros, limitada no tempo ao período da gravidez[184].

2-3.2.2. O tratamento de dados não requer um suporte específico

A lei constitucional e ordinária confere proteção ao tratamento de dados pessoais por meios, total ou parcialmente automatizados, conferindo-se igual proteção ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais[185], que devem ser estruturados[186] de acordo com critérios específicos relativos às pessoas que permitam um acesso fácil aos dados pessoais (Considerando 29, da Diretiva 95/46/CE e al) c), do art.º 3º, da LPDP), excluindo-se do âmbito de aplicação os ficheiros relativos ao tratamento de dados pessoais efetuado por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas. O conceito de tratamento de dados está delimitado, na al) b), do art.º 3º, da LPDP, ou seja, qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição (al) b), do art.º 2º, da Diretiva 95/46/CE e n.º 2, do art.º 4º, do RGPD); e dentro dos limites fixados pelos art.ºs 5º a 20º, da LPDP (art.ºs 5º a 21º, da Diretiva 95/46/CE, e n.º 2, do art.º 8, da CDFUE).

Acresce ainda que, nos termos do n.º 7, do art.º 4º, da LPDP, que a lei aplica-se ao tratamento

[181] Par. 17 e 19, do Ac. *Hoechst AG*, v. Comissão das Comunidades Europeias, do TJUE, apensos n.ºs 46/87 e 227/88, de 21/09/1989.

[182] Par. 98, do Ac. *Bodil Lindqvist*, do TJUE, nº C-101/01, de 06/11/2003.

[183] O RGPD refere que não se aplica aos dados pessoais de pessoas falecidas, cabendo aos Estados-Membros estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas (Considerando 27, do RGPD).

[184] GT29 - Parecer 4/2007 sobre o conceito de dados pessoais. [Em linha]. 01248/07/ PT, WP 136. Brussels (Belgium), (20/06/2007). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/ policies/privacy/docs/wpdocs/2007/wp136_pt.pdf>

[185] V. Deliberação da CNPD, n.º 14/2002, de 15/01 [Em linha]. [Consult. 29 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/orientacoes/DEL14-2002-REGIME-DADOS-MANUAIS.pdf>, sobre o regime relativo ao tratamento de dados pessoais em ficheiros manuais.

[186] Nos termos do n.º 6, do art.º 4º, do RGPD, «ficheiro é qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico»

de dados pessoais que tenham por objetivo a segurança pública, a defesa nacional e a segurança do Estado, sem prejuízo do disposto em normas especiais constantes de instrumentos de direito internacional a que Portugal se vincule e de legislação específica atinente aos respetivos setores.

2-3.2.3. O âmbito territorial do direito à proteção de dados pessoais

A LPDP prevê expressamente os casos de aplicação de âmbito territorial da lei nacional[187], cujos critérios para determinar a sua aplicação, dependem da localização do estabelecimento do responsável pelo tratamento e a localização dos meios ou equipamento utilizados. A lei nacional aplica-se:

a) No âmbito das atividades de estabelecimento do responsável do tratamento situado em território português (art.º 4º, nº 3, al) a), da LPDP). O conceito de estabelecimento deve ser flexível dependendo do grau de estabilidade como a realidade do exercício das atividades onde se encontra instalado e se o contexto do tratamento de dados é efetivado no contexto dessas atividades[188]. A sede formal do estabelecimento e o princípio da nacionalidade dos titulares dos dados é irrelevante para efeitos de aplicação da lei nacional[189] [190].

---

[187] O âmbito de aplicação territorial da Diretiva 95/46/CE não se limita aos 28 Estados-Membros da UE, incluindo também os Estados que não são membros da UE mas que fazem parte do Espaço Económico Europeu (EEE) – a saber, a Islândia, o Listenstaine e a Noruega. A RAR n.º 35/92, de 18 de Dezembro, aprovou para ratificação e publica em anexo o Acordo Sobre o Espaço Económico Europeu (EEE) e os respetivos anexos, protocolos e declarações, bem como a ata final, com os seus anexos, assinados no Porto, em 02/05/1992, concluído entre a Comunidade Económica Europeia, a Comunidade Europeia do Carvão e do Aço, o Reino da Bélgica, o Reino da Dinamarca, a República Federal da Alemanha, a República Helénica, o Reino de Espanha, a República Francesa, a Irlanda, a República Italiana, o Grão-Ducado do Luxemburgo, o Reino dos Países Baixos, a República Portuguesa, o Reino Unido da Grã-Bretanha e Irlanda do Norte, a República da Áustria, a República da Finlândia, a República da Islândia, o Principado do Liechtenstein, o Reino da Noruega, o Reino da Suécia e a Confederação Suíça e ratificados pelo DPR n.º 59/92, de 18/12, entrando em vigor na ordem jurídica portuguesa a 18/12/1992. O Espaço Económico Europeu (EEA) é composto pelos Estados-Membros da UE e 3 países da Associação Europeia de Comércio Livre (EFTA), Islândia, Listenstaine e Noruega.

[188] V. GT29 - Parecer 8/2010 sobre a lei aplicável [Em linha]. 0836-02/10/PT WP 179. Brussels (Belgium), (16/12/2010). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommenda tion/files/2010/wp179_pt.pdf>; e também, Ac. *Weltimmo*, do TJUE, n.º C-230/14, de 01/10/2015 e recordamos o parágrafo 60, do Ac. *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, do TJUE, n.º C-131/12, de 13/05/2014 «Decorre do que precede que há que responder à primeira questão, alínea a), que o artigo 4.°, n.° 1, alínea a), da Diretiva 95/46 deve ser interpretado no sentido de que é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro, na aceção desta disposição, quando o operador de um motor de busca cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar a promoção e a venda dos espaços publicitários propostos por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro», não sendo «determinantes, para este efeito, nem a nacionalidade, nem o local de residência habitual das pessoas em causa, nem a localização física dos dados pessoais» (do parágrafo 55, das Conclusões do advogado-geral *Niilo Jääskinen*, apresentadas em 25/06/2013, no Ac. *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, do TJUE, n.º C-131/12, de 13/05/2014).

[189] O âmbito territorial abrange o fornecedor de motores de pesquisa que trate dados pessoais na medida em que

b) Fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional (art.º 4º, nº 3, al) b), da LPDP), ou seja depende de critérios decorrentes do direito internacional público para situações específicas como, por exemplo, a determinação da lei aplicável por acordo internacional para uma embaixada, ou a previsão de um estatuto especial para uma missão ou organização internacional[191].

c) Por responsável (com representante designado em Portugal) que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia art.º 4º, nº 3, al) c), da LPDP). Trata-se de evitar lacunas no exercício do direito à proteção de dados pessoais desde que haja uma intenção inequívoca de proceder ao tratamento de dados no âmbito de uma determinada atividade do responsável pelo seu tratamento[192]. Assume extrema importância a identificação do papel do responsável de dados e os meios que são utilizados para recolher e tratar os dados. Por meios, no âmbito da IAm, podem entender-se todos os objetos que são utilizados para tratar os dados recolhidos através de dispositivos próprios (contadores de passos, detetores de fumos, relógios conectados, entre outros) e dispositivos terminais de utilizadores[193] (telemóveis inteligentes, computadores-tablete, televisores com ligação à internet, etc…) dotados de software específico para esse fim e que podem envolver diversas partes que assumem o papel de responsáveis de tratamento de dados: os fabricantes de dispositivos, as plataformas sociais, os criadores de aplicações de terceiros, os terceiros[194], etc.

Com a produção de efeitos a partir de maio de 2018, o art.º 3º do RGPD alarga o âmbito territorial, pois, aplica-se ao «tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União» (resolvendo algumas questões relacionadas com a Nuvem), e ainda, ao «tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento

---

é considerado como um responsável pelo tratamento destes dados pessoais (v. GT29 - Parecer 1/2008 sobre questões de protecção dos dados ligadas aos motores de pesquisa [Em linha]. 00737/PT, WP 148. Brussels (Belgium), (04/04/2008). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_pt.pdf>).

[190] V. GT29, cit. 189.

[191] V. GT29, cit. 188.

[192] V. GT29, cit. 188.

[193] V. nota n.º 4, sobre o conceito de equipamento.

[194] V. GT29, cit. 3.

estejam relacionadas com: a) a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) o controlo do seu comportamento, desde que esse comportamento tenha lugar na União» (cujo objetivo de proteção se relaciona com os modelos de negócio baseado em grandes dados e monitorização do comportamento em linha).

2-3.2.4. A transferência de dados para fora da União Europeia

A transferência de dados pessoais para países terceiros é determinada pelo nível de adequação do controlo da circulação de dados pessoais, nos termos do disposto dos art.ºs 19º e 20º, da LPDP e art.ºs 25º e 26º, da Diretiva 95/46/CE[195]. A adequação do nível de proteção num Estado que não pertença à União Europeia é apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, devem ser tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no Estado em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse Estado (art.º 19º, nº 2, da LPDP). A CNPD pode decidir se um Estado que não pertença à União Europeia assegura um nível de proteção adequado, salvo se a Comissão tiver considerado o contrário (art.º 19º, nº 3 e 5, da LPDP e art.º 25º, n.º 4, da Diretiva n.º 95/46/CE).

A Comissão tem o poder de determinar, com base no n.º 6, do art.º 25º da Diretiva 95/46/CE, se um país terceiro garante um nível de proteção adequado em virtude do seu direito interno ou dos compromissos internacionais assumidos[196].

---

[195] Dado que a «Diretiva 95/46/CE não define nem no artigo 25.º nem em qualquer outra disposição, nomeadamente, o art.º 2º, o conceito de transferência para um país terceiro» o TJUE fixou jurisprudência no sentido de que «não existe uma «transferência para um país terceiro de dados» na aceção do art.º 25.°, da Diretiva 95/46/CE quando uma pessoa que se encontra num Estado-Membro insere numa página Internet, armazenada num fornecedor de serviços de anfitrião que está estabelecido nesse mesmo Estado ou noutro Estado-Membro, dados de caráter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros» atendendo à evolução da internet à data da publicação da referida diretiva bem como não se poderia presumir algo que não estava previsto, conforme Parágrafos 52, 56 e 71, do Ac. *Bodil Lindqvist*, do TJUE, nº C-101/01, de 06/11/2003.

[196] A decisão da Comissão Europeia deve cumprir alguns procedimentos prévios tais como: (1) a Comissão elabora uma proposta (2) o GT29 elabora um parecer conforme consulta das autoridades de proteção de dados dos Estados-Membros e da Autoridade Europeia para a Proteção de Dados; (3) a aprovação do "Comité do artigo 31.º", composto por representantes dos Estados-Membros; (4) a adoção da decisão pelo Colégio de Comissários; (5) podendo ainda em qualquer momento, o Parlamento Europeu e o Conselho solicitar à Comissão que mantenha, altere ou retire a decisão de adequação com base no facto da sua proposta exceder as competências de execução previstas na diretiva. Até à data, a Comissão reconheceu que Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça e Uruguai fornecem uma proteção adequada. (*vide* 2-29, para o caso especial do novo equilíbrio encontrado entre a EU e os EUA). Estas decisões de adequação não abrangem as trocas no setor da aplicação da lei. Existem acordos especiais relativos às trocas de dados neste domínio, como por exemplo, os acordos PNR (*Passenger Name*

Com a produção de efeitos a partir de maio de 2018, e nos termos dos art.ºs 44º a 50º, do RGPD, qualquer transferência de dados pessoais que seja ou venha a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só pode ser efetuada, no estrito cumprimento de todas as normas do regulamento, e cujas condições devem ser respeitadas pelo responsável pelo tratamento e pelo subcontratante, incluindo o que diz respeito às transferências ulteriores. As transferências realizadas com base numa decisão de adequação, pela Comissão, não exigem autorizações específicas (n.º 1, do art.º 45º, do RGPD), porém, não tendo sido tomada qualquer decisão pela Comissão, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes (n.º 2, do art.º 46º, do RGPD). As garantias adequadas podem estar previstas (1) num instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos; (2) existirem regras vinculativas aplicáveis às empresas; (3) cláusulas-tipo de proteção de dados adotadas pela Comissão; (4) cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão; (5) um código de conduta; e (6) num procedimento de certificação.

Record) e TFTP (*Terrorist Financing Tracking Program*).

CAPÍTULO IV – CONCEITOS E DEFINIÇÕES DE DADOS PESSOAIS

2-4. Definição de dados pessoais

Portugal na transposição da Diretiva 95/46/CE acompanhou as iniciativas da Organizações Internacionais[197], nomeadamente, a Convenção 108 e das Diretrizes sobre a Privacidade[198], e a decisões proferidas pelo TEDH e TJUE, ampliando a definição legal.

Pese a máxima latina de que toda a definição em direito é perigosa[199], a al) a) do art.º 3º, da LPDP define dados pessoais como qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável, acrescentando que 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. São dados pessoais para além daqueles que possibilitam a identificação direta de uma pessoa, aqueles, que sem esforço excessivo, permitem chegar a essa identificação[200]. De acordo com o princípio do reconhecimento[201], os dados como uma sequência de símbolos quantificados ou quantificáveis apenas são relevantes se associados a uma pessoa, dependendo de três elementos não cumulativos e da análise das circunstâncias do caso concreto quanto: (1) ao conteúdo, ou seja, tudo o que é sobre determinada pessoa; (2) à finalidade, ou seja, quando os dados são tratados com um determinado objetivo; e (3) ao resultado, ou seja, a utilização dos dados provoca um determinado impacto na esfera jurídica do titular, sendo «suficiente que a pessoa possa ser tratada de forma diferente de outras pessoas como resultado do tratamento» dos dados pessoais[202].

2-4.1. Natureza da informação

A informação relativa a uma pessoa pode ser objetiva ou subjetiva.

A informação objetiva preocupa-se com a maior aproximação à realidade factual e mensurável, como qualquer informação numérica, alfabética, gráfica, imagética ou

[197] Com o objetivo de alcançar um elevado nível de proteção já reconhecido no art.º 8º da CEDH (Considerando 10, da Diretiva 95/46/CE).
[198] GONÇALVES, Maria Eduarda - Direito da Informação. Novos direitos e formas de regulação na sociedade da informação. Coimbra : Almedina, 2003. ISBN 978-972-4019-08-6. p. 88
[199] *Omnis definitio in jure civili periculosa est, parum est enim ut non subverti possit* (Toda a definição em direito é perigosa, porque há muito pouco que não possa ser impugnado).
[200] Vide Considerando 26, da Diretiva 95/46/CE e art.º 2º da Convenção 108.
[201] V. PINHEIRO, cit. 52.
[202] GT29, cit. 184, p. 11.

acústica[203], ainda que não tenha de ser necessariamente verdadeira, pois, a LPDP prevê o direito de acesso, retificação e eliminação dos dados pelo seu titular[204]. Mas há uma preocupação com a exatidão dos dados associados à pessoa, por exemplo, quanto ao nome, filiação, nacionalidade, data de nascimento, dados biométricos (relativos ao aspeto físico, tais como: sexo, altura, peso, imagem facial[205], geometria da mão e impressão digital, reconhecimento da íris e retina, números de identificação[206] (civil[207], fiscal[208], segurança social[209], passaporte[210], carta de condução[211]), domicílio[212], código postal[213], comunicações eletrónicas por endereço de correio eletrónico e telefone[214], informação genética e informação de saúde (passada, presente e futura, física e mental)[215], filiação sindical ou partidária, grau de instrução, profissão, orientação e vida sexual, origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas.

---

[203] No seguimento da redação do al) f) do art.º 5º, do RD 1.720/2007, de 21/12, *Reglamento de protección de datos de carácter personal.*

[204] GT29, cit. 184.

[205] Parágrafos 86, 89 e 90, do Ac. *Verlagsgruppe News GmbH and Bobi v. Austria*, do TEDH, n.º 59.631/09, de 04/12/2012. A rede social Facebook desenvolveu uma aplicação denominada DeepFace para reconhecer o rosto de pessoas na internet. Esta aplicação sugere que o Facebook recolhe e armazena fotografias e por isso encontra-se em discussão nos Tribunais Americanos, já que foi objeto de um processo judicial (*John Nadolenco, Lauren R. Goldman e Archis A. Parasharami v. Facebook, United States District Court Northern District of California San Francisco Division Inc*. - 3:15-cv-03747-JD *Document 69 Filed* 10/09/15).

[206] Nos termos do n.º 5, do art.º 35º, da CRP, é proibida a atribuição de um número nacional único aos cidadãos, que «funciona como garantia» dos direitos consagrados nos n.ºs 1 a 4, do art.º 35º, da CRP, «dificultando o tratamento de dados pessoais e a sua interconexão, que seria facilitada com um identificador numérico comum» (CANOTILHO & MOREIRA, cit. 179), entre diversos setores de atividade e sob pena de «temer a reprodução do mundo de Orwell e a total perda da privacidade e de algumas liberdades básicas do cidadão» (V. FARIA, cit. 175, p. 801).

[207] L n.º 7/2007, de 05/02, que cria o cartão de cidadão e rege a sua emissão e utilização (alterada pela L n.º 91/2015, de 12/08).

[208] DL n.º 14/2013, de 28/01, que procede à sistematização e harmonização da legislação referente ao número de identificação fiscal.

[209] L n.º 110/2009, de 16/09, que aprova o Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social, tendo sofrido diversas alterações.

[210] DL n.º 83/2000, de 11/05, que aprova o novo regime legal da concessão e emissão dos passaportes, tendo sofrido diversas alterações.

[211] DL n.º 138/2012, de 05/07, que altera o Código da Estrada e aprova o Regulamento da Habilitação Legal para Conduzir, transpondo parcialmente a Diretiva n.º 2006/126/CE, do Parlamento Europeu e do Conselho, de 20/12, alterada pelas Diretivas n.ºs 2009/113/CE, da Comissão, de 25/08, e 2011/94/UE, da Comissão, de 28/11, relativas à carta de condução, tendo sofrido diversas alterações.

[212] V. AEPD. Informe 182/2008 [Em linha]. [Consult. 20 mai. 2015]. Disponível em WWW <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0182_La-vivienda-es-un-dato-de-car-aa-cter-personal-sometido-a-la-ley-org-aa-nica-15-b-1999.pdf>.

[213] Nos Estados de Massachusetts e Califórnia (EUA) o código postal é um dado pessoal, nos termos da legislação em vigor v. PAYTON, CLAYPOOLE, cit. 1.

[214] *Ac. Copland v. the United Kingdom*, do TEDH, n.º 62.617/00, de 03/07/2007.

[215] L n.º 12/2005, de 26/01, que regula a informação genética pessoal e informação de saúde, alterada pela L n.º 26/2016, de 22/08, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Diretiva 2003/4/CE, 28/01, e Diretiva 2003/98/CE, 17/11, tendo sido regulamentada pelo DL n.º 131/2014, de 29/08, no que se refere à proteção e confidencialidade da informação genética, às bases de dados genéticos humanos com fins de prestação de cuidados de saúde e investigação em saúde.

A informação subjetiva inclui juízos de valor que podem ser extraídos das evidências factuais e observáveis, variando em função do recetor e do seu estado de conhecimento[216]. A informação subjetiva constrói-se e inter-relaciona-se com outros dados do conhecimento e a sensibilidade do analista, como, por exemplo, os traços comportamentais quanto ao padrão da escrita (para efeitos de prova que fundamente a prática de um crime de falsificação de assinatura), a presunção sobre o estado de gravidez com fundamento no registo de compras (com o fim de potenciar a venda de produtos específicos)[217], etc. O principal problema é que a abordagem atual no processamento de dados pessoais define características dos dados que podem dar origem a uma perceção distorcida atribuída a um determinado titular potenciando o risco de violação do direito à proteção dos dados pessoais. O tratamento de dados pelo analista, que os recebe e manipula, influencia a avaliação da informação, e em consequência, a confiança no resultado da informação extraída.

2-4.1.1. Identificação de objetos

O conceito de dados pessoais evolui e acompanha o ritmo acelerado da inovação tecnológica cujo contributo dos sistemas RFID foi fundamental na medida em que permitem identificar um objeto e não uma pessoa, embora seja evidente que por detrás da localização do objeto está o seu proprietário[218]. Se as informações relativas a objetos que registam o comportamento de uma pessoa, ainda que não identificada, apelam à eventual identificação tendo em conta o resultado ou finalidade que se pretendem alcançar[219] são consideradas dados pessoais. Esta questão, no entanto, suscita dúvidas tanto pelo espírito da LPDP como da Diretiva 95/46/CE, aplicáveis a pessoas identificadas ou identificáveis, nomeadamente, para exercer os direitos de acesso a informação na posse de terceiros. A questão foi colocada pelo Tribunal Federal Alemão ao TJUE sobre se os endereços IP[220] cabem no âmbito da definição de dados pessoais

[216] A informação vai sendo construída ao longo do ciclo da vida da pessoa que vai acumulando dados e informações desde que nasce até morrer.
[217] DUHIGG, Charles - *How Companies Learn Your Secrets* [Em linha*]*. *In The New York Times* (16/02/2012). [Consult. 18 de jun. 2014]. Disponível em WWW <http://emoglen.law.columbia.edu/twiki/pub/CompPriv Const/HowCompaniesLearnOurConsumingSecrets/How_Companies_Learn_Your_Secrets_NYTimes.com.pdf>.
[218] MARCOS, Isabel Davara Fernández de - *Hacia la estandarización de la protección de datos personales: Propuesta sobre una «tercera vía o tertium genus» internacional*. Madrid : La Ley, 2011. ISBN 978-84-8126-827-0. p. 142.
[219] V. *Working document on data protection issues related to RFID technology* [Em linha]. 10107/05/EN, WP 105. Brussels (Belgium), (19/01/2005). [Consult. 1 Abr. 2015]. Disponível em WWW <http://ec.europa.eu/ justice/policies/privacy/docs/wpdocs/2005/ wp105_en.pdf>.
[220] O Protocolo de Internet (IP) é o método pelo qual os dados são enviados de um dispositivo eletrónico (computador, impressora, telefone inteligente, etc.) para outro na Internet. Cada dispositivo na Internet tem pelo menos um endereço IP que o identifica de forma exclusiva de todos os outros computadores da Internet. Os dados quando são enviados estão divididos em partes e são recebidos por outro protocolo, o TCP (sigla oriunda do inglês: *Transmission Control Protocol* significa protocolo de controle de transmissão) que os coloca

foi respondida afirmativamente, ou seja, que a al) a), do art.º 2º da Diretiva 95/46/CE, deve ser interpretada no sentido de que «um endereço IP dinâmico registado por um prestador de serviços de meios de comunicação em linha aquando da consulta por uma pessoa de um sítio Internet que esse prestador disponibiliza ao público constitui, relativamente a esse prestador, um dado pessoal, (…) quando este disponha de meios legais que lhe permitam identificar a pessoa em causa graças às informações suplementares que o fornecedor de acesso à Internet dessa pessoa dispõe»[221]. O IP para o GT29 é um dado pessoal na medida em que permite estabelecer uma ligação entre o endereço IP estático ou dinâmico a determinada pessoa recorrendo a testemunhos de conexão ou aos sistemas modernos de extração de dados mesmo quando são processadas grandes quantidades de informação. A Diretiva 95/46/CE aplica-se ao tratamento de dados pessoais e a todas as questões que não sejam especificamente abrangidas pela Diretiva 2002/58/CE[222]. Os Estados-Membros têm tido posições distintas quanto a esta matéria[223]. Em Portugal, o IP é considerado, na doutrina, um dado pessoal na medida em que permite a identificação do seu utilizador através do rastreio dos dados transferidos[224]. Questões semelhantes podem ser colocadas quanto ao telemóvel que transmite informações sobre localização através do GPS[225], do serviço Google Latitude ou da rede geossocial Foursquare.

Note-se que o dado é operacionalizado no mundo abstrato de sistemas de informação mas é projetado especificamente como um identificador, ou pode ser um composto de dados relacionados com uma pessoa que a torna identificável. O uso potencial de informações inferidas de hábitos em linha pelos IP's pode ir muito além de apenas fornecer mensagens publicitárias, dado que podem ser usados para a classificação social e práticas discriminatórias, como os preços dinâmicos e discriminação de preços, limitando o princípio da liberdade de celebração de contratos.

---

novamente na ordem certa. A IANA ou Autoridade para Atribuição de Números da Internet (da sigla oriunda do inglês: *Internet Assigned Numbers Authority*) é a entidade mundial que supervisiona a atribuição global dos números na Internet - entre os quais estão os números das portas, os endereços IP, sistemas autónomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet.

[221] Parágrafo 49, do Ac. *Patrick Breyer v. Bundesrepublik Deutschland*, do TJUE, n.º C-582/14, de 19/10/2016.

[222] V. GT29 - Documento de trabalho, Privacidade na Internet - Uma abordagem integrada da EU no domínio da proteção de dados em linha [Em linha]. 5063/00/PT/FINAL, WP 37. Brussels (Belgium), (21/11/2000). [Consult. 14 Fev. 2015]. Disponível em WWW <http:// ec.europa.eu/justice/data-protection/article-29/ documentation/opinion-recommendation/files/2000/wp37_pt.pdf#h2-16>, e também, GT29, cit. 184.

[223] TIMELEX - *Study of case law on the circumstances in which IP addresses are considered personal data* (SMART 2010/12) D3. *Final report* [Em linha]. (2011) [Consult. 16 Abr. 2015]. Disponível em WWW <http:// www.timelex.eu/frontend/files/userfiles/files/publications/2011/IP_addresses_report_-_Final.pdf>

[224] V. CASTRO, cit. 38 e CASTRO, Catarina Sarmento - Artigo 8º (Proteção de dados pessoais). In SILVEIRA, Alessandra, CANOTILHO, Mariana, coord. - Carta dos Direitos Fundamentais da União Europeia Comentada. Coimbra : Almedina, 2013. ISBN 978-97-2405-120-8. p. 120-128.

[225] O Ac. *Uzun v. Germany*, do TEDH n.º 35.623/05, de 02/09/2010, considera uma ingerência na vida privada a vigilância por GPS.

2-4.2. Conteúdo e suporte da informação

Os dados pessoais incluem todo o tipo de informação desde que permita identificar, direta ou indiretamente, uma pessoa[226], ou seja, abrangem não só a informações relativas à vida privada mas, também, sobre a vida profissional[227] ou pública[228], no sentido *lactu sensu*[229]. Para o GT29, «a informação sobre pessoas coletivas pode ser considerada como relativa a pessoas singulares», … «quando o critério do conteúdo, da finalidade ou do resultado permitirem que a informação sobre a pessoa coletiva ou sobre a empresa seja considerada como relativa a uma pessoa singular, esta deverá ser considerada como dados pessoais e as regras de proteção de dados deverão aplicar-se»[230], apontando exemplos, como é o caso de quando o nome de uma pessoa coletiva deriva de uma pessoa singular ou o endereço eletrónico que é normalmente utilizado pelo colaborador.

A informação pode estar registada em qualquer suporte conhecido (manual, magnético, eletrónico, sistema em linha, etc.) ou que venha a ser conhecido (automatizado ou não). Os meios de transmissão desses dados não têm relevância para efeitos da legislação de proteção de dados[231], como por exemplo a fotografia[232].

2-4.3. Identificabilidade de uma pessoa

Nos termos da al) a), do n.º 1, do art.º 3º, da LPDP, é considerada identificável a pessoa que possa ser identificada direta ou indiretamente[233], 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.

A amplitude do conceito de dados pessoais parece infinita[234]. O termo identidade está omnipresente na ciência social contemporânea[235] e também para efeitos do conceito em análise devem ser consideradas todas as unidades de informação na sua aceção prática e

[226] Al) a) do art.º 2º, da Convenção 108 e al) a) do n.º 1, das Linhas Diretrizes da Privacidade.
[227] Parágrafo 29 do Ac. *Michaud* c. *France* do TEDH n.º 12.323 de 06/12/2012 e § 91 do Ac. *Niemietz* c. *Germany*, do TEDH n.º 13.710/88, de 16/12/1992.
[228] Ac. *Bodil Lindqvist*, do TJUE, nº C-101/01, de 06/11/2003.
[229] Parágrafo 65, do Ac. *Amann v. Switzerland*, do TEDH n.º 27.798/95, de 16/02/2000.
[230] GT29, cit. 184. p. 25.
[231] FRA; CdE - Manual da Legislação Europeia sobre Proteção de Dados [Em linha]. Luxemburgo : Serviço das Publicações da União Europeia, 2014. [Consult. 10 dez. 2014]. Disponível em WWW <http://www.cnpd.pt/bin/legis/internacional/fra-2014-handbook-data-protection-pt.pdf> ISBN 978-92-871-9939-3 (CdE) ISBN 978-92-9239-498-1 (FRA).
[232] Ac. *Sciacca v. Italy*, do TEDH n.º 50.774/99, de 11/01/2005.
[233] Neste sentido, anteriormente à publicação da LPDP, o Ac. do TC n.º 355/97, de 07/05/1997.
[234] MARCOS, cit. 218, p. 145.
[235] STRYKER, Sheldon; BURKE, Peter J. - *The Past, Present, and Future of an Identity Theory [Em linha]*. *In Social Psychology Quarterly*, Vol. 63, n.º 4 (dec. 2000), *Special Millenium Issue on the State of Sociological Social Psychology. American Sociological Association.* p. 284-297 [Consult. 19 jan. 2015]. Disponível em WWW <http://www.jstor.org/stable/2695840> ISSN 0190-2725.

teórica. Há uma dialética fundamental entre a pessoa desde que nasce subjacente à interação social manifestada através de gestos, linguagem, símbolos de *status* e todo o tipo de aparências[236]. A identificabilidade é construída em função dos dados criados por cada um ou determinados pelos outros, no contexto social em que se insere. A identidade pode ser definida como o conjunto de características[237] que representam uma pessoa na sua dimensão estática (física e fisiológica) ou dinâmica (como resultado do comportamento numa comunidade[238]).

A utilização dos serviços disponíveis em linha veio possibilitar a maior partilha de informação da esfera privada permitindo a terceiros identificar uma pessoa recorrendo à sua pegada digital. Os dados contidos na pegada digital permitem traçar perfis parciais[239] em diferentes domínios: relação com a família, atividade profissional, administração tributária, serviços de saúde, serviços bancários, redes sociais, compras, ócio, entre outros. As pessoas desempenham múltiplos papéis nas sociedades contemporâneas que são altamente diferenciados dando origem a perfis diferenciados.

2-4.3.1. Identificadores diretos e indiretos

O nome é o identificador direto por excelência da pessoa[240], mas não é o único meio de

---

[236] GOFFMAN, Erving - *The presentation of self in everyday life* [Em linha]. *Monograph n.º 2. Edinbourg : University of Edinburgh Social Sciences Research Centre 39 George Square*, 1956. [Consult. 12 de out. 2014]. Disponível em WWW < https://monoskop.org/images/1/19/ Goffman_Erving_The_Presentation_of_Self_in_ Everyday_Life.pdf>.

[237] Entende-se que a pessoa virtual é uma extensão de uma identidade real, pois, desempenha determinados papéis sob uma máscara, e que representa um desafio à sua regulação e segurança jurídico-tecnológica.

[238] O comportamento das pessoas pode incluir alterações físicas e fisiológicas que devem ser protegidas como é o caso do abandono irreversível dos sinais do sexo de origem, com consequências relevantes na emissão de documentos de identificação, em conformidade com o Ac. *B. v. France* do TEDH n.º 13.343/87, de 25/03/1992, decorrentes do fenómeno do transexualismo.

[239] STORF, Katalin; HANSEN, Marit; RAGUSE, Maren - From H1.3.5*: Requirements and concepts for identity management throughout life* [Em linha]. *PrimeLife*, 2009 [Consult. 16 jan. 2015]. Disponível em WWW <http://primelife.ercim.eu/images/stories/deliverables/h1.3.5-requirements_and_concepts_for_idm_throughout_ life-public.pdf>. p. 18 e segs.

[240] É discutível se o nome e morada são dados pessoais como indicam CASTRO, cit. 38, p. 70 e segs e GONÇALVES, cit. 198, p. 82 e segs, confrontando-se a LPDP e a LADA. A posição aqui tomada é considerá-los dados pessoais, não de forma autónoma mas integrados com outros princípios atinentes à proteção de dados: (1) o nome para além de ser o primeiro identificar de uma pessoa revela na melhor tradição romana os ancestrais dos seus titulares e não raras as vezes para honrar a família (constitui uma interferência na vida privada de uma pessoa, abrangida pela proteção do art.º 8º, da Convenção 108, a publicação de informação àcerca de uma pessoa mencionando o nome completo, conforme *Kurier Zeitungsverlag und Druckerei GmbH v. Austria* (no. 2), do TEDH, n.º 1.593/06, de 19/06/2006, assim como quando é mencionado por exemplo, num contexto que facilita a identificação da pessoa em causa para campanhas publicitárias, conforme parágrafo 45, do Ac. *Bohlen v. Germany*, n.º 53.495/09, do TEDH de 19/02/2015); (2) a morada pode expor o *status social* e condição económica de determinada pessoa, por exemplo, tendo em conta o preço por metro quadrado da zona residencial a que pertence (neste sentido, o Ac. do TRE, n.º 24/11.2T2GDL-A.E1, de 27/03/2014, que considera a «informação sobre a identidade e morada do titular de um identificador associado a um determinado veículo e os respetivos locais de circulação nas autoestradas, está a coberto da proteção de dados pessoais» e o *Ac. Alkaya v. Turkey*, do TEDH, n.º 42 811/06, de 09/10/2012, que refere que o domicílio está abrangido pela proteção do art.º

identificação[241], necessitando de ser articulado com outros elementos (imagem[242], número de identificação, família, morada, registos escolares, louvores...) com o fim evitar confusão.

A LPDP tutela, igualmente, os identificadores manifestados através de sinais, valores, símbolos, códigos, entre outros. Os identificadores indiretos levantam questões complexas, nomeadamente, o que pode ser considerado um identificador, porque para uns pode ser útil e para outros não, ou se é universal ou para um contexto específico. Tendo em vista o propósito do tema em discussão vejamos alguns identificadores que merecem reflexão.

As empresas através dos seus motores de pesquisa podem conhecer os hábitos e preferências dos seus utilizadores sem necessidade de login[243], dependendo de testemunhos de conexão e endereços IP, como identificadores. Os dados transferidos em bruto pelos testemunhos de conexão que articulados com os navegadores podem identificar local onde vive o utilizador, idioma preferido, o que faz, a sua capacidade económica, estilo de vida e até relações familiares de forma invisível[244]. O mesmo sucede com os motores de pesquisa que armazenam os endereços IP[245] juntamente com o histórico das consultas do utilizador[246], ou seja, a sequência de cliques. Pelo que, a utilidade da identificação indireta parece ser aferida tanto pelo responsável do tratamento de dados como de terceiros[247].

Dado que o tempo de vida de uma identidade não corresponde ao tempo de vida da entidade associada[248], a falta de atualização dos dados recolhidos através dos identificadores pode levantar questões pertinentes na medida em que a identidade é um conceito dinâmico que evolui de acordo com a própria idade das pessoas e as interações que tem com a sociedade. O titular dos dados, apesar da publicidade do tratamento, nos termos do art.º 21º, da LPDP, pode desconhecer o seu conteúdo e ficar assim impedido de exercer o seu direito de retificação, apagamento ou bloqueio.

O TEDH e o TJUE, na fundamentação das suas decisões, apelam ao contexto social,

---

8º, da Convenção 108).

[241] No caso de figuras públicas a referência ao Primeiro-ministro ou a Rainha de Inglaterra é suficiente para reconhecer a pessoa ou à sombra da popular personagem Indiana Jones.

[242] Ac. *P.G. and J.H. v. The United Kingdom*, do TEDH n.º 44787/98, de 25/09/2001 e Ac. *von Hannover v. Germany*, do TEDH n.º 59.320/00, de 24/09/2004.

[243] Login inclui autenticação do utilizador e chave de acesso.

[244] V. GT29, cit. 222.

[245] O IP como já se referiu identifica objetos.

[246] Colocam-se questões sobre a adequação da construção do perfil de um utilizador quando o mesmo endereço IP é utilizador por várias pessoas ou o tráfego na internet é encaminhado através de um *proxy* de uma organização.

[247] CASTRO, cit. 38.

[248] ALPÁR, Gergely; HOEPMAN, Jaap-Henk; SILJEE, Johanneke - *The Identity Crisis. Security, Privacy and Usability Issues in Identity Management*. [Em linha]. 2011. [Consult. 12 dez. 2014]. Disponível em WWW <http://arxiv.org/ftp/arxiv/papers/1101/1101.0427.pdf>.

económico e tecnológico em que os dados pessoais foram recolhidos, tratados e divulgados[249]. Por outro lado, a necessidade da interoperabilidade e esforços internacionais no intercâmbio de dados pessoais exige um elevado nível de coerência na sua proteção[250]. Assinala-se que identidade não é apenas aquilo que a pessoa revela de si própria mas sobretudo como é percebida de forma diferente entre os vários analistas e pelos mesmos analistas de forma diferente em tempo e espaço divergentes absolutamente influenciados pela cultura (atitudes, valores sociais, normas e práticas)[251].

O mercado digital oferece novos modelos e práticas de negócio pelo que parece-nos que o contexto considere que os consumidores, como titulares de dados pessoais, devem esperar que os operadores económicos tratem os seus dados no contexto em que foram fornecidos e recolhidos.

Em conclusão, os identificadores diretos representam a pessoa de forma descritiva e os identificadores indiretos requerem um processo de tratamentos de dados, desde a recolha num contexto que permite relacionar os dados e informação obtida (por exemplo, a monitorização de comportamentos) a uma determinada pessoa.

2-4.3.2. Meios utilizados na identificação

O considerando 26 da Diretiva 95/46/CE refere que para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa. Isto é, os meios devem ponderar os fatores objetivos para a identificação, como os custos, oportunidade de tempo e as atividades consideradas necessárias para a identificação (CdE, R (90) 19[252]; CdE, R (97) 18)[253] considerando a tecnologia explorada à data do tratamento dos dados, nomeadamente a sua difusão quanto ao acesso e uso. Uma pessoa singular não é considerada identificável se a sua identificação requerer tempo, custos elevados ou atividades

[249] Ac. *S. and Marper v. The United Kingdom*, do TEDH n.º 30562/04, de 04/12/2008 e Ac. *Gardel v. France*, do TEDH n.º 16.428/05, de 17/12/2009.
[250] NISSENBAUM, cit. 1.
[251] Para um estudo mais aprofundado, sugere-se a consulta do site <http://geert-hofstede.com/ countries.html>.
[252] CdE *Recommendation n.º R (90) 19 of the Committee of Ministers to Members States on the protection of personal data used for payment and other related operations* [Em linha]. (13/09/1990) [Consult. 9 abr. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=570709&SecMode=1&DocId=592684&Usage=2>.
[253] CdE *Recommendation n.º R (97) 18 of the Committee of Ministers to Members States concerning the protection of personal data collected and processed for statistical purposes* [Em linha]. (30/09/1997) [Consult. 12 mar. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2001724&SecMode=1&DocId=578856&Usage=2>.

desproporcionadas, que em rigor, só podem ser verificados no caso concreto[254]. De facto é necessário ter em conta conjunto de circunstâncias e a evolução tecnológica e organizacional que envolvem os meios disponíveis para proceder à identificação de uma pessoa.

Os dados serão considerados anónimos em caso de falta de meios técnicos ou a impossibilidade de realizar a identificação do titular dos dados pelo responsável do tratamento de dados. Os princípios da proteção de dados plasmados no regime dos distintos instrumentos regulatórios nacionais, comunitários ou internacionais não se aplicam aos dados anónimos[255].

2-4.3.3. A ampliação do conceito de dados pessoais no RGPD

A construção do conceito de dados pessoais elaborada pelas legislações da EU e dos Estados-Membros, pelas tendências jurisprudenciais e relevantes contributos de instituições e doutrina publicada, foi absorvida pelo RGPD, que altera e amplia o conceito de dados pessoais, conforme al) 1), do art.º 4º, e define como a «informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular».

Os identificadores por via eletrónica são expressamente reconhecidos como um meio para identificar os titulares dos dados pessoais, tais como endereços IP ou testemunhos de conexão ou outros identificadores, como as etiquetas de identificação por radiofrequência (Considerando 30, do RGPD).

Para efeitos de identificação, os dados genéticos (2-4.6) estão agora incorporados no RGPD, encontrando-se definidos no Considerando 34, «como os dados pessoais relativos às

[254] Cf. GUERRA, Amadeu – Informática e Tratamento de Dados Pessoais – os direitos dos cidadãos e as obrigações dos responsáveis pelos tratamentos automatizados. Lisboa : Vislis Editores, 1997. ISBN 972-52-0013-6. p. 22 e segs.

[255] O RGPD mantém este entendimento, no Considerando 26: «Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação».

características genéticas, hereditárias ou adquiridas, de uma pessoa singular que resultem da análise de uma amostra biológica da pessoa singular em causa, nomeadamente da análise de cromossomas, ácido desoxirribonucleico (ADN) ou ácido ribonucleico (ARN), ou da análise de um outro elemento que permita obter informações equivalentes».

2-4.4. Identidade e Autenticação

No mundo digital, os sistemas têm armazenado um volume enorme de informações exclusivamente vinculadas aos seus utilizadores e por isso tem de se antecipar e reagir ao comportamento humano de forma personalizada com o fim de proteger a sua privacidade. Pelo que, foram criados processos de autenticação que consistem no ato de provar que uma certa pessoa possui uma certa identidade e / ou está autorizada a realizar certas atividades[256]. Os processos de autenticação dependem da confiabilidade entre as partes envolvidas e geralmente são dispendiosos dependendo da natureza dos identificadores, atributos e credenciais e controles de acesso. A utilização de meios de autenticação deve respeitar a finalidade a que se destina em função do tipo de dados tratados.

A pessoa é reconhecida porque apresenta um identificador ou conjunto de identificadores cujo significado o destinatário aceita. Os testemunhos de conexão são exemplos de credenciais de identidade porque permitem a personalização da experiência do utilizador pelos prestadores de serviços que arquivam os dados de navegação, não tendo interesse pelo seu nome ou outros dados. O direito a realizar determinadas operações pode ser realizado por token[257] sem necessidade do destinatário ter conhecimento do seu portador. O controlo de acesso é o processo de controlo criado pelos prestadores de serviços que permite que cada pedido a um sistema determinar, com base nas regras específicas, se o pedido deve ser concedido ou negado.

O reconhecimento da identidade de uma pessoa tem várias abordagens que se exemplificam: (1) nas operações de pagamento cujos identificadores podem ser um código ou um PIN; (2) para contadores relativos a bens essenciais, com uma conta-cliente; (3) nos serviços em linha com um login ou ID[258]; (4) em determinados documentos a inclusão da assinatura eletrónica

[256] Por exemplo: o acesso a serviços de telecomunicações, internet, contas bancárias, acesso a subscrição de publicações em linha, etc. V. FRA, CdE, cit. 231.

[257] O *token* é um dispositivo físico que gera um identificador único temporário que é enviado ao servidor para iniciar uma sessão interativa e funciona como um testemunho de conexão. Quando um computador tem um *token*, é capaz de se comunicar com outros computadores e dispositivos na rede.

[258] ID significa Identidade e é uma sigla oriunda do original em inglês: *identity*, que nas ciências da computação e no contexto da Internet ID passou a referir-se à identidade que cada utilizador cria nos diversos dispositivos e aparelhos disponíveis no mercado. O nome do utilizador ou correio eletrónico é normalmente utilizado para a identificação pessoal na internet.

ou certificação digital; e (5) acesso a instalações de organizações através da autenticação por impressão digital[259].

2-4.5. Técnicas de proteção contra a identificabilidade

As organizações socorrem-se cada vez da tecnologia virtual e da interação com as pessoas em todos os domínios (negócio, entretenimento, investigação, *networking*…) transformando a gestão da identidade digital numa ciência. Os mecanismos mais conhecidos de proteção de dados pessoais são a anonimização, a pseudonimização, a codificação de dados, ferramentas de cifragem contra a pirataria informática, sistemas contra testemunhos de conexão e a plataforma P3P, entre outros.

2-4.5.1. Anonimização de dados

Os utilizadores da Internet não têm consciência dos riscos que correm em relação à sua privacidade sempre que estão em linha[260]. A necessidade de equilibrar os interesses económicos das organizações e o direito à proteção de dados pessoais está implícito na al) b), n.º 1, do art.º 6º e art.º 7º, da Diretiva 95/46/CE: os dados são "recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades" e nos termos do art.º 27º, do mesmo diploma, os Estados-Membros e a Comissão promoverão a elaboração de códigos de conduta para fornecer indicações sobre os meios através dos quais os dados podem ser tornados anónimos e conservados sob uma forma que já não permita a identificação da pessoa em causa[261]. A CNPD, nos termos do nº 2, do art.º 5º da LPDP, pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos, mediante requerimento do responsável pelo tratamento, e havendo interesse legítimo[262], se os dados pessoais deixarem de servir a sua finalidade inicial.

---

[259] Com interesse, o Parecer da CNPD, nº 11/2002 de 03/12 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_11_2002.pdf>, que refere que as «aplicações informáticas que permitem a identificação automática (quem sou?) ou a autenticação / escolha (sou quem digo ser?) de uma pessoa, permitindo-lhe o acesso a determinados direitos, como é o acesso a determinadas áreas, baseadas no reconhecimento de particularidades físicas como sejam a impressão digital»

[260] V. GT29 - Recomendação 3/97: O anonimato na Internet. [Em linha]. XV D/5022/97 final WP6. Brussels (Belgium), (03/12/1997). [Consult. 12 mar. 2015]. Disponível em WWW <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_pt.pdf>

[261] Considerando 26 da Diretiva 95/46/CE e § 52, al) d) do *Explanatory Memorandum* da CdE Recommendation *n.º R (97) 18 of the Committee of Ministers to Members States concerning the protection of personal data collected and processed for statistical purposes* [Em linha]. (30/09/1997) [Consult. 12 mar. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2001724&SecMode=1&DocId=578856&Usage=2>.

[262] Al) b), n.º 1, do art.º 6º, e considerandos 26 e 29 da Diretiva 95/46/CE e no mesmo sentido a Convenção 108.

A faculdade de optar pelo anonimato não é absoluta tendo em conta que é necessário ponderar que direitos fundamentais estão em jogo como a liberdade de expressão ou políticas de prevenção do crime[263].

Dados anónimos são aqueles dados que não podem ser relacionados com uma pessoa a partir dos próprios dados ou recorrendo a técnicas de combinação com outros dados (incluindo objetos) que impliquem o desenvolvimento de esforços onerosos num determinado momento. A anonimização de dados pode ser realizada através de procedimentos distintos tais como generalização, supressão da relação entre si de identificadores, encriptação ou mineração de dados.

Os princípios de proteção de dados não são aplicáveis aos dados anónimos porque não é possível identificar uma pessoa.

2-4.5.2. Pseudonimização de dados

A criação de pseudónimos[264] é outro mecanismo de proteção de dados pessoais pela sua obstaculização à identificação de pessoas. Contudo, os dados do portador do pseudónimo podem ser geridos pelos responsáveis do tratamento de dados e terceiros, em conformidade com as atividades registadas, criando por exemplo um perfil de consumidor de joias e relógios. O que releva na pseudonimização de dados é a faculdade de tratar dados sem contender com a identidade do seu titular, para salvaguardar a privacidade, sobretudo na recolha de dados sensíveis para efeitos de investigação nas ciências da saúde, proteção de testemunhas, agentes infiltrados, etc. A criação de pseudónimos na internet recorre normalmente aos procedimentos da encriptação que consiste na transformação da informação utilizando uma cifra[265] (composta por um ou mais algoritmos para cifrar e decifrar a informação) com um parâmetro denominado chave criptográfica apenas conhecida pelos responsáveis do tratamento de dados. O método de encriptação de dados é muito utilizada sobretudo no setor da saúde, como por exemplo nos ensaios clínicos, mas a reidentificação das pessoas pode não ser permitida na conceção dos protocolos. A «possibilidade de reidentificação, utilizando listas de identidades e os seus respetivos pseudónimos ou

[263] Os dados anónimos têm uma conotação obscura e normalmente associados a atos ilegais como a pedofilia, a divulgação de dados por *hackers* ou a violação de direitos de autor.

[264] Pseudónimo é uma palavra de origem grega que significa nome falso e que em termos jurídicos é um nome fictício que goza de proteção jurídica quando tenha notoriedade, nos termos do art.º 74º do CC, como pode ser o caso previsto de criação de pseudónimos, por escritores ou atores, nos termos do art.º 28º, do CDADC, embora possa ser vedado no exercício da atividade de determinadas profissões (art.º 82º, do EOROC).

[265] Em linguagem comum, um código secreto é o mesmo que uma cifra.

utilizando algoritmos de criptografia de duplo sentido»[266], estão sujeitos à legislação da proteção de dados pessoais[267].

A identidade de um pseudónimo[268] não é associada a uma determinada pessoa se não estiverem reunidas um conjunto de condições e procedimentos que interligam entre si os dados das duas identidades, por exemplo a emissão de um mandado de busca no decurso de uma investigação criminal.

2-4.5.3. Pseudonimização de dados no RGPD

A pseudonimização foi explicitamente introduzida no RGPD e é definida, na al) 5), do art.º 4º, como «o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável». Em síntese, a pseudonimização é uma técnica de reforço da privacidade. Embora esteja reconhecido que a pseudonimização «pode reduzir os riscos para as pessoas em causa» não é uma técnica para excluir os dados da aplicação de outras eventuais medidas de proteção de dados (Considerando 28, do RGPD). Os responsáveis do tratamento de dados são incentivados[269] a tomar medidas técnicas e organizativas adequadas[270], de pseudonimização desde que seja lícita, leal e transparente em relação ao titular dos dados e compatíveis com os propósitos iniciais da recolha (art.º 5º, do RGPD), salvo quando existam garantias adequadas (al) e), do n.º 4, do art.º 6º, e n.º 1, do art.º

[266] GT29, cit. 184.

[267] Parágrafo 127, do Ac. *Cisco Systems Inc.* e *Messagenet SpA*, v. Comissão Europeia, do TGUE, n.º T-79/12, de 11/12/2013 «admitindo que os utilizadores do produto da Skype constituem um grupo de consumidores comercialmente interessante, a Skype não permite que as empresas promovam ativamente a venda dos respetivos produtos junto deles. Com efeito, tal como foi indicado pela Comissão e pela interveniente, não é possível contactar os utilizadores do produto da Skype, que se servem normalmente de um pseudónimo, sem a sua autorização prévia».

[268] A pseudonimização mantém a ligação dos dados com a pessoa que através de processos baseados em informações e atributos para reidentificar a pessoa que a distingue da anonimização cujos processos destroem a capacidade de ligação (V. International Organization for Standardization - ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework* [Em linha]. 1ª ed., International Organization for Standardization, 2011. [Consult.14 out. 2016]. Disponível em WWW <https://www.iso.org/standard/45123.html>)

[269] Assim, o Considerando 29, do RGPD: «A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento e a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento.»

[270] Tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento tornando-se uma figura fundamental na proteção de dados desde a conceção.

25º, do RGPD)[271].

2-4.6. Dados sensíveis

Os dados pessoais processados de acordo com critérios e instruções previamente definidas para obter determinados resultados afetando a esfera mais íntima dos seus titulares e cuja utilização indevida podem dar origem a tratamentos ilegais, arbitrários e discriminatórios ou que podem causar aos seus titulares efeitos adversos, riscos ou prejuízos graves são considerados sensíveis. A LPDP para além de incluir as categorias indicadas no n.º 3, do art.º 35º, da CRP, no art.º 6º da Convenção 108 e do art.º 8º da Diretiva 95/46/CE entendeu ampliar a sua enumeração, considerando assim dados sensíveis os dados pessoais referentes a convicções filosóficas ou políticas[272], filiação partidária ou sindical[273], fé religiosa[274], vida privada[275] e origem racial[276] ou étnica[277], bem como o tratamento de dados relativos à saúde[278]

[271] Parece que a pseudonimização pode facilitar a abertura ao tratamento de dados para os fins que não estiveram subjacentes inicialmente.

[272] Ac. *Folgerø and Others v. Norway* do TEDH n.º 15.472/02, de 29/06/2007.

[273] Ac. *Sørensen & Rasmussen v. Denmark* do TEDH apensos n.ºs 52.562/99 e 52.620/99 de 11/01/2006.

[274] Ac. *CJ, JJ and EJ v. Poland* do TEDH n.º 23.380/94, de 16/01/1996.

[275] Ac. *Moreno Gómez v. Spain*, do TEDH n.º 4.143/02, de 16/11/2004, Ac. *Hatton and others v. The United Kingdom*, TEDH n.º 36.022/97, de 08/07/2003, Ac. do TRP n.º 648.07.2TALMG.P1, de 09/05/2012, in CJ em linha, Ac. do TC n.º 255/2002, de 12/06/2002, do Tribunal Constitucional. Os hábitos de bebida e hábito de fumador (Autorização da CNPD, n.º 845/2005, de 17/10 [Em linha]. [Consult. 13 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_845_2005.pdf>), a gravidez (Deliberação da CNPD, n.º 63/2006, de 13/02 [Em linha]. [Consult. 12 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/ bin/decisoes/Aut/10_63_2006.pdf>), o consumo de drogas (Autorização da CNPD, n.º 2/2000, de 18/01 [Em linha]. [Consult. 12 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_2_2000.pdf>), os dados biométricos (Autorização da CNPD n.º 1.123/2007, de 25/06) são exemplos que ilustram dados pessoais que se incluem na cláusula vida privada.

[276] Autorização da CNPD, n.º 7/2000, de 25/01 [Em linha]. [Consult. 19 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_7_2000.pdf>, refere que o tratamento de dados sobre a raça / etnia só será admissível nos termos aí referidos. Com interesse, a Autorização da CNPD, nº 192/2002, de 05/11 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Aut/10_192 _2002.pdf>, que permite o tratamento de dados com características físicas, como a «altura, peso, cor dos olhos, cor da pele» para candidatos num processo de recrutamento para a «área da fotografia e representação para cinema, televisão, publicidade, teatro, moda, dança e outros eventos».

[277] Ac. *Ciubotaru v. Moldova*, do TEDH n.º 27138/04, de 27/04/2010. Autorização da CNPD, nº 10/99, de 16/03 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/ Aut/10_ 10_1999.pdf> que considerou «que o dado etnia poderá ser tratado para efeitos de caracterização da população abrangida e apuramento estatístico. Esta informação, tal como se propõe, deverá ser processada de forma anonimizada».

[278] Ac. *Bodil Lindqvist*, do TJUE, nº C-101/01, de 06/11/2003. «Consideram-se dados de saúde, não só os que resultam do diagnóstico médico, como todos os outros que permitam apurá-lo». Segundo CASTRO, cit. 38, p. 91) e devido às suas particularidades, o nº 5 do art.º 11º, da LPDP prevê que o direito de acesso à informação, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados ou os seus herdeiros (Deliberação da CNPD, n.º 94/2001, de 15/07 [Em linha]. [Consult. 29 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/2001/htm/del/del094-01.htm>). A proteção dos dados médicos abrange os dados do feto ainda que os interesses da mãe devam ser tidos em conta tanto físico como mentais, e aplica-se ao passado, presente e futuro do seu titular (n.ºs 4.5 e 4.6 e parágrafos 5, 14 e 37 do *Explanatory Memorandum* da *Recommendation n.º R (97) 5 of the Committee of Ministers to Members States on the protection of medical data* [Em linha]. (13/02/1997) [Consult. 9 abr. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.mdBlobGet&InstranetImage=564487

e à vida sexual[279], incluindo os dados genéticos[280]. Portugal entendeu exercer o seu poder discricionário no que diz ao alargamento do tipo de dados e atividades de processamento para melhor adaptação à realidade envolvente da cultura e atitudes do público em geral (Diretrizes da Privacidade) mais entendendo que não impedia a harmonização das legislações europeias)[281]. Atualmente os dados sensíveis tipificados nos distintos instrumentos nacionais ou internacionais da proteção de dados não podem ser considerados universais pelo que as legislações dos Estados-Membros devem adequar o seu quadro regulamentar ao contexto tecnológico em que se inserem[282].

Os dados sensíveis exigem proteção reforçada daí que seja proibido o seu tratamento sistemático e automático com recurso a dispositivos eletrónicos. As derrogações à proibição dependem do consentimento expresso do titular dos dados autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis (art.º 35, da CRP) ou da autorização da CNPD por motivos de interesse público (n.º 2, do art.º 7º da LPDP).

Entende-se que a apreciação da natureza do dado sensível depende do tratamento automático que lhe é dado, por exemplo: um enfermeiro que presta apoio domiciliário a um idoso com a doença de Alzheimer incluindo a compra do medicamento com o seu cartão de débito e que o banco utiliza para construir o seu perfil de compras está a tratar dados sensíveis. A conexão entre o comprador e o produto não parece evidente dado que há uma aquisição por conta de outrem. O dado que originariamente não é sensível que depois de recolhido e tratado tem um determinado valor económico pode transformar-se em dado sensível dependendo da natureza da sua comunicação, isto é, o enfermeiro que mais tarde se dirige ao banco para celebrar um contrato de mútuo para aquisição de habitação poderá ser confrontado com a recusa da celebração de um contrato de seguro associado ao mútuo devido à doença que foi incluída no seu perfil[283].

Os dados relativos a pessoas suspeitas de atividades ilícitas, infrações penais,

---

&SecMode=1&DocId=560582&Usage=2.

[279] Ac. *Stübing v. Germany*, do TEDH nº 43547/08, de 12/04/2012.

[280] Ac. *S. and Marper v. The United Kingdom*, do TEDH n.º 30562/04, de 04/12/2008. Os dados genéticos para além de ser utilizados por razões de saúde, diagnóstico ou razões de prevenção (CdE, *Recommendation n.º R (92) 03 of the Committee of Ministers to Members States on genetic testing and screening for health care purposes* [Em linha]. (10/02/1992) [Consult. 9 abr. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command>; e Autorização da CNPD n.º 9/2000, de 25/01 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Aut/10_9_2000.pdf>) podem ser utilizados para outros fins como determinar a paternidade ou origem étnica de uma pessoa.

[281] A doutrina refere-se à adoção de uma linha aberta (cf. GUERRA, cit. 253 e v. PINHEIRO, cit. 52).

[282] V. *Explanatory Memorandum* das Linhas Diretrizes da Privacidade.

[283] Com interesse Ac. do TRP n.º 585/11.6PAOVR.P1, de 24/04/2013, *in* www.dgsi.pt.

contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias, nos termos do n.º 1, do art.º 8º da LPDP são dados sensíveis cujo processamento automático depende de atribuição de competência prevista na lei, com prévio parecer da CNPD.

CAPÍTULO V – CONSIDERAÇÕES GERAIS SOBRE AS ATIVIDADES DE MARKETING E OS DIREITOS DOS TITULARES DE DADOS PESSOAIS

3-5. Marketing

Marketing[284] é o processo pelo qual as empresas criam valor para o cliente e constroem fortes relacionamentos com o mesmo para capturar o seu valor em troca[285]. O relacionamento dos operadores económicos com o destinatário cujo objetivo é convertê-lo em consumidor dos seus produtos e serviços, é relevante no que respeita à proteção de dados pessoais. As estratégias de marketing tiveram uma evolução extraordinária nos últimos anos não só devido aos suportes tecnológicos inovadores para veicular a informação como devido às possibilidades de rastreamento do comportamento do consumidor pelos operadores económicos em ambientes inteligentes e tudo à escala global.

Os operadores já terão recolhido as informações necessárias dos destinatários para endereçar-lhe mensagens publicitárias, utilizando diversos suportes de informação quer materiais quer virtuais, recorrendo a técnicas de segmentação prévia. A publicidade[286], intimamente ligada

[284] Marketing é uma palavra inglesa que se impôs no seio da língua portuguesa, traduzida por mercadologia e definida como o "estudo das atividades comerciais que, a partir do conhecimento das necessidades e da psicologia do consumidor, tende a dirigir os produtos, adaptando-os, para o seu melhor mercado; estudo de mercado" (v. PRIBERAM INFORMÁTICA, S.A. - Marketing. In FLIP 10. - Dicionário Priberam de Língua Portuguesa contemporânea. [Em linha]. [Consult. 1 dez. 2016]. Módulo de software.

[285] V. GRÖNROOS, Christian – *Service Managment and Marketing*. 3ª ed., West Sussex (England) : John Wiley & Sons Ldt , 2007. ISBN 978-047-0028-62-9.

[286] O conceito de publicidade não é uniforme na legislação nacional, de facto, nos termos do art.º 3º, do Código da Publicidade, com a alteração dada pelo DL n.º 6/95, de 17/01, considera-se publicidade qualquer forma de comunicação feita por entidades de natureza pública ou privada, no âmbito de uma atividade comercial, industrial, artesanal ou liberal, com o objetivo direto ou indireto de: (a) promover, com vista à sua comercialização ou alienação, quaisquer bens ou serviços; e (b) promover ideias, princípios, iniciativas ou instituições, e o art.º 20º, da L n.º 7/2004, de 07/0, não define publicidade mas refere o que não está incluído no conceito de publicidade em rede, ou seja, as mensagens que se limitem a identificar ou permitir o acesso a um operador económico ou identifiquem objetivamente bens, serviços ou a imagem de um operador, em coletâneas ou listas, particularmente quando não tiverem implicações financeiras, embora se integrem em serviços da sociedade da informação, e as mensagens destinadas a promover ideias, princípios, iniciativas ou instituições, que resultam da definição de comunicação comercial prevista na al) f), do art.º 2º, da Diretiva 2000/31/CE como todas as formas de comunicação destinadas a promover, direta ou indiretamente, mercadorias, serviços ou a imagem de uma empresa, organização ou pessoa que exerça uma profissão regulamentada ou uma atividade de comércio, indústria ou artesanato. Não constituem comunicações comerciais as informações que permitam o acesso direto à atividade da sociedade, da organização ou da pessoa, nomeadamente um nome de área ou um endereço de correio eletrónico, e as comunicações relativas às mercadorias, aos serviços ou à imagem da sociedade, organização ou pessoa, compiladas de forma imparcial, em particular quando não existam implicações financeiras. Para efeitos deste texto considera-se as comunicações publicitárias em rede «destinadas a promover, direta ou indiretamente, mercadorias, serviços ou a imagem de uma empresa, organização ou pessoa que exerça uma profissão regulamentada ou uma atividade de comércio, indústria ou artesanato» nos termos da Diretiva 2000/31/CE. Por outro lado, O conceito de marketing direto é mais amplo do que o conceito de publicidade, ou seja as expressões "marketing direto" e "comunicações publicitárias" não são coincidentes. *(Vide* a definição constante do Considerando 32, a proposta de Regulamento do Parlamento Europeu e do Conselho, relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas), apresentada pela

ao marketing, assume, nos dias de hoje, uma importância e um alcance significativos, quer no domínio da atividade económica, quer como instrumento privilegiado do fomento da concorrência, e tanto assim é, que está regulada pelo DL n.º 330/90, de 23/10[287], que aprova o Código da Publicidade e com vista a uma maior proteção da privacidade e dos dados pessoais, o DL n.º 7/2004, de 07/01[288], regula as comunicações publicitárias em rede e introduz a problemática das comunicações não solicitadas estabelecendo que as comunicações para fins de marketing direto apenas podem ser autorizadas em relação a destinatários que tenham dado o seu consentimento prévio (art.ºs 1º e 13º).

O marketing direto[289] é uma forma de angariar e manter clientes e, ao fazê-lo, atender às necessidades dos clientes e da organização que os acompanha. Para tanto, a sua atividade é sustentada numa estrutura baseada essencialmente em três atividades: (1) numa base de dados que armazena e analisa toda a informação recolhida das pessoas em causa: (2) na utilização do conhecimento extraído da base de dados para definir as estratégias de implementação da comunicação, incluindo a escolha dos canais de comunicação; para (3) comunicar com as pessoas em causa com a maior personalização possível. O marketing direto foca-se no relacionamento com as pessoas em causa e não em bens e serviços promovidos pelas organizações, pelo que, a atividade de marketing é um dos setores com maior índice de risco no que respeita ao cumprimento da LPDP[290].

Comissão Europeia, de 10/01/2017, que define marketing direto como «a qualquer forma de publicidade através da qual uma pessoa singular ou coletiva envia diretamente comunicações comerciais diretas a um ou mais utilizadores finais identificados ou identificáveis através da utilização de serviços de comunicações eletrónicas. Para além da oferta de produtos e de serviços para fins comerciais, deve incluir igualmente as mensagens enviadas pelos partidos políticos que contactam pessoas singulares através de serviços de comunicações eletrónicas para promover os seus partidos. O mesmo deverá aplicar-se às mensagens enviadas por outras organizações sem fins lucrativos para apoiar os objetivos da organização».

[287] Entrou em vigor no continente a 24/10/1990, sofreu treze modificações legislativas, tendo sido a última operada pelo DL n.º 66/2015, de 29 de abril, que estabelece o regime jurídico dos jogos e apostas em linha e altera o Código da Publicidade.

[288] DL n.º 7/2004, de 07/01, transpõe para a ordem jurídica interna a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 08/06/2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Diretiva sobre Comércio Eletrónico) bem como o artigo 13.º da Diretiva n.º 2002/58/CE, de 12/07/2002, relativa ao tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à Privacidade e às Comunicações Eletrónicas). Entrou em vigor no continente a 12/01/2004 e nas Regiões Autónomas dos Açores e da Madeira a 22/01/2004, tendo sido altera pelo DL n.º 62/2009, de 10/03 e pela L n.º 46/2012, de 29/08.

[289] A versão portuguesa de numerosos documentos emitidos pelos organismos da EU tem traduzido a expressão de marketing direto por comercialização direta. Para efeitos, deste trabalho mantêm-se o o termo em inglês de marketing direto, com expressão e aceitação no sistema jurídico nacional.

[290] Conforme referido em GALEAN, Llanos Manzanares; CHINCHURRETA, Koldo Peciña - *Implicaciones de la protección de datos en el marketing* [Em linha]. In MK Marketing+Ventas, n.º 199, [feb. 2005]. [Consult. 13 mar. 2015]. Disponível em WWW <http://pdfs.wke.es/8/7/8/6/ pd0000018786.pdf>.

3-5.1. O sistema de gestão de relacionamento com o cliente

Com os sistemas de gestão de relacionamento[291] dos operadores económicos com o cliente no que respeita à recolha de dados pessoais e informação sobre as suas atividades do cidadão passamos a viver numa sociedade da classificação[292] e do cidadão transparente[293], na medida em que o registo das interações disponíveis para todos os departamentos da organização permite guiar a tomada de decisões, a nível estratégico e operacional de forma muito procedimental e analítica.

Hoje em dia as novas formas de comunicar e distribuir informação são essencialmente eletrónicas e baseadas na internet cuja infraestrutura está alicerçada nos dados pessoais. Os operadores económicos têm necessidade de obter informação pessoal para alcançar os seus propósitos e recorrem a programas de espionagem que podem ser maliciosos para a obtenção de dados e lucros ou apenas com vista à captura de informação, que independentemente da legalidade da sua utilização, se indicam os seguintes exemplos: vírus, endereços de remetentes falsificados (*spoofing*), testemunhos de conexão (*cookies*), comunicações não solicitadas, identificadores ocultos (*hidden identifiers*), gráficos espiões (*web bugs*), rastreadores da internet (w*eb crawlers* e os seus derivados como os *web spiders*, *web robot*, ou w*eb scutter*…), programas-espiões (*spyware),* ciber-iscagem *(phishing* e os seus derivados como o *scam, smishing, vishing*…) *ransomware, trojan, keylogger, adware, scareware, pharming, scavenging*[294], etc.

3-5.2. Os direitos dos titulares dos dados pessoais

Os sistemas de gestão de relacionamento incluem ficheiros de dados pessoais em suporte físico ou virtual que passam a ser objeto de regulação cada vez mais restrita. Os titulares de dados pessoais conquistam direitos sobre o seu conteúdo: o direito de informação e acesso aos dados incorporados em ficheiros ou bases de dados, corrigi-los, apagá-los, bloqueá-los ou opor-se à utilização dos seus dados para fins de marketing (L n.º 6/99, de 27/01, que regula a publicidade domiciliária por telefone e por telecópia, a L n.º 41/2004, de 18/08 e a Diretiva n.º

[291] O CRM, sigla oriunda do original em inglês *Customer Relationship Management*, com tradução portuguesa como Gestão de Relacionamento com o Cliente, é um software que inclui um conjunto de processos e tecnologias para recolha de dados pessoais (na interpretação do conceito de dados pessoais nos capítulos anteriores) e retenção em ficheiros estruturados que permite a identificação e compreensão do perfil dos seus titulares. O objetivo do CRM é a gestão do relacionamento com o cliente antecipando as suas necessidades.

[292] V. RODOTÀ, cit. 50, p. 111 e segs.

[293] REIDENBERG, Joel R. - *The Transparent Citizen* [Em linha]. *In Loyola University Chicago Law Journal*, Vol. 47, (2015), Fordham Law Legal Studies Research Paper No. 2674313. [Consult. 12 jun. 2016]. Disponível em WWW <https://ssrn.com/abstract=2674313>

[294] Mantém-se as expressões em inglês na medida em que são termos técnicos da ciência da computação e com significados de difícil tradução em português.

2002/58/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações, a LPDP, a CDFUE, o RGPD e a CRP).

3-5.2.1. O direito de informação

O titular dos dados deve ter direito a um conjunto mínimo de informações sobre os fins para os quais os seus dados pessoais serão tratados. O direito à informação está previsto na al) a), do art.º 8º, da Convenção 108, art.ºs 10º e 11º, da Diretiva 95/46/CE e art.º 10º da LPDP, e agora regulado nos art.ºs 13º e 14º do RGPD.

O direito do titular de ser informado nasce do dever que o responsável pelo tratamento tem de informar, pelo que o desenvolvimento sobre esta matéria será realizado no ponto 3-7.2.1.

3-5.2.2. O direito de acesso

O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições[295], a confirmação de serem ou não tratados dados que lhe digam respeito, não só à data da solicitação mas também no que respeita ao passado[296], bem como informação de forma inteligível sobre as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados, bem como a fonte de recolha (al) a) e b), do n.º 1, do art.º 11º, da LPDP, al) a), do art.º 12º, da Diretiva 95/46/CE, n.º 1, do art.º 35º, da CRP, al) b) do art.º 8º da Convenção 108 e nº 2, do art.º 8, da CDFUE). O direito de acesso é, igualmente, uma garantia para que o titular dos

[295] Neste sentido, o Ac. *Haralambie* v. *Roménia*, do TEDH, n.º 21.737/03, de 27/01/2010, decidindo que o responsável pelo tratamento não cumpriu a obrigação positiva que lhe incumbia de fornecer ao requerente um procedimento efetivo e acessível que lhe permitisse obter o acesso ao seu processo pessoal num prazo razoável, com todas as informações relevantes e apropriadas, não podendo a quantidade de ficheiros transferidos ou as insuficiências do sistema de arquivos pudessem, por si só, justificar um atraso de mais de seis anos pelas instituições em causa na concessão do pedido do requerente; e também, Ac. K.H. e outros v. *Slovakia*, do TEDH, n.º 32.881/04, de 06/11/2009, em que foi declarado que o Estado não pode recusar às requerentes o acesso e de fazer cópias dos registos médicos hospitalares, com fundamento na necessidade de proteger informações relevantes de abusos.

[296] Neste sentido: «…o artigo 12.°, al) a), da Diretiva 95/46/CE (...) determina que os Estados-Membros garantirão um direito de acesso à informação sobre os destinatários ou categorias de destinatários e sobre o conteúdo da informação comunicada não apenas relativamente ao presente mas também no que respeita ao passado. Cabe aos Estados-Membros fixar o prazo durante o qual essa informação deve ser conservada e o acesso correlativo a esta que representem um equilíbrio justo entre, por um lado, o interesse da pessoa em causa em proteger a sua vida privada, designadamente através das vias de intervenção e de recurso previstas pela Diretiva 95/46, e, por outro, o ónus que a obrigação de conservar essa informação representa para o responsável pelo tratamento», conforme Parágrafo n.º 70, do Ac. *College van burgemeester en wethouders van Rotterdam* v. *M. E. E. Rijkeboer*, do TJUE, n.º C-533/07, de 07/05/2009. Em sentido contrário: «…o artigo 13.°, n.° 1, da Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, deve ser interpretado no sentido de que os Estados-Membros não têm a obrigação, mas a faculdade, de transporem para o seu direito nacional uma ou várias das exceções que este artigo prevê à obrigação de informar as pessoas em causa sobre o tratamento dos respetivos dados pessoais», conforme Parágrafo 55, do Ac. *Institut professionnel des agents immobiliers (IPI)* v. *Geoffrey Englebert*, do TJUE, n.º C-473/12, de 07/11/2013.

dados possa exercer o seu direito de oposição ao tratamento de dados pessoais ou o direito de recurso quando sofra um prejuízo[297].

O direito de acesso pode ser restringido em casos expressamente previstos na lei[298] e nos casos em que manifestamente não exista qualquer perigo de violação dos direitos, liberdades e garantias do titular dos dados, designadamente do direito à vida privada, e os referidos dados forem exclusivamente utilizados para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas. (n.º 6, do art.º 11, da LPDP, art.º 13, da Diretiva 95/46/CE e art.º 9, da Convenção 108).

O RGPD reforça o direito de acesso aos dados que fundamenta no conhecimento e verificação da legalidade do tratamento (Considerando 63, do RGPD), pois para além das informações previstas na LPDP e na Diretiva 95/46/CE, o titular dos dados tem direito a uma cópia dos dados pessoais em fase de tratamento e às seguintes informações: (a) o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; (b) o direito de apresentar reclamação a uma autoridade de controlo; (c) a existência de decisões automatizadas, incluindo a definição de perfis, e as informações úteis relativas à lógica subjacente[299], bem como a importância e as consequências previstas de tal tratamento para o titular dos dados; (d) quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas. O direito de acesso, também, pode ser restringido pelo direito da EU ou

[297] A recusa de acesso pelo titular dos dados ao registo policial a que teve acesso a entidade empregadora e que constitui fundamentos distintos aos requerentes o convite à demissão, transferência de posições e congelamento de promoções, constituíram um prejuízo nas carreiras profissionais e uma violação ao respeito da vida privada e uma restrição das suas liberdades políticas nos termos dos art.º 10º, 11º, e 13º da CEDH, conforme decisão no Ac. *Segerstedt- Wiberg e* outros *v. Suécia, do TEDH* de 06/06/2006, n.º 62.332/00.

[298] O direito de acesso pelo titular dos dados de forma direta pode estar sujeito a restrições e ser exercido através da CNPD ou de outra autoridade independente a quem a lei atribua a verificação do cumprimento da legislação de proteção de dados pessoais, nomeadamente, se a comunicação dos dados ao seu titular puder prejudicar a segurança do Estado, a prevenção ou a investigação criminal ou ainda a liberdade de expressão e informação ou a liberdade de imprensa, a CNPD limita-se a informar o titular dos dados das diligências efetuadas, ou por intermédio de médico escolhido pelo titular dos dados no acesso à informação relativa a dados da saúde, incluindo os dados genéticos, etc. (n.º 2 e seguintes, do art.º 11º, da LPDP).

[299] A construção de perfis pode resultar de uma técnica ou algoritmos sujeita a proteção intelectual devido não só ao seu valor económico como aos benefícios que reporta à organização e por isso faz parte do segredo do negócio. Trata-se de conhecimento tecnológico que deve ser protegido sob pena de espionagem comercial. O segredo do negócio está protegido pelo direito interno e da EU, pelo que o exercício do direito de acesso deve merecer cautelas e ser conciliado com outros direitos do ordenamento jurídico (que se pode ilustrar com alguns exemplos regulados: o art.º 318º, do CPI considera a utilização de segredos de negócios de um concorrente, sem o consentimento do mesmo, um ato ilícito, nos termos aí previstos; o art.º 30º da L n.º 19/2012, de 08/05, que aprova o novo regime jurídico da concorrência, protege o segredo de negócio, a Diretiva 2016/943/UE do Parlamento Europeu e do Conselho, de 08/06/2016, relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais, entre outros)

dos Estados-Membros desde que respeitem as exigências estabelecidas na CDFUE e na CEDH. (Considerando 73, do RGPD).

O RGPD permite explicitamente que o responsável pelo tratamento possa exigir dos interessados para exercer os seus direitos de acesso, retificação, apagamento e oposição, prova de identidade para executar os seus direitos, com o objetivo de diminuir o risco de terceiros obterem acesso ilícito a dados pessoais, contudo, não os obriga a investigar ou procurar as informações necessárias para identificação dos titulares dos dados.

A CNPD pode autorizar a cobrança[300] de um valor não excessivo pelo responsável do tratamento de dados (al) h), do n.º 1, do art.º 23º, da LPDP). O RGPD prevê que o responsável pelo tratamento deve fornecer a informação de forma gratuita, contudo, pode exigir o pagamento de uma taxa razoável[301] tendo em conta os custos administrativos, quando o pedido é manifestamente infundado ou excessivo, especialmente se é repetitivo (art.º 15, do RGPD).

3-5.2.3. O direito de retificação

O direito de retificação (al) d), do n.º 1, do art.º 11º, da LPDP, al) b), do art.º 12º, da Diretiva 95/46/CE, al) c) do art.º 8.º da Convenção 108), resulta dos princípios da atualização e da qualidade dos dados (al) d), do n.º 1, do art.º 5º e al) g), do n.º 1, do art.º 23º, da LPDP, e (al) d), do n.º 1, do art.º 6º, da Diretiva 95/46/CE) com fundamento na inexatidão ou incompletude[302] dos dados.

O direito de retificação está regulado nos art.ºs 16º e 19º, do RGPD, prevendo-se, agora, que o responsável pelo tratamento deve fornecer ao titular dos dados as informações sobre as medidas tomadas, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido, podendo ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos (n.º 3, do art.º 12 e art.º 19º, do RGPD)[303].

O responsável do tratamento de dados poderá exigir prova, para aceitar o pedido de

[300] V. Parecer da CNPD, n.º 16/2005, de 24/05 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_16_2016.pdf>, dado ao Banco de Portugal sobre a exigência de uma taxa moderadora na prestação de informação por escrito aos beneficiários de um crédito e Autorização da CNPD, n.º 1102/2010, de 15/03 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Aut/10_1102_2010.pdf>, concedida à Vodafone para cobrança de um determinado valor pela disponibilização de uma cópia em suporte durável de gravação de chamadas.

[301] O princípio n.º 15, das Diretrizes da Privacidade, sugere a fixação de um preço não excessivo e eventual pela disponibilização da informação de dados pessoais em ficheiros, a pagar pelo titular.

[302] O TEDH, no Ac. *Cemalettin Canli v. Turquia*, n.º 22.427/04, *de* 18/11/2008, considerou que os registos sobre as pessoas devem conter não apenas a acusação deduzida mas também o resultado do processo relacionado com as acusações.

[303] A introdução de prazos específicos no âmbito do GDPR agrava as condições para o cumprimento das obrigações dos responsáveis pelo tratamento de dados.

retificação e dentro de limites razoáveis, ao titular dos dados[304].

3-5.2.4. O direito ao apagamento ou bloqueio de dados

O titular dos dados tem o direito de solicitar ao responsável pelo tratamento o apagamento ou a eliminação dos seus dados no sentido de que o responsável cessa a utilização dos mesmos, com fundamento na inexatidão, alteração das finalidades para que forem recolhidos ou tratados posteriormente[305], e ainda, por razões ponderosas e legítimas relacionadas com a sua situação particular dos dados conservados para além do prazo legalmente previsto (al) e), do n.º 1, e n.º 2, do art.º 5.º da LPDP). O apagamento dos dados implica que o tratamento de dados está impedido salvo para apuramento de eventuais responsabilidade e colocados à disposição, por exemplo, dos órgãos administrativos[306] ou judiciais durante o prazo de prescrição de qualquer ilícito contraordenacional ou criminal.

O RGPD prevê e alarga o âmbito do direito de apagamento, também denominado como o direito de ser esquecido[307], nos termos da epígrafe no art.º 17º, embora não seja considerado um direito absoluto, na medida em que será realizado pelo responsável do tratamento desde que as medidas que se afigurarem razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, e cujo pedido está sujeito à verificação de

---

[304] Os entraves à retificação dos dados em documento de identificação com fundamento na origem étnica podem configurar uma violação no acesso à vida privada quando são exigidos requisitos com fundamento subjetivo e não fundamentado, conforme Ac. *Ciubotaru v. Moldávia,* do TDEH, n.º 27.138/04, de 27/04/2010, e ainda, a recusa de oportunidade de retificar as informações recolhidas e armazenadas em ficheiros secretos, conforme o Ac. *Rotaru v. Roménia*, do TEDH, n.º 28.341/95, de 04/05/2000.

[305] A manipulação indiscriminada de dados pessoais incorporados num ficheiro representa uma violação às normas previstas na LPDP, conforme Ac. do TCAS, n.º 06895/03, de 08/11/2007.

[306] *V.* Deliberação da CNPD, nº 165/2001, de 13/11 [Em linha]. [Consult. 24 Mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Delib/20_165_2001.pdf>, sobre o bloqueamento de dados cujo tratamento tinha como finalidade existência de programa de fidelização baseada em cartões de cliente e a Deliberação da CNPD, nº 1205/2000, de 04/06 [Em linha]. [Consult. 29 mar. 2015]. Disponível em WWW <https://www. cnpd.pt/bin/decisoes/Delib/20_1205_2000.pdf>, quanto ao bloqueio temporário dos tratamentos relativos ao cartão jovem da Câmara Municipal de Valongo.

[307] *V.* Ac. *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), e Mario Costeja González*, do TJUE, do TJUE, n.º C 131/12, de 13/05/2014, com enorme impacto no direito ao acesso de dados pessoais, para além da colisão entre as políticas e procedimentos das empresas dos motores de busca com as políticas socioeconómicas da EU e países terceiros. O direito a ser esquecido não é uma questão nova na jurisprudência (recorde-se que o Tribunal do Estado da Califórnia considerou que todos tem direito à felicidade e a garantia de reparar os erros do passado e por isso não se pode atacar a reputação das pessoas, conforme decidido em *Melvin vs. Reid*, em 1931, devido à produção de um filme - O Kimono Vermelho – em que retratava a vida de ex-prostituta acusada de homicídio e absolvida (PROSSER, cit. 54) e o Tribunal de Paris, considerou que as reminiscências da vida privada de um indivíduo fazem parte de seu capital moral e que ninguém tem o direito, mesmo de boa fé, de publicá-las sem a autorização clara e explícita da pessoa cuja vida está sendo relatada como se fosse a própria, conforme o Ac. *Marlene Dietrich v. Société France-Dimanche Subsequent Developments, Cour d'Appel*, disponível em <https://law.utexas.edu/transnational/foreign-law-translations/ french/case.php?id=1254)>, mas ganhou uma relevância sem precedentes no contexto virtual. A regulação do direito a ser esquecido resulta das características da internet no que respeita à comunicação e à universalização da informação, porque a internet não esquece nem deixa que outros se esqueçam.

uma das seguintes circunstâncias, em que: (a) os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; (b) há uma cessão do consentimento; (c) há oposição ao tratamento sem que existam interesses legítimos prevalecentes que justifiquem o tratamento; (d) existe um tratamento ilícito; (e) é necessário o cumprimento de uma obrigação legal; e (f) os dados foram recolhidos no contexto da oferta de serviços da sociedade da informação dirigida a uma criança. O responsável pelo tratamento pode recusar um pedido de apagamento, quando o tratamento se revele necessário para: (a) o exercício da liberdade de expressão e de informação; b) o cumprimento de uma obrigação legal; (c) satisfazer uma obrigação legal para o desempenho de uma tarefa de interesse público ou exercício da autoridade pública; (d) fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos; ou (e) o exercício ou defesa de um direito num processo judicial. (Considerandos 65 e 66, art.ºs 17º e 19º, do RGPD) (3-7.4.). O RGPD cria um direito ao apagamento mais amplo do que o direito de que dispõem os titulares dos dados ao abrigo da Diretiva 95/46/CE e da LPDP, pelo que as organizações enfrentam um espetro mais amplo de solicitações pelos titulares dos dados.

3-5.2.5. O direito de oposição

O titular dos dados tem o direito de, com base em razões preponderantes e legítimas relacionadas com a sua situação específica, se opor ao tratamento dos dados que lhe dizem respeito (al) a) do art.º 12º, da LPDP, Considerando 45 e al) a), do art.º 14º, da Diretiva 95/46/CE), salvo disposição legal em contrário (art.º 6º, da LPDP e art.º 7º, da Diretiva 95/46/CE). O direito de oposição está estreitamente ligado aos casos em que não foi necessário obter o consentimento do interessado para o seu tratamento. As disposições legais distinguem expressamente três situações para o exercício do direito de oposição ao tratamento dos dados e em qualquer momento:

1) O direito de oposição devido à situação particular da pessoa em causa, com fundamento em razões ponderosas[308], e que o responsável pelo tratamento deve ponderar a solução caso a caso e em concreto, para interromper o tratamento de dados[309].

[308] V. o Ac. *Heinz Huber v. Bundesrepublik Deutschland*, do TJUE, n.º C 524/06, de 16/12/2008, em que há «que interpretar o art.º 12º, primeiro parágrafo, no sentido de que se opõe à instauração, por um Estado-Membro, de um sistema de tratamento de dados pessoais específico para os cidadãos da União que não são nacionais desse Estado-Membro, com o objetivo de combater a criminalidade»; e o Ac. *M.S. v. Suécia*, do TEDH, n.º 20.837/92, de 27/08/1997, em que foram comunicados dados de saúde médicos sem consentimento e sem a possibilidade de oposição, por uma companhia de seguros a uma entidade pública.
[309] CASTRO, cit. 38, p. 254.

2) O direito de oposição a decisões individuais automatizadas[310], salvo as exceções previstas[311], destinadas a avaliar determinados aspetos da sua personalidade, designadamente o desempenho e capacidade profissional, o seu crédito[312], a confiança de que é merecedora ou o seu comportamento (art. 13º, da LPDP, art.º 15º, da Diretiva 95/46/CE). O RGPD estabelece garantias às pessoas singulares contra o risco de uma decisão automatizada ser potencialmente prejudicial, devendo o responsável pelo tratamento aplicar medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão (art.ºs 9º e 22º, do RGPD). As decisões automatizadas estão intrinsecamente ligadas à construção de perfis que o RGPD define como qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações (n.º 4, do art.ºs 4, do RGPD)[313].
3) O direito de oposição à utilização para fins de marketing direto (al) b), do art.º 12º, da LPDP, al) b), do art.º 14º, da Diretiva 95/46/CE).

A Diretiva 95/46/CE e a LPDP permitem que os responsáveis pelo tratamento continuem a tratar de dados pertinentes salvo se o seu titular demonstrar que não se justifica. O RGPD vem inverter o ónus da prova e o responsável pelo tratamento que cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial (Considerandos 50, 59, 69, 70 e 73 art.º 21, do RGPD).

---

[310] V. CdE *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, cit. 82.

[311] As exceções estão previstas no art.º 15º, da Diretiva 95/46/CE e n.ºs 2 e 3, do art.º 13, da LPDP, ou seja, a pessoa pode ficar sujeita a uma decisão automatizada (1) desde que 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; (2) existam medidas adequadas que garantam a defesa dos seus interesses legítimos, designadamente o seu direito de representação e expressão; e (3) quando a CNPD o autorize, definindo medidas de garantia da defesa dos interesses legítimos do titular dos dados. O RGPD mantém os mesmos fundamentos, e ainda, prevê outro fundamento, se for baseada no consentimento explícito do titular dos dados, conforme al) c), do n.º 1, do art.º 22ª, do RGPD.

[312] Por exemplo, a proibição do *credit scoring* que consiste na «atribuição ou denegação automática de crédito pessoal, consoante a pessoa que solicita esse crédito responde ou não a certa características pessoais ou profissionais, previamente definidas no programa do computador» (CASTRO, cit. 38, p. 252).

[313] De acordo com o plano de trabalho do GT29 serão publicadas as diretrizes sobre a elaboração de perfis, em 2017.

3-5.2.6. O direito de oposição para fins de marketing direto

Nos termos da al) b, do art.º 12º, da LPDP, o titular dos dados pode opor-se, gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de marketing direto[314] ou a qualquer outra forma de prospeção, por exemplo, as relacionadas com a publicidade domiciliária, designadamente por via postal, distribuição direta, telefone ou telecópia, (n.º 1 do art.º 4º e n.º 2, do art.º 5º, da L n.º 6/99, de 27/01); e ainda de ser informado, antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de marketing direto ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações.

O direito de oposição à utilização posterior dos dados para efeitos de marketing direto não está sujeito a objeções nem a fundamentos para ser recusado.

Os ficheiros de não receção de comunicações comerciais não solicitadas[315], ou listas *Robinson*, incorporam uma lista de interessados que não desejem receber de comunicações para fins de marketing direto[316] ou outras formas de prospeção[317]. Os ficheiros podem

---

[314] V. CdE *Recommendation n.º R(85) 20 on the protection of personal data used for the purposes of direct marketing*, cit. 81, já reconhecia o direito de oposição ao tratamento de dados para efeitos de marketing.

[315] Note-se que os ficheiros de não receção de comunicações comerciais não solicitadas, são ficheiros de dados pessoais que obedecem aos princípios preconizados na LPDP, Diretiva 46/95/CE, CDFUE e Convenção 108.

[316] A lei portuguesa indica, designadamente através da utilização de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares, conforme o n.º 1, do art.º 13ºB, da L n.º 41/2004, de 18/08. A al) h), do art.º 2º, da Diretiva 2002/58/CE, define correio eletrónico como qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que pode ser armazenada na rede ou no equipamento terminal do destinatário até o destinatário a recolher, vindo o GT29, indicar que a definição tem um sentido lato e é exemplificativo, na medida em que de pretende proporcionar a proteção de dados pessoais e da privacidade aos utilizadores de serviços de comunicações publicamente disponíveis e independentemente das tecnologias utilizadas (Considerando 4, da Diretiva 2002/58/CE). Assim os serviços, sujeitos a revisão em função dos desenvolvimentos tecnológicos, abrangidos atualmente pela definição de correio eletrónico incluem: correio SMPT (*Simple Mail Transport Protocol*); serviço de mensagens curtas ou "SMS" (Considerando 40 da Diretiva 2002/58/CE); serviço de mensagens multimédia ou "MMS"; mensagens deixadas em atendedores de chamadas; sistemas de serviços de mensagens vocais, incluindo nos serviços da rede móvel; comunicações enviadas pela Internet e transmitidas diretamente para um endereço IP; e os boletins informativos enviados por correio eletrónico (v. GT29 - Parecer 5/2005 sobre as comunicações não solicitadas para fins de comercialização no âmbito do Artigo 13.º da Diretiva 2002/58/CE. [Em linha]. 11601/PT, WP 90. Brussels (Belgium), 27/02/2004. [Consult. 16 Fev. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp90_pt.pdf>).

[317] As aplicações de comercialização do *Bluetooth* poderiam configurar uma tecnologia similar (v. GT29, Parecer 1/2009 sobre as propostas de alteração da Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (diretiva da privacidade eletrónica) [Em linha]. 00350/09/PT GT 159. Brussels (Belgium), (10/02/2009). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp159_pt.pdf>, 2009) e as comunicações por *wireless* (cf. OCDE - Anti-Spam Regulation. [Em linha]. OECD 2005 DSTI/CP/ICCP/SPAM(2005)10/FINAL [Consult. 10 Nov. 2015]. Disponível em WWW <https://www. oecd.org/sti/ieconomy /35670414.pdf>).

diferenciar-se em três modalidades:

a) A lista *Robinson*, também conhecida por lista de oposição ou lista de registo negativo, que registam os nomes de pessoas singulares e coletivas (associados com dados de endereços de correio postal e eletrónico e números de telefone e telefax), que é mantida e atualizada pelos responsáveis pelo tratamento de dados dos operadores económicos que promovam o envio de comunicações para fins de marketing direto ou outras formas de prospeção, dos seus produtos ou serviços ou por conta de terceiros.
b) A lista *Robinson*, também denominada por lista de oposição ou lista comum de exclusão, que a Associação Portuguesa de Marketing Direto, Relacional e Interativo, administra nos termos dos n.ºs 4 e 5, do art.º 4, da L n.º 6/99 de 27/01, sujeita à supervisão da CNPD, de pessoas singulares que se lhe dirigem e manifestam o direito de oposição ao tratamento dos seus dados pessoais, que atualiza trimestralmente e disponibiliza a todos os operadores económicos interessados.
c) Nos termos do n.º 2 a 5, do art.º 13º-B, da L n.º 41/2004, de 18/08, compete à Direção-Geral do Consumidor manter atualizada uma lista *Robinson* de âmbito nacional de pessoas coletivas que manifestem expressamente a oposição à receção de comunicações não solicitadas para fins de marketing direto, bastando preencher de formulário eletrónico disponibilizado e não podendo ser cobrada qualquer quantia. As entidades que promovam o envio de comunicações para fins de marketing direto são obrigadas a consultar a lista, atualizada mensalmente pela DGC, que a disponibiliza a seu pedido.

O RGPD, apesar de alterar a terminologia e referir-se à comercialização direta, mantém as disposições essenciais, incluindo a definição de perfis na medida em que esteja relacionada com a referida comercialização, para o exercício do direito à oposição ao tratamento dos dados pessoais das pessoas singulares. (Considerando 70 e n.º 2 e 3, do art.º 21º, do RGPD).

3-5.3. Os direitos dos titulares dos dados pessoais no RGPD

A Diretiva 95/46/CE e a LPDP preveem, expressamente, um conjunto de direito dos titulares dos dados que incide sobre as operações do tratamento de dados (informação, acesso, retificação, apagamento ou bloqueio dos dados e oposição ao tratamento) que foi ampliada pelo RGPD, para além de reforçar os direitos já existentes. Assim, faz-se apenas referência aos seguintes direitos:

a) Direito à limitação do tratamento: isto é, implica um direito de bloquear o tratamento dos dado de modo que o responsável do tratamento pode conservar os dados mas não tratá-los, quando esteja perante uma das seguintes situações: (a) quando conteste a exatidão

dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; (b) o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; (c) o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; e (d) se tiver oposto ao tratamento, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

b) A notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento. Nos termos da al) e) do nº 1, do art.º 12º, da LPDP e al) c) do art.º 12º da Diretiva 95/46/CE, sempre que um responsável pelo tratamento tenha revelado dados pessoais a terceiros e a pessoa em causa tenha posteriormente exercido qualquer dos direitos de retificação, apagamento ou bloqueio, o responsável pelo tratamento deve notificar esses terceiros do exercício desses direitos por parte da pessoa em causa, salvo, se for impossível ou exigir um esforço desproporcionado. Nos termos do art.º 19.º, *in fine*, do RGPD, o direito é reforçado, ou seja, se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários. Os operadores económicos são obrigados a implementar sistemas e procedimentos para notificar os terceiros afetados sobre o exercício desses direitos. Para as organizações que divulgam dados pessoais a um grande número de terceiros, pode ser particularmente oneroso.

c) O direito de portabilidade dos dados, ou seja, o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, se o tratamento se basear no consentimento dado ou num contrato e o tratamento for realizado por meios automatizados (art.º 20º, do RGPD)[318]. O responsável poderá transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir. A transmissão dos dados não implica por exemplo o apagamento ou a oposição do tratamento de dados pelo responsável que os

[318] Para algumas organizações, este novo direito de transferir dados pessoais entre controladores exige investimentos substanciais em novos sistemas e processos, mas também uma oportunidade de atração de novos clientes. Os operadores económicos podem atrair clientes que anteriormente não estavam dispostos a mudar de um concorrente, devido às dificuldades associadas à definição de uma nova conta: por exemplo de correio eletrónico. Já existiam iniciativas como o projeto MIDATA (https://www.midata.coop/) no Reino Unido, em que os utilizadores podem transferir os seus dados bancários para plataformas que os ajudem a compreender os seus hábitos de consumo e encontrar as propostas mais adequadas para cada pessoa.

transmite. O direito à portabilidade não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; aos dados que o titular tenha facilitado de terceiros; e aos dados que tenham sido facilitados por terceiros ao responsável do tratamento.

PARTE III – TRATAMENTO DE DADOS PESSOAIS

CAPÍTULO VI – CONSIDERAÇÕES GERAIS SOBRE O TRATAMENTO DE DADOS PESSOAIS

3-6. O tratamento de dados pessoais

Os operadores económicos independentemente do seu tamanho ou propósito criam dados para tratar de eventos e transações que ocorrem dentro da sua organização. O tratamento de dados consubstancia-se no ato de manipular os dados por qualquer forma, independentemente das atividades desenvolvidas, para atribuir-lhes um determinado significado e com determinado fim, nomeadamente prosseguir os seus interesses lucrativos. Daí que para o bom funcionamento do mercado interno da EU se imponha que a livre circulação de dados pessoais na União não possa ser restringida ou proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais (Considerando 13, do RGPD).

Contudo, uma vez consagrado o direito fundamental à proteção de dados, e para evitar o sério risco de ser contornada a proteção de dados das pessoas singulares, são estabelecidas obrigações compatíveis com a concretização de tal direito, no que respeita ao seu tratamento de forma leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei e que todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação (conforme o n.º 2, do art.º 8, da CDFUE).

A legislação interna e europeia definem a expressão de tratamento em matéria de proteção de dados sempre que uma organização manipule dados pessoais.

3-6.1. O conceito de tratamento de dados pessoais

Nos termos da al) b), do art.º 3, da LPDP, o tratamento de dados pessoais consiste numa qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição, que resulta da

transposição *ispsis verbis* da Diretiva n.º 95/46/CE.[319] A definição legal permite extrair a seguintes conclusões:

1) O termo tratamento é muito amplo e significa tudo o que pode ser feito com os dados pessoais, ou seja, o tratamento de dados pessoais consiste numa qualquer operação ou conjunto de operações sobre dados pessoais. A disposição legal é exemplificativa[320] e enumera apenas algumas dessas operações[321].
2) A LPDP aplica-se ao tratamento de dados pessoais automatizado e manual que merecem, igualmente, tutela constitucional (conforme n.ºs 1 e n.º 7, do art.º 35º, da CRP). O tratamento manual[322] de dados (normalmente constituídos em suporte de papel, por exemplo, fichas de clientes organizadas por profissionais liberais ou a conta corrente de estabelecimentos comerciais tradicionais) está sujeito a proteção legal se estiverem organizados e estruturados segundo critérios específicos relativos às pessoas que permitam um acesso fácil aos dados pessoais (Considerando 15, da Diretiva 95/46/CE). A al) c) do n.º 2, do art.º 3º, da Convenção 108, já referia que as suas normas e princípios abrangiam tanto os ficheiros automatizados e como os ficheiros de dados de caráter pessoal que não sejam objeto de tratamento automatizado, estão sujeitos. O âmbito de aplicação material mantém-se no RGPD, conforme n.º 1, do art.º 2º.

   A definição de tratamento de dados pessoais está intimamente relacionada com o conceito de ficheiro[323] como conjunto estruturado de dados pessoais, acessível segundo

[319] O RGPD introduz pequenas alterações na definição de tratamento de menor relevância e sem consequências práticas nas organizações. É curioso que as Diretrizes sobre a Privacidade não incluam a definição de tratamento de dados pessoais, embora preveja um conjunto de definições tais como dados pessoais, responsável do ficheiro ou transferência de dados pessoais. O tratamento de dados pessoais, contudo no decorrer das negociações, foi um dos aspetos mais discutidos tendo desencadeado várias reações com a computação ubíqua e a distinção entre o tratamento automático e não automático da informação.

[320] O TJUE considerou que por exemplo «uma operação que consiste na referência, feita numa página da Internet, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos, constitui um «tratamento de dados pessoais por meios, total ou parcialmente, automatizados» na aceção da Diretiva 95/46 (Parágrafo 27, do Ac. *Bodil Lindqvist*, do TJUE, nº C-101/01, de 06/11/2003 e Parágrafo 129, do Ac. *The Bavarian Lager Co. Ltd* contra Comissão das Comunidades Europeias, do TPI, n.º T-194/04, de 08/11/2007).

[321] A al) c), do art.º 2º, da Convenção 108 refere que tratamento automatizado compreende as operações, efetuadas, no todo ou em parte, com a ajuda de processos automatizados, de registo de dados, aplicação a esses dados de operações lógicas e ou aritméticas, bem como a sua modificação, supressão, extração ou difusão.

[322] V. o entendimento sobre o tratamento manual de dados pessoais constante da Deliberação da CNPD, n.º 14/2002, cit. 177, sobre o regime relativo ao tratamento de dados pessoais em ficheiros manuais.

[323] A definição mantém-se no RGPD, conforme o n.º 6, do art.º 4º. Os dados pessoais são inseridos em ficheiros que se caracterizam por um sistema organizado segundo determinados critérios e cuja configuração permite incorporar e extrair a informação pretendida. O conceito de ficheiro não está vinculado a uma única localização podendo estar distribuído por vários locais geográficos, mas deve segundo o preceito legal estar de algum modo submetido a determinada gestão centralizada ou descentralizada. A doutrina distingue conceptualmente entre ficheiros físicos (que se podem localizar geograficamente, em suporte de papel ou informático), lógicos (a sistematização depende da configuração lógica do sistema de informação com uma finalidade ou finalidades compatíveis) e jurídicos (determinados pela natureza dos dados e a finalidade com que são tratados pelo

critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico (al) c), do art.º 2º da LPDP e al) c), do art.º 2º, da Diretiva 95/46/CE). Isto é, apenas se aplica a LPDP ao tratamento de dados pessoais quando o referido tratamento esteja contido num determinado ficheiro (Considerando 27, da Diretiva 95/46/CE). O n.º 6, do art.º 4º, do RGPD, mantém a definição de ficheiro da Diretiva e da LPDP, contudo, decorre da interpretação da norma e sobretudo, atendendo aos novos direitos dos titulares dos dados, que os ficheiros devem ter formatos interoperáveis que permitam a portabilidade dos dados. O TJUE refere que a mera indicação num relatório do nome de pessoas e respetivos rendimentos constitui um tratamento de dados[324]. A falta de conhecimento sobre o local do armazenamento dos ficheiros que contém dados pessoais como é o caso da computação em nuvem[325], não impede a aplicação da LPDP na medida em que o conceito deve ser conjugado com as condições e princípios que devem reger o tratamento de dados pessoais e os direitos do titular dos dados objeto de tratamento.

3-6.2. O papel do responsável pelo tratamento de dados pessoais

O responsável pelo tratamento de dados assume uma especial importância uma vez que garante o cumprimento da legislação nacional e da EU em matéria de proteção de dados

---

responsável do tratamento) (PULIDO, Emilia Zaballos - *La protección de datos personales en España : evolución normativa y criterios de aplicación* [Em linha]. Madrid. *Universidad Complutense de Madrid* (2013). *Tesis de doctorado*. [Consult. 10 jun. 2016]. Disponível em WWW <http://eprints.ucm.es/22849/1/T34733.pdf>; RODRIGUEZ DAVARA, Miguel Ángel – *Manual de Protección de Datos para Abogados.* Madrid : *Thompson Aranzadi*, 2008. ISBN 978-8497-676-49-6).

[324] Ac. *Rechnungshof v. Österreichischer Rundfunk* e outros, do TJUE apensos n.ºs C-465/00, C-138/01 e C-139/01, de 20/05/2003.

[325] A utilização de uma rede de computadores para otimizar o desempenho do processamento da informação teve origem na década de cinquenta e o termo de para designar esta partilha de tarefas foi pela primeira vez utilizado pelos engenheiros da Compaq, celebrizado junto dos consumidores por Steve Jobs com o prefixo "i", dois anos mais tarde (v. SILVA, Fernando Resina da, et al. – Cloud, a Lei e a Prática. Coimbra : Almedina, 2016. ISBN ISBN 9789724065045). A definição computação em nuvem (*cloud computing*) refere-se a um modelo de prestação de serviços tecnológicos que permite o acesso aos recursos computacionais configuráveis e interligados pela internet. Existem várias modalidades de serviços que são importantes diferentes devidos às distintas consequências a nível jurídico (que aqui não serão tratadas): (1) *IaaS - Infrastructure as a Service* (Infraestrutura como Serviço) quando se utiliza parte de um servidor; (2) PaaS - Plataform as a Service (Plataforma como Serviço) quando se utiliza para suporte de uma base de dados; (3) *DaaS - Development as a Service* (Desenvolvimento como Serviço) quando se utiliza para desenvolver serviços partilhados; (4) *SaaS - Software as a Service* (Software como Serviço) quando se utiliza um software na web, por exemplo, o Google Docs ou o *Microsoft SharePoint Online*; (5) *CaaS - Communication as a Service* (Comunicação como Serviço): quando se utiliza uma solução de Comunicação Unificada hospedada em Data Center do provedor, por exemplo, a *Microsoft Lync*; (6) *EaaS - Everything as a Service* (Tudo como Serviço) quando se utiliza todos os serviços que envolve a tecnologia da informação e comunicação; e (7) *DBaas - Data Base as a Service* (Banco de dados como Serviço) quando utiliza a parte de servidores de bases de dados. (v. MELL, Peter; GRANCE, Timothy - *The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology, NIST, U.S. Department of Commerce*, (2011). [Consult. 16 jan. 2016]. Disponível em WWW <http://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-145.pdf>).

pessoais. O responsável pelo tratamento é a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem (al) d), do art.º 3º, da LPDP), determina[326], de forma autónoma, as finalidades, o conteúdo e os meios de tratamento, a utilização do referido tratamento de dados pessoais e facilita ao titular dos dados o exercícios dos direitos (particularmente no acesso, retificação, cancelamento e oposição). O responsável pelo tratamento assegura o cumprimento dos princípios da proteção de dados (n.º 2, do art.º 5º e art.º 6º da LPDP, nº 2, do art.º 6 e art.º 7º, da Diretiva 95/46/CE e a) d), do art.º 2º, da Convenção 108).

As obrigações impostas à realização do tratamento de dados, pelo responsável, operam-se em três grandes momentos: (1) antes da recolha dos dados, (2) durante o tratamento dos dados e (3) a utilização dos dados por qualquer meio.

3-6.2.1. O responsável pelo tratamento de dados pessoais no âmbito do RGPD

O conceito de responsável pelo tratamento não foi alterado no âmbito do RGPD[327], mas as suas obrigações foram revistas conforme capítulo IV (art.ºs 24º a 44º), nomeadamente, quanto à aplicação das medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o regulamento (n.º 2, do art.º 5, e nº 1, do art.º 24º, do RGPD)[328].

Embora não esteja expressamente referido, resulta da interpretação do RGPD, que responsável pelo tratamento assume todos os deveres da legalização pelo tratamento de dados pessoais, e por isso, deve especificar, documentar e conservar[329] todos os registos das

[326] Note-se que o responsável pode nunca realizar nenhuma operação de tratamento de dados porque pode encarregar terceiros mediante determinadas instruções para a realização de tratamento de dados. A identificação do responsável do tratamento é importante para apurar as responsabilidades no tratamento de dados quando seja efetuado de forma ilícita. (v. GT29 - Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante» [Em linha]. 00264/10/PT WP 169. Brussels (Belgium), (16/02/2010). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_pt.pdf>).

[327] Conforme n.º 7, do art.º 4º, do RGPD, o responsável pelo tratamento é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro,

[328] Trata-se estimular o princípio da autorresponsabilidade ou responsabilidade proativa ou reativa, inspirado no modelo de origem anglo-saxónica de *accountability*, complementado com a elaboração de códigos de conduta e da certificação (v. GT29 - *The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* [Em linha]. 02356/09/EN WP 168. Brussels (Belgium), (01/12/2009). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf>).

[329] Para ter em conta a situação particular das micro, pequenas e médias empresas, o presente regulamento prevê

atividades de tratamento (Considerando 82 e art.º 30º, do RGPD), nomeadamente, de realizarem auditorias e avaliações periódicas, adoção de normas, procedimentos e sistemas tecnológicos que assegurem um elevado nível de segurança e as notificações de violação de segurança de dados pessoais.

3-6.3. A legalização do tratamento de dados pessoais

Atualmente, os art.ºs 27º a 30º, da LPDP, estabelecem as regras necessárias à legalização do tratamento de dados, bem como a qualquer alteração que venha a ocorrer, dependendo os formalismos da natureza dos dados pessoais, cuja iniciativa é desencadeada pelo responsável do tratamento, previamente à CNPD, por notificação[330] ou pedido de autorização, bem como podem ser solicitados pareceres (confr. art.º 18º e seguintes da Diretiva 95/46/CE). A legalização do tratamento de dados pessoais é obrigatória para entidades públicas e privadas.

Os art.ºs 29º e 30º, da LPDP, indicam quais são os elementos obrigatórios quanto aos pedidos de parecer ou de autorização, bem como as notificações, remetidos à CNPD: (a) nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante; (b) as finalidades do tratamento; (c) a descrição da ou das categorias de titulares dos dados e dos dados ou categorias de dados pessoais que lhes respeitem; (d) os destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições; (e) a entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento; (f) as eventuais interconexões de tratamentos de dados pessoais; (g) o tempo de conservação dos dados pessoais; (h) a forma e condições como os titulares dos dados podem ter conhecimento ou fazer corrigir os dados pessoais que lhes respeitem; (i) as transferências de dados previstas para países terceiros; e (j) a descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação dos art.ºs 14º e 15º, da LPDP.

O envio da notificação, o pedido de autorização ou parecer é feito por via eletrónica, através do preenchimento de formulário adequado ao tipo de tratamento de dados a tratar e que se

---

uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades. Além disso, as instituições e os órgãos da União, e os Estados-Membros e as suas autoridades de controlo, são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito de aplicação do presente regulamento. A noção de micro, pequenas e médias empresas ter em conta deverá inspirar-se do art.º 2º, do anexo da Recomendação 2003/361/CE da Comissão, de 06/05/2003, relativa à definição de micro, pequenas e médias empresas (Considerando 13 e art.º 30, do RGPD).

[330] O objetivo global da notificação teve como antecedente o acompanhamento seletivo da legitimidade das operações de tratamento de dados por parte da autoridade de controlo (GT29 - Documento de trabalho: A notificação [Em linha]. XV/5027/97-PT final WP 8. [s.l.], (03/12/1997). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp8_pt.pdf>)

encontra disponível na página web da CNPD. O formulário inclui as instruções de preenchimento e as regras para o envio de documentação em ficheiros anexos ao formulário. A submissão eletrónica do formulário implica o pagamento de uma taxa no prazo de três dias.
O tratamento dos dados pessoais, sujeito a notificação ou autorização constando de um registo na CNPD, é público e aberto à consulta por qualquer pessoa de determinados dados: (a) o nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante; (b) as finalidades do tratamento; (c) a descrição da ou das categorias de titulares dos dados e dos dados ou categorias de dados pessoais que lhes respeitem; (d) os destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições; e (e) as transferências de dados previstas para países terceiros (conforme n.º 2, do art.º 31º, da LPDP).
Nos termos do art.º 43º, da LPDP, o não cumprimento da obrigação, de forma intencional, de notificar ou pedir autorização para o tratamento de dados, a que se referem os art.ºs 27º e 28º, da LOPD, configura um crime, punido com prisão até um ano ou multa até 120 dias.

3-6.3.1. A notificação à CNPD

O tratamento de dados autonomizado ou parcialmente autonomizado que não envolva dados sensíveis, destinados à prossecução de uma ou mais finalidades interligadas, é antecipadamente notificado pelo responsável pelo tratamento à CNPD (nos termos do n.º 1, do art.º 27º, da LPDP). O tratamento de dados para utilização em campanhas de marketing deve ser comunicado à CNPD, e ainda informar o titular bem como facultar o exercício efetivo do direito de oposição. O responsável pelo tratamento pode dar início ao tratamento de dados pessoais após a submissão da notificação eletrónica à CNPD. A notificação tem natureza declarativa e no âmbito das atribuições de controlo (art.º 22º, da LPDP) a CNPD pode verificar o tratamento de dados em conformidade à lei e em caso de encontrar ilegalidades recusar a notificação.

3-6.3.2. A isenção da notificação à CNPD

A CNPD pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamentos que, atendendo aos dados a tratar, não sejam suscetíveis de pôr em causa os direitos e liberdades dos titulares dos dados e tenham em conta critérios de celeridade, economia e eficiência (nos termos do n.º 2, do art.º 27º, da LPDP). O responsável pelo tratamento deve cumprir as condições e princípios de proteção de dados e direitos dos titulares, previstos na LPDP, em conformidade e limites determinados pela CNPD.

A autorização da isenção[331] está sujeita a publicação no Diário da República e deve especificar as finalidades do tratamento, os dados ou categorias de dados a tratar a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados.

Tendo em conta que não existe nenhum registo de notificação na CNPD, o responsável pelo tratamento está obrigado a prestar, de forma adequada, a qualquer pessoa que lho solicite, pelo menos as seguintes informações: (a) a identidade do responsável do ficheiro e, se for caso disso, o seu representante; (b) as categorias de dados pessoais tratados; (c) as finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos; (d) a forma de exercício do direito de acesso e de retificação; (e) eventuais interconexões de tratamentos de dados pessoais; e (f) as transferências de dados previstas para países terceiros.

3-6.3.3. A autorização concedida pela CNPD

A CNPD exerce o controlo prévio do tratamento de dados pessoais através da autorização concedida ao responsável pelo tratamento quando estejam em causa o tratamento de dados pessoais de dados sensíveis (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) previstos no n.º 1, do art.º 7º, da LPDP, ou a criação e a manutenção de registos centrais relativos a pessoas suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias, previsto no n.º 1, do art.º 8º, da LPDP, o tratamento dos dados pessoais relativos ao crédito e à solvabilidade dos seus titulares, a interconexão de dados pessoais[332], a utilização de dados pessoais para fins não determinantes da recolha[333] e a

[331] A Deliberação da CNPD, nº 60/2000, de 27/01. [Em linha]. Diário da República - 2.ª Série, nº 22, de 27/01/2000, p. 1813 - 1816 [Consult. 29 mar. 2015]. Disponível em WWW <https://dre.pt/web/guest/pesquisa-avancada/-/asearch/2028668/details/maximized?search=Pesquisar&sortOrder=ASC&tipo_facet=Delibera%C3%A7%C3%A3o&perPage=25&types=SERIEII&dataPublicacaoInicio=2000-01-27>, determina a isenção de notificação à CNPD dos seguintes tratamentos de dados: o processamento de retribuições, prestações, abonos de funcionários ou empregados (Autorização de Isenção da CNPD, n.º 1/99); a gestão de utentes de bibliotecas e arquivos (Autorização de Isenção da CNPD, n.º 2/99); a faturação e gestão de contactos com clientes, fornecedores e prestadores de serviços (Autorização de Isenção da CNPD, n.º 3/99); a gestão administrativa de funcionários empregados e prestadores de serviços (Autorização de Isenção da CNPD, n.º 4/99); o registo de entradas e saídas de pessoas em edifícios (Autorização de Isenção da CNPD, n.º 5/99); e a cobrança de quotizações em associações e contactos com os respetivos associados (Autorização de Isenção da CNPD, n.º 6/99). Define os prazos de conservação a que estão sujeitos os dados atrás referidos, bem como os destinatários a quem podem ser comunicados esses dados.

[332] A interconexão de dados é a forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade, conforme definição legal da al) i), do art.º 3º da LPDP). É proibido o acesso a ficheiros e registos informáticos para conhecimento de dados pessoais relativos a terceiros e respetiva interconexão, salvo em casos excecionais previstos na lei – art.º 35º, n.º 2, da CRP.

transferência de dados pessoais sem o recurso à celebração das cláusulas-tipo aprovadas pela Comissão Europeia. Não carecem de autorização da CNPD quando o tratamento de dados esteja previsto e autorizado em diploma legal (art.º 28º, da LPDP)[334].

O responsável pelo tratamento apenas pode dar início ao tratamento de dados pessoais com a concessão da autorização da CNPD.

Com a produção de efeitos do regime do RGPD, o responsável pelo tratamento de dados continua isento de autorização por transferências de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. A isenção de autorização pode ser revogada após a avaliação periódica da adequação do nível de proteção. As decisões já adotadas pela Comissão, nos termos do n.º 6, do art.º 25, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por outra decisão da Comissão (n.º 8, do art.º 45º, do RGPD).

A lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais a Comissão declare, mediante decisão, se asseguram ou não um nível de proteção adequado é publicada no Jornal Oficial da EU (art.º 45º do RGPD).

«Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade»

---

[333] O Ac. do STA, n.º 857/02, de 29/03/2006, refere que é necessário demonstrar que tratamento informatizado de dados pessoais é para a prossecução dos fins de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde. O facto de o programa da Associação Nacional de Farmácias assentar no consentimento do titular dos dados, não implica que se verifiquem os pressupostos para a CNPD autorizar o tratamento de dados. A autorização não pode ser genérica e abstratamente concedida num dado momento para ser depois aplicada em concreto a qualquer pessoa, ainda que seja dado o seu consentimento.

[334] A título de exemplos, o DL n.º 294/2001, de 20/11, que estabelece, no âmbito da atividade estatística oficial do SEN, regras relativas ao acesso, recolha e tratamento pelo INE de dados pessoais de caráter administrativo; a L n.º 38/2012, de 28/08, que aprova a lei antidopagem no desporto, adotando na ordem jurídica interna as regras estabelecidas no Código Mundial Antidopagem (disponível aqui: AGÊNCIA MUNDIAL ANTIDOPAGEM - Código Mundial Antidopagem. Montreal [Em linha]. (2015) [Consult. 1 dez. 2016]. Disponível em WWW <http://www.adop.pt/media/8381/C%C3%B3digo%20Mundial%20Antidopagem%202015.pdf>) e a L n.º 147/2015, de 09/09, que aprova o regime jurídico de acesso e exercício da atividade seguradora e resseguradora, bem como o regime processual aplicável aos crimes especiais do setor segurador e dos fundos de pensões e às contraordenações cujo processamento compete à Autoridade de Supervisão de Seguros e Fundos de Pensões.

(Considerando 108, do RGPD).

3-6.3.4. A consulta prévia e a autorização previstas no RGPD

O responsável pelo tratamento de dados deve consultar previamente a autoridade de controlo antes de proceder a um determinado tratamento em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, conforme resulte da avaliação prévia de impacto sobre a proteção de dados (n.º 1, do art.º 35º e n.º 1, do art.º 36º, do RGPD). Os Estados-Membros podem exigir, no direito interno, que os responsáveis pelo tratamento consultem a autoridade de controlo e dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública.

Os responsáveis pelo tratamento de dados devem obter autorização, da autoridade de controlo competente, na ausência de decisão da Comissão e de garantias adequadas à proteção de dados pessoais dos seus titulares, para a transferência de dados pessoais para um país terceiro ou uma organização, por meio de: (a) cláusulas contratuais entre os responsáveis pelo tratamento e os responsáveis pelo tratamento, destinatários dos dados pessoais no país terceiro ou organização internacional; ou (b) disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados (n.º 3, do art.º 46, do RGPD).

CAPÍTULO VII – OS PRINCÍPIOS DO TRATAMENTO DE DADOS PESSOAIS

3-7. Os princípios do tratamento de dados pessoais

A Diretiva 95/46/CE é a manifestação dos princípios plasmados no art.º 5º, da Convenção 108 (Considerando 11, da Diretiva 95/46/CE), e que foram ampliados e consolidados nas legislações dos Estados-Membros. As disposições sobre os critérios subjacentes ao tratamento de dados da Diretiva 95/46/CE têm efeito direto na aplicação pelos tribunais nacionais dos Estados-Membros, conforme orientação do TJUE[335]. Nos termos do art.º 2º, da LPDP, 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, regendo-se o responsável pelo tratamento pelos princípios previstos na secção I, do Capítulo II, da LPDP, quanto à qualidade dos dados (art.º 5º, da LPDP) e às condições de legitimidade do tratamento de dados (art.º 6º, da LPDP)[336].

Seguindo a estrutura da LPDP, os princípios que regem o tratamento de dados são os seguintes: (1) o princípio da licitude, (2) o princípio da lealdade, (3) o princípio da transparência, (4) princípio relativo à qualidade dos dados, (5) o princípio da finalidade, (6) o princípio da segurança; e (7) o princípio da responsabilidade.

3-7.1. O princípio da licitude

O princípio da licitude do tratamento de dados afere-se do cumprimento das normas de direito nacional, da UE e de direito internacional[337], e ainda dos princípios gerais do direito, nomeadamente, da boa-fé (al) a), do n.º 1, do art.º 6º da Diretiva 95/46/CE, al) a), do n.º 1, do art.º 5º da LPDP). O tratamento de dados pode constituir uma ingerência[338] no exercício do

---

[335] Ac. *Asociación Nacional de Establecimientos financeiros de crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, do TJUE, apensos n.ºs C-468/10 e 469/10, de 24/11/2011.

[336] Por não caber no objeto deste texto, são omitidas as considerações sobre o regime excecional, quanto aos tratamentos de dados sensíveis (art.º 7º, da LPDP) e aos tratamentos de dados relativos a pessoas suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias (art.º 8º, da LPDP e *vide* n.º 2, do art.º 9º da Convenção 108 e n.º 2, do art.º 13º, da Diretiva 46/95/CE).

[337] CASTRO, cit. 38, p. 235.

[338] O conceito de ingerência justificada tem sido objeto da jurisprudência do TEDH que estabeleceu três critérios que têm de ser satisfeitos para assegurar que qualquer ingerência respeita o disposto no n.º 2, do art.º 8.º, da CEDH. Assim, uma ingerência tem de: (1) estar prevista na lei, (2) prosseguir um dos objetivos legítimos definidos no n.º 2, do art.º 8.º, da CEDH; e (3) constituir uma providência que seja necessária numa sociedade democrática (v. GT29 - Parecer 01/2014 sobre a aplicação dos conceitos de necessidade e proporcionalidade e a proteção de dados no setor da aplicação coerciva da lei [Em linha]. 536/14/PT, WP 211. Brussels (Belgium), (27/02/2014). [Consult. 12 Dez. 2016]. Disponível em WWW <http://ec. europa.eu/justice/data-protection/ article-29/documentation/opinion-recommendation/files/ 2014/wp211_pt.pdf>), p. 5; e também, Ac. MM v. Reino Unido, do TEDH, n.º 24.029/07, de 29/04/2013, em que a recolha sistemática de dados para efeitos de

direito ao respeito pela vida privada pelo que qualquer exceção deve estar prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros, conforme o n.º 2, do art.º 8 da CEDH, n.º 2, do art.º 9º, da Convenção 10, n.º 1, do art.º 51º da CDFUE e previsto no art.º 6º da LPDP[339].

A concretização do princípio da licitude do tratamento de dados pessoais deve ser conforme aos princípios da qualidade dos dados (art.º 6º, da Diretiva 95/46/CE e art.º 5º, da LPDP) (3-7.4.) e das condições de legitimidade do tratamento de dados (art.º 7º, da Diretiva 95/46/CE e art.º 6º, da LPDP). (3-8.)

O RGPD, quando produza efeitos, prevê que a licitude do tratamento para a atividade de marketing está sujeita ao consentimento prévio do titular dos dados[340] (conforme previsto na al) a), do art.º 5º, conjugado com a al) a) do n.º 1, do art.º 6º do RGPD).

---

registo criminal, continuavam disponíveis mesmo quando já não tinha sentido continuar a divulgá-los, não era compatível com o Estado de Direito, para que o seu titular pudesse regular a sua conduta. No Ac. *Peck v. the United Kingdom*, do TEDH, n.º 44.647/98, de 28/04/2003, o tribunal considera que a divulgação de imagens captadas por canais de CCTV e nos órgãos de comunicação social sem serem acompanhadas de salvaguardas suficientes, nomeadamente a desfocalização da face, constituía uma interferência desproporcional e injustificada na vida privada do requerente e uma violação do art.º 8º da CEDH. O TJUE, reitera que as restrições aos direitos fundamentais devem: (1) estar previstas por lei; (2) respeitar o conteúdo essencial desses direitos; (3) e, na observância do princípio da proporcionalidade, serem necessárias e (4) corresponder efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros, nos termos do n.º 1, do art.º 52º, da CDFUE. Parágrafo n.º 34, do Ac. *Michael Schwarz* v. *Stadt Bochum*, do TJUE, nº C-291/12, de 17/10/2013, em que o requerente contestou a recusa das autoridades alemãs em emitir-lhe um passaporte (UE) a menos que ele autorizasse a recolha das suas duas impressões digitais para incorporar no referido passaporte. Tal obrigação decorre do Regulamento (CE) n.º 2252/2004 do Conselho, de 13/12/2004, que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros. O parágrafo 18, do Ac. *Hubert Wachauf* v. República Federal da Alemanha, do TJUE, n.º 5/88, de 13/07/1989, refere que «os direitos fundamentais reconhecidos pelo Tribunal não devem, todavia, ser entendidos como prerrogativas absolutas antes devendo ser tomados em consideração com referência à sua função na sociedade. Por conseguinte, podem ser introduzidas restrições ao exercício desses direitos, designadamente no âmbito de uma organização comum de mercado, desde que essas restrições tenham, efetivamente, por fundamento objetivos de interesse geral prosseguidos pela Comunidade e não constituam, face a esses objetivos, uma intervenção desproporcionada e intolerável suscetível de atentar contra a própria essência desses direitos» E no mesmo sentido, o parágrafo 45, do Ac. *Kjell Karlsson* e o., do TJUE, n.º C-292/97, de 13/04/2000.

[339] Ainda que os textos legais referidos divirjam quanto à sistemática e redação, é absolutamente adequada a anotação ao art.º 52º, da CDFUE, no âmbito dos direitos e princípios, ao referir que a fórmula utilizada inspira-se na jurisprudência do TJUE no que respeita às restrições ao direito para prosseguir os interesses gerais da EU protegidos por disposições específicas dos Tratados, evocando expressamente que as disposições relevantes da CEDH é reforçada pelo n.º 3, do art.º 6.º, do TUE, que estabelece que do «direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais».

[340] Considerando 40, do RGPD: «Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento do titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar».

3-7.2. O princípio da lealdade

A relação entre o responsável pelo tratamento e o titular dos dados é regido pelo princípio da lealdade considerando que este deve ter conhecimento da existência dos tratamentos e obter, no momento em que os dados lhe são pedidos, uma informação rigorosa e completa das circunstâncias dessa recolha (Considerandos 38 e 39, da Diretiva 95/46/CE), que deve incidir sobre dados adequados, pertinentes e não excessivos em relação às finalidades explícitas e legítimas e serem determinadas aquando da recolha dos dados para o tratamento (Considerando 28, da Diretiva 95/46/CE). O princípio da lealdade concentra o espírito de todos os outros princípios que fundamentam e legitimam o tratamento dos dados, contribuindo para a transparência e segurança jurídica. O princípio da lealdade do tratamento dos dados está previsto na al) a), do art.º 5º, do RGPD.

3-7.3. O princípio da transparência

O princípio da transparência[341] tem como objetivo o controlo e conhecimento do tratamento dos dados bem como as circunstâncias que o rodeiam pelos seus titulares, e efetiva-se, sobretudo, pela publicidade dos tratamentos (art.º 21º, da Diretiva 95/46/CE e art.º 31, da LPDP) pelo direito à informação (art.ºs 10º e 11º, da Diretiva 95/46/CE e da art.º 10º, da LPDP) e pelo direito de acesso (art.º 12º, da Diretiva 95/46/CE e da art.º 11, da LPDP). A facultação do controlo de determinados procedimentos no que diz respeito à recolha, armazenamento de utilização dos dados aos seus titulares tem efeitos positivos sobre a perceção dos riscos da privacidade e no aumento da confiança nas atividades do responsável do tratamento[342]. O fator confiança pode afetar os interesses legítimos dos operadores económicos[343] na prossecução das suas atividades comerciais[344].

---

[341] Podemos encontrar o princípio da transparência, na recomendação nº 12, das Diretrizes da Privacidade e aí denominado «princípio de abertura. 12. Deveria haver uma política geral de abertura a respeito do desenvolvimento, da prática e da política, referente a dados pessoais. Deveriam estar prontamente disponíveis meios de estabelecer a existência e natureza de dados pessoais, as finalidades principais de seu uso, bem como a identidade e residência habitual do controlador de dados».

[342] Por exemplo, certas plataformas web, como o Facebook, disponibilizam ferramentas para controlar a informação partilhada, e o Google, um controlo sobre o armazenamento do histórico das pesquisas.

[343] De acordo com o Código da FEDMA, ao fazer menção ao princípio da transparência, invoca-se o dever das empresas estarem identificadas nas páginas web e proporcionando permanente as informações sobre os seus serviços de forma clara e acessível (v. GT29 - Parecer 3/2003 sobre o código de conduta europeu da FEDMA relativo ao uso de dados pessoais em operações de marketing direto. [Em linha]. 10066/03/PT final WP 77. Brussels (Belgium), (13/07/2003). [Consult. 16 Fev. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp77_pt.pdf>).

[344] A este propósito, o Considerando 29, da Diretiva 2000/31/CE: «A comunicação comercial é essencial para o financiamento dos serviços da sociedade da informação e para o desenvolvimento de uma grande variedade de novos serviços gratuitos. No interesse dos consumidores e da lealdade das transações, a comunicação comercial, incluindo descontos, ofertas e jogos promocionais, deve respeitar um certo número de obrigações relativas à transparência».

3-7.2.1. O dever de informação

A recolha de dados inicia-se por meio de um conjunto de operações pelo responsável do tratamento que está sujeito a um conjunto de obrigações prévias[345], e nomeadamente, a informação prestada ao titular dos dados, nos termos da al) a), do art.º 5º, al) a), do art.º 8º, da Convenção 108, da al) a), do n.º 1, do art.º 6º, art.º 10º e art.º 11º, da Diretiva 95/46/CE, e art.ºs 2º e 10º, da LPDP. A informação deve ser prestada, até ao momento da recolha, em formato legível e de forma inteligível, ou seja em linguagem adequada aos destinatários, que deve variar em função da audiência prevista[346]: adultos ou crianças, público em geral ou académicos especializados, pessoas com necessidades especiais, entre outros[347].

Assim, o responsável pelo tratamento, quando recolher dados pessoais diretamente dos interessados, deve fornecer à pessoa em causa junto da qual recolhe dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento:

a) A existência de um ficheiro ou a existência da possibilidade de um tipo de tratamento concreto de dados (3-6.3).
b) A identidade e os dados de contacto do responsável pelo tratamento.
c) Os destinatários ou categorias de destinatários dos dados, ou seja, o responsável deve informar se os dados recolhidos irão ser comunicados a terceiros ou postos à sua disposição, como é o caso de empresas subsidiárias, colaboradores comerciais, entre outros. Se os dados forem transmitidos para países exteriores à UE, o responsável pelo tratamento deve indicar se o país de destino proporciona, ou não, uma proteção adequada das pessoas em causa no que se refere ao tratamento dos seus dados pessoais, no sentido do art.º 25º da Diretiva 95/46/CE e art.º 19º, da LPDP.
d) As finalidades do tratamento a que os dados se destinam. A informação sobre as finalidades deve ser explícita e determinada, evitando-se ambiguidades e expressões muito genéricas, tais como para «fins comerciais», para «envio com fins publicitários», para «comercialização por catálogo» ou utilização de expressões em idioma estrangeiro. (3-7.5)
e) O caráter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder (a informação obrigatória é a informação que é necessária para a realização

[345] Como anteriormente referido no ponto 3-6.3. no que respeita à legalização do tratamento de dados pessoais, o responsável terá regularizado o ficheiro junto da CNPD e tomadas as medidas de segurança previstas nos art.ºs 14 e seguintes, da LPDP, para iniciar o tratamento de dados.

[346] A informação prestada às pessoas em causa não deve consistir em políticas de privacidade excessivamente longas ou difíceis de compreender.

[347] V. GT29 - Parecer 10/2004 sobre a prestação mais harmonizada da informação. [Em linha]. 11987/04/PT GT100. Brussels (Belgium), (25/11/2004). [Consult. 16 Fev. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp100_pt.pdf>

do serviço solicitado, por exemplo a falta de informação sobre o número de contribuinte para efeitos de faturação de produtos e serviços ou o domicilio para entrega de produtos comprados em linha, sob pena de não se poder concluir o negócio jurídico). A não disponibilização de informação facultativa ou adicional não pode ter quaisquer consequências negativas para essa pessoa.

f) A existência do direito de acesso, retificação, apagamento ou bloqueio dos dados (3-5.2).

g) O exercício do direito de oposição, sem despesas, às comunicações para efeitos de marketing direto ou qualquer outra forma de prospeção, de forma expressa (3-5.2.4).

h) A circulação em rede dos dados sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados, no caso de recolha de dados em redes abertas (n.º 4, do art.º 10º, da LPDP) (3-7.6.).

i) O acesso ao registo público, consagrado no art.º 31, da LPDP, e que por deliberação da CNPD, do registo público deve constar mais informação «por revelar-se ou constituir elemento importante para a transparência do tratamento de dados», como seja, a forma do exercício do direito de acesso aos dados pessoais, o número de processo da CNPD, a data do registo ou da autorização e o número da autorização[348].

O responsável não pode realizar operações de tratamento em segredo[349], e o tratamento invisível de dados[350], associado à utilização de aplicações em IAm, como os testemunhos de conexão, tecnologias RFID, etc., que recolhem automaticamente, e de forma não detetável pelos utilizadores comuns[351], os dados de utilização em rede, dados de emissores e recetores,

[348] V. Deliberação da CNPD, nº 1/2000, de 04/01 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/2000/htm/del/del001-00.htm>

[349] CASTRO, cit. 38, p. 242 e segs.

[350] A doutrina norte americana refere que a captação de dados de forma oculta para ficheiros pode ser levada a cabo tendo em conta quatro características: (1) por sequência de cliques (*clickstream data)*, ou seja por cada clique que o utilizador realiza em ambiente digital deixa um rasto que inclui informação sobre o titular, tempo, data e tipo de transação concretizada; (2) fontes de multinacionais (*multinacional sourcing)*, a arquitetura da captação e processamento da informação torna irrelevante a distância e a localização geográfica, das empresas globalmente dispersas dada a partilha interna da informação agregando-lhe valor; (3) base de dados especializada (*data warehousing*) e rastreamento de dados (*data creep)*, que implica o armazenamento de milhões de bits de informações pessoais para análise futura, os dados mínimos são irrelevantes mas agregados assumem uma importância enorme, na medida em que podem revelar padrões de comportamento e categorizar a informação; e (4) a pressão do uso secundário e a construção de perfis (*pressures for secondary use and profiling)* que se baseia na recolha de informação para criar perfis e utilizá-la posteriormente com outras finalidades *(*REIDENBERG, Joel R. - *Resolving Conflicting International Data Privacy Rules in Cyberspace* [Em linha].*Stanford. Law Review*, Vol. 52 (1999-2000) p. 1315-1371 [Consult. 12 jun. 2016]. Disponível em WWW <http://ir.lawnet.fordham.edu/faculty_scholarship/41>). Note-se que estes processos permitem recolher dados sem determinação prévia da finalidade para que são recolhidos e só em fase posterior é que são definidas as suas finalidades, o que é contrário ao direito da EU e do direito interno.

[351] «As informações e a possibilidade de se opor à recolha devem ser comunicadas antes da utilização de qualquer procedimento automático que desencadeie a ligação do computador pessoal do utilizador a outro *site* – por exemplo, quando o utilizador é levado, automaticamente, por um *site* a contactar outro para ver publicidade sob a forma de "*banners*" – a fim de evitar que este segundo *site* possa recolher dados sem conhecimento do

data e hora etc., está sujeito ao direito da EU e do direito interno[352].

O dever de informação pelo responsável do tratamento não se aplica quando, nomeadamente, no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação da pessoa em causa se revelar impossível ou implicar esforços desproporcionados ou quando a lei dispuser expressamente o registo dos dados ou a sua divulgação (art.º 9º, da Convenção 108, Considerando n.º 40, n.º 2, do art.º 11º da Diretiva 95/46/CE), e ainda, sendo ser dispensado, mediante disposição legal ou deliberação da CNPD, por motivos de segurança do Estado e prevenção ou investigação criminal, e, bem assim, ao tratamento de dados efetuado para fins exclusivamente jornalísticos ou de expressão artística ou literária (n.ºs 5 e 6, do art.º 10, da LPDP).

3-7.2.2. O dever de informação no RGPD

O RGPD para além das informações descritas em 3-7.2.1., antes da recolha dos dados ou no momento da recolha, acrescenta outras informações a facultar quando os dados pessoais são recolhidos e dependendo da fonte: (1) diretamente junto do titular (art.º 13, do RGPD); ou (2) quando não são recolhidos diretamente do titular.

As informações a prestar ao titular dos dados quando recolhidos junto do titular são:

a) A identidade e os dados de contacto do encarregado da proteção de dados.
b) Quanto à finalidade, se o responsável tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes (por exemplo, quando os dados são recolhidos para a celebração de um contrato e pretende posteriormente enviar comunicações para fins de marketing direto, o responsável tem de declarar estas duas finalidades de forma clara e explícita).
c) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo.
d) O fundamento jurídico para o tratamento de dados.
e) A indicação dos interesses legítimos do responsável pelo tratamento ou de um terceiro.
f) O direito de se opor ao tratamento de dados pessoais o mais tardar no momento da

utilizador» (v. GT29 - Recomendação sobre determinados requisitos mínimos para a recolha de dados pessoais em linha na União Europeia [Em linha]. 5020/01/PT/Final WP 43. Brussels (Belgium), (17/05/2001). [Consult. 14 Fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/ data-protection/article-29/documentation/ opinion-recommendation/files/2001/wp43_pt.pdf>. p. 7.

[352] V. GT29, cit. 43.

primeira comunicação com a pessoa em causa. Esta informação deve ser fornecida de forma clara e separada de qualquer outra informação prestada[353].

g) A existência de decisões automatizadas[354], incluindo a definição de perfis.

h) A previsão da transferência de dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

i) A existência do direito de retirar consentimento em qualquer altura.

j) O direito de apresentar reclamação a uma autoridade de controlo.

Quando os dados não se obtenham diretamente do interessado, o responsável deve informá-lo:

a) Dentro de um prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;

b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou

c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados (al) a) a c), do n.º 3, do art.º 14º, do RGPD).

d) Deve, ainda, informar o titular das informações disponíveis sobre a origem desses dados e das categorias dos dados recolhidos (art.º 15º, do RGPD).

Os responsáveis pelo tratamento são obrigados a fornecer informações adicionais aos titulares dos dados, o que exige a revisão de políticas-padrão de proteção de dados e avisos de privacidade.

3-7.4. O princípio relativo à qualidade dos dados

O princípio da qualidade dos dados está destinado a assegurar que os dados sejam exatos, completos (se necessário, atualizados) e conservados apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior. O princípio da

[353] Conf. al) b), nº 2, art.º 13; al) c), nº 2, art.º 14; al) e), nº 1, art.º 15º, e art.º 21º do RGPD.

[354] O art.º 15º, da Diretiva 95/46/CE e o art.º 13º, da LPDP, já referiam que qualquer pessoa tem o direito de não ficar sujeita a uma decisão que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados, a não ser que a decisão seja tomada no âmbito da celebração de um contrato ou autorizada por lei, bem como o direito de conhecer a lógica subjacente a qualquer tratamento automático de dados relativos à sua pessoa.

qualidade dos dados[355] está previsto (al) c) a e), do art.º 5º, da Convenção 108, al) c) a e), do n.º 1, do art.º 6º, da Diretiva 95/46/CE, e al) c) a e), do n.º 1, do art.º 5º, da LPDP). Assim, o responsável pelo tratamento deve garantir que os dados, em todas as fases do tratamento e em função das finalidades determinadas e legítimas para que foram recolhidos, devem ser:

a) Adequados: os dados recolhidos são delimitados às finalidades do tratamento[356].
b) Pertinentes: a recolha de dados deve restringir-se absolutamente aos dados necessários à prossecução das finalidades para o tratamento. O preenchimento de formulários nas páginas web, com o fim de se receber um bem ou serviço gratuito, é uma prática aparentemente inofensiva de recolha de dados, e embora, o interessado esteja consciente da disponibilização de dados, não sabe que a maioria é desnecessária e desconhece o fim e razão do tratamento[357].
c) Proporcionais e não excessivos: deve ser encontrado um equilíbrio em função da finalidade de cada tratamento[358].
d) Exatos e atualizados: para assegurar que os dados são verdadeiros, o responsável deve garantir o direito à retificação, apagamento ou bloqueio dos dados pelo seu titular, pois, só assim pode prosseguir a promoção da informação comercial junto do seu público e sem repercussões negativas para o seu titular, por exemplo na avaliação de ofertas ou descontos especiais exclusivos para determinado grupo de clientes, assente em elementos de prova, estatísticas, previsões, etc.
e) Conservados durante um período limitado[359] e proporcional à finalidade[360] da recolha ou

[355] Igualmente referido nas Diretrizes sobre a Privacidade: «Princípio de qualidade dos dados. 8. Os dados pessoais deveriam ser relacionados com as finalidades de sua utilização e, na medida necessária, devem ser exatos, completos e permanecer atualizados.
[356] A CdE *Resolution (73) 22*, cit. 70, já referia que a recolha dos dados devem ser «adequada e pertinente no que respeita à finalidade para que foram armazenados» e - na falta de autorização adequada - proíbe a sua utilização para fins diferentes daqueles para os quais foi armazenado, bem como a sua comunicação a terceiros.
[357] O princípio da minimização dos dados incorpora os critérios de adequação, pertinência e limitação da recolha de dados ao que é necessário relativamente às finalidades para as quais são tratados, na nova denominação referida na al) c), do n.º 1, do art.º 5º, do RGPD.
[358] V. a Autorização da CNPD, nº 192/2002, cit. 251, sobre o tratamento de dados de candidatos de modelos para uma campanha publicitária, nomeadamente a raça e o sexo, e Ac. do TCAS, n.º 07118/11, de 10/02/2011, tendo considerado que um sistema de videovigilância para controlo do tráfego em Lisboa é excessivo face à finalidade pretendida de deteção de acidentes e prestação de socorro dos acidentados.
[359] Nos termos do n.º 2, do art.º 5º, a CNPD pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos por período superior ao necessário. Os dados podem ser armazenados se forem anonimizados ou pseudonimizados. A al) e), do n.º 1, do art.º 4º, do RGPD, prevê que os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o n.º 1, do art.º 89º, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados.
[360] Ac. *S. And Marper* v. *The United Kingdom*, do TEDH, apensos 30.562/04 e 30.566/04, de 04/12/2008, em que o princípio da conservação de dados exige que os dados sejam conservados durante o mínimo possível de tempo.

do tratamento posterior, em função de cada tipo de dados. Os dados das pessoas que manifestaram o direito de oposição à receção de comunicações comerciais devem ser conservados indefinidamente até que venha a prestar o seu consentimento em voltar a recebê-las. A limitação temporal da conservação dos dados só aplicável na medida em que se possa identificar o titular dos referidos dados. A conservação de dados para fins científicos, históricos ou estatísticos, e quando sejam anonimizados ou pseudonimizados, constitui uma exceção ao princípio da limitação da conservação dos dados.

As normas sobre a limitação da conservação dos dados, no RGPD, devem ser conjugadas com o direito a ser esquecido, previsto no art.º 17º, ou seja o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, e nalguns casos antes do termo do período máximo de retenção. (3-5.2.3.)

3-7.5. O princípio da finalidade

O princípio da finalidade, também designado por princípio da especificação dos fins[361], ou princípio da limitação dos dados, agora expressamente referido na al) c), do n.º 1, do art.º 5º, do RGPD, significa que tratamento dos dados só é lícito se as finalidades para a recolha dos dados estiverem previamente determinadas pelo responsável do tratamento[362], de forma explícita e legítima. A utilização posterior dos dados para uma finalidade incompatível com a finalidade original, exige outra base legal[363] (al) b), do art.º 5º, da Convenção 108, al) b) do n.º 1, do art.º 6º, da Diretiva 95/46/CE e al) b) do n.º1, do art.º 5º, da LPDP), de forma a garantir a transparência, segurança jurídica e a expectativas[364] criadas aos titulares dos dados.

[361] FRA, CdE, cit. 231.

[362] As finalidades do tratamento são determinadas pelo responsável do tratamento (al) d), do art.º 2º, da Diretiva 46/95/CE, al) d), do art.º 3º da LPDP e agora no n.º 7, do art.º 4º, do RGPD).

[363] As CdE *Resolution (73) 22*, cit. 70, CdE *Resolution (73) 23*, cit. 71, e CdE *Resolution (74) 29*, cit. 72, já tinham uma abordagem que foi evoluindo no que respeita à recolha da informação adequada e pertinente para as finalidades que foram conservadas, bem como as condições excecionais que os dados poderiam ser utilizados para outros fins. A CdE *Resolution (74) 29*, cit 72, refere-se à utilização dos dados para fins diferentes dos que foram definidos se for expressamente permitida por lei», ou autorizada por uma autoridade de controlo, ou se as regras de utilização da base de dados forem alteradas.

[364] Considerou o Ac. *Lüdi v. Switzerland*, do TEDH, n.º 12.433/86, de 15/06/1992, de certa forma que existiu uma alteração às finalidades da utilização das telecomunicações, no caso sem violação do n.º 2 do art.º 8º, da CEDH, proíbe qualquer ingerência da autoridade pública no exercício do direito à privacidade, salvo, se estiver prevista na lei, numa sociedade democrática, a fim de satisfazer determinados tipos de interesses públicos especificamente enumerados e convincentes, nomeadamente para prevenção das atividades criminosas, na medida em que existia a expectativa razoável junto da pessoa, da interceção de comunicações telefónicas, no contexto de tráfico de cocaína com o objetivo de deter os traficantes. O requerente devia ter consciência do risco da referida interceção bem como estar sob vigilância de polícias disfarçados.

3-7.5.1. A finalidade deve ser específica

A finalidade deve ser claramente determinada ou especificada para delimitar o âmbito do tratamento dos dados, e em consequência, os dados recolhidos são, apenas, os adequados e pertinentes. O n.º 2, do art.º 8º, da CDFUE estabelece claramente que os dados pessoais devem ser tratados «de forma justa para fins específicos», ou seja, o responsável pelo tratamento não deve recolher dados pessoais que não sejam necessários, adequados ou relevantes para os fins que se destinam, sendo uma condição necessária para o cumprimento da LPDP e do apuramento de responsabilidades.

O grau de especificação depende do contexto e em que os dados são recolhidos, devendo evitar-se a indicação de razões de forma muito vaga como, por exemplo, para «fins de marketing»[365]. Os dados podem ser recolhidos para mais do que uma finalidade relacionada ou não, desde que se cumpram os princípios e condições de legitimidade do tratamento todos inter-relacionados entre si.

3-7.5.2. A finalidade deve ser explícita

A finalidade deve ser explícita, ou seja deve ser explicada de forma clara, inequívoca e inteligível[366], sem ambiguidades ou dar lugar a dúvidas de interpretação, para qualquer tipo de audiência, no momento da recolha. A forma como a informação se transmite é flexível desde que cumpra os requisitos das normas que regulam a proteção de dados. Os recetores da informação, sobre os fins da recolha, são todos os intervenientes no processo do tratamento de dados, das autoridades de controlo, e bem assim, dos próprios titulares dos dados pessoais. As deficiências de comunicação podem dar lugar à impossibilidade do tratamento, ainda que os fins do tratamento estejam publicamente difundidos, por exemplo, nas páginas web, e reduz o risco de criar expectativas distintas não só dos titulares dos dados mas também do responsável pelo tratamento. Num mundo em que as pessoas são cada vez mais transparentes e o mundo virtual cada vez mais opaco (vide 2-2.4.), complexo e ambíguo, conforme já referido, a forma escrita assume extrema relevância, devendo o responsável pelo tratamento estar disponível para esclarecimentos adicionais.

[365] No caso sugere-se que se indique que os dados são tratados para fins de marketing dos bens e serviços promovidos pela entidade responsável pelo tratamento (há uma expectativa razoável da delimitação de receção de informação restringida à atividade comercial do responsável).

[366] A globalização dos suportes de informação introduz questões relacionadas com a linguística e respetivas traduções para as organizações, pelo que é necessário um cuidado acrescido, tendo em conta o público a quem se dirige tendo em conta a necessidade de traduções de contratos e políticas de privacidade.

3-7.5.3. A finalidade deve ser legítima

A finalidade deve ser legítima e vai além das condições de legitimidade referidas no art.º 7º da Diretiva 95/46/CE e art.º 6º, da LPDP, devendo ser interpretada no contexto do tratamento e em conformidade com os objetivos do tratamento. A legitimidade afere-se, igualmente, da concordância com os princípios gerais do direito, do direito internacional, do direito da EU, do direito nacional, podendo incluir outros elementos como os códigos de conduta e de ética dos setores, para determinar se os fins determinados para a recolha dos dados são legítimos. Dadas as circunstâncias do mundo em que se vive atualmente, e em constante mudança, a legitimidade de um determinado propósito também pode mudar ao longo do tempo, dependendo do desenvolvimento científico e tecnológico, e transformações na sociedade e atitudes culturais[367].

A utilização de programas de espionagem não maliciosos poderão ser autorizados, para recolha de dados, nomeadamente os testemunhos de conexão, que podem ser úteis na análise da eficácia da conceção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transações em linha. Sempre que se destinem a um fim legítimo, como por exemplo a facilitar a prestação de serviços de informação, a sua utilização deverá ser autorizada, na condição de que sejam fornecidas aos utilizadores informações claras e precisas, em conformidade com a Diretiva 95/46/CE, acerca da finalidade dos testemunhos de conexão por forma a assegurar que os utilizadores tenham conhecimento das informações colocadas no equipamento terminal que utilizam (Considerandos 24 e 25 da Diretiva 2002/58/CE).

Desde que sujeita a autorização da CNPD, nos termos do art.º 28º, da LPDP, em «determinadas circunstâncias é possível tratar os dados recolhidos para uma finalidade, no âmbito de outra finalidade diferente»[368] [369].

3-7.5.4. A incompatibilidade da finalidade

A utilização posterior dos dados para uma finalidade não pode ser incompatível com os fins para os quais os dados pessoais foram recolhidos inicialmente. Os dados pessoais só podem ser tratados para fins diferentes daqueles para os quais foram recolhidos se a mudança de

[367] V. GT29 - *Opinion 03/2013 on purpose limitation* [Em linha]. 00569/13/EN, WP 203. Brussels (Belgium), (02/04/2013). [Consult. 12 dez. 2016]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/ article -29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>

[368] CASTRO, cit. 38, p. 230.

[369] Por exemplo, os pedidos de comunicação do nome e morada de uma pessoa a um órgão da administração publica para que outra entidade instrua determinado expediente ou processo administrativo (*v.* o Parecer da CNPD, nº 22/2001, de 04/12 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/ bin/decisoes/Par/40_22_2001.pdf>).

finalidade for expressamente autorizada[370] pelo direito interno dos Estados-Membros ou do direito da UE[371], pelo que a conceptualização da incompatibilidade depende do sistema jurídico[372] e da apreciação das circunstâncias concretas da alteração da finalidade do tratamento[373] (art.º 8º, da CEDH, art.º 9, da Convenção 108, e al) d), do n.º 1, do art.º 28º, da LPDP).

Os dados obtidos através das diversas fontes de informação por meio de dispositivos inteligentes em IAm são suscetíveis de ser reutilizados e tornaram-se num desafio aos princípios e condições do tratamento de dados pessoais relacionados ou não com a finalidade do tratamento inicial. A reutilização[374] secundária dos dados para fins de marketing, salvo se for possível que as finalidades sejam compatíveis, deve cumprir as exigências previstas na al) b), do n.º 1, do art.º 6º, da Diretiva 95/46/CE e da al) b) do n.º 1, do art.º 5º, da LPDP. O interessado poderá não se opor à partilha inicial dos dados mas pode não querer que sejam utilizadas para outros fins.

A avaliação da compatibilidade dos fins deve começar pela relação entre os fins da recolha inicial e os propósitos de tratamento posterior, o contexto anterior e posterior à recolha dos dados, bem como as expectativas que tanto o responsável pelo tratamento como o titular dos

[370] A Deliberação 143/2002 da CNPD, de 09/06 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Delib/20_143_2002.pdf>, considerou o tratamento de dados relativos a nomes e moradas de cidadãos eleitores residentes no estrangeiro, da base de dados do recenseamento eleitoral, não é incompatível mas conexa com a propagando eleitoral, fundamentado no princípio da justificação social e interesse público relevante.

[371] «O tratamento posterior de dados pessoais para fins históricos, estatísticos ou científicos não é de modo geral considerado incompatível com as finalidades para as quais os dados foram previamente recolhidos, desde que os Estados-Membros estabeleçam garantias adequadas; que tais garantias devem em especial impedir a utilização de dados em apoio de medidas ou de decisões tomadas em desfavor de uma pessoa» (Considerando 29 e al) b) *in fine*, do n.º 1, do art.º 6º, da Diretiva 95/46/CE e n.º 2, do art.º 5º da LPDP).

[372] Num estudo citado pelo GT29, a noção de incompatibilidade nos Estados-Membros da UE fundamenta-se em distintos critérios: nas «expectativas razoáveis» da pessoa em causa (Bélgica) à aplicação de testes de equilíbrio (Alemanha e Países Baixos) ou intimamente ligados a outros princípios de salvaguarda da transparência, da legalidade e da equidade (Reino Unido e Grécia) (GT29, cit. 367, p. 10)

[373] Parágrafo 62, do Ac. *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi Oy, Satamedia Oy,* do TJUE, n.º C-73/07, de 16/12/2008, refere que o art.º 9.° da diretiva «deve ser interpretado no sentido de que as atividades referidas nas alíneas a) a d) da primeira questão, relativas a dados contidos em documentos que são públicos nos termos da legislação nacional, devem ser consideradas atividades de tratamento de dados pessoais efetuadas «para fins exclusivamente jornalísticos», na aceção dessa disposição, se as referidas atividades tiverem por única finalidade a divulgação ao público de informações, de opiniões ou de ideias, o que compete ao órgão jurisdicional nacional apreciar». A divulgação de dados a terceiros constitui frequentemente uma nova finalidade pelo que é necessário uma fundamentação legal distinta da que foi estabelecida para a recolha dos dados.

[374] É frequente, o Estado impor alguns limites àquilo que os cidadãos (e as empresas) podem fazer com a informação pública. A al) g), n.º 1, do art.º 3º, do L n.º 26/2016, de 22/08, que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo as Diretiva 2003/4/CE, 2/01 e 2003/98/CE, 17/11, encontramos uma definição de reutilização que *mutatis mutandis* se pode considerar para os efeitos indicados, ou seja, «a utilização, por pessoas singulares ou coletivas, de documentos administrativos, para fins comerciais ou não comerciais diferentes do fim inicial de serviço público para o qual os documentos foram produzidos». A definição constante do n.º 4, do art.º 2, da 2003/98/CE, 17/11 acrescenta que «o intercâmbio de documentos entre organismos do setor público exclusivamente no desempenho das suas funções não constitui reutilização».

dados tem sobre a reutilização dos dados invariavelmente para efeitos de promoção comercial e marketing. A avaliação da compatibilidade deve ter em conta todos os fatores e circunstâncias do caso em concreto, a natureza dos dados pessoais e as garantias adotadas para evitar impactos negativos na esfera jurídica dos titulares, sempre e quando não foi prestado o consentimento prévio ou foi cerceada a liberdade de escolha do titular dos dados. O responsável pelo tratamento deve considerar os critérios anteriormente descritos sem esquecer que a utilização dos dados para outros fins deve estar em conformidade com os princípios e condições de legitimidade previstos na LPDP.

O GT29[375] pronunciou-se, por diversas ocasiões, no sentido de que a recolha de endereços eletrónicos disponíveis nas páginas da internet[376], sem o conhecimento informado da pessoa interessada, é ilícita, e não poderão ser utilizados para fins de comercialização direta ou para marketing[377]. A utilização de endereços de correio eletrónico para marketing implica que o tratamento seja leal, lícito, transparente e obedeça às condições de legitimidade; e ainda, o facto de existir um desequilíbrio entre um custo adicional de tempo de ligação e o transtorno causado pelas grandes quantidades de publicidade não desejada pelo recetor, ou consumidor final, impossibilitando que o teste do equilíbrio[378], conforme previsto na Diretiva 95/46/CE, da LPDP, da Diretiva 2002/58/CE e da L n.º 41/2004, de 18/08. Sobre esta matéria, o envio

[375] Já anteriormente o CdE recomendava cautelas em relação à reutilização dos dados pessoais detidos pelas administrações publicas considerando fundamental a não utilização para fins incompatíveis para os quais foram inicialmente recolhidos, salvo se for considerada em conformidade com a Convenção 108 (CdE *Recommendation (91) 10 of the Committee of Ministers to Member States on the communication to third parties of personal data held by public bodies* [Em linha]. (09/09/1991) [Consult. 9 abr. 2015]. Disponível em WWW <https://search.coe.int/cm/Pages/ result_details.aspx?ObjectID=09000016804c1486>).

[376] A internet é uma rede de computadores que comunicam entre si com base no *Transport Control Protocol/Internet Protocol* (TCP/IP) e por isso constitui um canal de distribuição de informação e conhecimentos dos meios de comunicação e não um meio de comunicação em si mesmo e que tem diversos serviços disponíveis, por exemplo: o correio eletrónico, navegação, pesquisa, newsgroups, a *World Wide Web*, etc. O GT29 considera que «os serviços da internet são serviços de comunicações eletrónicas. Assim, a internet faz parte do setor público de telecomunicações» (GT29, cit. 222. p. 23).

[377] V. a título exemplificativo GT29 - Parecer 1/2000 relativo a certos aspetos da proteção de dados no comércio eletrónico. [Em linha]. 5007/00/PT/FINAL WP 28 Brussels (Belgium), (03/02/2000). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp28_pt.pdf>; Parecer 2/2000 relativo à revisão geral do quadro jurídico em matéria de telecomunicações. Apresentado pela *Task-Force* Internet [Em linha]. 009/00/PT/final WP 29 Brussels (Belgium), (03/02/2000). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/ justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp29_pt.pdf>; Parecer 5/2000 relativo ao uso de listas telefónicas públicas para serviços de pesquisa invertida ou multicritério (Listas invertidas) [Em linha]. 5058/00/ PT/FINAL, WP 33. Brussels (Belgium), (13/07/2000). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp33_en.pdf>; - Parecer 7/2000 sobre a Proposta de Diretiva do Parlamento Europeu e do Conselho apresentada pela Comissão Europeia relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas [Em linha]. 5042/00/PT/FINAL WP 36. Brussels (Belgium), (12/07/2000). [Consult. 10 nov. 2014]. Disponível em WWW <http://ec.europa.eu/justice/policies/privacy/docs/wp docs/2000/wp36pt.pdf>; GT29, cit 222 e 351.

[378] Conforme indicado na al) f), do art.º 7º, da Diretiva e al) e) do art.º 6º, da LPDP.

de comunicações não solicitadas para fins de marketing, está sujeito ao consentimento prévio expresso da pessoa em causa, conforme estabelecido no art.º 15º da Diretiva 2002/58/CE e o art.º 13º-A, da L 41/2004, de 18/08. (3.7.6).

A CNPD indica numerosos exemplos de incompatibilidade das finalidades posteriores por desvio às finalidades de recolha original[379], dos quais citamos os seguintes constantes do Parecer nº 22/2001, de 04/12/2001: «tendo o ficheiro da Ordem dos Advogados Portugueses como finalidade a gestão dos serviços da Ordem e gestão da informação atualizada da situação profissional dos advogados, considera-se compatível com a finalidade a utilização dos nomes e moradas com vista à divulgação de informações de interesse para a formação inicial ou permanente dos advogados – designadamente a realização de palestras, cursos e conferências. Os titulares dos dados podem opor-se à cedência de etiquetas a Universidades ou ao Centro de Estudos Judiciários. Não é compatível com a finalidade a utilização dos dados por organizações ou entidades, para fins de marketing estranhos às finalidades indicadas e às funções estatutárias da Ordem» e a cedência de informação dos ficheiros da Ordem dos Médicos «a laboratórios ou empresas que comercializam medicamentos não é compatível com as razões determinantes da recolha, na medida em que está em causa a informação e formação de médicos em relação a novos medicamentos. Os titulares uma vez informados da intenção de cedência a terceiros, podem opor-se à comunicação dos seus dados a estas empresas ou entidades».

Acresce ainda que as alterações dos fins para que foram recolhidos os dados podem ter um impacto negativo na esfera jurídica do titular dos dados em caso de considerar que perdeu o controlo sobre os seus dados, cujas consequências são desconhecidas porque dependem da reação de cada interessado. O critério da compatibilidade só se aplica às finalidades entre um tratamento inicial de dados e o tratamento posterior que se pretende realizar sobre os dados que foram recolhidos para um determinado tratamento original. Poderia colocar-se a questão da construção de perfis (3-9.3.5) mas esta não constitui uma finalidade mas um método de tratamento de dados pessoais que está ao serviço dos objetivos de marketing e comercialização direta pelos operadores económicos. A construção de perfis coloca questões relacionadas com a legitimidade sendo necessário o consentimento expresso e inequívoco prestado pelo cliente, por exemplo, no contexto de cartões de fidelização[380].

Os fornecedores de motores de pesquisa interessados em propostas comerciais diversas e

[379] O tratamento dos dados recolhidos em listas telefónicas e listas de correio eletrónico devem obedecer aos princípios referidos.
[380] V. GT29, cit. 219.

personalizadas generalizam as finalidades dos tratamentos dos dados pessoais, dando origem a opiniões contraditórias, quanto à legitimidade do tratamento, e que se apressam a fundamentar na prestação do consentimento, na necessidade da execução do contrato e na necessidade de prosseguir interesses legítimos do responsável pelo tratamento (al) a), b) e f), do n.º 1, do art.º 7º, da Diretiva 95/46/CE e al) a), b) e e), do n.º 1, do art.º 6º, da LPDP), com o fim de melhorar a prestação dos serviços, prevenir eventuais de fraudes, e manter segurança dos sistema informático, entre outros[381]. De igual modo, e dado que o marketing direto constitui uma parte essencial do modelo de negócios das plataformas das redes sociais e utiliza os dados pessoais dos utilizadores para apresentar comunicações comerciais com base na análise do seu comportamento em linha sua atividade, pelo que os responsáveis pelo tratamento de dados devem cumprir as regras estabelecidas nas Diretivas 95/46/CE e 2002/58/CE e LPDP e a L n.º 41 /2004, de 18/08[382].

3-7.5.5. Os critérios da aferição da compatibilidade das finalidades no RGPD

A Diretiva 95/46/CE e a LPDP permitem o tratamento de dados pessoais para novos fins, desde que esses novos fins não sejam incompatíveis com a finalidade inicial. O RGPD vem dificultar o tratamento de dados pessoais para novos fins, na medida em que a determinação dos critérios de compatibilidade pode ser onerosa. O n.º 6, do art.º 7º, do RGPD, indica os critérios a ter em conta para aferir da compatibilidade das finalidades: «quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da UE ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos incluindo o do direito de oposição, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:

a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais

[381] GT29, cit. 189.
[382] GT29 - Parecer 5/2009 sobre as redes sociais em linha [Em linha]. 01189/09/PT WP 163. Brussels (Belgium), (12/06/2009) [Consult. 12 dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommenda tion/files/2009/wp163_pt.pdf>

forem tratadas, ou se os dados pessoais relacionados com condenações penais e infrações[383];

d) As eventuais consequências, do tratamento posterior pretendido, para os titulares dos dados; e

e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização».

Nos termos da Diretiva 95/46/CE, da LPDP e do RGPD, os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, podendo ser posteriormente tratados de forma compatível com essas finalidades, contudo, a al) c), do n.º 1, do art.º 5º, RGPD, ao substituir a obrigação da recolha dos dados pessoais não sejam excessivos por uma obrigação mais restritiva no sentido de garantir que os dados pessoais sejam limitados ao necessário, obriga à reconsideração das operações de tratamento no que respeita ao tratamento de dados que não sejam estritamente necessários em relação aos fins relevantes.

3-7.6. O princípio da segurança

A segurança do tratamento de dados é uma obrigação do responsável do tratamento que deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito[384] (n.º 1, do art.º 14º, da LPDP). O nível de segurança é determinado pelos conhecimentos técnicos disponíveis, pelos custos resultantes da sua aplicação, e pelos riscos que o tratamento apresenta tendo em conta a natureza dos dados a proteger (art.º 15º, da LPDP). O princípio da segurança tem como objetivo essencial o impedimento de acesso por pessoas não autorizadas, a integridade[385], disponibilidade[386] e a confidencialidade[387] dos dados tratados (art.º 7º, da Convenção 108; art.ºs 16º e 17º, da

[383] «…deverá ser proibido proceder à transmissão no interesse legítimo do responsável pelo tratamento ou ao tratamento posterior de dados pessoais se a operação não for compatível com alguma obrigação legal, profissional ou outra obrigação vinculativa de confidencialidade…», conforme Considerando 50, do RGPD.

[384] *V.* n.º 11, das Linhas Diretrizes da Privacidade: «Os dados pessoais devem ser protegidos por salvaguardas de segurança razoáveis contra riscos como perda, acesso não autorizado, destruição, uso, modificação ou divulgação de dados».

[385] A informação manipulada durante o tratamento mantém as características originais ou as que foram sujeitas a retificação e atualização pelo titular dos dados.

[386] Consiste na capacidade que tem utilizador autorizado de aceder à informação.

[387] *V.* Ac. I. vs. Finlândia, do TEDH, nº 25.511/03, de 17/07/2008, em que à data dos factos, as fichas clínicas podiam ser lidas pelo pessoal hospitalar que não estava diretamente envolvido no processo da requerente à qual foi diagnosticado uma infeção pelo vírus VIH. Embora o hospital tenha tomado posteriormente passos para colocá-la a salvo de divulgação não autorizada, limitando acesso ao seu arquivo e registo da requerente sob um nome falso e um novo número segurança social, estas medidas foram tomadas demasiado tarde.

Diretiva 95/46/CE). A segurança dos dados inclui a infraestrutura que a suporta, os sistemas informáticos, mecanismos de cifração, de controlo de acesso e certificação, protocolos, medidas preventivas e documentação que fazem parte do tratamento de dados.

O dever de confidencialidade sobre os dados objeto do tratamento é tratado de forma específica (art.º 16º, da diretiva 95/46/CE, art.º 17º, da LPDP), na medida em que deve ser cumprido por todos os intervenientes[388] no processo de tratamento não só enquanto dura como subsiste após a finalização do mesmo e em relação a outras normas (nomeadamente o dever de sigilo das profissões reguladas). A violação do dever de sigilo é punida com prisão até dois anos ou multa até 240 dias (art.º 47º, da LPDP).

Portugal na transposição da Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, introduziu o art.º 3º-A, na L n.º 41/2004, de 18/08, regula as notificações com violações da segurança dos dados, o qual prevê que as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem, sem demora injustificada, notificar a CNPD da ocorrência de violação de dados pessoais e quando possa afetar negativamente[389] os dados pessoais do assinante ou utilizador, devem ainda, sem demora injustificada, notificar a violação ao assinante ou ao utilizador, para que estes possam tomar as precauções necessárias.

3-7.6.1. O princípio da segurança no RGPD

Nos termos da al) f), do n.º 1, do art.º 5º, e 32º a 34º, do RGPD, o responsável pelo tratamento deve garantir a segurança dos dados, «incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)». Os responsáveis pelo tratamento gozam de liberdade na escolha dos meios que consideram adequadas, em função dos factos e das circunstâncias de cada caso particular, com especial atenção para o risco associado ao tratamento e aos tipos de dados. O RGPD estabelece uma obrigação de resultado aos responsáveis pelo tratamento porque para além de serem capazes

[388] Ainda que a obrigação de confidencialidade esteja prevista na LPDP, seria altamente recomendável incluir clausulas de confidencialidade nos contratos de prestação de serviços ou contratos de trabalho que as respetivas parte contratantes se obrigavam ao sigilo profissional, mesmo após o termo das suas funções, no que respeita ao conhecimento de dados pessoais incorporados nos ficheiros da organização onde presta a atividade profissional, considerando diversos aspetos, como por exemplo, a definição do período de tempo da obrigação, indicar quais são as informações consideradas confidenciais e em caso aplicável, as exceções, a obrigação de entrega de cópias ou documentos, independentemente do suporte, que se teve acesso em resultado da atividade profissional; entre outras consideradas oportunas.

[389] Nos termos do n.º 3, do art.º 3º-A, da L n.º 41/2004, de 18/08, «uma violação de dados pessoais afeta negativamente os dados ou a privacidade do assinante ou utilizador sempre que possa resultar, designadamente, em usurpação ou fraude de identidade, danos físicos, humilhação significativa ou danos para a reputação, quando associados à prestação e utilização de serviços de comunicações eletrónicas acessíveis ao público».

de implementar as medidas referidas devem, igualmente, de ser capazes de demonstrar que atuaram com diligência (n.º 2, do art.º 5, do RGPD), com a promoção e implementação de uma cultura da proteção de dados desde a conceção e por defeito (Considerando 78 e art.º 25º, do RGPD), dentro da sua organização. O responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. O resultado das avaliações pode influenciar a decisão na escolha das medidas de segurança. O RGPD também promove o recurso aos códigos de conduta aprovados pela CNPD (art.ºs 40, 41º e 57º, nº 1, do RGPD) assim como aos mecanismos de certificação[390] acreditados pelas autoridades de controlo (art.ºs 42 e 43º, do RGPD), sem obrigatoriedade, mas a demonstração do cumprimento das normas de proteção de dados pessoais torna-se mais fácil tal como potenciais colaborações com terceiros.

A violação da segurança da informação pode conduzir o incumprimento de uma norma da proteção de dados e deixar uma organização exposta a sanções cujo impacto pode ser muito relevante[391]. As entidades que sofram uma violação de dados pessoais[392] devem notificar a

[390] A norma ISO/IEC 27001:2013 - Tecnologia da informação - técnicas de segurança - sistemas de gerência da segurança da informação», aprovada e publicada em outubro de 2005, revista em 2013 pela *International Organization for Standardization* e pela *International Electrotechnical Commission*, é a principal norma internacional para a segurança da informação e certificada de acordo com a metodologia dos Sistemas de Gestão de Segurança da Informação (SGSI) que permite a gestão da segurança de forma clara e demonstrara que estão implementados e estão em conformidade com uma norma padrão e é considerada como uma das opções para a implementação dos processos necessários ao tratamento dos dados com segurança (V. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO/IEC 27001:2013(en) *Information technology — Security techniques — Information security management systems — Requirements* [Em linha]. 1ª ed., International Organization for Standardization, 2013. [Consult.14 out. 2016]. Disponível em WWW <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>).

[391] Os profissionais de marketing precisam de ter cuidado na partilha de informação de clientes, especialmente quando é considerado sensível ou existirem os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares. Os danos específicos decorrentes da partilha de informações incluem, entre outros: (1) violação da confidencialidade: quando terceiros se apropriam, por exemplo, de dados bancários por terceiros para pagamento de bens e serviços; (2) divulgação: quando a reputação de uma pessoa é afetada por revelar informações verdadeiras sobre eles; (3) exposição: quando questões íntimas são expostas publicamente; (4) chantagem: quando se exige algo em troca para não divulgar informações consideradas normalmente inadequadas; (5) apropriação: quando alguém, por exemplo, se apropria da identidade de outro; e (6) distorção: quando se revelem informações enganosas ou falsos sobre os titulares dos dados, por um lado, podendo ocorrer que sejam tomadas decisões com base em informações desatualizadas dos clientes, sobre tudo quando se recorre à construção de perfis. A empresa Yelp processou uma sociedade de advogados por afixar comentários falsificados, no decorrer da investigação, o procurador-geral de Nova Iorque anunciou US $ 350.000 em multas contra 19 empresas por escrever críticas negativas falsas nas suas páginas e noutras como por exemplo, nas páginas web Yelp, Google Local e CitySearch. A Yelp avalia organizações empresariais baseada nas críticas dos consumidores e constrói perfis que ficam disponíveis para consulta e que se vieram a revelar totalmente irreais, dando origem a problemas de reputação de imagem para a própria empresa Yelp como também para os seus clientes (v. MASNICK, Mike - *The war on fake reviews ramps up: NY fines companies for fake Yelp reviews. In Techdirt.* [Em linha]. (27/09/2013) [Consult. 19 jan. 2016]. Disponível em WWW <https://www.techdirt.com/articles/20130927/01425424673/war-fake-reviews-ramps-up-ny-fines-companies-fake-yelp-reviews.shtml>)

[392] O n.º 12, do art.º 4º, do RGPD define a violação de dados pessoais como «uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento».

autoridade de controlo competente sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares (n.º 1, do art.º 33º, do RGPD) e quando seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, também, comunica a violação de dados pessoais ao titular dos dados sem demora injustificada (n.º 1, do art.º 34º, do RGPD).

No contexto atual, é tecnicamente impossível garantir a segurança e a proteção absoluta dos dados pessoais, por isso a obrigação específica do princípio consiste na garantia razoável e adequada de que o responsável pelo tratamento utilizou os procedimentos técnicos necessários, pelo que não será exigível considerar a existência de violação de dados sempre que haja a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados aos dados na medida em que se requer um juízo razoável e fundamentado perante cada caso concreto.

3-7.7. O princípio da responsabilidade

O princípio da responsabilidade procurar garantir a aplicação das normas que regulam a proteção de dados (art.º 4º, da diretiva 2002/58/CE, n.º 2, do art. 6º, da Diretiva 95/46/CE e art.ºs 15º e 34º, da LPDP). Este princípio está intimamente relacionado com a transmissão de dados e acautelar o acesso aos ficheiros por pessoas não autorizadas, bem como evitar que o titular perca o controle sobre suas informações pessoais.

O n.º 2, do art.º 5º, e art.º 24º, do RGPD prevê que o responsável pelo tratamento é responsável pelo cumprimento dos princípios do tratamento de dados (tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis) aplica as medidas técnicas e organizativas que forem adequadas para assegurar, para poder comprová-lo. A disposição teve inspiração no conceito oriundo do direito anglo-saxónico que significa que a responsabilidade é assumida pelo responsável do tratamento e é capaz de o demonstrar, ou seja, é capaz de explicar as suas ações. E é por isso que o responsável pelo tratamento de dados deve designar, se for o caso, um encarregado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções descritas pelo regulamento (n.º 5, do art.º 37, e art.º 39º, do RGPD).

CAPÍTULO VIII – AS CONDIÇÕES DE LEGITIMIDADE DO TRATAMENTO DE DADOS PESSOAIS

3-8. As condições de legitimidade do tratamento de dados pessoais

As condições de legitimidade do tratamento de dados, na organização sistemática tanto da Diretiva 95/46/CE como da LPDP, são enumeradas imediatamente a seguir aos princípios do tratamento dos dados. O tratamento de dados, ainda que sejam cumpridas todas as disposições quanto aos princípios, não é possível se não houver fundamento.

A relevância das condições de legitimidade do tratamento é refletida na CDFUE, que estabelece no n.º 2, do art.º 8º, que os dados são tratados «com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei», tendo-se baseado no artigo 8.º da CEDH, na Convenção 108 e da própria Diretiva 95/46/CE[393]. É certo que não existe uma correspondência direta do art.º 8º, da CEDH, mas a jurisprudência do TEDH tem sido abundante desde que considerou que a recolha de dados dos órgãos públicos, conservação e transferência de dados é suscetível de representar uma violação sobre a referida norma[394].

O art.º 7º, da Diretiva 95/46/CE e o art.º 6º, da LPDP, estabelece que o tratamento de dados pessoais só pode ser efetuado se o seu titular tiver dado, de forma inequívoca, o seu consentimento ou se o tratamento for necessário para: (1) a execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido; (2) o cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito; (3) a proteção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento; (4) a execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; e (5) a prossecução de interesses legítimos (3-9.1.) do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.

A legitimidade do tratamento é fundamentada no consentimento do titular dos dados, salvo exceção prevista na lei, sendo o eixo central do direito à proteção de dados pessoais. A enumeração, indicada no art.º 7º, da Diretiva 95/46/CE, das condições de legitimidade é taxativa e não pode ser alterada pelos Estados-Membros nem acrescentar outros requisitos[395].

---

[393] Conforme anotação ao art.º 8, relativa à carta dos direitos fundamentais (2007/C 303/02).
[394] Ac. *Leander v. Sweden*, do TEDH nº 9.246/81, de 26/03/1987.
[395] Neste sentido, o Ac. *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación*

A seleção de um ou mais fundamentos de legitimidade pelo responsável pelo tratamento[396], embora não esteja expresso na LPDP, deve ser efetuada antes de iniciar o tratamento dos dados. A escolha pelo responsável (com exceção do consentimento) não está isenta de realizar um «teste de necessidade que limita de forma estrita o seu âmbito de aplicação»[397]. O conceito de necessidade é um conceito autónomo de direito da EU, não podendo ter conteúdo variável consoante os Estados-Membros[398] e limita o contexto em que cada fundamento é aplicável. A escolha do fundamento para legitimar o tratamento dos dados não exime o responsável pelo tratamento de cumprir com os princípios do tratamento de dados previstos no art.º 6º, da Diretiva 95/46/CE e do art.º 5º, da LPDP. Os fundamentos de legitimidade são alternativos no art.º 7º, da Diretiva 95/46/CE e do art.º 6º, da LPDP, mas cumulativos com os princípios previstos no art.º 6º, da Diretiva 95/46/CE e do art.º 5º, da LPDP[399].

A reflexão sobre o consentimento é analisada com maior detalhe dada a importância e impacto sobre o tratamento dos dados pessoais para fins de marketing.

3-8.1. O consentimento

O consentimento é o eixo central das normas sobre a proteção de dados na medida em que é o titular dos dados quem decide, como, quando e porque é que os seus dados são tratados – poder de decisão que deriva do direito à autodeterminação informativa[400] e porque o «regime da proteção de dados é subscrito por uma ética de direitos e quando esta ética é baseada numa escolha duma teoria de direitos, não há forma como escapar ao facto que o consentimento tem de ser central para este regime»[401]. O tratamento de dados pessoais pode ser efetuado se o seu

---

de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, do TJUE, apensos n.ºs C-468/10 e C-469/10, de 24/11/2011 *(vide* os parágrafos 36 a 39 e 95 a 99).

[396] Um simples contrato de compra e venda pode abranger todos os fundamentos de legitimidade do tratamento de dados.

[397] GT29 - Parecer 15/2011 sobre a definição de consentimento [Em linha]. 01197/11/PT WP 187. Brussels (Belgium), (13/07/2011). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/ files/2011/wp187_pt.pdf>, p. 8.

[398] Conforme parágrafo 52, do Ac. *Heinz Huber v. Bundesrepublik Deutschland*, do TJUE, n.º C-524/06, de 16/12/2008: «Por conseguinte, face ao objetivo de assegurar um nível de proteção equivalente em todos os Estados-Membros, o conceito de necessidade, tal como ele resulta do artigo 7.º, alínea e), da Diretiva 95/46, que se destina precisamente a delimitar uma das hipóteses em que o tratamento de dados pessoais é lícito, não pode ter um conteúdo variável consoante o Estado-Membro. Logo, trata-se de um conceito autónomo de direito comunitário que deve receber uma interpretação suscetível de cumprir plenamente o objetivo dessa diretiva, definido no seu artigo 1.º, n.º 1».

[399] V. GT29 - Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE [Em linha]. 844/14/PT, WP 217. Brussels (Belgium), (09/04/2014). [Consult. 12 Dez. 2016]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf>.

[400] MARCOS, cit. 218, p. 229.

[401] V. BROWNSWORD, Roger - *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*. in GUTWIRTH; Serge [*et al.*] - *Reinventing Data Protection*? [Em linha]. New York [etc.]:

titular tiver dado[402] de forma inequívoca o seu consentimento. Nos termos da al) h), do art.º 2º, da Diretiva 95/46/CE e al) h), do art.º 3º da LPDP, o consentimento é definido como «qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento»[403]. O consentimento está intimamente ligado à obrigação de informar, nos termos dos art.ºs 10º e 11º da Diretiva 95/46/CE e do art.º 10º, da LPDP, a cargo do responsável para ser prestado conforme a seguir se descreve tendo em conta a definição legal, interpretação jurisprudencial e administrativa, e ainda doutrinal.

3-8.1.1. O consentimento inequívoco

O consentimento é inequívoco quando resulta de ações cometidas e expressas pelo titular dos dados, manifestando a sua aceitação sem dar origem a interpretações duvidosas e ambíguas, independentemente do tipo de mecanismo para a sua obtenção. O consentimento não se deduz nem pode ser baseado na omissão ou silêncio[404], sobretudo num contexto em linha. O consentimento é suscetível de fazer prova[405] e os responsáveis pelo tratamento devem adotar as medidas e os procedimentos adequados para demonstrar que o consentimento foi dado. «Quanto mais complexo for o ambiente em que aqueles atuam, mais medidas serão necessárias para assegurar que o consentimento é suscetível de ser verificado»[406], ou seja, quanto menor for a capacidade de compreensão de um cidadão médio de entender, maiores serão os esforços do responsável pelo tratamento em demonstrar que prestou todas as

---

Springer Science + Business Media B.V. 2009. [Consult. 10 dez. 2014]. Disponível em WWW <https://link.springer.com/book/10.1007/978-1-4020-9498-9> ISBN 978-1-4020-9498-9. p. 87. Tradução da responsabilidade da mestranda, do original em inglês: «*Where a data protection regime is underwritten by an ethic of rights and where (as I take it) the ethic is based on a choice (or will) theory of rights, there is no escaping the fact that consent must be central to that regime*».

[402] Ao consentimento, também, são aplicáveis outros requisitos previstos no direito civil, nomeadamente os da declaração negocial e da capacidade jurídica, e aplicáveis no contexto da proteção de dados sob pena de ser inválido.

[403] O tratamento de dados sensíveis com base no consentimento exige um consentimento (para além de inequívoco, livre, específico e informado) explícito, nos termos da al) a), n.º 2, do art.º 8º, da Diretiva 95/46/CE, ou expresso na redação portuguesa, nos termos do n.º 2, do art.º 7º da LPDP.

[404] Neste sentido, o GT29: «A clarificação deveria procurar sublinhar que o requisito do consentimento inequívoco obriga ao uso de mecanismos que não deixem qualquer dúvida de que a pessoa em causa teve a intenção de dar o seu consentimento. Simultaneamente deve ser clarificado que a utilização de configurações predefinidas, que têm de ser alteradas pela pessoa em causa para rejeitar o tratamento (consentimento baseado no silêncio) não conduz a um consentimento inequívoco. Isto é especialmente verdade num ambiente em linha» (GT29, cit. 397, p. 25).

[405] A este propósito o GT29 refere que os «responsáveis pelo tratamento podem desejar ou necessitar de provar que o consentimento foi efetivamente prestado, designadamente numa situação de litígio. Com efeito, em alguns casos, tal prova pode ser exigida no contexto de medidas de aplicação coerciva. Os responsáveis pelo tratamento de dados devem, por conseguinte, e por uma questão de boa prática, gerar e conservar provas de que o consentimento foi efetivamente dado, ou seja, o consentimento deve ser suscetível de verificação» (GT29, cit. 382, p. 24).

[406] GT29, cit. 397. p. 28.

informações necessárias no momento do pedido e aceitação do consentimento pelo titular dos dados. A questão da prova assume especial relevância no RGPD, na medida em que o consentimento deve estar documentado e o responsável ser capaz de comprovar (n.ºs 1 e 2, do art.º 7º, do RGPD) que foi aceite pela pessoa em causa (3-7.7.).

3-8.1.2. O consentimento livre

O consentimento é livre quando resulta de uma decisão voluntária tomada de acordo com os princípios gerais de direito civil e do direito à proteção de dados, sem qualquer tipo de coação, de caráter social, financeiro, psicológico, sem consequências que possam comprometer a liberdade de escolha da pessoa[407], ou outro. O RGPD esclarece que se a declaração do consentimento estiver previamente formulada pelo responsável do tratamento deverá ser apresentada ao titular dos dados «de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas[408]» (Considerando 42, do RGPD).

O consentimento é livre na medida em que o titular dos dados puder recusar o seu tratamento sem consequências, por exemplo, de ordem económica[409] ou emocional, e puder revogar sem penalizações[410] e com efeitos retroativos[411]. O RGPD refere expressamente que o consentimento não será válido se existir «um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento» nos poderes em que é investido ou se não puder ser separado para diferentes operações de tratamento (Considerando 43 e 44, do RGPD).

---

[407] O GT29 realça que o «consentimento de uma pessoa em causa a quem não foi concedida uma liberdade de escolha genuína ou que foi confrontada com um facto consumado não pode ser considerado válido» (v. GT29 - Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos (RSE) [Em linha]. 00323/07/PT, WP 131. Brussels (Belgium), (15/02/2007). [Consult. 12 dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files /2007/wp131_pt.pdf>, p. 9).

[408] A questão da confiança na notificação das políticas de privacidade e condições de utilização disponíveis nas páginas web foi objeto de um estudo no Reino Unido, concluindo-se que os indicadores não conseguiram alcançar a complexidade do seu conteúdo bem como estava fora de controlo dos utilizadores. O estudo revelou que a política de privacidade e condições de utilização de PayPal com 36.275 palavras superava a obra "Hamlet" de Shakespeare, de Apple iTunes com 19.972 palavras superava a obra "Macbeth" de Shakespeare; de Facebook com 11.195 palavras superava a obra "Teoria Geral da Relatividade" de Einstein, entre muitas outras referências. A extensão e a complexidade jurídica dos documentos levam a que o utilizador aceite os termos e condições na íntegra sem ler (ou tomar conhecimento) antes de concordar em utilizar os serviços propostos. Ler ou não ler (PayPal), ouvir ou não ouvir (Apple iTunes), eis a questão! O estudo pode ser consultado aqui: <https:// conversation.which.co.uk /technology/length-of-website-terms-and-conditions/>

[409] Uma das consequências poderá ser perda de um emprego quando o titular dos dados se encontre num contexto laboral que diminua a sua liberdade de escolha.

[410] Exceto as que resultarem da cessação dos benefícios que possam, eventualmente, resultar da utilização de dados objeto do consentimento dado anteriormente, por exemplo, o acesso gratuito a determinados serviços.

[411] *V.* Deliberação da CNPD, n.º 227/2007, de 28/05 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Delib/20_227_2007.pdf>, aplicável aos tratamentos de dados pessoais efetuados no âmbito de estudos de investigação científica na área da saúde.

O exercício do direito de revogação não está sujeito a justificação ou a prazos[412]. O n.º 3, do art.º 7º do RGPD, prevê que o titular dos dados tem direito a retirar o seu consentimento a qualquer momento de forma tão fácil como aquela em que foi dado.

3-8.1.3. O consentimento específico

O consentimento específico refere-se a um tratamento de dados para fins (3-7.5.) determinados[413] e legítimos do responsável do tratamento. Dado que o consentimento específico se refere a uma «contextualização factual concreta, a uma atualidade cronológica precisa e balizada e a uma operação determinada»[414], deve conformar-se com as expectativas do titular dos dados que assume caráter relevante, quanto a um tratamento razoável e necessário em relação ao fim que se destina[415]. A análise da contextualização deve ser flexível e interpretar-se de forma razoável tendo em conta o ambiente tecnológico que evolui rapidamente e varia segunda as circunstâncias de cada caso. O consentimento específico «afasta os casos de consentimento preventivo e generalizado, prestado de modo a cobrir uma pluralidade de operações»[416].

3-8.1.4. O consentimento informado

A informação é o pressuposto do consentimento informado (3-7.2.1.). O consentimento informado requer que o titular dos dados, e do direito à informação, tenha conhecimento prévio[417] do tratamento de dados assim como das suas finalidades[418]. O responsável pelo

[412] O consentimento prestado pode sempre ser revogável nos termos do n.º 2, do art.º 81º do CC. «A revogação do consentimento deve dar lugar à imediata destruição dos dados e é lícita, embora possa fazer incorrer o titular na obrigação de indemnizar os danos causados pela revogação» (v. VASCONCELOS, Pedro Pais de - Proteção de Dados Pessoais e Direito à Privacidade, in Direito da Sociedade da Informação, Coimbra : Coimbra Editora, 1999. ISBN:972-32-0916-0. Vol. I, p. 252).

[413] Com interesse, Ac. *Deutsche Telekom AG vs Bundesrepublik Deutschland*, do TJUE, n.º C-543/09, de 05/05/2011, o requerente tendo prestado consentimento para a publicação dos números de números que lhe foram atribuídos, numa lista de assinantes de determinada sociedade e transmitida a outra empresa com vista à publicação de uma lista pública impressa ou eletrónica, ou à disponibilização para consulta de tais listas por intermédio de serviços de informações, não deve ser objeto de um novo consentimento pelo assinante. O consentimento diz respeito ao fim a que se destina a publicação dos dados de caráter pessoal numa lista pública e não à identidade de um fornecedor de lista em concreto.

[414] *Vide* Deliberação da CNPD, n.º 227/2007, cit. 411.

[415] GT9, cit. 397

[416] *V.* nota 18.

[417] O tratamento de dados só pode ser realizado após obtenção do consentimento que depende da informação prestada pelo responsável do tratamento.

[418] A noção de consentimento informado teve origem no contexto da investigação médica e do desenvolvimento do Código de Nuremberga, que estabeleceu o direito de deixar a investigação médica e revogando efetivamente qualquer consentimento implícito (v. HOEYER, Klaus (2009) *Informed consent: The making of a ubiquitous rule in medical practice.* [Em linha]. Organization, Vol. 16, n.º 2, p. 267-288. Washington DC : SAGE Publications, 2009. [Consult. 17 out. 2015]. Disponível em WWW <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1. 838.6147&rep=rep1&type=pdf> ISSN 1350–5084.).

tratamento, entre o dever de informar e a obtenção do consentimento, deve verificar se o titular dos dados tomou conhecimento do objeto do consentimento sem dificuldades, em linguagem adequada e compreensível. A acessibilidade e a visibilidade das informações são elementos importantes quando estão disponíveis em linha. De facto, nas páginas web podem existir tratamentos automatizados de dados pessoais que são realizados de forma invisível representados, sobretudo, pelos testemunhos de conexão e o utilizador não tem consciência que os seus dados podem ser recolhidos, tratados e utilizados para fins que desconhece. O titular dos dados deve ser informado previamente de que a página em visualização utiliza um ou mais testemunhos de conexão para recolher e conservar os dados fornecidos (3-9.3.).

3-8.2. O consentimento no RGPD

Nos termos do n.º 11, do art.º 4º, do RGPD, o consentimento do titular dos dados é uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

O RGPD vem acrescentar à manifestação de vontade, livre, específica e informada que seja explícita e que seja prestado mediante declaração ou ato positivo inequívoco. O consentimento explícito, ou expresso, afasta o valor declarativo das declarações tácitas[419], privilegiando-se a segurança jurídica e a obtenção dos meios de prova. A validade da declaração do consentimento expresso não depende de nenhuma forma especial[420], salvo quando a lei o exigir (art.º 219.º, do CC), e desde que traduza uma vontade séria, livre e esclarecida do titular.

O conceito de consentimento foi reforçado e os responsáveis pelo tratamento dependem do consentimento separado de outros termos e condições, assim como das políticas de privacidade, para o tratamento de dados no âmbito do RGPD. E tanto assim é que a relevância dada ao consentimento pode basear-se em vários fundamentos, de que se destacam os

[419] «O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento» (Considerando 32, do RGPD)

[420] Neste sentido, «O consentimento do utilizador pode ser dado por qualquer forma adequada que permita obter uma indicação comunicada de livre vontade, específica e informada sobre os seus desejos, incluindo por via informática ao visitar um sítio na internet» (Considerando 17, da Diretiva 2002/58/CE). Também o n.º 2, do art.º 7º, que parece não limitar à forma escrita a prestação do consentimento: «Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples» e o Considerando 32 «uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais», ambos do RGPD.

seguintes: (1) capacidade de demonstração de que o titular dos dados consentiu no seu tratamento, (2) os requisitos para apagamento dos dados (o RGPD refere que dever ser tão fácil para os titulares dar como retirar o consentimento, isto é uma forma que o titular tem de poder controlar em todas as fases o tratamento dos seus dados), (3) os titulares consentem no tratamento dos dados mas também tem um direito à portabilidade, ou seja o responsável deve ter a capacidade de extrair os dados para transferi-los caso seja solicitado, (4) tendo em conta os elementos da definição do consentimento, o responsável pelo tratamento enfrenta o risco de invalidade de políticas de privacidade e condições de utilização demasiado extensas e complexas.

As alternativas ao consentimento, para a legitimidade do tratamento dos dados, estão taxativamente previstas nas al) b) a f), do n.º 1, do art.º 6º, do RGPD, que se transcrevem:

1. O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
2. O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
3. O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
4. O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
5. O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

CAPÍTULO IX – AS REGRAS ESPECÍFICAS DO TRATAMENTO DE DADOS PESSOAIS PARA MARKETING

3-9. As regras específicas do tratamento de dados pessoais para marketing

Com a evolução da tecnologia surgiram novas práticas de marketing recorrendo à promoção comercial e distintas formas de publicidade incorporadas em objetos inteligentes interligados na IdC. As comunicações são cada vez mais automatizadas, sofisticadas e direcionadas de acordo com os padrões de comportamento previamente rastreados. A par da L n.º 6/99, de 27/01, que regula a publicidade domiciliária, a L nº 41/2004, de 18/08, aplica-se ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação, especificando e complementando as disposições da LPDP. Assim, a LPDP, que transpõe a Diretiva 95/46/CE, estabelece o regime geral da proteção de dados, sem excluir outros direitos fundamentais, regula também o tratamento dos dados para efeitos de marketing, independentemente do canal de comunicação utilizado e aplica-se sempre que não exista norma especial. Tendo em conta o tipo de marketing e o suporte da promoção de bens e serviços, serão considerados os regimes[421] seguintes:

1. O direito incondicional de oposição ao marketing direto, concebido para o contexto tradicional do correio postal e para a publicitação de produtos análogos, por telefone ou telecópia, nos termos dos art.ºs 3º e 4º, da L n.º 6/99, de 27/01.
2. A exigência de consentimento no que respeita à utilização de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares, nos termos do n.º 1, do art.º 13º-A, da L n.º 41/2004, de 18/08.
3. A exigência de consentimento no que respeita ao armazenamento de informações e a possibilidade de acesso à informação armazenada no equipamento terminal, nos termos do art.º 5º, da L n.º 41/2004, de 18/08.

Atualmente encontra-se em discussão a pRPCE, com o objetivo de «proporcionar um nível elevado de proteção da privacidade aos utilizadores de serviços de comunicações eletrónicas e

[421] Seguindo as orientações GT29 em numerosos pareceres.

condições de concorrência equitativas para todos os intervenientes no mercado (…) e garantindo a coerência com o RGPD»[422].

3-9.1. O direito incondicional de oposição

A promoção de bens e serviços é concretizada através da publicidade que nas denominadas economias de mercado livre goza de proteção constitucional, conforme resulta das liberdades de iniciativa privada, da liberdade de expressão e informação, e da criação cultural, todos previstos no art.ºs 61º, 37º e 42º, da CRP[423]. Nos termos do n.º 2, do art.º 60º, da CRP, a publicidade é disciplinada por lei, sendo proibidas todas as formas de publicidade oculta, indireta ou dolosa. A atividade da publicidade e os meios de promoção de bens e serviços estão submetidos a um determinado regime legal em conformidade aos direitos dos consumidores e titulares dos dados.

Nos termos da al) e) do art.º 6º, da LPDP e da al) f), do art.º 7º, da Diretiva 95/46/CE, o responsável pelo tratamento ou terceiro a quem os dados sejam comunicados, pode ter um interesse legítimo no tratamento de dados para promover os bens e serviços da sua organização, ou seja para fins de marketing direto.

O interesse legítimo está subordinado a um teste de ponderação, realizado *a priori*, de relação

[422] *A lex specialis* sobre o tratamento de dados está prevista no art.º 6º da pRPCE, referindo que os fornecedores de redes e de serviços de comunicações eletrónicas podem tratar dados de comunicações eletrónicas: (a) se for necessário para assegurar a transmissão da comunicação, se for necessário para manter ou restabelecer a segurança das redes e serviços de comunicações eletrónicas, e ainda, para detetar falhas técnicas e/ou erros na transmissão das comunicações eletrónicas, durante o período necessário para esse efeito; (b) exclusivamente para efeitos da prestação de um serviço específico a um utilizador final, se tiver dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas e a prestação desse serviço não puder ser efetuada sem o tratamento desse conteúdo; ou se todos os utilizadores finais em causa tiverem dado o seu consentimento para o tratamento do conteúdo das suas comunicações eletrónicas para uma ou mais finalidades específicas que não possam ser atingidas através do tratamento de informações tornadas anónimas e o fornecedor tiver consultado a autoridade de controlo, segundo as regras previstas no RGPD; e (c) o tratamento dos metadados pode ser efetuado se for necessário para cumprir as obrigações em matéria de qualidade do serviço, proceder à faturação, calcular o pagamento das interligações, detetar ou impedir a utilização abusiva ou fraudulenta de serviços de comunicações eletrónicas ou a subscrição desses serviços, e ainda, se o utilizador final em causa tiver consentido o tratamento dos metadados das suas comunicações para uma ou várias finalidades específicas, desde que a finalidade ou finalidades em causa não possam ser atingidas através do tratamento de informações tornadas anónimas. O ac. do TC, nº 403/2015 de 27/08/2015, pronunciou-se sobre uma questão colocada sobre o tratamento e acesso aos metadados dos utilizadores dos serviços de telecomunicações, em sede de fiscalização preventiva da constitucionalidade do Decreto n.º 426/XII da AR, que aprova o Regime Jurídico do Sistema de Informações da República Portuguesa, declarando inconstitucional o n.º 2, do art.º 78º, dado que o acesso aos metadados previsto (fonte, destino, data, hora, duração, tipo de comunicação, equipamento de telecomunicações, localização) configura uma ingerência nas telecomunicações e não oferece garantias suficientes de salvaguarda de direitos fundamentais, como a vida privada (v. COMISSÃO - Proposta de Regulamento Do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas) [Em linha]. COM(2017) 10 final 2017/0003 (COD), Bruxelas, (10/01/2017) [Consult. 1 fev. 2017]. Disponível em WWW <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017PC0010 &from=EN>)

[423] V. CANOTILHO, MOREIRA, cit. 179, p. 787-797, 569-576 e 618-623.

entre os interesses legítimos do responsável pelo tratamento e aos interesses ou aos direitos fundamentais das pessoas em causa, cujos fatores devem ser flexíveis para atingir um justo equilíbrio na avaliação final, nomeadamente: (1) a natureza e a origem do interesse legítimo; (2) os impactos nas pessoas em causa - por exemplo, a forma como os dados são tratados, as expectativas razoáveis do titular, o estatuto do responsável pelo tratamento dos dados e da pessoa em causa; e (3) outras garantias complementares para evitar um impacto indevido nas pessoas em causa - a minimização dos dados, medidas técnicas e organizativas para assegurar que os dados não possam ser utilizados para tomar decisões ou outras medidas em relação às pessoas, e medidas complementares para aumentar a transparência e a responsabilidade[424]. O conceito de interesse legítimo deve estar contextualizado, ser real e atual. O responsável pelo tratamento deve justificar o interesse legítimo para o tratamento de dados sem descurar o cumprimento das demais normas previstas na LPDP, e nomeadamente, os princípios do tratamento[425].

3-9.1.1. O caso da publicidade domiciliária

O direito incondicional de oposição ao marketing direto está, atualmente e essencialmente, dirigido ao contexto tradicional do correio postal e publicitação de forma análoga, nos termos dos art.ºs 3º e 4º, da L n.º 6/99, de 27/01, consagrando-se um sistema de opção negativa ou de opt-out, pelo que a publicidade entregue no domicílio do destinatário[426] deve ser identificável exteriormente de forma clara e inequívoca, contendo, designadamente, a identificação do

[424] GT29, cit. 399.

[425] Ilustramos o tratamento de dados com fundamento num "interesse legítimo" previsto na al) e) do art.º 6º, da LPDP e da al) f), do art.º 7º, da Diretiva 95/46/CE com o seguinte exemplo: A Ordem dos Advogados, ao recolher os dados pessoais de advogados e de advogados estagiários para efeitos de inscrição e para outros efeitos internos - comunicações, notificações, efeitos disciplinares, etc. - ao proceder ao seu tratamento informatizado, em momento algum acautela a possibilidade ou faculdade de os transmitir a terceiros mediante a obtenção de autorização dos interessados. Numa questão suscitada ao Conselho Geral da Ordem dos Advogados, a propósito da cedência e utilização de ficheiros de dados pessoais de advogados e advogados estagiários à Universidade Católica do Porto dando notícia de especializações do MBA, foi considerado que se enquadrava num serviço de divulgação de assuntos de interesse para o exercício da atividade profissional e formação dos advogados e advogados estagiários e, como tal, inserir-se-ia na prossecução de interesses legítimos tanto do Conselho Distrital como da Universidade Católica, e ainda que: (1) os dados pessoais comunicados eram comuns ou neutros - ou seja eram aqueles dados facilmente acessíveis por simples consulta de outros meios ao dispor do público em geral - a terceira entidade, não coloca em crise nem os interesses, nem os direitos, nem as liberdades e garantias dos titulares dos dados; (2) a cedência das etiquetas, com os dados das pessoas em causa, a terceiro foi para uma finalidade concreta, precisa, individual e para uma única vez; (3) trata-se de um procedimento comum de cedência de dados entre instituições do ensino superior e portanto expectável por parte dos titulares dos dados; e (4) o exercício do direito de oposição estava acautelado (v. ORDEM DOS ADVOGADOS PORTUGUESES - Parecer n.º E-30/03, de 22/09/2003 [Em linha]. [Consult. 10 Nov. 2016]. Disponível em WWW <https://www.oa.pt/Conteudos/ Pareceres/detalhe_parecer.aspx?idc=5&idsc=158&ida=39887>).

[426] O n.º 1, do art.º 23.º, do Código da Publicidade, define publicidade domiciliária como a publicidade entregue no domicílio do destinatário, por correspondência ou qualquer outro meio (entende-se a distribuição direta nas caixas de correio, como por exemplo, panfletos, catálogos, jornais publicitários, etc.)

anunciante e do tipo de bem ou serviço publicitado, nos termos do art.º 2º, da L n.º 6/99, de 27/01 (3-7.2.1.). O direito incondicional de oposição ao marketing direto está, igualmente, previsto na al) b), do art.º 12º, da LPDP e da al) b), do art.º 14º, da diretiva 95/46/CE, e é exercido a pedido do titular dos dados sem custos, diferenciando-se no modo de execução consoante a publicidade domiciliária seja não endereçada ou endereçada.

A distribuição de publicidade não endereçada é proibida sempre que a oposição do destinatário seja reconhecível no ato de entrega, nomeadamente através da afixação, de forma visível, no local destinado à receção de correspondência, de dístico apropriado contendo mensagem clara e inequívoca nesse sentido (art.º 3º, da L n.º 6/99, de 27/01). O envio de publicidade endereçada é proibido, por via postal ou por distribuição direta, quando o destinatário tenha expressamente manifestado o desejo de não receber material publicitário (n.º 1, do art.º 4º, da L n.º 6/99, de 27/01). Os responsáveis pelo tratamento de dados que promovam o envio de publicidade para o domicílio manterão, por si ou por organismos que as representem, uma lista (3-5.2.6.) das pessoas que manifestaram o desejo de não receber publicidade endereçada. Os titulares de listas de endereços utilizadas para efeitos de marketing direto devem mantê-las atualizadas, eliminando trimestralmente os nomes constantes da lista referida no número anterior (n.ºs 3 e 5, do art.º 4º, da L n.º 6/99, de 27/01)[427].

O responsável do tratamento no contexto da execução de um contrato em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a pedido deste, utilizar as respetivas coordenadas eletrónicas de contacto, para fins de marketing direto dos seus próprios produtos ou serviços análogos[428] aos

[427] Ainda que a reflexão da presente dissertação incida sobre as pessoas singulares note-se que o regime do direito à oposição sem necessidade de fundamento se aplica às pessoas coletivas. Na verdade, o n.º 3, do art.º 13º-A, da L n.º 41/2004, de 18/08, prevê que o fornecedor de determinado produto ou serviço que tenha obtido dos seus clientes, e desde que sejam pessoas coletivas, nos termos da LPDP, no contexto da venda de um produto ou serviço, as respetivas coordenadas eletrónicas de contacto, pode utilizá-las para fins de marketing direto dos seus próprios produtos ou serviços análogos aos transacionados, desde que garanta aos clientes em causa, clara e explicitamente, a possibilidade de recusarem, de forma gratuita e fácil, a utilização de tais coordenadas no momento da respetiva recolha e por ocasião de cada mensagem, quando o cliente não tenha recusado inicialmente essa utilização.

[428] A exceção para além de se restringir aos clientes, limita a comercialização de produtos e serviços análogos, isto é, na perspetiva do destinatário é expectável que recebe informação sobre os produtos estritamente comercializados pela organização responsável pelo tratamento de dados. Parece expectável que não sejam apenas os produtos e serviços por si criados e produzidos mas também outros desde que prossigam o objeto social do operador económico. O Código de Conduta Europeu da FEDMA relativo ao uso de dados pessoais no marketing direto, estabelece uma exigência adicional de que o cliente deve ser informado pelo responsável do tratamento de dados sobre o que entende por serviços análogos (v. GT29 - Parecer 4/2010 sobre o código de conduta europeu da FEDMA relativo ao uso de dados pessoais no marketing direto [Em linha]. 00065/2010/PT WP 174. Brussels (Belgium), (13/07/2010). [Consult. 12 dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_pt.pdf >.

transacionados, desde que, clara e explicitamente, a possibilidade de recusarem, de forma gratuita e fácil, a utilização de tais coordenadas no momento da recolha e por ocasião de cada mensagem, quando não tenha recusado inicialmente essa utilização (al) a), do art.º 6º, da LPDP e al) b), do art.º 7º, da Diretiva 95/46/CE, conjugados com o n.º 3, do art.º 13º-A, da L n.º L n.º 41/2004, de 18/08 e n.º 2, do art.º 13º, da Diretiva 2002/58/CE). A comunicação comercial para a promoção de bens e serviços é expectável por parte do titular dos dados bem como é «razoável permitir a utilização de coordenadas eletrónicas do contacto» (Considerando 41, da Diretiva 2002/58/CE) por parte da mesma empresa que obteve os elementos da comunicação junto do cliente em conformidade com a LPDP e a Diretiva 95/46/CE.

3-9.1.2. O caso do telemarketing

O n.º 1, do art.º 5º, da L n.º 6/99, de 27/0, estabelece a proibição da publicidade por telefone, com utilização de sistemas automáticos com mensagens vocais pré-gravadas, e a publicidade por telecópia, salvo quando o destinatário a autorize antes do estabelecimento da comunicação, que deve ser conjugado com o art.º 13º-A, da L n.º 41/2004, de 18/08.

A receção de publicidade por telefone e telecópia pode causar problemas e transtornos com a ocupação das linhas que suportam este meio de comunicação, destinados a outros fins, quer pessoais quer profissionais, podendo ter custos. Os destinatários que não desejem receber publicidade por telefone e telecópia podem inscrever o número de telefone de assinante de que são titulares numa lista própria (3-5.2.6.).

Sendo a técnica de telemarketing mais intrusiva na privacidade dos destinatários a sua disciplina é mais rigorosa, assim, nos termos do DL n.º 134/2009, de 02/06[429]:

a) As chamadas telefónicas dirigidas aos consumidores ou aos utentes devem ser efetuadas num horário que respeite os períodos de descanso em uso e nunca antes das 9 horas nem depois das 22 horas do fuso horário do consumidor ou dos utentes; o operador que efetue a chamada deve identificar-se imediatamente após o atendimento, bem como ao profissional em nome do qual atua e a finalidade do contacto; a prestação de informação obedece aos princípios da legalidade, boa-fé, transparência, eficiência, eficácia, celeridade e cordialidade.
b) Quando o destinatário manifeste ou expresse a vontade de não prosseguir a chamada, esta

[429] DL n.º 134/2009, de 02/06, estabelece o regime jurídico aplicável à prestação de serviços de promoção, informação e apoio aos consumidores e utentes através de centros telefónicos de relacionamento (*call centers*), entrou em vigor no continente a 29/11/2009, tendo sido alterado pelo DL n.º 72-A/2010, de 18 de Junho que estabelece as normas de execução do Orçamento do Estado para 2010.

deve ser desligada com urbanidade.

3-9.1.3. O caso do telemarketing na pRPCE

A pRPCE, reforça a proteção contra comunicações não solicitadas através das técnicas de telemarketing ao prever expressamente, nos n.ºs 3 e 4, do art.º 16º, que as pessoas singulares ou coletivas que utilizam serviços de comunicações eletrónicas para efetuarem chamadas de marketing direto devem obter o consentimento prévio dos utilizadores finais, e ainda, apresentar a identificação de uma linha na qual podem ser contactados, ou um código ou prefixo de identificação específico que indique que se trata de uma chamada comercial e a possibilidade de bloquear as chamadas de números indesejados, sem prejuízo dos Estados-Membros preverem através de medidas legislativas, que a realização de chamadas vocais de marketing direto para utilizadores finais que sejam pessoas singulares só possa ser permitida em relação aos utilizadores finais que sejam pessoas singulares que não tenham manifestado a sua objeção a receber essas comunicações.

3-9.2. As comunicações não solicitadas

O art.º 7º, da Diretiva 2000/31/CE, na redação original, estabeleceu que os Estados-Membros que permitam a comunicação comercial não solicitada[430] por correio eletrónico deveriam tomar medidas e garantir a consulta regular das listas de exclusão voluntária ou registo de opção negativa ou «*opt-out*», situação que foi alterada com a Diretiva 2002/58/CE prevendo-

[430] A Internet introduziu na linguagem novos termos e deu novos significados a algumas palavras antigas. Os lexicógrafos do ciberespaço adotaram a palavra spam para fazer menção ao envio de mensagens comerciais indesejadas pelo correio eletrónico, e que originalmente, referindo-se a uma marca de carne enlatada. O termo spam não é um termo legal e invariavelmente é denominado como correio não solicitado (*junk-mail*), correio em massa (*bulk-mail*) ou correio comercial não solicitado, desde que cumpra três critérios: não ser solicitado pelo destinatário, ter natureza comercial e ser enviado em massa, o que cria problemas quanto ao conceito, desde logo quantas comunicações configura o conceito de envio em massa (v. HUH, Soon Chul - *Invasion of privacy v. Commercial speech: Regulation of spam with a comparative constitutional point of view.* [Em linha]. *Albany Law Review*, Vol. 70, n.º 1, 2006, p. 181-207. [Consult. 12 out. 2015]. Disponível em WWW <http://www. albanylaw review.org/Articles/Vol70_1/70.2.0181>). Na EU, o termo *spam* é utilizado para referir-se às comunicações não solicitadas embora não exista uma definição comum cujo fenómeno ocorre em distintos países. O *spam* é comummente pensado em termos de correio eletrónico, no entanto, uma variedade de mensagens em vários suportes tecnológicos, podem estar sujeitas aos mesmos fins do correio eletrónico quando se trata de spam, pelo que é necessário uma abordagem convergente à criação de novos meios de comunicação e à mudança de forma dos já existentes, incluindo-se assim para além do correio eletrónico, SMS, MMS, EMS, fax símile, seria de incluir o *Bluetooth*, *Wireless*, etc. (OECD, cit. 317). A doutrina utiliza as siglas UCE (*unsolicited commercial e-mail*) para indicar o *spam* de teor comercial e UBE (*unsolicited bulk e-mail*) para referir o spam como as mensagens sem a prévia solicitação ou consentimento do seu destinatário, enviadas de modo massivo, independentemente do seu caráter comercial ou não comercial (V. SORKIN, David E. - *Technical and Legal Approaches to Unsolicited Electronic Mail. In University of San Francisco Law Review* [Em linha]. Vol. 35, n.º 2, [Winter 2001] p. 325-384 [Consult. 14 Fev. 2017]. Disponível em WWW: <http://www.spamlaws. com/f/articles /usf.pdf>; Parecer da CNPD, nº 13/2003, de 03/06 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_13_2003.pdf> e GT29, cit. 316.

se o regime oposto, ou seja o sistema de opção positiva ou «*opt-in*» como regra geral[431]. No direito nacional as comunicações não solicitadas eram reguladas pelo art.º 22º, do DL 7/2004/2004, de 07/01; atualmente com as alterações introduzidas pela L n.º 46/2012, de 29/08, o regime das comunicações não solicitadas passou a estar previsto na L n.º 41/2004, de 18/08.

O envio de comunicações não solicitadas para fins de marketing direto por correio eletrónico, através de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), nos termos do n.º 1, do art.º 13º-A, da L n.º 41/2004, de 18/08, está sujeito ao consentimento prévio expresso do titular dos dados. Os critérios para determinar a validade do consentimento são os estabelecidos na al) h) do art.º 2º e al) a) do art.º 7º, da Diretiva 95/46/CE e da al) h), do art.º 3º e proémio do art.º 6º, da LPDP para dar início ao tratamento dos dados (3-8.1.). Reitera-se que o consentimento baseado na omissão ou no silêncio não consubstancia um consentimento válido na medida em que deve existir um ato positivo que signifique que a aceitação do consentimento foi obtida, podendo ser revogado a todo o tempo (3-8.1.2.).

A definição de correio eletrónico como «qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha», está plasmada na al) b), n.º 1, do art.º 2º, da L n.º 41/2004, de 18/08 e al) h) do art.º 2º, da Diretiva 2002/58/CE, e tem um «sentido lato e pretende ser neutra no plano tecnológico»[432], pelo que os sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, são exemplificativos: SMPT (*simple mail transport protocol*, o designado correio eletrónico clássico) SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia), mensagens deixadas em atendedores de chamadas, comunicações enviadas pela internet transmitidas diretamente por um IP, boletins informativos e outros tipos de aplicações similares utilizadas ou que venham a ser

[431] O sistema de opt-in da Diretiva 2002/58/CE foi suavizado com exceções o que foi denominado pela doutrina de sistema "*opt-in* modificado" ou simplesmente "*soft opt-in*", assim conjugando as disposições do ecossistema legal da proteção de dados, destaca-se a exceção prevista na al) a), do art.º 6º, da LPDP e al) b), do art.º 7º, da Diretiva 95/46/CE, e o n.º 3, do art.º 13º-A, da L n.º L n.º 41/2004, de 18/08 e n.º 2, do art.º 13º, da Diretiva 2002/58/CE, que legitima o interesse dos operadores económicos em continuar a manter contactos de natureza ante ou pós-contratual para fins de marketing, presumindo-se o interesse do cliente (v. MAGEE, John - *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective. In Santa Clara High Technology Law Journal* [Em linha]. Vol. 19, n.º 2, (2002). [Consult. 19 jan. 2016]. Disponível em WWW <http://digital commons.law.scu.edu/cgi/viewcontent.cgi?article=1322&context=chtlj>).

[432] V. GT29, cit. 397, p. 4.

utilizadas[433].

A obtenção do consentimento prévio não isenta o responsável pelo tratamento das obrigações previstas na LPDP, nomeadamente, quanto ao respeito dos princípios no tratamento dos dados. As organizações que adquiram ficheiros de dados pessoais com endereços de correio eletrónico[434] (2-4.1.) devem certificar-se que foram tratados em conformidade com os princípios e condições de legitimidade do tratamento de dados. Refira-se que o art.º 8º, do DL n.º 24/2014, de 14/08, que transpõe a Diretiva n.º 2011/83/UE, relativa aos direitos dos consumidores, contratos a distância, ao domicílio e equiparados e vendas automáticas e as vendas especiais esporádicas, com o fim de promover a transparência das práticas comerciais e salvaguardar os interesses legítimos dos consumidores, exige o consentimento prévio expresso do consumidor nos termos da L n.º 41/2007, de 07/0, para o envio de comunicações não solicitadas através da utilização de técnicas de comunicação à distância.

As comunicações não solicitadas são de divulgação rápida e com um custo muito reduzido e por isso uma fonte de grandes vantagens económicas. Assim, e com o fim de acautelar o recurso à violação dos sistemas de segurança e filtragem por parte das organizações para garantir a sua distribuição, o legislador entendeu proibir o envio de correio eletrónico para fins de marketing direto, em caso de ocultação ou dissimulação da identidade da pessoa em nome de quem é efetuada a comunicação, em violação do art.º 21.º do DL n.º 7/2004, de 07/01, e sem a indicação de um meio de contacto válido para o qual o destinatário possa exercer o seu direito de oposição (n.º 4, do art.º 13º-A, da L n.º 41/2004, de 18/08). A disposição vem reforçar o dever de informação do responsável pelo tratamento, previsto no art.º 10º, da LPDP (3-7.2.1.)

O envio de comunicações não solicitadas sujeito ao consentimento prévio dos titulares dos dados – e destinatários das mesmas - é um obstáculo[435] à invasão da privacidade[436] e à

[433] A OCDE acrescenta outros exemplos*: bluetooth* e *wireless communication* (OECD, cit. 317). Em sentido contrário, a COMISSÃO entende que o Bluetooth não integra a definição de correio eletrónico dado que as mensagens enviadas via Bluetooth não podem ser armazenadas no equipamento terminal do destinatário até que sejam recolhidas pelo destinatário (v. COMISSÃO, cit. 422).

[434] Os endereços de correio eletrónico são dados pessoais (2-4.1.).

[435] Outra forma utilizada para combater as comunicações não solicitadas é a criação de códigos e regras de conduta, muito promovido pelas normas que regulam a proteção de dados pessoais (art.º 32º, da LPDP e art.º 42º, da L n.º 7/2004, de 07/01) Os Códigos de Conduta constituem uma forma de autorregulação que incluem as melhores práticas do setor em que se inserem, quanto ao comportamento dos operadores económicos e da proteção dos consumidores, que tomaram como modelo as diretrizes da OCDE. O Código FEDMA relativo ao uso de dados pessoais em operações de marketing direto foi submetido à opinião do GT29 (v. GT29, cit. 343) e o Código de Conduta das Empresas de Marketing Direto foi submetido pela AMD à apreciação da CNPD (Parecer da CNPD, nº 44/2003, de 11/11 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_44_2003.pdf>). Os códigos de conduta costumam utilizar-se com selos de confiança como o Selo Europeu de Privacidade ou EuroPriSE.

[436] Nos EUA, esta questão, também, tem merecido, há muito tempo, a atenção dos tribunais: no caso de *Rowan v.*

violação do direito à proteção de dados[437]. Na verdade, o destinatário das referidas comunicações considera-as lixo informático, que invariavelmente bloqueiam a caixa de correio eletrónico, devido à dimensão ou quantidade, com consequências negativas económicas para as pessoas em causa que utilizem o correio eletrónico pessoal ou o correio eletrónico facilitado pela entidade patronal[438]. O excesso de comunicações pode dar origem a custos elevados com o aumento de largura de banda e espaço disponibilizado, para manter a velocidade de acesso adequados, acrescendo ainda que nos locais de trabalho é necessário implantar sistemas e mecanismos de filtros *anti-spam* para minimizar os prejuízos, tudo aliado à comprovada baixa de produtividade, desconcentração e tempo despendido com tarefas de eliminação de mensagens publicitárias[439].

3-9.2.1. As comunicações não solicitadas na pRPCE

A pRPCE, em discussão, vem alargar o âmbito da proteção do direito à privacidade e do direito à proteção dos dados pessoais como incorpora nas normas e conceitos que a interpretação jurisprudencial e doutrinária foi estabelecendo, e ainda as boas práticas aceites pelas organizações. Assim e com interesse:

a) Maior abrangência dos direitos dos titulares dos dados em relação à proteção prevista no n.º 1, do art.º 13º, da Diretiva 2002/58/CE, com o fim de abarcar não só os assinantes, mas também os utilizadores dos serviços de telecomunicações sem diferenciar as pessoas singulares das coletivas[440].

United States Post Office Department, 397 US 728, de 04/05/1970, o Supremo Tribunal decidiu que um destinatário de correio postal tem o poder discricionário de decidir quer receber correio de um determinado remetente - admitiu que havia um direito individual a ser deixado sozinho, ou o direito à privacidade sobre o correio indesejado, e em consequência o direito fundamental à comunicação deve parar na caixa de correio de um destinatário não recetivo. O acórdão pode ser consultado aqui <https://www.law.cornell.edu/supremecourt/ext/397/728>.

[437] A CNPD e a ANACOM são as entidades responsáveis pela supervisão e fiscalização do cumprimento das regras aplicáveis ao envio de comunicações eletrónicas não solicitadas. O envio de comunicações não solicitadas contrário às normas previstas constitui uma contraordenação punível com a coima mínima de € 1.500,00 e máxima de € 25.000,00 quando praticada por pessoas singulares, e com coima mínima de € 5.000, 00 e máxima de € 5.000.000,00, quando praticada por pessoas coletivas. A prática de envio de comunicações não solicitadas pode constituir vários tipos de ilícitos autónomos, nomeadamente a violação da proteção de dados pessoais (LPDP) e a publicidade enganosa (Código da Publicidade).

[438] As pessoas singulares que recebam comunicações não solicitadas e ainda que utilizem o endereço de correio eletrónico disponibilizado pela entidade laboral, continuam protegidas pelas LPDP e L n.º 41/2004, de 18/08.

[439] A receção de conteúdos embaraçosos e obscenos levantaria, ainda, outras questões relacionadas com a ética, moral e até a possibilidade de configurarem ilícitos penais, como a divulgação de conteúdos relacionados com a pornografia infantil. O envio de mensagens pode incluir programas espiões ou maliciosos (ou outros meios fraudulentos) que capturam informação com prejuízos graves para o titular dos dados, que podem ser extensíveis a terceiros.

[440] O Considerando 3, da pRPCE, refere expressamente que as suas disposições se aplicam tanto a pessoas singulares como coletivas, dado que as «comunicações eletrónicas podem também revelar informações sobre pessoas coletivas, tais como os seus segredos comerciais ou outras informações sensíveis com valor económico».

b) A al) e), do n.º 1, do art.º 4º, da pRPCE define correio eletrónico como «qualquer mensagem eletrónica que contenha informações sob a forma de texto, voz, vídeo, som ou imagem, enviada através de uma rede de comunicações eletrónicas, que possa ser armazenada na rede ou em centros de computação conexos, ou no equipamento terminal do seu destinatário» de forma a alcançar o maior número de possibilidades de comunicação da sociedade de informação, tendo em conta a velocidade da inovação tecnológica. Deixa de fazer sentido a discussão sobre o *Bluetooth*[441], *wireless*, bloqueio de anúncios (*ad blockers)* ou a filtragem de anúncios (*ad filtering*)[442], NFC e se as mensagens que são trocadas por todos os tipos de plataformas em linha, como *WhatsApp, Skype*, *LinkedIn, Facebook Messenger* ou *Twitter*, integram o conceito de correio eletrónico, uma vez que são enviados através de uma rede de comunicações públicas[443] e armazenados no servidor do fornecedor de plataforma (o que está na rede).

c) Os art.ºs 9º e 10º, da pRPCE reforça o controlo por parte do utilizador final ao esclarecer que ao consentimento é aplicável a definição e condições previstas no RGPD, podendo ser expresso através de predefinições técnicas adequadas e serem recordados da possibilidade de o retirar com intervalos regulares de 6 meses, se tiverem consentido no tratamento de metadados e enquanto continuar. O consentimento prévio é exigido para todos os tipos de marketing digital, exceto no contexto da venda de um produto ou serviço (art.º 16º, da pRPCE).

3-9.3. O marketing comportamental em linha

Um dos pilares do marketing é a base de dados (3-5.) cujas fontes de recolha dependem da «monitorização dos utilizadores da internet e da criação de perfis ao longo do tempo, que mais tarde são utilizados para lhes apresentar anúncios baseados nos seus interesses»[444].

O marketing comportamental em linha[445] envolve o rastreamento das atividades que não é

[441] As mensagens *Bluetooth* ainda que não pudessem ser qualificadas como correio eletrónico, tem de ser necessariamente consideradas como enviadas por meio de um sistema de comunicações automatizado.

[442] O bloqueio de anúncios ou a filtragem de anúncios é um tipo de software que pode remover ou alterar o conteúdo de publicidade de uma página da internet ou de um aplicativo para dispositivos móveis.

[443] Conforme o considerando 13, da pRPCE: «O facto de os serviços de comunicações eletrónicas sem fios poderem ser acessórios de outros serviços não deve impedir a proteção da confidencialidade dos dados das comunicações e a aplicação do presente regulamento. Por conseguinte, o presente regulamento deve aplicar-se aos dados de comunicações eletrónicas que utilizam serviços de comunicações eletrónicas e redes de comunicações públicas».

[444] GT29 - Parecer 2/2010 sobre publicidade comportamental em linha [Em linha]. 0909/10/PT WP 171. Brussels (Belgium), (22/06/2010). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp171_pt.pdf>, p. 3.

[445] O GT29 utiliza, frequentemente e de forma alternada, os conceitos de publicidade e marketing para os contextos que resulta difícil diferenciar. Para efeitos do presente texto adapta-se o conceito de marketing no que

pessoalmente identificável no sentido tradicional (endereços, nomes, etc.), ou seja, os operadores económicos utilizam software (3-5.1.) e outros dispositivos análogos para entrarem nos terminais dos utilizadores sem o seu conhecimento a fim de obter acesso a informações para enviar-lhes publicidade personalizada, constituindo uma grave intrusão na privacidade desses utilizadores. Contudo, alguns dispositivos como, por exemplo, «os testemunhos de conexão podem ser um instrumento legítimo e útil, nomeadamente na análise da eficácia da conceção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transações em linha» (Considerando 25, da diretiva 2002/58/CE).

A estratégia do Mercado Único Digital tem como objetivo aumentar a confiança e a segurança no comércio eletrónico que assenta nos serviços facilitados pela sociedade de informação, que passam pelos prestadores de serviços da Internet que operam servidores que permitem o acesso à rede, a transmissão de mensagens comerciais, o armazenamento de dados, o correio eletrónico, os motores de pesquisa, a publicidade, entre outros impossíveis de enumerar, no respeito pelo direito fundamental da liberdade de exercício (ou da desnecessidade de autorização prévia) de atividades económicas na Internet, da liberdade de comunicação e de navegação na Internet, articulado com o primado do direito comunitário na regulação do mercado interno do comércio eletrónico, consagrado no DL n.º 7/2004, de 07/01, mas sujeitas aos princípios da transparência e da privacidade nas comunicações eletrónicas modelados na L n.º 41/2004, de 18/08.

O princípio da transparência impõe deveres de informação e exigência do consentimento informado prévio (3-8.1.) nos termos do art.º 5º, da L n.º 41/2004, de 18/08 e do proémio, do art.º 6º, da LPDP que transpõe o n.º 3, do art.º 5.º, da Diretiva 2002/58/CE e al) a), do art.º 7º, da Diretiva 95/46/CE), no que respeita à instalação de testemunhos de conexão ou de dispositivos análogos no equipamento terminal dos utilizadores com o objetivo de recolher os dados, tendo em conta o seu elevado grau de intrusão na privacidade das pessoas. Os restantes princípios e condições do tratamento de dados previstos na LPDP e na Diretiva 95/46/CE são aplicáveis como referido o n.º 2, do art.º 1º, da L DL n.º 7/2004, de 07/01, esta aplica-se ao

---

for possível. O GT29 classifica os diferentes métodos para criar anúncios em linha em: (1) publicidade comportamental que «tem por base a observação do comportamento das pessoas ao longo do tempo, procurando estudar as características deste comportamento através das suas ações (várias visitas ao mesmo sítio Web, interações, palavras-chave, produção de conteúdo em linha, etc.), com vista a criar um perfil específico e, deste modo, apresentar-lhes anúncios que correspondem aos interesses implícitos no seu comportamento»; (2) publicidade contextual que é «constituída por anúncios selecionados com base no conteúdo que a pessoa em causa está a visualizar naquele momento. No caso de um motor de pesquisa, o conteúdo pode ser inferido a partir das palavras-chave utilizadas na pesquisa, a interrogação anterior ou o endereço IP do utilizador caso indique a sua provável localização geográfica; e (3) publicidade selecionada «com base em características conhecidas da pessoa em causa (idade, sexo, localização, etc.), que esta forneceu na fase de registo» (GT29, cit. 441, p. 5).

«tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação, especificando e complementando as disposições» da LPDP[446].

O sistema legal da proteção de dados não se refere expressamente aos testemunhos de conexão mas sim às tecnologias de recolha e retenção de dados. Contudo, as preocupações, tanto a nível do direito da UE como do direito interno, têm sido centradas nos testemunhos (3-9.3.1.), nos motores de pesquisa (3-9.3.2.), nas redes sociais (3-9.3.3.) e na IdC (3-9.3.4.). A inquietação é maior quando os utilizadores que aderem a serviços em linha gratuitos fornecem os seus dados pessoais para utilização posterior como moeda de troca, sem existir uma versão alternativa configurando um desequilíbrio na prestação do consentimento que afeta a liberdade de escolha e, portanto, dificilmente o consentimento poderá ser considerado livre.

3-9.3.1. Os testemunhos de conexão

O responsável pelo tratamento deve ter em conta as especificidades do ambiente virtual para obter o consentimento dos utilizadores para o tratamento dos dados, pois, implica programas de navegação e aplicações pré-configurados de informação (3-7.3.) com vista à aceitação ou recusa dos testemunhos de conexão (3-8.1.).

O consentimento não é necessário em relação a todos os tipos de testemunhos de conexão, tendo em conta as finalidades, utilização e os objetivos associados aos mesmos, conforme melhor regulado no n.º 2, do art.º 5º, da L n.º 41/2004, de 18/08 e no n.º 3, do art.º 5º, da Diretiva 2002/58/CE. Assim, é excecionado o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação solicitado expressamente pelo assinante ou pelo utilizador.

De acordo o GT29, os testemunhos de conexão[447] podem ser classificados em testemunhos de

[446] No mesmo sentido o Considerando 10, da Diretiva 95/46/CE, refere que «no setor das comunicações eletrónicas, é aplicável a Diretiva 95/46/CE, especialmente no que se refere a todas as questões relacionadas com a proteção dos direitos e liberdades fundamentais não abrangidos especificamente pelas disposições da presente diretiva, incluindo as obrigações que incumbem à entidade que exerce o controlo e os direitos das pessoas singulares».

[447] Um testemunho de conexão é um pequeno ficheiro de texto que uma página da internet instala no computador ou dispositivo móvel quando o visita. Estes ficheiros permitem que durante um certo período de tempo página da internet se *lembre* das ações e preferências, nomeadamente do nome de utilizador, das palavras-chave gravadas, de cliques, do idioma, das compras, das páginas visualizadas, etc.

sessão[448] ou persistentes[449] e testemunhos de terceiros[450]. Tendo em conta a análise de cada testemunho de conexão e as exceções supra referidas, estão isentos de consentimento: os testemunhos alimentados pelo utilizador[451], os testemunhos de autenticação[452], os testemunhos de segurança centrados no utilizador[453], os testemunhos de sessão criados por um leitor multimédia[454], os testemunhos de sessão para equilibrar a carga[455], os testemunhos de personalização da interface do utilizador[456] e os testemunhos relativos a módulos de extensão para partilha de conteúdos em redes sociais[457]. Os testemunhos de conexão que carecem do consentimento do utilizador são, essencialmente: (1) os testemunhos de extensão de redes sociais, para seguimento[458], dado que permitem o rastreio dos utilizadores, membros e não membros da rede dos utilizadores, para fins publicitários, análise e estudos de mercado; (2) os testemunhos de terceiros[459] que utilizam os identificadores únicos dos utilizadores, para envio de publicidade após análise do seu comportamento em linha; e (3) os testemunhos de analítica de origem[460], para a medição estatística de audiência das páginas de internet visitadas pelos utilizadores, por exemplo, a medição de visitantes únicos, a pesquisa por palavras-chave, número de visualizações, data de consulta, número de horas de visualização de documentos,

[448] Um testemunho de sessão é «aquele que é automaticamente suprimido quando o utilizador encerra o seu programa de navegação» (GT29 - Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão [Em linha]. 00879/12/PT WP 194. Brussels (Belgium), (07/06/2012). [Consult. 12 dez. 2014]. Disponível em WWW <http://ec.europa.eu/ justice/data-protection/article-29/documentation/opinion-recommendation/files/2012 /wp194_pt.pdf>, p. 4).

[449] Um testemunho persistente é «aquele que permanece armazenado no equipamento terminal do utilizador até atingir uma data de expiração definida, que pode ser de minutos, dias ou vários anos no futuro» (GT29, cit. 448, p. 4).

[450] Um testemunho de terceiros refere-se àquele que é criado pelo responsável pelo tratamento de dados diferente daquele que explora o sítio Web visitado pelo utilizador (tal como definido pelo URL – endereço Internet) que aparece na barra de endereços do programa de navegação (GT29, cit. 448, p. 4).

[451] Estão vinculados a uma ação do utilizador como por exemplo o preenchimento de formulários ao longo de uma página para realizar uma compra.

[452] São utilizados para identificar um utilizador quando se inicia uma sessão e é o utilizador que o solicita para determinados fins, por exemplo a consulta de um saldo bancário. Não devem ser utilizados para finalidades secundárias sob pena de carecer de consentimento.

[453] São utilizados para comprovar a identidade do utilizador para iniciar uma sessão numa determinada página e detetar potenciais tentativas de acesso sem os dados previamente fornecidos – são distintos dos testemunhos relacionados com a segurança das páginas de internet.

[454] São aqueles que incorporam dados técnicos para reproduzir conteúdos de vídeo ou áudio, mais conhecidos como *flash cookies* dado que a tecnologia mais utilizada é a *Adobe Flash* e terminam quando a sessão termina.

[455] São aqueles que identificam os pedidos do utilizador enquanto dura a sessão e que permite a sua distribuição sobre os vários servidores com a única finalidade efetuar a transmissão de informações.

[456] São aqueles que guardam as preferências solicitadas pelos utilizadores, por exemplo, de idioma, número de resultados a apresentar por página, visualização de documentos, tamanho de letra, etc.

[457] São aqueles que se destinam a partilhar conteúdos numa plataforma de rede social e não devem ser utilizados para finalidades secundárias sob pena de carecer de consentimento.

[458] Conhecidos sob a sigla inglesa de *social plug-in tracking cookies*.

[459] Conhecidos sob a sigla inglesa de *third party advertising.*

[460] Conhecidos sob a sigla inglesa de *third party analytics.* O *Google Analytics* é uma aplicação que incorpora inúmeras funcionalidades de medição da audiência das páginas web. O GT29 recomendou que não deveria ser exigível o consentimento, tal como a legislação holandesa. Esta posição veio a ser incluída na pRPCE (3-9.5.)

local de acesso, origem do acesso, etc.

O consentimento é dado pelo titular dos dados conforme descrito em 3-8.1. O GT29 com o objetivo de harmonizar as distintas práticas dos Estados-Membros da EU emitiu um documento de trabalho para implementar os elementos do consentimento válido através de um mecanismo que requer aviso imediatamente visível para concordar e aceitar os testemunhos de conexão, e outro para recusar os testemunhos e informações que podem ser prestadas por meio de hiperligações[461], recorrendo a parâmetros adequados do programa de navegação ou de outra aplicação, de forma tão simples quanto possível[462]. O responsável pelo tratamento deve fornecer as informações em conformidade com a LPDP e da Diretiva 95/46/CE (3-7.2.1.), e nomeadamente a existência e as finalidades do testemunho, a possibilidade de instalação de testemunhos de terceiros, respetivas finalidades e identidade da entidade terceira, as condições do tratamento e a duração do testemunho.

3-9.3.2. Os motores de pesquisa

Os motores de pesquisa são programas desenhados para ajudar a encontrar informação na internet por palavras-chaves fornecidas pelos utilizadores em documentos e bases de dados[463]. Os motores de pesquisa têm capacidades de elaboração de perfis de utilizadores baseados em dados pessoais disponíveis em qualquer local da internet e no contexto do comércio eletrónico foram classificados como um tipo de serviço da sociedade da informação[464] (n.º 1, do art.º 3º,

---

[461] GT29 - *Working Document 02/2013 providing guidance on obtaining consent for cookies* [Em linha]. 1676/13/EN, WP 208. Brussels (Belgium), (02/10/2013). [Consult. 12 Dez. 2016]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf>

[462] *V.* Considerando 66, da Diretiva 2009/136/CE, de 25/11.

[463] As maiores empresas proprietárias de motores de pesquisa são o Google, o Yahoo, o Bing, o Lycos, o Cadê e, mais recentemente, a Amazon.com com o seu mecanismo de busca A9.

[464] O GT29 refere que os motores de pesquisa da Internet são considerados na legislação europeia relativa aos serviços da sociedade da informação, definidos na al) a) do art.º 2º, da Diretiva 2000/31/CE, que remete para a Diretiva 98/34/CE, que especifica o conceito de serviço da sociedade da informação e que se encontra revogada pela Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 09/09/2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (v. GT29, cit. 189). Ilustra-se o texto com o caso *Repubblica Italiana vs Drummond, De Los Reyes e Fleischer, doTribunale Ordinario Di Milano in composizione monocrática, Sezione 4 Penale*, sentença n.º 1972/2010, de 12/04/2010, em que foram condenados três administradores da Google até seis meses de prisão, por violar a privacidade de uma criança autista. Em maio de 2006, a agressão física e a proferição de insultos a uma criança autista em Turim foi reproduzida em vídeo no Google. Apesar do vídeo ter sido removido duas horas depois atraiu mais de 5.500 visualizações e foi classificado como o vídeo mais engraçado do Google Itália, com base na utilização de *adwords* e interrogações no motor de pesquisa. O Google gera mais receitas com vídeos populares. O tribunal considerou que o vídeo é um serviço da sociedade da informação fornecedor e os administradores eram responsáveis pelos requisitos das leis da privacidade teriam de ser condenados com fundamento no tratamento ilícito dos dados, falta de consentimento dos titulares dos dados e com prejuízos graves (cf. SARTOR, Giovanni, CUNHA, Mario Viola de Azevedo - *The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*. [Em linha*]. In International Journal of Law and Information Technology*, Vol 18, n.º 4, Oxford : Oxford University Press, (2010). pp 356-

da L n.º 7/2004, de 07/01 e al) a) do art.º 2º, do DL n.º 58/2000, de 18/04), ou seja, como ferramentas de localização de informação.

Os serviços da sociedade da informação desenvolvem uma atividade económica, prestam serviços que não são remunerados pelo respetivo destinatário, relacionados com a informação em linha ou comunicações comerciais, e ainda fornecem ferramentas de pesquisa, acesso e descarregamento de dados (Considerando 18 da Diretiva 2000/31/CE). O modelo económico dominante dos motores de pesquisa é baseado na publicidade.

Os motores de pesquisa registam conteúdo das interrogações (data, hora e fonte), endereço IP, os testemunhos de conexão, a URL de referência, as preferências do utilizador e dados referentes ao computador do utilizador (configuração, o navegador, o sistema operativo, o idioma, entre outros). Os ficheiros de dados da responsabilidade dos proprietários dos motores de pesquisa incluem dados pessoais (2-4), e pese embora o referido no Considerando 2, da Diretiva 95/46/CE, de que os «que os sistemas de tratamento de dados estão ao serviço do Homem e devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos», a LPDP e as al) a) e c) do n.º 1, do art.º 4º, da Diretiva 95/46/CE, são aplicáveis ao tratamento de dados, ainda que as suas sedes se encontrem localizadas fora do EEE (2-3.2.). A obtenção do consentimento dos utilizadores é necessário para legitimar o tratamento dos dados recolhidos (3-7. e 3-8.), nomeadamente o endereços IP, recurso a testemunhos de conexão, as funcionalidades de cache entre outros, com o objetivo de enviar comunicações publicitárias (n.º 3, do art.º 5, e art.º 13º, da Diretiva 2002/58/CE e art.º n.º 2, do art.º 5º; e art.º 13º-A, da L n.º 41/2004, de 18/08)[465].

Os sujeitos que participam nas atividades do marketing comportamental têm distintos interesses assim como desempenham funções distintas entre si. O GT29 destaca os fornecedores de redes de publicidade que estabelecem a relação entre editores e anunciantes; os anunciantes que promovem bens e serviços no mercado e os editores que são os proprietários das páginas web com espaços para mostrarem os anúncios[466]. O papel que cada

---

378 [Consult. 19 set. 2015]. Disponível em WWW <https://academic.oup.com/ijlit/article/18/4/356/744617/The-Italian-Google-Case-Privacy-Freedom-of-SpeechThe Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents>ISSN 1464-3693.

[465] O GT29, considera que os fornecedores motores de pesquisa não podem invocar a legalidade do tratamento de dados com fundamento na necessidade de execução de um contrato (porque não cumprem a limitação estrita da necessidade) e na necessidade de prosseguir interesses legítimos do responsável pelo tratamento (porque a melhoria dos serviços e garantir a segurança dos sistemas pode ser realizada sem identificar os utilizadores, como a prevenção de fraude) (v. GT29, cit. 189).

[466] GT29, cit. 419.

um destes sujeitos desempenha é importante porque sendo os responsáveis pelo tratamento de dados, estão sujeitos às normas gerais e especiais relativas ao direito à privacidade e à proteção dos dados pessoais, devendo cumprir as condições gerais do tratamento quanto às finalidades, meios e demais responsabilidades, salientando-se o dever de informação previsto na LPDP e na Diretiva 95/46/CE (3-7.2.1.) se o testemunho é utilizado para criar perfis, que tipo de informação é recolhida para o efeito e se serão utilizados para direcionar publicidade.

3-9.3.3. Os serviços de redes sociais em linha

Os SRS podem ser definidos, *lacto sensu*, como «plataformas de comunicação em linha que permitem a indivíduos aderirem a redes de utilizadores com interesses semelhantes ou criarem redes deste tipo»[467] e que são, juridicamente, considerados serviços da sociedade de informação. Os SRS podem ser classificados em função do contexto onde atuam, como, por exemplo, redes relacionais (*Facebook, Twitter, Instagram, Google+, Youtube, MySpace, Badoo*), redes profissionais (*Linkedin)*, redes desportivas (*Strava*) redes comunitárias, redes políticas, etc., que permitem analisar a forma como as organizações e as pessoas desenvolvem a sua atividade, armazenando dados que analisados são muito úteis para a tomada de decisões. Os SRS disponibilizam ferramentas que permitem aos utilizadores fornecer dados para construir um perfil, conteúdos de texto, imagem e vídeo, para partilhar com outros utilizadores. Os dados pessoais disponíveis nas redes sociais podem ser utilizados por «terceiros para uma grande variedade de fins, incluindo os comerciais, e podem apresentar riscos graves, como o roubo de identidade, prejuízos financeiros, perda de oportunidades de negócios ou de emprego e danos físicos»[468] configurando uma invasão à privacidade e violação do direito à proteção de dados pessoais.

A LPDP e a Diretiva 95/46/CE e nos casos em que prestam serviços de comunicações eletrónicas, nomeadamente o rastreamento por endereço IP, os testemunhos de conexão, dados de localização, aplica-se a L 41/2004, de 18/08 e a Diretiva 2002/58/CE aplica-se ao tratamento de dados pelos SRS, ainda que as suas sedes estejam situadas fora do EEE. A proteção de dados dos utilizadores não se pode centrar no perfil do utilizador que é muito redutor, pois, o verdadeiro risco está nas aplicações informáticas que captam o seu comportamento em linha e as suas interações que seja informado. Salvo que se aplique a isenção de âmbito doméstico, o utilizador poderia ser considerado responsável[469] pelo

[467] GT29, cit. 382, p. 5.
[468] GT29, cit. 382, p. 4.
[469] O TJUE pronunciou-se em sentido contrário no Ac *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy e*

tratamento de dados em relação ao ficheiro que constitui a sua conta nos SRS, no entanto, os SRS são considerados responsáveis pelo tratamento dos dados, pois criam ficheiros de dados[470] com o registo dos perfis dos utilizadores, dados de tráfego, localização, etc., que podem utilizar para fins de marketing direto, incluindo a publicidade feita por terceiros, ficando sujeitos ao cumprimento dos princípios e condições de legitimidade previstas na LPDP, L n.º 7/2004, de 07/01 e nas Diretiva 95/46/CE e 2002/58/CE (3-7., 3-8., 3-9.3.1).

3-9.3.4. A Internet das Coisas

Como referido em 2-2 e em 3-9, a evolução da tecnologia surgiram novas práticas de marketing recorrendo à promoção comercial e distintas formas de publicidade incorporadas em objetos inteligentes interligados na IdC. Os dados gerados em IAm combinando técnicas de análise e cruzamento dos mesmos são suscetíveis de serem tratados para finalidades distintas do tratamento inicial sem que o utilizador tenha tido conhecimento e consentido no tratamento dos seus dados pessoais, nem os responsáveis pelo tratamento tem o cuidado de conceber as coisas vestíveis dotadas de *software* adequado para cumprimento das normas da proteção de dados.

Os dispositivos da IdC são, juridicamente, equipamentos terminais nos termos do n.º 2, do art.º 5º, da L n.º 41/2004, de 18/08 e no n.º 3, do art.º 5º, da Diretiva 2002/58/CE[471], pelo que a recolha de dados está sujeita à prestação do consentimento do utilizador (3-8.1.).

O responsável pelo tratamento de dados em IAm e a assunção de responsabilidades em matéria da proteção de dados depende do papel que é desempenhado num mundo cada vez mais complexo e de intervenção combinada, de que se destacam os fabricantes de dispositivos[472], plataformas sociais[473], corretores de dados[474] ou plataformas de dados[475].

Satamedia Oy, do TJUE, nº C-73/07, de 16/12/2000, conforme parágrafo 44: «Daí decorre que esta segunda exceção deve ser interpretada no sentido de que tem apenas por objeto as atividades que se inserem no quadro da vida privada ou familiar dos particulares … manifestamente, não é esse o caso das atividades da *Markkinapörssi* e da *Satamedia*, cujo objeto é dar a conhecer os dados recolhidos a um número indefinido de pessoas». O tratamento de dados transcende, neste caso, a atividade do titular.

[470] Os SRS detêm aplicações com capacidade de converter dados inócuos e inofensivos, não estruturados e aparentemente sem sentido em dados que permitem identificar pessoas.

[471] V. GT29, cit. 3.

[472] Os fabricantes de dispositivos da IdC para além de vender as coisas vestíveis incorporam no sistema operativo programas que permitem rastrear as atividades do utilizador.

[473] Os utilizadores podem partilhar em redes sociais os dados registados nas coisas vestíveis utilizando aplicações disponibilizadas nessas plataformas pelos SRS.

[474] Os corretores de dados compram dados para análise e categorizar em listas, podendo conter informações demográficas, rendimentos, interesses, etc.

[475] Plataformas de dados IdC são **c**onstituídas por um conjunto de interfaces e formato de dados, como, por exemplo, os *smartphones* e os *tablets* considerados portais de acesso naturais dos dados recolhidos através de muitos dispositivos IdC à Internet e são consideradas responsáveis pelo tratamento ao abrigo da legislação da UE em matéria de proteção de dados, quando implica a recolha dos dados pessoais dos utilizadores para os seus

3-9.3.5. A construção de perfis

O marketing com que hoje nos deparamos já não é um marketing massivo mas um marketing personalizado ou seja um marketing *one-to-one*[476]. Os novos modelos de negócio assentes em recursos publicitários e nos meios para alcançá-los, proporcionados pelo IAm levam o marketing direto a ser mais preciso com a utilização e seleção da informação extraída das bases de dados para determinados consumidores de forma personalizada em conformidade com os seus hábitos de compra (e até predizer o que necessitam de comprar) de forma imediata recorrendo a estratégias invisíveis e despercebidas (não só aos próprios consumidores mas também aos seus concorrentes, podendo ocorrer situações de práticas desleais entre as empresas) para o envio de mensagens comerciais e publicitárias, que parece não ter limites com o crescente aumento de empresas que se dedicam a vender dados pessoais organizados em listas[477].

Os problemas relacionados com as novas tecnologias disponíveis mostram que é, fundamental, o controlo sobre os dados pessoais que parecem permanentemente ameaçados e manipulados até psicologicamente afetando o comportamento dos consumidores[478]. Não se trata só do direito à privacidade e à proteção dos dados pessoais mas também de assegurar outras liberdades fundamentais como do pensamento, da religião, cultural, entre outras, conforme à CDFUE e da Convenção 108. Os processos dos preços dinâmicos e indexação de utilizadores às listas negras[479], fundamentados em critérios obscuros, podendo provocar descriminações com consequências danosas para os titulares dos dados.

A Convenção 108 não contém qualquer disposição que proíba o processamento automático de dados para definir um perfil de determinada pessoa, o que não significa que seja legal e legítimo com fundamento no art.º 8º, da CEDH. Porém, o art.º 13º, da LPDP e o art.º 15º, da Diretiva 95/46/CE, preveem que ninguém pode ficar sujeito a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da

---

próprios fins.

[476] PEPPERS, Don, ROGERS, Marta, DORF, Bob - *One-to-one field book*. New York : Currency Doubleday, 1999. ISBN 0-385-49369-X.

[477] A venda de dados pessoais obtidos em linha através de um concurso dirigido a menores de 13 anos sem consentimento dos pais pela empresa *Toysmart.com* foi considerada ilícita pelo *United States District Court of Massachusetts*, e a repercussão social tomou proporções de tal forma graves que passados dois meses o Senado Americano aprovou uma lei que proibia as companhias de vender ou alugar os dados dos seus clientes consentimento prévio. A informação completa sobre a sentença e repercussões legislativas, pode ser consultada aqui <https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc>.

[478] O uso da RFID para diferentes fins tem merecido a preocupação do GT29. O uso desta tecnologia em expansão e contínuo desenvolvimento está em todos os setores da economia desde os transportes e distribuição, aviação, saúde, segurança e controlo, etc. (v. GT29, cit. 219).

[479] GT29, cit. 36.

sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento. A norma deve ser interpretada no sentido de que os titulares têm o direito de conhecer a lógica e os critérios subjacentes à decisão automatizada.

O RGPD vem considerar que um perfil é «qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações», em conformidade com o n.º 4, do art.º 4º, pelo que é exigido o consentimento explícito do titular dos dados, nos termos da al) c) do n.º 1, do art.º 22º, sem prejuízo do cumprimento dos princípios e condições de legitimidade e salvo as exceções previstas.

3-9.5. O marketing comportamental em linha na pRPCE

O art.º 8º, da pRPCE sob a epígrafe de «proteção das informações armazenadas nos equipamentos terminais dos utilizadores finais e relacionadas com esses equipamentos» proíbe a recolha de informações provenientes dos equipamentos terminais dos utilizadores finais, incluindo sobre o seu *software* e *hardware*, exceto se: (a) se forem necessárias exclusivamente para assegurar a transmissão de uma comunicação eletrónica através de uma rede de comunicações eletrónicas; (b) se o utilizador final tiver dado o seu consentimento; ou (c) se forem necessárias para uma medição de audiência da web, desde que tal medição seja efetuada pelo prestador do serviço da sociedade de informação solicitado pelo utilizador final. É igualmente proibida a recolha de informações emitidas pelos equipamentos terminais para permitir a sua ligação a outro dispositivo e/ou equipamento de rede, exceto se: (a) for exclusivamente efetuada para estabelecer uma ligação e durante o tempo necessário para o efeito; (b) for afixado um aviso claro e visível contendo, no mínimo, informações sobre as modalidades da recolha, o seu objetivo, a pessoa responsável e as outras informações exigidas ao abrigo do art.º 13.º do RGPD, quando forem recolhidos dados de caráter pessoal, bem como qualquer medida que o utilizador final dos equipamentos terminais pode tomar para reduzir ao mínimo ou fazer cessar a recolha. As informações a fornecer podem ser associadas a ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível uma útil perspetiva geral da recolha, a cargo da COMISSÃO, contribuindo para a transparência do mecanismo do consentimento; ou (c) a recolha dessas informações deve ser subordinada à aplicação de medidas técnicas e organizativas adequadas para garantir um nível

de segurança adequado aos riscos, tal como estabelecido no art.º 32º, do RGPD.

As configurações adequadas dos programas de navegação ou outras aplicações contribuem não só para uma maior clareza na prestação do consentimento prévio informado[480] para o tratamento de dados e outras informações, mas também para a harmonização das regras entre os Estados-Membros diminuindo as condições de desigualdade da concorrência e das distorções do mercado. Dado que as páginas da internet não estão limitadas por fronteiras reconhece-se que a normalização deveria ter lugar preferencialmente a nível mundial, para assegurar a confidencialidade das informações armazenadas nos equipamentos terminais dos utilizadores, nomeadamente através da sensibilização e da capacitação dos utilizadores.

O Considerando 1, da pRPCE, reitera a garantia do cumprimento do princípio da confidencialidade deve ser aplicável às formas de comunicação atuais e futuras, incluindo chamadas, acesso à Internet, mensagens instantâneas, correio eletrónico, chamadas telefónicas pela Internet e mensagens pessoais nas redes sociais, conforme o art.º 7º, da CDFUE (3-9.1.2.).

O direito incondicional de oposição na pRPCE é, ainda, particularizado no art.º 16º, referindo-se que os operadores económicos que tenham obtido as coordenadas eletrónicas de contacto para correio eletrónico, no contexto da venda de produtos ou serviços, em conformidade com o RGPD, de uma pessoa singular ou coletiva, podem utilizá-las para fins de marketing direto dos seus próprios produtos ou serviços análogos, desde que aos clientes tenha sido dada clara e distintamente a possibilidade de se oporem, de forma gratuita e fácil, a essa utilização. O direito de oposição deve ser oferecido na data da recolha e sempre que uma mensagem é enviada, após a informação prévia acerca da natureza comercial da comunicação e do remetente, e bem assim, com todas as informações necessárias sobre o modo de exercício do direito e do seu consentimento em relação à receção de novas comunicações comerciais (n.ºs 2 e 6, do art.º 16º, da pRPCE).

[480] Em conformidade com as normas do RGPD.

PARTE IV – CONCLUSÕES

CAPÍTULO X – CONCLUSÕES

10-1. Conclusões

O IAm assenta em sistemas tecnológicos que alteraram o paradigma da comunicação em redes abertas e cujos protocolos de interação podem conduzir a uma invasão da privacidade das pessoas. O rastreamento dos dados, inúmeras vezes de forma oculta, que permitem aos operadores económicos conhecer o comportamento, gostos e interações dos utilizadores, alteraram o conhecimento das formas de consumo, e em consequência da promoção de comunicações comerciais através das técnicas do marketing. As infraestruturas dos sistemas tecnológicos assentam no processamento de dados que quando relacionados com as pessoas estão sujeitos a proteção legal, cuja abordagem pode resumir-se nas considerações seguintes:

1) A proteção de dados encontra as suas reminiscências históricas no movimento do direito à privacidade iniciado, no século XIX, por Brandeis e Warren nos EUA, tendo as instituições e organizações governamentais iniciado estudos, envolvendo a sapiência das comunidades tecnológica e jurídica, para a positivação da proteção de dados consagrada em convenções e acompanhadas de recomendações, resoluções e pareceres. A UE na década de noventa inicia a aprovação de normas para consolidar o direito à proteção de dados e a sua harmonização entre os Estados-Membros. Os Estados, simultaneamente, passaram a incluir no seu direito interno ao direito à proteção de dados, dos quais Portugal é pioneiro na consagração constitucional.
2) O direito à proteção de dados configura-se como um direito fundamental complexo para garantir a autodeterminação informativa do titular no processo de tratamento e utilização dos seus dados pessoais. Os meios de exercício de controlo pelo titular dos dados estão previstos na lei e consubstanciam-se essencialmente no direito de acesso, retificação, alteração ou apagamento. O RGPD fortalece e alarga o catálogo dos poderes dos titulares dos dados prevendo expressamente o direito de ser esquecido e o direito de portabilidade dos dados. O direito à proteção de dados não é um direito absoluto na medida em que depende das ações do responsável do tratamento tendo em conta as circunstâncias e a tecnologia disponível, por um lado; e do equilíbrio de interesses com outros direitos, liberdades e garantias, destacando-se as relacionadas com as liberdades económicas que são fundamentais para consolidar o mercado único digital, por outro lado.
3) O conceito de dados pessoais é um conceito dinâmico *in construhendo* pela

jurisprudência, pela atos emitidos das organizações da proteção de dados e pela doutrina autoral mais prestigiada, incorporado nos atos normativos aprovados pelas mais altas instâncias da EU, de que é exemplo o RGPD que plasma no n.º 1, do art.º 4º, como a «informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular». O conceito legal de dados pessoais revela grande preocupação para acompanhar a inovação tecnológica recorrendo a conceitos gerais e abstratos, de modo a prevenir conceitos aprazados e obsoletos, como por exemplo, propondo-se enquadrar novas realidades como os dispositivos que abrem portas para o rastreamento indetetável ao titular, através das coisas vestíveis, como a captação ultra-sónica que usa sinais de áudio de alta frequência em linha ou não, o *fingerprinting* (níveis de bateria dos dispositivos) cujas configurações existem em todos os dispositivos com elevada sofisticação e que podem alcançar o armazenamento de metadados, os testemunhos de conexão, o registo dos movimentos geográficos, etc.

4) A LPDP é aplicável aos dados pessoais, no sentido que é relativa a pessoas singulares identificadas ou identificáveis, embora exista uma corrente doutrinária que entenda ser extensiva às pessoas coletivas em determinadas circunstâncias. O RGPD refere expressamente que a proteção se dirige às pessoas singulares, independentemente da sua nacionalidade ou local de residência.
5) A LPDP prevê expressamente os casos de aplicação de âmbito territorial da lei nacional, cujos critérios para determinar a sua aplicação, dependem da localização do estabelecimento do responsável pelo tratamento e a localização dos meios ou equipamento utilizados. O RGPD alarga o âmbito territorial não exigindo uma conexão física dos responsáveis pelo tratamento de dados, pois, aplica-se ao «tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União», e ainda, ao «tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) a oferta de bens ou serviços a esses

titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) o controlo do seu comportamento, desde que esse comportamento tenha lugar na União».

6) A lei constitucional e ordinária conferem proteção ao tratamento de dados pessoais por meios, total ou parcialmente automatizados, conferindo-se igual proteção ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais, que devem ser estruturados de acordo com critérios específicos relativos às pessoas que permitam um acesso fácil aos dados pessoais, excluindo-se do âmbito de aplicação os ficheiros relativos ao tratamento de dados pessoais efetuado por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.
7) O tratamento de dados pessoais está sujeito às formalidades de notificação ou autorização pelo responsável do tratamento junto da CNPD e do cumprimento dos princípios (da licitude, da lealdade, da transparência, da transparência, da qualidade e da finalidade) e condições de legitimidade (consentimento, execução de um contrato, obrigações legais, interesses vitais do titular, ou interesses legítimos) previstos na LPDP e da Diretiva 95/46/CE. O RGPD *declara* o fim das notificações e autorizações sendo o responsável pelo tratamento o garante pelo cumprimento dos princípios do tratamento de dados, e só nos casos previstos necessita de autorização ou parecer para dar início às operações de tratamento de dados.
8) O tratamento de dados que se encontrem em curso à data de entrada em vigor do RGPD deve incorporar as suas disposições à data da produção dos seus efeitos. As decisões da Comissão adotadas e as autorizações emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, são válidas até à sua substituição, alteração ou simplesmente revogadas.
9) O princípio da transparência é fundamental na relação de confiança entre os operadores económicos e os titulares dos dados pessoais para que o consentimento seja prestado de forma livre, informada, inequívoca e específica, e evitar que as expectativas sejam defraudadas quanto aos fins, ou seja, na receção de comunicações de promoção comercial. O consentimento é o eixo central das normas sobre a proteção de dados na medida em que é o titular dos dados quem decide, como, quando e porque é que os seus dados são tratados – poder de decisão que deriva do direito à autodeterminação informativa.
10) A publicidade domiciliária, por telefone ou telecópia consagram um sistema de opção negativo. A pRPCE, alinhada com o RGPD e de forma a alcançar coerência no

ecossistema da proteção de dados, prevê que as pessoas singulares ou coletivas que utilizam serviços de comunicações eletrónicas para efetuarem chamadas de marketing direto devem obter o consentimento prévio dos utilizadores finais.

11) O binómio consentimento do titular / finalidade do tratamento de dados pessoais, é reforçado na Diretiva 2002/58/CE, contra a intrusão na privacidade bem como assegurar um nível de proteção adequado aos titulares dos dados por comunicações não solicitadas para fins de marketing direto através de correio eletrónico, aos serviços SMS, MMS e a outros tipos de aplicações similares, por um lado; e o armazenamento ilícito de informações sobre o equipamento ou coisas vestíveis dos utilizadores, e bem assim as interações com os motores de pesquisa e os serviços de redes sociais, por outro lado.
12) As comunicações comerciais não solicitadas com origem nas técnicas de rastreamento, aplicações, etc. e do marketing comportamental consagram um sistema de opção positivo. A pRPCE prevê a consagração da doutrina jurisprudencial, administrativa e autoral ao alargar outros sistemas de rastreamento dos utilizadores da internet.
13) O direito de oposição do titular é incondicional, em qualquer circunstância e sem necessidade de fundamento ou sujeição a prazos, contra a receção de comunicações comerciais não solicitadas, assim como o rastreamento de dados que obtenham informação sobre o seu comportamento em linha, de forma ilícita, contribuindo para um efetivo direito à proteção de dados.
14) O responsável pelo tratamento de dados que procurava garantir a aplicação das normas que regulam a proteção de dados, passa a ser o responsável pelo cumprimento dos princípios do tratamento de dados (tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares) cujas medidas técnicas e organizativas utilizadas são capazes de o demonstrar.

BIBLIOGRAFIA

DOCUMENTOS IMPRESSOS

ASCENSÃO, José de Oliveira - Sociedade de Informação. in **Direito da Sociedade da Informação**, Vol. I, p. 163-184. Coimbra : Coimbra Editora, 1999. ISBN:972-32-0916-0.

CANOTILHO, J.J. Gomes, MOREIRA, Vital - **Constituição da República Portuguesa Anotada**, Vol. I. 4.ª ed. rev. e reimp., Coimbra : Coimbra Editora, 2014. ISBN 978-972-32-2286-9.

CASTRO, Catarina Sarmento e - **Direito da Informática, Privacidade e Dados Pessoais.** 1ª ed, Coimbra : Almedina, 2005. ISBN 978-97-2402-424-0.
– Artigo 8º (Proteção de dados pessoais). In SILVEIRA, Alessandra, CANOTILHO, Mariana, coord. - **Carta dos Direitos Fundamentais da União Europeia Comentada**. Coimbra : Almedina, 2013. ISBN 978-97-2405-120-8. p.120-128

DONEDA, Danilo C. Maganhoto - **Da privacidade à proteção de dados pessoais.** Rio de Janeiro : Renovar, 2006. ISBN 85-7147-562-8

FARIA, Maria Paula Ribeiro de – Artigo 35º (Utilização da Informática). In MIRANDA, Jorge; MEDEIROS, Rui, coord. - **Constituição Portuguesa Anotada**, Tomo I. 2.ª ed., Coimbra : Wolters Kluwer Portugal, 2010. ISBN 978-972-32-1822-0. p. 779-801

GONÇALVES, Maria Eduarda - **Direito da Informação. Novos direitos e formas de regulação na sociedade da informação**. Coimbra : Almedina, 2003. ISBN 978-972-4019-08-6.

GRINOVER, Ada Pellegrini [*et al.*] - **Código Brasileiro de Defesa do Consumidor, Comentado pelos autores do Anteprojeto**, 6ª ed., Rio de Janeiro, Forense Universitária, 2000. ISBN 87-218-02-49-8

GRÖNROOS, Christian – **Service Managment and Marketing**. 3ª ed., West Sussex (England) : John Wiley & Sons Ldt , 2007. ISBN 978-047-0028-62-9.

GUERRA, Amadeu – **A privacidade no local de trabalho**. Coimbra : Almedina, 2004. ISBN 978-972-4022-24-6.
- Informática e Tratamento de Dados Pessoais – os direitos dos cidadãos e as obrigações

dos responsáveis pelos tratamentos automatizados. Lisboa : Vislis Editores, 1997. ISBN 972-52-0013-6.

LOPES, Joaquim Seabra - A Proteção da Privacidade e dos Dados Pessoais na Sociedade da Informação: Tendências e Desafios numa Sociedade em Transição. in SILVA, Germano Marques da, coord. - **Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa**. Lisboa : Universidade Católica, 2002. ISBN 978-972-5400-44-9, p. 779-807.

LÓPEZ, Jordi Verdaguer; JANÉ, Mª Antonia Bergas – **Todo protección de datos**. Valencia : CISS, 2013. ISBN 978-84-9954-489-2).

MARCOS, Isabel Davara Fernández de - **Hacia la estandarización de la protección de datos personales: Propuesta sobre una «tercera vía o tertium genus» internacional**. Madrid : La Ley, 2011. ISBN 978-84-8126-827-0.

MEDEIROS, Rui; CORTÊS, António – Artigo 26º (Outros direitos pessoais) In MIRANDA, Jorge; MEDEIROS, Rui, coord. - **Constituição Portuguesa Anotada**, Tomo I. 2.ª ed., Coimbra : Wolters Kluwer Portugal, 2010. ISBN 978-972-32-1822-0. p. 603-632.

MIRANDA, Jorge - Artigo 60º ***(***Direitos dos consumidores) In MIRANDA, Jorge; MEDEIROS, Rui, coord. - **Constituição Portuguesa Anotada**, Tomo I. 2.ª ed., Coimbra : Wolters Kluwer Portugal, 2010. ISBN 978-972-32-1822-0. p. 1169-1179.

NISSENBAUM, Helen – **Privacy in Context, Technology, Policy, and Integrity of Social Life**. Stanford, California : Stanford Law Books, 2010. ISBN 978-0804752374.

NANCLARES, José Martín y Pérez de – Artigo 8º (Protección de dato de caráter personal). In MARTÍN, Araceli Mangas e ALONSO, Luis N. González, coord. **- Carta de los Derechos Fundamentales de la Unión Europea - Comentario artículo por artículo**, 1.ª ed., Bilbao : Fundación BBVA, 2008. ISBN 978-84-96515-80-2. p. 223-243.

PAYTON, Theresa M.; CLAYPOOLE, Theodore - **Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family**, Lanham (Maryland) [etc.] : Rowman & Littlefield, 2014. ISBN 978-1-4422-2545-9.

PEPPERS, Don, ROGERS, Marta, DORF, Bob - **One-to-one field book**. New York : Currency Doubleday, 1999. ISBN 0-385-49369-X

PINHEIRO, Alexandre Sousa – **Privacy e Proteção de dados pessoais: a construção**

dogmática do direito à identidade informacional. Lisboa : Associação Académica da Faculdade de Direito de Lisboa, 2015. 978-612-0002-60-5

POMBO, Eugenio Llamas, coord. - **Ley General para la Defensa de los Consumidores y Usuários, Comentarios y Jurisprudencia de la Ley veinte años después**. Las Rozas (Madrid) : La Ley-Actualidad, 2005. ISBN 84-9725-603-4

RODOTÀ, Stefano – **A vida na sociedade de vigilância, A privacidade hoje**. Trad. Danilo Doneda e Luciana Cabral Doneda, Rio de Janeiro : Renovar, 2008. ISBN 978857147-688-2
- Data Protection as a Fundamental Right. in GUTWIRTH; Serge; LEENES, Ronald; HERT, Paul De; - **Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges** [Em linha]. Dordrecht : Springer Science+Business Media Dordrecht 2014. [Consult. 7 ago. 2016]. Disponível em WWW <http://www.springer.com/la/book/9789400775398> ISBN 978-94-007-7540-4. Cap. 3, p. 77-82

RODRIGUEZ DAVARA, Miguel Ángel – **Manual de Protección de Datos para Abogados.** Madrid : Thompson Aranzadi, 2008. ISBN 978-8497-676-49-6.

SOLÍS, David Ordóñez - **Privacidad y protección judicial de los datos personales.** 1.º ed., Barcelona : Bosch, 2011. ISBN 978-84-9790-853-5

VASCONCELOS, Pedro Pais de - Proteção de Dados Pessoais e Direito à Privacidade, in **Direito da Sociedade da Informação**, Coimbra : Coimbra Editora, 1999. ISBN:972-32-0916-0. Vol. I, p. 241-253.

VAZAK, Karel – **As Dimensões Internacionais dos Direitos do Homem – manual destinado ao ensino dos direitos do homem nas universidades**. Lisboa : Editora Portuguesa de Livros Técnicos e Científicos / UNESCO, 1983.

VENÂNCIO, Pedro Dias - A previsão constitucional da utilização da informática. In **Revista de Estudos Politécnicos** Vol. 8, 2007, p. 243-264. [Consult. 19 out. 2015]. Disponível em WWW <http://www.scielo.mec.pt/pdf/tek/n8/v5n8a12.pdf>

DOCUMENTOS ELETRÓNICOS

AGÊNCIA MUNDIAL ANTIDOPAGEM - Código Mundial Antidopagem. Montreal [Em linha]. (2015) [Consult. 1 dez. 2016]. Disponível em WWW <http://www.adop.pt/media/8381/C%C3%B3digo%20Mundial%20Antidopagem%202015.pdf>

ALPÁR, Gergely; HOEPMAN, Jaap-Henk; SILJEE, Johanneke - **The Identity Crisis. Security, Privacy and Usability Issues in Identity Management.** [Em linha]. 2011. [Consult. 12 dez. 2014]. Disponível em WWW <http://arxiv.org/ftp/arxiv/papers/1101/1101.0427.pdf>

ARAYA, Agustin A. - Questioning Ubiquitous Computing. In **HWANG,** C. Jinshong; **HWANG**, Betty W. (Coord.) - **Proceedings of the 1995 ACM 23rd annual conference on Computer science.** [Em linha]. New York : ACM, 1995 [Consult. 22 nov. 2015]. Disponível em WWW <http://www.cc.gatech.edu/~keith/classes/ubicomplexity/pdfs/crit/araya-questioning-ubicomp.pdf >. ISBN:0-89791-737-5. p.230-237

AUGUSTO, Juan C. [*et al*.] - Intelligent Environments: a manifesto. **Human-centric Computing and Information Sciences** [Em linha]. Vol. 3, n.º 12 (2013) [Consult. 19 nov. 2015]. Disponível em WWW <http://www.hcis-journal.com/content/3/1/12> ISSN: 2192-1962.

BENDICH, Albert M. - Privacy, Poverty, and the Constitution [Em linha]. In **California Law Review**, Vol. n.º 54, n.º 2, (1966). [Consult. 12 ago. 2016]. Disponível em WWW <http://scholarship.law.berkeley. edu/californialawreview/vol48/iss3/1/>

BOBBIO, Noberto - **A Era dos Direitos** [Em linha]. 7.ª Reimp. Trad. Carlos Nelson Coutinho, Rio de Janeiro: Elsevier, 2004. Título original L'età dei Diritti. [Consult. 20 ago. 2015]. Disponível em WWW <https://direitoufma2010.files.wordpress.com/2010/05/norberto-bobbio-a-era-dos-direitos.pdf> ISBN 10: 85-352-1561-1

BREY, Philip - Freedom and Privacy in Ambient Intelligence. In **Ethics and Information Technology** [Em linha]. Vol. 7, n.º 3 (set. 2005). p. 157-166. Dordrecht [etc.] : Springer Business Media Dordrecht. [Consult. 19 nov. 2015]. Disponível em WWW <https://link.springer.com/article/10.1007/s10676-006-0005-3> ISSN: 1572-8439.

BROWNSWORD, Roger - Consent in Data Protection Law: Privacy, Fair Processing and

Confidentiality. in GUTWIRTH; Serge [*et al*.] - **Reinventing Data Protection?** [Em linha]. New York [etc.]: Springer Science + Business Media B.V. 2009. [Consult. 10 dez. 2014]. Disponível em WWW <https://link.springer.com/book/10.1007/978-1-4020-9498-9> ISBN 978-1-4020-9498-9. p. 83-110

CABALLERO, Susana Sanz - Interferencias entre el Derecho Comunitario y el Convenio Europeo De Derechos Humanos (Luxemburgo *versus E*strasburgo: ¿quién es la última instancia de los derechos fundamentales en Europa?). In **Revista de Derecho Comunitario Europeo** [Em linha]. Año 8. n.º 17. (enero-abril 2004) p. 117-160. [Consult. 12 nov. 20165]. Disponível em WWW <https://dialnet.unirioja.es/ejemplar/93104> ISSN: 1989-5569.

CATE, Fred H. - **The EU Data Protection Directive, Information Privacy, and the Public Interest** [Em linha]. Indiana University Maurer School of Law. Paper 646, (1995) [Consult. 12 nov. 2015]. Disponível em WWW <http://www.repository.law.indiana.edu/facpub/646/>

CAVOUKIAN, Anna - Privacy by Design: Leadership, Methods, and Results. in GUTWIRTH, Serge [*et al*.] coord. - **European Data Protection: Coming of Age** [Em linha]. Dordrecht [etc.]: Springer Science+Business Media Dordrecht, 2013. Disponível em WWW <http://www.springer.com/br/book/9789400751842> ISBN 978-94-007-5170-5. Cap. 8, p. 175-202.

COOK, Jared R. (Realizador) - **Life Simplified with Connected Devices** [Registo vídeo], (5 minutos e 37 segundos), com texto em inglês : Provo, Utah : The Connected Devices Laboratory at Brigham Young University, 2014 [Consult. 16 out. 2015]. Disponível em WWW <https://www.youtube.com/watch?v=NjYTzvAVozo>

CONSELHO DA EUROPA – **Guidelines of the Committee of Ministers to Members States on Human Rights and the Fight Against Terrorism adopted by the Committee of Ministers at its 804th meeting**. [Em linha]. (11/07/2002) [Consult. 12 mar. 2015]. Disponível em WWW < http://www.coe.int/t/dlapil/cahdi /Source/Docs2002/H_2002_ 4E.pdf>

- Resolution (73) 22 of the Committee of Ministers to Members States on the protection of the privacy of individuals Vis-a-vis electronic data banks in the private sector [Em linha]. (26/09/1973) [Consult. 12 mar. 2015]. Disponível em WWW <https://rm.coe.int/ CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502 830>

- Resolution (73) 23 of the Committee of Ministers to Members States on harmonisation measures in the field of legal data processing in the Member States of the Council Of Europe [Em linha]. (26/09/1973) [Consult. 12 mar. 2015]. Disponível em WWW < https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?

- Resolution (74) 29 of the Committee of Ministers to Members States on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector [Em linha]. 20/09/1974 [Consult. 12 mar. 2015]. Disponível em WWW <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51>

- Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments (16th Sitting) [Em linha]. (31/01/1968) [Consult. 12 mar. 2015]. Disponível em WWW <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp? fileid=14546&lang=en>

- Recommendation n.º R(85) 20 on the protection of personal data used for the purposes of direct marketing [Em linha]. (25/10/1985) [Consult. 14 mar. 2015]. Disponível em WWW <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804bd336>

- Recommendation n.º R (90) 19 of the Committee of Ministers to Members States on the protection of personal data used for payment and other related operations [Em linha]. (13/09/1990) [Consult. 9 abr. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=570709&SecMode=1&DocId=592684&Usage=2>

- Recommendation (91) 10 of the Committee of Ministers to Member States on the communication to third parties of personal data held by public bodies [Em linha]. (09/09/1991) [Consult. 9 abr. 2015]. Disponível em WWW <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804c1486>

- Recommendation n.º R (92) 03 of the Committee of Ministers to Members States on genetic testing and screening for health care purposes [Em linha]. (10/02/1992) [Consult. 9 abr. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=573883&SecMode=1&DocId=601492&Usage=2

- Recommendation n.º R (97) 5 of the Committee of Ministers to Members States on the protection of medical data [Em linha]. (13/02/1997) [Consult. 9 abr. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.mdBlobGet&InstranetImage=564487&SecMode=1&DocId=560582&Usage=2>

- Recommendation n.º R (97) 18 of the Committee of Ministers to Members States concerning the protection of personal data collected and processed for statistical purposes [Em linha]. (30/09/1997) [Consult. 12 mar. 2015]. Disponível em WWW <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2001724&SecMode=1&DocId=578856&Usage=2

Recommendation n.º R(99) 5 for the protection of privacy on the Internet [Em linha]. 23/02/1999 [Consult. 12 mar. 2015]. Disponível em WWW <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f4429>

- Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling [Em linha]. (23/07/2010) [Consult. 12 mar. 2015]. Disponível em WWW <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00>

COSTA, Francisco Bruto da, BRAVO, Rogério – **Spam e Mail-Bomb subsídios para uma perspectiva penal**. Lisboa : Quid Juris, 2005. ISBN 972-724-239-1

DAVENPORT, Thomas H., PRUSAK, Laurence - **Working Knowledge: How Organizations Manage what They Know** [Em linha]. Cambridge (Massachusetts) : Harvard Business Press, 1998 [Consult. 11 mai. 2012]. Disponível em WWW <https://encrypted.google.com/books?id=-4-7vmCVG5cC&printsec=copyright&hl=pt-T&source=gbs_pub_info_r#v=onepage&q&f=false>

DUHIGG, Charles - How Companies Learn Your Secrets [Em linha]. In **The New York Times** (16/02/2012). [Consult. 18 de jun. 2014]. Disponível em WWW <http://emoglen. law.columbia.edu/twiki/pub/CompPrivConst/HowCompaniesLearnOurConsumingSecrets/How_Companies_Learn_Your_Secrets_-_NYTimes.com.pdf >

FRIEDEWALD, Michael, [*et al.*] - Perspectives of ambient intelligence in the home environment [Em linha]. In **Telematics and Informatics**, Vol. 22, n.º 3 (aug. 2005) p. 221-238. [S.l.] : Elsevier B.V. 2005. [Consult. 18 de jun. 2016]. Disponível em WWW <http://www. sciencedirect.com/science/article/pii/S0736585304000590> ISSN: 0736-5853.

FOX-BREWSTER, Tom - Londoners give up eldest children in public Wi-Fi security horror show [Em linha]**. The Guardian, (**29/09/2014). [Consult. 12 de out. 2015]. Disponível em WWW <https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause>

FUSTER, Gloria González - **The Emergence of Personal Data Protection as a Fundamental Right of the EU** [Em linha]. Cham [etc,] : Springer International Publishing Switzerland, 2014. (Law, Governance and Technology Series, Vol. XVI.) ISBN 978-3-319-05023-2 [Consult. 17 de out. 2015]. Disponível em WWW < http://www.springer.com/br/book/9783319050225>

GALEAN, Llanos Manzanares; CHINCHURRETA, Koldo Peciña - Implicaciones de la protección de datos en el marketing [Em linha]. In **MK Marketing+Ventas**, n.º 199, (feb. 2005). [Consult. 13 mar. 2015]. Disponível em WWW <http://pdfs.wke.es/8/7/8/6/pd0000018786.pdf>

GOFFMAN, Erving - **The presentation of self in everyday life** [Em linha]**.** Monograph n.º 2. Edinbourg **:** University of Edinburgh Social Sciences Research Centre 39 George Square, 1956. [Consult. 12 de out. 2014]. Disponível em WWW < https://monoskop.org/images/1/19/Goffman_Erving_The_Presentation_of_Self_in_Everyday_Life.pdf>

GUPTA, Jatinder N. D., SHARMA, Sushil K. - Cyber Shopping and Privacy. In FAZLOLLAHI, Bijan coord. - **Strategies for eCommerce Success.** Hershey, Pennsylvania **:** IRM Press, 2002. ISBN 1-931777-08-7. Cap. 1, p. 1-16.

HILDEBRANDT, Mireille – Profiling and the Identity of the European Citizen. In HILDEBRANDT, Mireille, GUTWIRTH, Serge coord. – **Profiling the European Citizen Cross-Disciplinary Perspectives** [Em linha]. [S.l.] : Springer Science + Business Media B.V. 2008, ISBN 978-1-4020-6914-7. p. 303–344. [Consult. 10 dez. 2014]. Disponível em WWW <http://www.springer.com/la/book/9781402069130>

HERT, Paul De; GUTWIRTH; Serge - Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. in GUTWIRTH; Serge [*et al.*] - **Reinventing Data Protection?** [Em linha]. New York [etc.]: Springer Science + Business Media B.V. 2009. [Consult. 10 dez. 2014]. Disponível em WWW <https://link.springer.com/book/10.1007/978-1-4020-9498-9> ISBN 978-1-4020-9498-9. Cap. 1, p. 3-44.

HOEYER, Klaus (2009) Informed consent: The making of a ubiquitous rule in medical practice. [Em linha]. **Organization,** Vol. 16, n.º 2, p. 267-288. Washington DC : SAGE Publications, (2009). [Consult. 17 out. 2015]. Disponível em WWW <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.838.6147&rep=rep1&type=pdf> ISSN 1350–5084.

HUH, Soon Chul - Invasion of privacy v. Commercial speech: Regulation of spam with a comparative constitutional point of view. [Em linha]. **Albany Law Review**, Vol. 70, n.º 1, 2006, p. 181-207. [Consult. 12 out. 2015]. Disponível em WWW <http://www.albanylaw review.org/Articles/Vol70_1/70.2.0181>

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS - **Report and Guidance on Data Protection and Privacy on the Internet - Budapest-Berlin Memorandum** [Em linha]. (19/11/1996) [Consult. 14 out. 2015]. Disponível em WWW <https://datenschutz-berlin.de//content/europa-international /international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group>

- Working Paper on Cross-Border Telemarketing [Em linha]. 04/09/2009 [Consult. 14 out. 2015]. Disponível em WWW <https://datenschutz-berlin.de//content/europa-international /international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group>

- Report and Guidance on Privacy in Social Network Services - Rome Memorandum [Em linha]. 04/03/2008 [Consult. 14 out. 2015]. Disponível em WWW <https://datenschutz-berlin.de//content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group>

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - **ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework** [Em linha]. 1ª ed., International Organization for Standardization, 2011. [Consult.14 out. 2016]. Disponível em WWW <https://www.iso.org/standard/45123.html>

- ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements [Em linha]. 1ª ed., International Organization for Standardization, 2013. [Consult.14 out. 2016]. Disponível em WWW <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>

KRISHNA, P. Radha - Big Data Search and Mining. In MOHANTY, Hrushikesha, CHENTHATI, Deepak, BHUYAN, Prachet, coord. **Big Data A Primer** [Em linha]. New Delhi [etc.]: Springer Índia, 2015. (Studies in Big Data, Vol. XI) [Consult. 12 ago. 2016]. Disponível em WWW <http://www.springer.com/gp/book/9788132224938> ISBN 978-81-322-2494-5. p 93-120

LALANA, Ángel Daniel Oliver - Código invisible y pequeño gran hermano: Nuevas condiciones de posibilidad del derecho de protección de datos. [Em linha]. In **Revista de la Facultad de Derecho de la Universidad de la República**, n.º 22, p. 235-262, (jul. 2014). [Consult. 12 out. 2015]. Disponível em WWW <http://www.revistafacultadderecho.edu.uy/ojs-2.4.2/index.php/rfd/article/view/210>. ISSN 2301-0665

LANGHEINRICH, Marc - Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In ABOWD, Gregory D., BRUMITT, Barry, SHAFER, Steven, coord. In **Ubicomp 2001: Ubiquitous Computing - Lecture Notes In Computer Science**, **Proceedings of the 3rd international conference on Ubiquitous Computing, Atlanta, Georgia, USA** [Em linha]. Berlim [etc.]: Springer-Verlag Berlin Heidelberg New York, 2001. (Lecture Notes in Computer Science, Vol. 2201). ISBN 978-3-540-45427-4, pp 273-291.

LOUCHEZ, Alain - The Internet of things: Machines, businesses, people, everything. In **ITU News** [Em linha]. N.º 6. [2013?] Genéve : International Telecommunication Union, 2013. [Consult. 19 jan. 2016]. Disponível em WWW <https://itunews.itu.int/En/4291-The-Internet-of-things-Machines-businesses-people-everything-.note.aspx>

MAGEE, John - The Law Regulating Unsolicited Commercial E-Mail: An International Perspective. In **Santa Clara High Technology Law Journal** [Em linha]. Vol. 19, n.º 2, (2002). [Consult. 19 jan. 2016]. Disponível em WWW <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1322&context=chtlj>

MANTELERO, Alessandro - The Future of Consumer Data Protection in the E.U. Rethinking the Notice and Consent Paradigm in the New Era of Predictive Analytics. In **Computer Law and Security Review** [Em linha]. Vol. 30, n.º 6, [dez. 2014], p. 643-660. Amsterdam : Elsevier, 2014. [Consult. 11 jan. 2016]. Disponível em WWW <http://www.sciencedirect.com/science/article/pii/S026736491400154X>

MASNICK, Mike - The war on fake reviews ramps up: NY fines companies for fake Yelp reviews. In **Techdirt.** [Em linha]. (27/09/2013) [Consult. 19 jan. 2016]. Disponível em WWW <https://www.techdirt.com/articles/20130927/01425424673/war-fake-reviews-ramps-up-ny-fines-companies-fake-yelp-reviews.shtml>

MELL, Peter; GRANCE, Timothy - **The NIST definition of cloud computing, Recommendations of the National Institute of Standards and Technology** [Em linha]. NIST, U.S. Department of Commerce, (2011). [Consult. 16 jan. 2016]. Disponível em WWW

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

ORDEM DOS ADVOGADOS PORTUGUESES - Parecer n.º E-30/03, de 22/09/2003 [Em linha]. [Consult. 10 Nov. 2016]. Disponível em WWW <https://www.oa.pt/Conteudos/Pareceres/detalhe_parecer.aspx?idc=5&idsc=158&ida=39887>

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - **Guidelines for the regulation of computerized personal data file** [Em linha]. 14/12/1990 [Consult. 13 Nov. 2015]. Disponível em WWW <https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/564/84/IMG/NR056484.pdf?OpenElement>

- Security Council resolution 1368 (2001) Threats to international peace and security caused by terrorist acts [Em linha]. S/RES/1368, (12/09/2001) [Consult. 9 out. 2015]. Disponível em WWW <http://www.refworld.org/docid/3c4e94557.html>

- **Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin** [Em linha]. A/HRC/13/37, (28/12/2009) [Consult. 9 out. 2015] Disponível em WWW <http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf.>

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO - **The OECD Privacy Framework** [Em linha]. OECD 2013 [Consult. 10 Nov. 2014]. Disponível em WWW <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>

- Guidelines for Cryptography Policy [Em linha]. (27/03/1997) [Consult. 10 nov. 2015]. Disponível em WWW <http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm>

- **Guidelines for Multinational Enterprises** [Em linha]. Ed.ª 2011, OECD Publishing. [Consult. 10 nov. 2015]. Disponível em WWW <http://www.oecd.org/daf/inv/mne/48004323.pdf>. ISBN ISBN 978-92-64-11528-6

- **Anti-Spam Regulation**. [Em linha]. OECD 2005 DSTI/CP/ICCP/SPAM(2005)10/FINAL [Consult. 10 nov. 2015]. Disponível em WWW <https://www.oecd.org/sti/ieconomy/35670414.pdf>

- **Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam** [Em linha]. (13/04/2006) [Consult. 10 nov. 2015]. Disponível em WWW <http://www.oecd.org/fr/sti/ieconomie/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm>

- **Anti-Spam Regulation**. [Em linha]. OECD 2005 DSTI/CP/ICCP/SPAM(2005)10/FINAL

[Consult. 10 Nov. 2015]. Disponível em WWW <https://www.oecd.org/sti/ieconomy/35670414.pdf>

- **Consumer Protection in E-commerce** [Em linha]. OECD Publishing, 2016 [Consult. 18 ago. 2015]. Disponível em WWW <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>

- **Machine-to-machine communications: connecting billions of devices.** [Em linha]. DSTI/ICCP/CISP(2011)4/FINAL, OECD Digital Economy Papers, n.º 192, OECD Publishing (2012). [Consult. 12 Mar. 2016]. Disponível em WWW <http://www.oecd-ilibrary.org/docserver/download/5k9gsh2gp043.pdf?expires=1460899221&id=id&accname=guest&checksum=EB86294E2B573CC92443177E517D66AB>

PARLAMENTO EUROPEU - **Interim Report drawn on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing (Rapporteur: Lord Mansfield)** [Em linha]. Working Documents 1974-1975, Document 487/74, PE 39.608/fin, (19.feb.1975), p. 14. [Consult. 16 ago. 2016]. Disponível em WWW < http://aei.pitt.edu/65083/ 1/WD3126. pdf>

- **Report drawn up on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of technical developments in data processing (Rapporteur: Mr A. Bayerl)** [Em linha]. Working Documents 1979-1980, Document 100/79 [04.may.1975], p. 3. [Consult. 16 ago. 2016]. Disponível em WWW <http://aei.pitt.edu/view/eusubjects/ H019.html>

POULLET, Yves - Data protection legislation: What is at stake for our society and democracy? In **Computer Law and Security Review** [Em linha]. Vol. 25, n.º 3, (2009), p. 211–226. Amsterdam : Elsevier, 2009. [Consult. 11 jan. 2016]. Disponível em WWW <http://www.sciencedirect.com/science/article/pii/S0267364909000612>

PRIBERAM INFORMÁTICA, S.A. - Marketing. In **FLIP 10. - Dicionário Priberam de Língua Portuguesa contemporânea.** [Em linha]. [Consult. 1 dez. 2016]. Módulo de software.

PROSSER, William J. – Privacy [Em linha]. In **California Law Review**, Vol. n.º 48, n.º 3, (1960). [Consult. 12 mar. 2016]. Disponível em WWW <http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1/>

PULIDO, Emilia Zaballos - **La protección de datos personales en España : evolución normativa y criterios de aplicación** [Em linha]. Madrid. Universidad Complutense de Madrid (2013). Tesis de doctorado. [Consult. 10 jun. 2016]. Disponível em WWW <http://eprints.ucm.es/22849/1/T34733.pdf>

REIDENBERG, Joel R. - The Transparent Citizen [Em linha]. In **Loyola University Chicago Law Journal**, Vol. 47, (2015), Fordham Law Legal Studies Research Paper No. 2674313. [Consult. 12 jun. 2016]. Disponível em WWW <https://ssrn.com/abstract=2674313
- Resolving Conflicting International Data Privacy Rules in Cyberspace [Em linha].Stanford. Law Review, Vol. 52 (1999-2000) p. 1315-1371 [Consult. 12 jun. 2016]. Disponível em WWW <http://ir.lawnet.fordham.edu/faculty_scholarship/41>

REINO DE ESPAÑA. Constitución Española [Em linha]. **Boletín Oficial del Estado**, n.º 311, (29/12/1978), p. 29313-29424 [Consult. 11 out. 2015]. Disponível em WWW <https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229>

REINO DE ESPAÑA. Tribunal Constitucional - **Sentencia del Tribunal Constitucional** 292/2000, de 30/11. [Em linha]. **Boletín Oficial del Estado** n.º 4, (04/01/2001), p. 104-118 [Consult. 11 out. 2015]. Disponível em WWW https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

REINO DE ESPAÑA. Agencia Española de Protección de Datos. **Informe 182/2008** [Em linha]. [Consult. 20 mai. 2015]. Disponível em WWW <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0182_La-vivienda-es-un-dato-de-car-aa-cter-personal-sometido-a-la-ley-org-aa-nica-15-b-1999.pdf>

REPÚBLICA PORTUGUESA. Comissão Nacional da Proteção de Dados - **Autorização da CNPD, nº 10/99, de 16/03** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_10_1999.pdf>
- **Autorização da CNPD, n.º 2/2000, de 18/01** [Em linha]. [Consult. 12 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_2_2000.pdf>
- **Autorização da CNPD, n.º 7/2000, de 25/01** [Em linha]. [Consult. 19 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_7_2000.pdf>
- **Autorização da CNPD n.º 9/2000, de 25/01** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Aut/10_9_2000.pdf>

- **Autorização da CNPD, nº 192/2002**, **de 05/11** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Aut/10_192_2002.pdf>
- **Autorização da CNPD, n.º 845/2005, de 17/10** [Em linha]. [Consult. 13 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_845_2005.pdf>
- **Autorização da CNPD, n.º 1123/2007, de 25/06** [Em linha]. [Consult. 12 mar. 2015]. Disponível em WWW <http:// www.cnpd.pt/bin/decisoes/Aut/10_1123_2007.pdf>
- **Autorização da CNPD, n.º 1102/2010, de 15/03** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Aut/10_1102_2010.pdf>
- **Deliberação da CNPD, nº 1/2000, de 04/01** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/2000/htm/del/del001-00.htm>
- **Deliberação da CNPD, nº 60/2000, de 27/01**. [Em linha]. Diário da República - 2.ª Série, nº 22, de 27/01/2000, p. 1813 - 1816 [Consult. 29 mar. 2015]. Disponível em WWW <https://dre.pt/web/guest/pesquisa-avancada/-/asearch/2028668/details/maximized?search=Pesquisar&sortOrder=ASC&tipo_facet=Delibera%C3%A7%C3%A3o&perPage=25&types=SERIEII&dataPublicacaoInicio=2000-01-27>
- **Deliberação da CNPD, nº 1205/2000, de 04/06** [Em linha]. [Consult. 29 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Delib/20_1205_2000.pdf>
- **Deliberação da CNPD, n.º 94/2001, de 15/07** [Em linha]. [Consult. 29 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/2001/htm/del/del094-01.htm>
- **Deliberação da CNPD, nº 165/2001**, **de 13/11** [Em linha]. [Consult. 24 Mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Delib/20_165_2001.pdf>
- **Deliberação da CNPD, n.º 14/2002, de 15/01** [Em linha]. [Consult. 29 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/orientacoes/DEL14-2002-REGIME-DADOS-MANUAIS.pdf>
- **Deliberação 143/2002 da CNPD, de 09/06** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Delib/20_143_2002.pdf>
- **Deliberação da CNPD, n.º 63/2006, de 13/02** [Em linha]. [Consult. 12 mar. 2015]. Disponível em WWW <http://www.cnpd.pt/bin/decisoes/Aut/10_63_2006.pdf>
- **Deliberação da CNPD, n.º 227/2007**, **de 28/05** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Delib/20_227_2007.pdf>
- **Parecer da CNPD, nº 22/2001, de 04/12** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_22_2001.pdf>
- **Parecer da CNPD, nº 11/2002 de 03/12** [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_11_2002.pdf>

- Parecer da CNPD, nº 13/2003, de 03/06 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_13_2003.pdf>
- Parecer da CNPD, nº 44/2003, de 11/11 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_44_2003.pdf>
- Parecer da CNPD, n.º 16/2005, de 24/05 [Em linha]. [Consult. 24 mar. 2015]. Disponível em WWW <https://www.cnpd.pt/bin/decisoes/Par/40_16_2016.pdf>

RODOTÀ, Stefano – **A vida na sociedade de vigilância, A privacidade hoje**. Trad. Danilo Doneda e Luciana Cabral Doneda, Rio de Janeiro : Renovar, 2008.
- *Data Protection as a Fundamental Right*. in GUTWIRTH; Serge; LEENES, Ronald; HERT, Paul De; - **Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges** [Em linha]. Dordrecht : Springer Science+Business Media Dordrecht 2014. [Consult. 7 ago. 2016]. Disponível em WWW <http://www. springer.com/la/book/ 9789400775398> ISBN 978-94-007-7540-4. Cap. 3, p. 82

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñero; FINGER, Brunize - O direito à proteção de dados pessoais e a privacidade [Em linha]. In **Revista da Faculdade de Direito – UFPR**, n.º 53, Curitiba, 2011. [Consult. 16 set. 2015]. Disponível em WWW <http:// revistas.ufpr.br/direito/article/download/30768/19876> ISSN 2236-7284. p. 45-66

SARTOR, Giovanni, CUNHA, Mario Viola de Azevedo - The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents. [Em linha]. In **International Journal of Law and Information Technology**, Vol 18, n.º 4, Oxford : Oxford University Press, 2010. pp 356-378 [Consult. 19 set. 2015]. Disponível em WWW <https://academic.oup.com/ijlit/article/18/4/356/744617/The-Italian-Google-Case-Privacy-Freedom-of-SpeechThe Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents>ISSN 1464-3693

SILVA, Fernando Resina da, *et alea* – **Cloud, a Lei e a Prática**. Coimbra : Almedina, 2016. ISBN 978-972-4065-04-5

SOLOVE, Daniel J. - A Brief History of Information Privacy Law [Em linha]. In **Proskauer On Privacy**, Pli (07 feb. 2017). GWU Law School Public Law Research Paper n.º 215 [Consult. 14 Fev. 2017]. Disponível em WWW: <http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications>

SORKIN, David E. - Technical and Legal Approaches to Unsolicited Electronic Mail. In

University of San Francisco Law Review [Em linha]. Vol. 35, n.º 2, [Winter 2001] p. 325-384 [Consult. 14 fev 2017]. Disponível em WWW: <http://www.spamlaws.com/f/articles/usf.pdf>

STEELE, Brian; CHANDLER, Jonh; REDDY, Swarna - **Algorithms for Data Science** [Em linha]. 1.ª ed., Cham : Springer International Publishing Switzerland, 2016. ISBN 978-3-319-45797-0. [Consult. 1 jan. 2017]. Disponível em WWW: < http://www.springer.com/in/book/9783319457956>

STORF, Katalin; HANSEN, Marit; RAGUSE, Maren - **From H1.3.5: Requirements and concepts for identity management throughout life** [Em linha]. PrimeLife 2009 [Consult. 16 jan. 2015]. Disponível em WWW <http://primelife.ercim.eu/images/stories/deliverables/h1.3.5-requirements_and_concepts_for_idm_throughout_life-public.pdf>

STRYKER, Sheldon; BURKE, Peter J. - The Past, Present, and Future of an Identity Theory [Em linha]. In **Social Psychology Quarterly**, Vol. 63, n.º 4 (dec. 2000), Special Millenium Issue on the State of Sociological Social Psychology. American Sociological Association. p. 284-297 [Consult. 19 jan. 2015]. Disponível em WWW <http://www.jstor.org/stable/2695840> ISSN 0190-2725

TAMM, Ditlev - The History of the Court of Justice of the European Union Since its Origin. In Court of Justice of the European Union, Coord. - **The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law.** 1ª ed. Hague : Springer, 2013. [Consult. 16 out. 2015]. Disponível em WWW <http://www.springer.com/la/book/9789067048965>. ISBN 978-90-6704-897-2. p. 9-35

TIMELEX - **Study of case law on the circumstances in which IP addresses are considered personal data** (SMART 2010/12) D3. Final report [Em linha]. (2011) [Consult. 16 Abr. 2015]. Disponível em WWW <http://www.timelex.eu/frontend/files/userfiles/files/publications/2011/IP_addresses_report_-_Final.pdf>

UNIÃO EUROPEIA. Agência dos Direitos Fundamentais da União Europeia; CONSELHO DA EUROPA - **Manual da Legislação Europeia sobre Proteção de Dados** [Em linha]. Luxemburgo : Serviço das Publicações da União Europeia, 2014. [Consult. 10 dez. 2014]. Disponível em WWW <http://www.cnpd.pt/bin/legis/internacional/fra-2014-handbook-data-protection-pt.pdf> ISBN 978-92-871-9939-3 (Conselho da Europa) ISBN 978-92-9239-498-1.

UNIÃO EUROPEIA. Comissão Europeia **- Community policy on data processing. Communication of the Commission to the Council.** [Em linha]. SEC (73) 4300 final, (21/11/1973) [Consult. 10 Dez. 2015]. Disponível em WWW <http://aei.pitt.edu/view/eudocno/SEC_=2873=29_4300_final.html>

- Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Identificação por radiofrequências (RFID) na Europa: rumo a um quadro político [Em linha]. COM(2007) 96 final. [Consult. 10 Dez. 2015]. Disponível em WWW <http://www.umic.pt/images/stories/publicacoes200710/com2007_0096pt01.pdf>

- Proposta de Regulamento Do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas) [Em linha]. COM(2017) 10 final 2017/0003 (COD), Bruxelas, (10/01/2017) [Consult. 1 fev. 2017]. Disponível em WWW <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017PC0010&from=EN>

UNIÃO EUROPEIA. Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - **Recomendação 3/97: O anonimato na Internet.** [Em linha]. XV D/5022/97 final WP6. Brussels (Belgium), 03/12/1997. [Consult. 12 mar. 2015]. Disponível em WWW <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_pt.pdf>

- Documento de trabalho: A notificação [Em linha]. XV/5027/97-PT final WP 8. [s.l.], (03/12/1997). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp8_pt.pdf>

- Recomendação 1/99 sobre o tratamento invisível e automatizado de dados pessoais na Internet realizado por *software* e *hardware.* [Em linha]. 5093/98/PT/final WP17. Brussels (Belgium), (23/02/1999). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf>

- Parecer 3/99 relativo a Informação do sector público e protecção de dados pessoais Contribuição para a consulta iniciada com o Livro Verde da Comissão Europeia intitulado "Informação do sector público: um recurso fundamental para a Europa" COM(1998) 585. [Em linha]. WP 20. Brussels (Belgium), (03/05/1999). [Consult. 14 fev. 2015]. Disponível em WWW<http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp20_en.pdf >

- Parecer 1/2000 relativo a certos aspetos da protecção de dados no comércio eletrónico. [Em linha]. 5007/00/PT/FINAL WP 28 Brussels (Belgium), (03/02/2000). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp28_pt.pdf>

- **Parecer 2/2000 relativo à revisão geral do quadro jurídico em matéria de telecomunicações.** Apresentado pela *Task-Force* Internet [Em linha]. 009/00/PT/final WP29 Brussels (Belgium), (03/02/2000)). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp29_pt.pdf>

- Parecer 5/2000 relativo ao uso de listas telefónicas públicas para serviços de pesquisa invertida ou multicritério (Listas invertidas) [Em linha]. 5058/00/ PT/FINAL, WP 33. Brussels (Belgium), (13/07/2000). [Consult. 14 fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp33_en.pdf>

- **Parecer 7/2000 sobre a Proposta de Diretiva do Parlamento Europeu e do Conselho apresentada pela Comissão Europeia relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas** [Em linha]. 5042/00/PT/FINAL WP 36. Brussels (Belgium), 12/07/2000. [Consult. 10 nov. 2014]. Disponível em WWW <http://ec.europa. eu/justice/policies/privacy/docs/wp docs/2000/wp36pt.pdf>

- Documento de trabalho, Privacidade na Internet - Uma abordagem integrada da EU no domínio da proteção de dados em linha [Em linha]. 5063/00/PT/FINAL, WP 37. Brussels (Belgium), (21/11/2000). [Consult. 14 Fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation /files/2000/wp37_pt.pdf#h2-16>

- Recomendação sobre determinados requisitos mínimos para a recolha de dados pessoais em linha na União Europeia [Em linha]. 5020/01/PT/Final WP 43. Brussels (Belgium), (17/05/2001). [Consult. 14 Fev. 2015]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp43_pt.pdf>

- **Documento de trabalho sobre listas negras.** [Em linha]. 11118/02/PT/final, WP 65. Brussels (Belgium), (03/10/2002). [Consult. 16 Fev. 2014]. Disponível em WWW <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_pt.pdf>

- Parecer 3/2003 sobre o código de conduta europeu da FEDMA relativo ao uso de dados

pessoais em operações de marketing directo. [Em linha]. 10066/03/PT final WP 77. Brussels (Belgium), (13/07/2003). [Consult. 16 Fev. 2014]. Disponível em WWW <http:// ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/ files/2003/wp77_pt.pdf>

- Parecer 5/2005 sobre as comunicações não solicitadas para fins de comercialização no âmbito do Artigo 13.º da Directiva 2002/58/CE. [Em linha]. 11601/PT, WP 90. Brussels (Belgium), (27/02/2004). [Consult. 16 Fev. 2014]. Disponível em WWW <http://ec. europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/ 2004/wp90_pt.pdf>

- Parecer 10/2004 sobre a prestação mais harmonizada da informação. [Em linha]. 11987/04/PT GT100. Brussels (Belgium), (25/11/2004). [Consult. 16 Fev. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documen tation/opinion-recommendation/files/2004/wp100_pt.pdf>

- Working document on data protection issues related to RFID technology [Em linha]. 10107/05/EN, WP 105. Brussels (Belgium), (19/01/2005). [Consult. 1 Abr. 2015]. Disponível em WWW <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/ wp105_en.pdf>

- Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE) [Em linha]. 00323/07/PT, WP 131. Brussels (Belgium), (15/02/2007). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa. eu/justice/data-protection/article-29/documentation/opinion-recommendation /files/2007/wp131_pt.pdf>

- **Parecer 4/2007 sobre o conceito de dados pessoais.** [Em linha]. 01248/07/ PT, WP 136. Brussels (Belgium), (20/06/2007). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf>

- Parecer 1/2008 sobre questões de protecção dos dados ligadas aos motores de pesquisa [Em linha]. 00737/PT, WP 148. Brussels (Belgium), (04/04/2008). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/ opinion-recommendation/files/2008/wp148_pt.pdf>

- Parecer 1/2009 sobre as propostas de alteração da Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (diretiva da privacidade eletrónica) [Em linha]. 00350/09/PT GT 159. Brussels (Belgium), (10/02/2009). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu /justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp159 _pt.pdf>

- **Parecer 5/2009 sobre as redes sociais em linha** [Em linha]. 01189/09/PT WP 163. Brussels (Belgium), (12/06/2009). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_pt.pdf>

- **The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data** [Em linha]. 02356/09/EN WP 168. Brussels (Belgium), (01/12/2009). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/ documentation/opinion-recommendation/files/2009/wp168_en.pdf>

- **Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»** [Em linha]. 00264/10/PT WP 169. Brussels (Belgium), (16/02/2010). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_pt.pdf>

- **Parecer 2/2010 sobre publicidade comportamental em linha** [Em linha]. 0909/10/PT WP 171. Brussels (Belgium), (22/06/2010). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp171_pt.pdf>

- **Parecer 4/2010 sobre o código de conduta europeu da FEDMA relativo ao uso de dados pessoais no marketing direto** [Em linha]. **00065/2010/PT WP 174**. Brussels (Belgium), (13/07/2010). [Consult. 12 dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_pt.pdf >

- **Parecer 8/2010 sobre a lei aplicável** [Em linha]. 0836-02/10/PT WP 179. Brussels (Belgium), (16/12/2010). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_pt.pdf>

- **Parecer 15/2011 sobre a definição de consentimento** [Em linha]. 01197/11/PT WP 187. Brussels (Belgium), (13/07/2011). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_pt.pdf>

- **Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão** [Em linha]. 00879/12/PT WP 194. Brussels (Belgium), (07/06/2012). [Consult. 12 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/ justice/data-protection/article-29/documentation/opinion-recommendation/files/2012 /wp194_pt.pdf>

- **Opinion 03/2013 on purpose limitation** [Em linha]. 00569/13/EN, WP 203. Brussels (Belgium), (02/04/2013). [Consult. 12 Dez. 2016]. Disponível em WWW <http:// ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>

- **Working Document 02/2013 providing guidance on obtaining consent for cookies** [Em linha]. 1676/13/EN, WP 208. Brussels (Belgium), (02/10/2013). [Consult. 12 Dez. 2016]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/ documentation/opinion-recommendation/files/2013/wp208_en.pdf>

- **Parecer 01/2014 sobre a aplicação dos conceitos de necessidade e proporcionalidade e a proteção de dados no setor da aplicação coerciva da lei** [Em linha]. 536/14/PT, WP 211. Brussels (Belgium), (27/02/2014). [Consult. 12 Dez. 2016]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_pt.pdf>

- **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE** [Em linha]. 844/14/PT, WP 217. Brussels (Belgium), (09/04/2014). [Consult. 12 Dez. 2016]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf>

- **Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas** [Em linha]. **1471/14/PT**, WP 223. Brussels (Belgium), **26/09/2014**. [Consult. 10 Dez. 2014]. Disponível em WWW <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-ecommendation/files/2014/wp223_pt.pdf>

WEISER, Mark D. - **The Computer of the 21st Century. Scientific American**, vol. 265, n.º 3, [sept 1991], p. 94-104 [Em linha]. [Consult. 7 jul. 2015]. Disponível em WWW <http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf>. ISSN 1559-1662.

ZANFIR, Gabriela - Forgetting About Consent. Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. in GUTWIRTH; Serge; LEENES, Ronald; HERT, Paul De; - **Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges** [Em linha]. Dordrecht : Springer Science+Business Media Dordrecht 2014. [Consult. 7 ago. 2016]. Disponível em WWW <http://www. springer.com/la/book/9789400775398> ISBN 978-94-007-7540-4. Cap. 12, p. 237-257

ZARZA, Ángeles Gutiérrez - **Exchange of Information and Data Protection in Cross-**

border Criminal Proceedings in Europe [Em linha]. Heidelberg [etc.] : Springer-Verlag Berlin Heidelberg 2015. [Consult. 7 ago. 2016]. Disponível em WWW <http://www.springer.com/la/book/9783642402906> ISBN 978-3-642-40291-3.

PÁGINAS WEB

JURISPRUDENCIA

PÁGINA WEB DE JURISPRUDÊNCIA DOS TRIBUNAIS PORTUGUESES
<http://www.dgsi.pt/>
PÁGINA WEB DE JURISPRUDÊNCIA DO TJUE
<http://curia.europa.eu/jcms/jcms/j_6/pt/>
PÁGINA WEB DE JURISPRUDÊNCIA DO TEDH
<ttp://hudoc.echr.coe.int/eng#{"docname":["herbecq"]}>

LEGISLAÇÃO

PÁGINA WEB DE LEGISLAÇÃO PORTUGUESA
<https://dre.pt/>
PÁGINA WEB DE LEGISLAÇÃO DA UE
<http://eur-lex.europa.eu/oj/direct-access.html?locale=pt>

OUTRAS PÁGINAS

PÁGINAS WEB GERAIS DE INTERESSE

<http://www.w3.org/Consortium/>