A PRIVACIDADE DOS CONSUMIDORES

RUTE COUTO
Docente e Directora do Curso de Solicitadoria do Instituto Politécnico de Bragança
Presidente da delegação de Trás-os-Montes da Associação Portuguesa de Direito do Consumo

1. INTRODUÇÃO

"Todo o progresso técnico é, ao mesmo tempo, fonte de libertação e servidão"[1]

Na história da humanidade, nem sempre a privacidade foi uma dimensão valorizada[2], podendo atribuir-se a génese deste direito a Samuel Warren e Louis Brandeis quando afirmaram o *right to be let alone* no seu artigo "The right to privacy" publicado no Harvard Law Review em 1890.[3] Desde então, as instâncias internacionais e os diferentes ordenamentos jurídicos acolheram a privacidade como essencial na tutela da pessoa humana.[4]

Em Portugal, a Constituição da República Portuguesa (CRP) eleva à categoria de direitos fundamentais o direito à reserva da intimidade da vida privada (artigo 26.º n.º 1 CRP) e o "direito à autodeterminação informativa", no que se refere à protecção dos dados pessoais face à informática (artigo 35.º CRP).[5] Por sua vez, o Código Civil (CC) português consagra este direito especial de personalidade, estabelecendo, no seu artigo 80.º, que "todos devem guardar reserva quanto à intimidade da vida privada de outrem" e que "a extensão da reserva é definida conforme a natureza do caso e a condição das pessoas".

Mas, tomando Faria Costa, "a historicidade trouxe-nos o bálsamo do refúgio da privacidade, mas trouxe-nos também – talvez em relação de recíproca causalidade – os instrumentos, a técnica, que permite violar avassaladoramente aquele mesmo valor"[6].

---

[1] Garcia Marques, *Telecomunicações e protecção de dados (Do número nacional único aos novos atentados à vida privada)*. (In As Telecomunicações e o Direito na Sociedade da Informação, p. 90)

[2] Cf. Diogo Leite de Campos (*A Imagem que dá Poder: Privacidade e Informática Jurídica*, p. 294 e segs.), a propósito da contemporaneidade do conceito de privacidade, "desconhecido, mais, rejeitado, nas sociedades que precederam a nossa"

[3] Para a contextualização deste célebre escrito, cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 17-18.

[4] A propósito da evolução de diversas legislações nesta matéria, cf. Têmis Limberger, *Da evolução do direito a ser deixado em paz a protecção dos dados pessoais*, p. 276-280.

[5] Cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 22-39.

[6] Cf. José de Faria Costa, *As Telecomunicações e a privacidade: o olhar (in)discreto de um penalista*, p. 77

RESUMO

Na moderna sociedade de consumo, muitas práticas e formas de comunicação comercial comportam riscos para a privacidade dos consumidores. O regime jurídico de protecção de dados pessoais é o mote para uma reflexão em torno de algumas situações particularmente lesivas da intimidade do cidadão-consumidor, como sejam a videovigilância, as comunicações publicitárias não solicitadas (spam) e os testemunhos de conexão online (cookies).

O *Big Brother* está presente, ainda que em moldes diferentes dos prenunciados por George Orwell no seu "1984". Bastará atentar no relato de Wolfgang Sofsky[7] para os mais desatentos se consciencializarem que vivemos numa sociedade "aquário"[8], em que quase todos os movimentos quotidianos são registáveis e controláveis. Os rastos que deixamos são "o custo, o perigo e o bem de vivermos neste tempo"[9].

Mais do que uma construção doutrinal destas temáticas, pretendemos neste texto apresentar os traços fundamentais do regime de protecção dos dados pessoais e da privacidade na ordem jurídica nacional, e partilhar um conjunto de preocupações sobre alguns dos riscos que hoje se verificam relativamente à protecção da privacidade dos cidadãos.

Escolhemos como sujeito das nossas reflexões o *consumidor*, pela sua vulnerabilidade num contexto histórico e social em que os dados não valem por si só, mas pelo seu conteúdo económico e valor de mercado. Os dados pessoais, na medida em que traduzem aspectos de personalidade, incluindo perfis de consumo, têm importância "para a propaganda e o comércio"[10] e, nessa medida, são frequentes os tratamentos ilícitos de dados pessoais no âmbito da actividade de marketing e publicidade, com consequente lesão da privacidade dos consumidores.

2. PROTECÇÃO DOS DADOS PESSOAIS E DA PRIVACIDADE

A Lei da Protecção de Dados Pessoais (LPDP)[11] define *dados pessoais* como "qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados')". Na medida em que se considera ser identificável "a pessoa que possa ser identificada directa ou indirectamente, 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" [artigo 3.º *a)* LPDP], estão incluídos neste conceito dados tais como os números de identificação, matrícula da viatura, dados biométricos (impressão digital, íris, etc.), perfil de ADN, sistemas de GPS, perfis de consumo, etc., de índole e susceptibilidade diversas.

Escolhemos como sujeito das nossas reflexões o consumidor, pela sua vulnerabilidade num contexto histórico e social em que os dados não valem por si só, mas pelo seu conteúdo económico e valor de mercado.

A qualificação como "dados pessoais" não exige, portanto, a menção do nome de alguém, mas sim que seja possível atribuir informações a pessoas. Aliás, como realça Catarina Sarmento e Castro, "o que verdadeiramente torna 'apetecível' uma listagem de nomes, é o facto de estes estarem associados a outras características"[12].

Ainda no plano dos principais conceitos, a LPDP define *tratamento de dados pessoais* de forma abrangente como "qualquer operação ou conjunto de operações sobre dados pessoais, efectuada com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição" [artigo 3.º *b)* LPDP], sendo o *responsável pelo tratamento* "a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento de dados pessoais" [artigo 3.º *d)* LPDP].

---

[7] O autor de "Privacy, a Manifesto" descreve, no capítulo "Traces", um dia na vida de um cidadão, sob escrutínio constante. Cf. *http://press.princeton.edu/chapters/s8725.html*

[8] Paulo Mota Pinto (*O Direito à Reserva sobre a Intimidade da Vida Privada*, p. 585) alude à necessidade de tutela jurídica eficaz "para evitar que que cada um de nós se sinta a viver numa «casa de cristal» com «paredes de vidro» que não pode sequer embaciar a seu gosto". Também José de Faria Costa (*O Direito Penal, a Informática e a Reserva da Vida Privada*, p. 308) refere o "risco de «vitrificação» da nossa existência".

[9] Cf. José de Faria Costa, *O Direito Penal, a Informática e a Reserva da Vida Privada*, p. 308.

[10] Cf. Têmis Limberger, *Da evolução do direito a ser deixado em paz à protecção dos dados pessoais*, p. 269

[11] Lei n.º 67/98, de 26 de Outubro (com a Rectificação n.º 22/98, de 28 de Novembro), que transpõe para a ordem jurídica portuguesa a Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

[12] Cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 70. Como exemplos dessas características, a autora refere a profissão e a doença.

O tratamento de dados pessoais é uma "tarefa de responsabilidade"[13], que impõe ao seu responsável um conjunto de obrigações. Apresentamos aqui os traços gerais desse regime jurídico, em cinco dos seus aspectos cruciais: a qualidade dos dados, a legitimidade do tratamento, os direitos do titular dos dados, as garantias de segurança e confidencialidade e a intervenção da Comissão Nacional de Protecção de Dados (CNPD).

A **qualidade dos dados pessoais** afere-se pela concretização dos critérios vertidos no artigo 5.º LPDP: licitude e boa fé, finalidade, adequação e proporcionalidade, exactidão e conservação.

Os dados pessoais devem ser tratados de forma *lícita* e conforme à *boa fé*. Tal imperativo reflecte ainda o princípio geral de que "o tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais" (artigo 2.º LPDP).

É determinante a questão da *finalidade* na utilização de dados pessoais, quer na recolha dos dados ("para finalidades determinadas, explícitas e legítimas"), no seu tratamento ("não podendo ser posteriormente tratados de forma incompatível com essas finalidades"[14]) e na conservação ("...apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior"). A finalidade constitui ainda o referencial de valoração para a *adequação, pertinência e proporcionalidade* dos dados. Como adiante melhor referiremos, a finalidade é elemento essencial dos direitos do titular dos dados, nomeadamente o de ser informado, na recolha, sobre o destino dos dados recolhidos e o de posteriormente obter do responsável pelo tratamento mais informações. E a utilização de dados pessoais para fins que não foram determinantes na recolha impõe um controlo adicional por parte da autoridade de controlo.

Os dados pessoais devem ser *exactos e actualizáveis*, o que fundamenta o correspondente direito dos titulares de acesso de apagamento ou rectificação dos dados inexactos ou incompletos. Finalmente, os dados pessoais não podem ser *conservados* de forma ilimitada temporalmente, mas tão somente de forma a permitir a identificação dos seus titulares durante o período necessário para a prossecução das finalidades da recolha. A lei salvaguarda a possibilidade de conservação por período superior para fins históricos, estatísticos ou científicos, mediante autorização da CNPD.

Ao reflectirmos sobre os vários tratamentos de dados pessoais a que somos sujeitos no nosso quotidiano, facilmente concluímos que se muitos só se realizam porque nós em tal assentimos[15], outros há em que a falta de consentimento do titular não inviabiliza a realização da operação sobre os seus dados[16]. São, portanto, duas as condições de **legitimidade do tratamento** de dados: *consentimento* do titular[17] (corpo do artigo 6.º LPDP) ou *necessidade* do tratamento para um dos efeitos previstos na lei [artigo 6.º *a)* a *e)* LPDP], a saber: execução de contrato(s) em que o titular dos dados seja parte ou diligências contratuais prévias; cumprimento de obrigação legal do responsável pelo tratamento; protecção de interesses vitais do titular dos dados, se este estiver incapaz (física ou legalmente) de dar o seu consentimento; execução de missão de interesse público ou exercício de autoridade pública; e prossecução de interesses legítimos do responsável pelo tratamento (ou de terceiros a quem os dados sejam comunicados) desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.[18]

Há situações em que a natureza dos dados ou do seu tratamento ditaram a especificação deste regime geral, e que aqui apenas enunciaremos. É o caso dos *dados sensíveis*, *i. e.* referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, saúde e vida sexual, incluindo os dados genéticos (artigo 7.º LPDP)[19], dados

[13] Cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 65.

[14] Para exemplos de compatibilidade ou incompatibilidade com as finalidades da recolha, cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 231-235.

[15] Muitas vezes pelo simples clicar de um "aceito" em inúmeros formulários na internet.

[16] Não poderíamos, por exemplo, exigir que se desligassem as câmaras de videovigilância num banco à nossa entrada ou negar-nos a fornecer um conjunto de informações imperativas num contrato de seguro, crédito ou outro.

[17] Definido como "qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objecto de tratamento" [artigo 3.º *h)* LPDP].

[18] Cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 205-213.

[19] Sobre o fundamento de dados sensíveis, nomeadamente a regra geral de proibição e os dois fundamentos de excepção (lei ou consentimento), cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 88-99 e p. 215-227.

relativos a suspeitas de *actividades ilícitas*, infracções penais e contra-ordenações(artigo 8.º LPDP) e a *interconexão* de dados, ou seja, a "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" [artigos 3.º *i)* e 9.º LPDP].

Como contraponto dos princípios gerais de qualidade dos dados pessoais, os seus titulares beneficiam de determinados **direitos**. A lei refere quatro: direito de informação (artigo 10.º LPDP), de acesso (artigo 11.º LPDP), de oposição (artigo 12.º LPDP) e de não ficar sujeito a uma decisão individual automatizada (artigo 13.º LPDP).[20]

Ao titular de dados pessoais deve ser prestado um conjunto de informações, nomeadamente quanto à identidade do responsável pelo tratamento, as finalidades, o destinatário dos dados[21], o carácter obrigatório ou facultativo da resposta e as condições do direito de acesso e rectificação. De forma particular, no caso de recolha de dados em redes abertas, o titular deve ser informado dos riscos inerentes à circulação na rede sem condições de segurança e eventual acesso por terceiros não autorizados.[22] Além disso, tem o titular o direito de obter do responsável pelo tratamento – "livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos" – confirmação daquelas informações, conhecimento da lógica subjacente ao tratamento automatizado, rectificação, apagamento ou bloqueio. Por último, o titular dos dados tem direito de se opor ao tratamento dos dados pessoais que lhe digam respeito, "por razões ponderosas e legítimas relacionadas com a sua situação particular" [artigo 12.º *a)* LPDP] ou no caso de dados pessoais usados para efeitos de marketing directo ou prospecção [artigo 12.º *b)* LPDP].

O responsável pelo tratamento deve providenciar pela **segurança** dos dados pessoais, implementando medidas técnicas e organizativas, que impeçam qualquer ofensiva à integridade daqueles dados. Tais medidas podem incluir a segurança física nas instalações (restrição de acesso, sistemas de alarme, etc.) e segurança do sistema informático (*passwords*, cópias de *backup*, informação encriptada, etc.), de forma especialmente acautelada no caso de dados sensíveis e registos de dados de natureza criminal ou contra-ordenacional. Além disso, todas as pessoas que nas suas funções tenham conhecimento de dados pessoais tratados ficam obrigadas a **sigilo** profissional (artigo 17.º LPDP), e a sua violação é considerada crime (artigo 47.º LPDP).

A **Comissão Nacional de Protecção de Dados** (CNPD) é uma entidade administrativa independente, que funciona junto da Assembleia da República, e que tem como principal atribuição controlar e fiscalizar o cumprimento das disposições normativas relativas à protecção de dados pessoais.[23] Em matéria de tratamento de dados pessoais, e no que se refere ao grau de intervenção da CNPD, podemos recorrer a uma metáfora com um semáforo e as suas três cores:

- Como "luz verde", temos as situações de *isenção de notificação*, por razões de celeridade, economia e eficiência para as categorias de dados insusceptíveis de pôr em causa os direitos e liberdades dos titulares (artigo 27.º n.º 2 LPDP).[24]
- Em "luz amarela", a generalidade dos tratamentos de dados pessoais implica a obrigatoriedade de *notificação* à CNPD para efeitos de *registo*[25] (artigo 27.º LPDP). Esta notificação deve ser

---

[20] De forma mais detalhada, Catarina Sarmento e Castro (*Direito da Informática, Privacidade e Dados Pessoais*, p. 239-262) explana os direitos ao esquecimento, à curiosidade, de informação, de acesso, de rectificação e actualização, de pagamento ou bloqueio dos dados, de não se ficar sujeito a uma decisão individual automatizada, de oposição (em particular no marketing directo) e ao não tratamento de dados sensíveis.

[21] Cf. artigo 3.º *g)* LPDP, "a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro, sem prejuízo de não serem consideradas destinatários as autoridades a quem sejam comunicados dados no âmbito de uma disposição legal".

[22] Cf. artigo 10.º n.º 4 LPDP.

[23] Cf. artigos 21-31 LPDP.

[24] Foram assim considerados o processamento de retribuições, prestações, abonos de funcionários ou empregados (autorização de isenção n.º 1/99), a gestão de utentes de bibliotecas e arquivos (autorização de isenção n.º 2/99), a facturação e gestão de contactos com clientes, fornecedores e prestadores de serviços (autorização de isenção n.º 3/99), a gestão administrativa de funcionários, empregadores e prestadores de serviços (autorização de isenção n.º 4/99), o registo de entradas e saídas de pessoas em edifícios (autorização de isenção n.º 5/99) e a cobrança de quotizações em associações e contactos com os respectivos associados (autorização de isenção n.º 6/99). Todas as isenções, publicadas no *Diário da República* n.º 22, II série, de 27 de Janeiro de 2000, podem ser consultadas em *http://www.cnpd.pt/bin/legal/isencoes.htm*.

[25] O registo público esta disponível em *http://www.cnpd.pt/bin/registo/registo.htm*.

feita antes da realização do tratamento de dados, mediante um formulário disponível *online* no sítio da CNPD.[26] A omissão desta obrigação de notificação implica responsabilidade contra-ordenacional (se por negligência)[27] ou criminal (em caso de conduta intencional)[28].

- Os casos de "luz vermelha" são os tratamentos de dados que carecem de *autorização* da CNPD (artigo 28.º CNPD). Já não se trata aqui de um mero registo, mas sim de um controlo prévio a que ficam sujeitos: *a)* os tratamentos de dados pessoais sensíveis, ou dados relativos a suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias; *b)* o tratamento de dados relativos ao crédito e solvabilidade; *c)* a interconexão de dados pessoais; e *d)* a utilização de dados pessoais para fins não determinantes da recolha.[29]

Atentemos agora em algumas situações especialmente danosas da privacidade dos consumidores.

3. "SORRIA, ESTÁ A SER FILMADO": A VIDEOVIGILÂNCIA

O legislador inclui na definição de dados pessoais o "som e imagem" [artigo 3.º *a)* LPDP] e expressamente dispõe que o regime jurídico de protecção de dados pessoais se aplica "à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas" (artigo 4.º n.º 4 LPDP).[30]

Presente em vários domínios do quotidiano[31], a videovigilância está normalmente associada à segurança de pessoas e bens, mas pode encobrir outras finalidades. Têmis Limberger alerta que "pode haver câmaras em locais sob o pretexto de vigilância que, na realidade, servem para observar perfis de consumo, em um completo desvio de finalidade" e cita o caso de um estabelecimento comercial norte-americano que filma as reacções dos seus consumidores, para avaliar, por exemplo, quais os produtos que lhes prendem mais a atenção e as expressões faciais perante os preços praticados.[32]

Os tratamentos de videovigilância estão sujeitos a notificação à CNPD, que para o efeito disponibiliza no seu sítio um formulário geral e outros adaptados às exigências de actividades específicas[33]. A Comissão definiu os "princípios sobre o tratamento de dados por videovigilância"[34], discriminando os parâmetros a considerar no controlo prévio a estes tratamentos de dados.

---

[26] Em *http://www.cnpd.pt/bin/legal/forms.htm*, subdivididos em "Formulário Geral de Notificação"; "Formulário Biometria" (controlo de acessos e/ou assiduidade dos trabalhadores) e "Formulários de Videovigilância".

[27] Cf. artigo 37.º LPDP.

[28] Cf. artigo 43.º n.º 1 *a)* LPDP.

[29] Cf. tabela anexa à Deliberação da CNPD n.º 50/2011, disponível em *http://www.cnpd.pt/bin/legal/Del50_2011.pdf*

[30] São ainda relevantes, neste domínio, o Decreto-Lei n.º 35/2004 (alterado pelos DL n.º 198/2005, de 10/11, Lei n.º 38/2008, de 08/08, DL n.º 135/2010, de 27/12 e DL n.º 114/2011, de 30/11), que regula o exercício da actividade de segurança privada, e a Lei n.º 1/2005 (alterada pelas Lei n.º 39-A/2005, de 29/07, Lei n.º 53-A/2006, de 29/12 e Lei n.º 9/2012, de 23/02), que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. Existe ainda legislação avulsa, referente a instituições de crédito, recintos desportivos, estabelecimentos de restauração e bebidas com espaços de dança, etc.

[31] Catarina Sarmento e Castro (*Direito da Informática, Privacidade e Dados Pessoais*, p. 123) aponta, como exemplos de utilização, o controlo de fluxos de trânsito, o acesso de veículos a zonas de circulação limitada, a protecção do ambiente e património cultural, a protecção de pessoas e bens, e a garantia das condições de segurança em meio laboral. Para além destas, Garcia Marques e Lourenço Martins (*Direito da Informática*, p. 170) mencionam a detecção precoce de fogos e a fiscalização do cumprimento da obrigação de permanência na habitação. Os autores referem ainda (p. 171, nota 207) um estudo segundo o qual no centro de Londres [num país onde os sistemas de videovigilância têm um elevado grau de penetração] uma pessoa é filmada em média 300 vezes por dia.

[32] Cf. Têmis Limberger, *Da evolução do direito a ser deixado em paz à protecção dos dados pessoais*, p. 271.

[33] Actualmente estão disponíveis (em *http://www.cnpd.pt/bin/legal/forms_video.htm*) formulários para: Armeiros; Bancos e outras instituições financeiras; Casinos / Bingos; Condomínios; Discotecas com lotação entre 101-1000 lugares; Discotecas com lotação superior a 1000 lugares; Escolas e outros estabelecimentos de ensino; Escritórios e Serviços; Farmácias, parafarmácias e similares; Gasolineiras; Hospitais e outros estabelecimentos de saúde; Hotéis e outros estabelecimentos de hotelaria; Igrejas e outros locais de culto; Indústrias e outras instalações de fabrico ou reparação; Lares e outros estabelecimentos para a 3.ª idade; Moradias e outras residências unifamiliares; Museus/Bibliotecas/Salas de espectáculo; Ourivesarias/Joalharias/Relojoarias; Parques de estacionamento; Recintos desportivos; Restaurantes e outros estabelecimentos de restauração; Outros estabelecimentos comerciais de venda ao público.

[34] Cf. Deliberação da CNPD n.º 61/2004, disponível em *http://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf*.

Importa realçar que a única finalidade admitida pela CNPD é a *"protecção de pessoas e bens"*, admitindo-se a utilização posterior das imagens nos termos da lei processual penal.[35] O legislador expressamente proíbe – no artigo 20.º do Código do Trabalho – que estes meios de vigilância sejam utilizados para controlar o desempenho profissional dos trabalhadores, norma que a CNPD traduz na determinação de que as câmaras não podem incidir regularmente sobre os trabalhadores durante a actividade laboral.

Catarina Sarmento e Crasto faz notar a dupla exigência ao nível do cumprimento do princípio da *proporcionalidade*: proporcionalidade *da* utilização (no sentido de que, atentas as finalidades, só deverão ser implementados meios de videovigilância se não existirem outros meios menos onerosos para a privacidade) e proporcionalidade *na* utilização (relevando aspectos tais como o número de câmaras, a sua localização e orientação, o alcance do zoom, etc.).[36]

Quanto ao prazo de conservação dos dados, quando não exista diploma específico que o preveja, o entendimento da CNPD tem sido no sentido de fixar o prazo máximo de 30 dias (previsto no artigo 13.º do Decreto-Lei n.º 35/2004, de 21 de Fevereiro, que regula a segurança privada), findo o qual as gravações devem ser destruídas.[37]

Os responsáveis pela implementação de sistemas de videovigilância ficam adstritos à obrigação de informar os titulares dos dados (aqueles cuja imagem for captada pelas câmaras) sobre tal recolha, mediante a afixação de aviso com o teor "Para sua protecção, este lugar encontra-se sob vigilância de um circuito fechado de televisão" ou "Para sua protecção, este lugar encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som", seguido de símbolo identificativo (artigo 13.º n.º 3 do Decreto-Lei n.º 35/2004).

Uma observação ainda para o "terrorismo psicológico" que tem justificado muitas das actuais tecnologias de videovigilância, sobretudo no período pós-11 de Setembro[38]. A esse propósito, ponderam Garcia Marques e Lourenço Martins que "com os progressos da tecnologia, cada vez menos coisas, cada vez menos actos da nossa vida fugirão à atenção dessas máquinas sofisticadas e invasoras. Importa, por isso, procurar evitar que as preocupações de segurança – razoáveis e imperiosas – que tanto têm contribuído para o apertar da malha tecnológica da vigilância levem à perda da privacidade e à devassa permanente da vida dos cidadãos comuns".[39]

O mesmo se diga quanto à preocupação com as crianças, em que os legítimos receios dos progenitores pela sua segurança poderiam conduzir a mecanismos de hiper-vigilância com consequências na conformação de comportamentos e personalidades. Luísa Neto refere a propósito a decisão, pela CNPD, de não-autorização de câmaras em determinados espaços de uma creche, já que tal podia criar nas crianças "a habituação ou aceitação natural da sujeição a tal modo de controlo, na sua vida futura".[40]

Presente em vários domínios do quotidiano, a videovigilância está normalmente associada à segurança de pessoas e bens, mas pode encobrir outras finalidades

[35] A propósito do fundamento legitimante do tratamento de dados pessoais por via de videovigilância, Catarina Sarmento e Castro (*Direito da Informática, Privacidade e Dados Pessoais*, p. 136 e segs) analisa várias hipóteses. Desde logo, pode considerar-se a imagem (e som) como um dado relativo à vida privada e, como tal, enquadrável nos "dados sensíveis" objecto da especial regulamentação do artigo 7º LPDP. A autora defende que o fundamento não deverá ser o do artigo 8.º n.º 2 LPDP, já que "o texto deste dispositivo da Lei não aponta num sentido de prevenção referida a uma vigilância indistinta e genérica, como será o caso da videovigilância para finalidades de protecção de pessoas e bens, mas para uma ideia de 'suspeita de actividades ilícitas', de vigilância concreta, dirigida a indivíduos específicos previamente determinados (...) ou para situações em que já existe ou está em curso a aplicação de sanção por 'infracções penais', ou em que se verifiquem 'contra-ordenações' ou 'decisões que decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias". Também o facto de existirem avisos a alertar os consumidores para o facto de estarem a ser filmados não poderá considerar-se um consentimento tácito – tanto mais que para dados sensíveis se exige consentimento expresso – mas antes o cumprimento, por parte do responsável pelo tratamento, da obrigação de informação prevista no artigo 10.º LPDP.

[36] Cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 150. A título exemplificativo, aludimos à Autorização n.º 1011/2009 (disponível em *http://www.cnpd.pt/bin/decisoes/aut/10_1011_2009.pdf*) em que a CNPD considerou legítima a instalação de câmaras na entrada e saída de um parque de campismo, mas já não na zona de campismo, por considerar que tal captação seria excessiva e desproporcional. Outras especificações frequentes nas autorizações da CNPD são as de que as câmaras não estejam direccionadas para os terminais de pagamento (por forma a não serem captadas imagens relativas à digitação dos códigos dos cartões bancários) e que se limitem ao perímetro da propriedade em questão (não envolvendo recolha de imagens de zonas limítrofes ou da via pública).

[37] Cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, p. 148.

[38] A título de exemplo, refira-se os *scanners* corporais nos aeroportos.

[39] Cf. Garcia Marques e Lourenço Martins, *Direito da Informática*, p. 172.

[40] Cf. Luísa Neto, *Acórdãos do TC n.ºs 213/2008 e 486/2009: a prova numa sociedade transparente*, p. 343.

4. "SPAM NÃO, OBRIGADO!": AS COMUNICAÇÕES PUBLICITÁRIAS NÃO SOLICITADAS

Luís Menezes Leitão[41] preludia o tratamento desta temática com a constatação de que "as denominadas 'autoestradas da informação' não têm restrições à colocação de publicidade, ao contrário do que acontece com as autoestradas comuns. Esta situação é preocupante, uma vez que a conversão da internet num mar de publicidade pode levar a que se venha a perder o triunfo da humanidade que representou a sua criação"[42].

A publicidade reveste essencialmente duas funções, por um lado de *informação* ao consumidor e, por outro, de *persuasão* ou apelo à compra dos produtos ou serviços do anunciante. Como refere Carla Amado Gomes, a necessidade de estar informado para tomar convenientemente as suas decisões de consumo, expõe o consumidor à *"radiação publicitária"*; e se é evidente a utilidade informativa da publicidade, "a sua componente é predominantemente promocional, e nessa medida pode facilmente tornar-se desgastante"[43]. No "cerco tentacular da publicidade"[44], a necessidade de protecção "contra o ataque da *publicidade indiscreta*, que agride o consumidor pela sua cadência e volume, violando a sua esfera mais privada"[45] fundamenta a regulamentação normativa do fenómeno comummente designado por *spam*[46] ou "lixo".[47]

O *spam* constitui um óbice ao desenvolvimento do comércio electrónico por duas ordens de razões. Por um lado, pelo carácter *indesejado* e a *multiplicidade* de mensagens[48], que podem inclusivamente qualificar a prática comercial como desleal[49]. Por outro lado, pelo *conteúdo*, já que muitas vezes o *spam* é utilizado com intentos ilícitos[50], tais como a difusão de conteúdos ilegais, a prática de crimes informáticos e económicos, e a recolha ilegítima de dados pessoais, esta última aproveitando o desleixo dos utilizadores mais incautos que reenviam massivamente todo o género de "correntes", sem confirmar a fidedignidade da informação veiculada e sem ocultar os endereços dos sucessivos destinatários das mensagens reencaminhadas.[51]

Em matéria de comunicações publicitárias não solicitadas, importa distinguir dois âmbitos: por um lado, o da *publicidade domiciliária*, que inclui a publicidade por via postal, distribuição directa, telefone e telecópia (regulada pela Lei n.º 6/99 de 27 de Janeiro) e por outro lado as

---

[41] O autor tem publicados três escritos sobre "spam": *A distribuição de mensagens de correio electrónico indesejadas (SPAM)* (In Estudos em homenagem à Professora Doutora Isabel de Magalhães Collaço, p. 219-240), *A distribuição de mensagens de correio electrónico indesejadas (SPAM)* (In Direito da Sociedade da Informação, Volume IV - Separata 2003, p. 191-212) e *Comunicações não solicitadas (spam)* (In Lei do Comércio Electrónico Anotada, p. 213-238). Por serem no essencial análogos, referenciaremos aqui este último, o mais recente e actualizado face à Lei da privacidade nas comunicações electrónicas.

[42] Cf. Luís Menezes Leitão, *Comunicações não solicitadas (spam)*, p. 213

[43] Cf. Carla Amado Gomes, *O direito à privacidade do consumidor - A propósito da Lei 6/99, de 27 de Janeiro*, p. 102

[44] Cf. Carla Amado Gomes, *O direito à privacidade do consumidor - A propósito da Lei 6/99, de 27 de Janeiro*, p. 103.

[45] Cf. Carla Amado Gomes, *O direito à privacidade do consumidor - A propósito da Lei 6/99, de 27 de Janeiro*, p. 90

[46] Sobre a origem do termo *spam*, cf. Cf. Luís Menezes Leitão, *Comunicações não solicitadas (spam)*, p. 214, nota (1).

[47] O *spam* é apelativo sobretudo pelo baixo custo e facilidade de disseminação para quem promove o seu envio. São incalculáveis, porém, os prejuízos que acarreta, quer para o fornecedor de acesso à rede quer para os utilizadores. Ao primeiro, por exigir do sistema maior capacidade de tráfico de mensagens e pelos danos à própria imagem do servidor. Aos utilizadores, sobretudo em termos de tempo, desconfiança perante o comércio electrónico, e privacidade. Cf. Luís Menezes Leitão (*Comunicações não solicitadas (spam)*, p. 215. No mesmo texto (p. 218-232), o autor analisa as três formas de reacção contra o spam: através das normas sociais e da auto-regulação, através da técnica e a reacção jurídica (americana e europeia).

[48] Cf. Luís Menezes Leitão (*Comunicações não solicitadas (spam)*, p. 218). Alexandre Sousa Pinheiro (*Comunicações não solicitadas (spam)*, p. 239 e segs) afirma que "o facto de a mensagem não ser solicitada não determina, de imediato, uma prática censurável", ressalvando as situações em que se trate de uma única comunicação destinada a promover uma actividade lícita.

[49] Cf. artigo 12.º *c)* do Decreto-Lei n.º 57/2008, de 26 de Março (que estabelece o regime aplicável às práticas comerciais desleais das empresas nas relações com os consumidores): *"São consideradas agressivas, em qualquer circunstância, as seguintes práticas comerciais: (...) c) Fazer solicitações persistentes e não solicitadas, por telefone, fax, e-mail ou qualquer outro meio de comunicação à distância, excepto em circunstâncias e na medida em que tal se justifique para o cumprimento de obrigação contratual".*

[50] Cf. Luís Menezes Leitão (*Comunicações não solicitadas (spam)*, p. 215) e Alexandre Sousa Pinheiro (*Comunicações não solicitadas (spam)*, p. 243).

[51] São disso exemplo os falsos pedidos de dádivas de sangue e de procura de crianças desaparecidas. Por vezes, uma simples pesquisa num motor de busca permite identificar o expediente fraudulento, cuidado a que se deve aliar a utilização da funcionalidade de bcc no envio das mensagens de correio electrónico.

comunicações electrónicas, nomeadamente a publicidade por correio electrónico (agora reguladas na Lei n.º 41/2004 de 18 de Agosto, alterada pela Lei n.º 46/2012 de 29 de Agosto[52])[53].

A salvaguarda dos direitos constitucionais à liberdade de expressão e iniciativa económica não se compadece com a proibição absoluta de qualquer comunicação não solicitada[54], daí a ténica ser colocada no consentimento do receptor à recepção de comunicações publicitárias, por uma de duas vias: o sistema de opção positiva (ou *opt-in*) significa que apenas pode ser enviada uma comunicação comercial se o seu destinatário previamente tiver manifestado esse desejo de recebimento; o sistema de opção negativa (ou *opt-out*) permite o envio de comunicações publicitárias até ao momento em que o receptor manifesta a vontade de não mais as receber.[55] Os dois sistemas convivem na ordem jurídica nacional, consoante o suporte publicitário em causa.

No que se refere à publicidade recebida por **via postal ou distribuição directa**, rege o princípio do *opt-out*, *i. e.*, o consumidor que não deseje receber publicidade no espaço físico da sua "caixa do correio", terá de manifestar a sua oposição. No caso da publicidade *não endereçada*, essa oposição traduz-se na afixação de um dístico no local de recepção da correspondência[56]. Tratando-se de publicidade *endereçada*, a forma do destinatário manifestar o desejo de não receber material publicitário dependerá do alcance da sua recusa: se for uma oposição casuística, a um ou mais anunciantes em particular, o consumidor terá de contactar individualmente cada uma das entidades e exercer o seu direito de oposição [nos termos supra referidos do artigo 12.º *b)* LPDP]; já se se tratar de uma atitude de recusa generalizada, pode inscrever-se na designada "lista Robinson"[57] ou lista de pessoas que manifestaram o desejo de não receber publicidade endereçada.

Quanto às **comunicações electrónicas** não solicitadas para fins de marketing directo – e a lei inclui aqui as comunicações 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 electrónico*, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares (artigo 13.º-A Lei 41/2004) – o legislador consagrou um sistema de *opt-in*, ou seja, o envio de tais comunicações está sujeito a consentimento prévio e expresso do seu destinatário.[58] Não tendo o legislador europeu optado por um *opt-in* generalizado, justifica-se aqui "tendo presente a sua natureza mais agressiva e intrusiva relativamente à publicidade por via postal"[59] Admitem-se no entanto duas *excepções*, em que vigorará o sistema de *opt-out*: quando o destinatário seja uma pessoa colectiva (n.º 2 do artigo 13.º-A) ou um cliente com quem o fornecedor de bens ou serviços anteriormente contratou, desde que seja dada possibilidade de recusa no momento da recolha e em cada mensagem (n.º 3 do artigo 13.º-A).

Para efeitos de aplicação deste regime, as entidades que promovam o envio de comunicações electrónicas para fins de marketing directo devem manter uma lista das pessoas que manifestaram o consentimento para a recepção deste tipo de comunicações (*opt-in*), bem como dos

A salvaguarda de direitos constitucionais à liberdade de expressão e iniciativa económica não se compadece com a proibição absoluta de qualquer comunicação não solicitada, daí a ténica ser colocada no consentimento do receptor à recepção de comunicações publicitárias,

---

[52] Esta lei transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas). Até à alteração de 2012, a matéria das comunicações não solicitadas estava enxertada no Decreto-Lei n.º 7/2004 de 7 de Janeiro ("lei do comercio electrónico"), no seu artigo 22.º

[53] O artigo 2.º n.º 1 *a)* da Lei n.º 41/2004, de 18 de Agosto define comunicação como "qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações electrónicas acessível ao público" A Lei n.º 6/99 de 27 de Janeiro inclui na publicidade domiciliária a publicidade por telefone e telecópia (artigo 5.º) e remete para o anterior regime jurídico da privacidade nas telecomunicações (Lei n.º 69/98 de 28 de Outubro), devendo hoje essa remissão ser entendida para o artigo 13.º-A da Lei n.º 41/2004, de 18 de Agosto (aditado pela Lei n.º 46/2012 de 29 de Agosto).

[54] Cf. Luís Menezes Leitão, *Comunicações não solicitadas (spam)*, p. 222

[55] Quanto aos prós e contras de cada um dos sistemas, cf. Luís Menezes Leitão (*Comunicações não solicitadas (spam)*, p. 223).

[56] Os mais usuais são os autocolantes amarelos facultados pela Direcção-Geral do Consumidor com a mensagem "Publicidade não endereçada, aqui não, obrigado!" (disponível em *http://www.consumidor.pt?cfl=3818*).

[57] Assim apelidada numa alusão ao isolamento do famoso náufrago com o mesmo nome. Na realidade, se assim o pretender, o consumidor tem o direito a ficar sozinho numa "ilha" livre de comunicações exteriores.

[58] Não é portanto lícita a prática habitual de incluir no final das mensagens de correio electrónico a menção de que "o email não poderá ser considerado SPAM, quando incluir uma forma do receptor ser removido da lista" já que tal traduz um sistema de *opt-out* e não de *opt-in*.

[59] Cf. Garcia Marques e Lourenço Martins, *Direito da Informática*, p. 172, a propósito da publicidade por telefone e telecopia

clientes que não se opuseram à sua recepção. Já os consumidores que manifestem expressamente opor-se à recepção de comunicações não solicitadas para fins de marketing directo (*opt-out*) devem inscrever-se na "lista Robinson" mensalmente actualizada pela Direcção-Geral do Consumidor (DGC)[60] e que aquelas entidades devem consultar. O incumprimento destas regras implica responsabilidade contra-ordenacional [artigo 14.º n.º 1 *f)-j)* Lei 41/2004]. Proíbe-se ainda o envio de correio electrónico para fins de marketing directo, ocultando ou dissimulando a identidade do anunciante, ou sem a indicação de um meio de contacto válido para exercício do *opt-out*, ou ainda que incentive os destinatários a visitar sítios na internet que violem estes normativos.

Uma nota final para as dificuldades práticas da coexistência de dois sistemas diferenciados de regulação do *spam* – o europeu e o norteamericano[61] – face ao carácter universal da internet.

5. "ACEITAR *COOKIES*?": OS TESTEMUNHOS DE CONEXÃO NA INTERNET

Sempre que acedemos a um sítio na internet, a nossa navegação fica registada. "Um site não pode ser visitado sem que se deixem *traços*"[62] e esses traços, quiçá pela analogia com a criança que vai deixando um rasto de migalhas quando come bolachas, são conhecidos por *cookies*.

Um *cookie* é um arquivo de texto (ficheiro) colocado, através de sítios na internet, no computador, para armazenar informações sobre o utilizador e respectivas preferências, informações essas que podem ser "relidas" em futuras visitas ao sítio.[63] Um exemplo de *cookie* é o criado para guardar informações de *login* (utilizador e palavra-passe) para o utilizador não ter de iniciar a sessão de cada vez que visitar um sítio em particular.

Os *cookies* podem ser *temporários* (também designados "cookies de sessão") quando são removidos do computador após encerrar o browser de internet, como por exemplo, o *cookie* utilizado por um determinado sítio de comércio electrónico para armazenar os itens no 'carrinho de compras' durante o processo de compra. Mas os que constituem maior risco para a privacidade do utilizador de comunicações electrónicas são os *cookies* permanentes ou *persistentes* (os "cookies guardados") que permanecem armazenados no computador, provenientes do próprio sítio que o utilizador está a visitar (cookies "originais") ou de terceiros (através de anúncios publicitários em *banners* ou janelas *pop-up* no sítio visitado), estes últimos frequentemente utilizados para finalidades de marketing.

Os *cookies* traduzem operações de recolha de informações pessoais, na maior parte das vezes sem conhecimento ou consentimento do seu titular, permitindo traçar perfis de comportamento, incluindo dados sensíveis, como a orientação sexual ou religiosa. Para os direitos dos consumidores, o grande perigo dos *cookies* advém da "exploração comercial das informações que recolhem" sendo inegável que "é efectivamente no âmbito da publicidade que a actuação dos cookies se torna mais valiosa"[64]. Por exemplo, é possível registar quais os bens pesquisados ou comprados num dado sítio de comércio electrónico, para numa futura visita o gestor do sítio destacar, nos espaços de publicidade, produtos ou serviços que sejam consonantes com as preferências daquele utilizador em concreto.[65]

---

[60] A inscrição na lista nacional de não recepção de comunicações publicitárias podes ser feita no sítio da DGC ou Portal do Consumidor, em *http://www.consumidor.pt*.

[61] Cf. Luís Menezes Leitão, *Comunicações não solicitadas (spam)*, p. 222-232

[62] Cf. Garcia Marques e Lourenço Martins, *Direito da Informática*, p. 433.

[63] Cf. Catarina Sarmento e Castro (*Direito da Informática, Privacidade e Dados Pessoais*, p. 160), Garcia Marques e Lourenço Martins (*Direito da Informática*, p. 440-441) e Luís Menezes Leitão, (*Os testemunhos de conexão (cookies)*, p. 764). Na 'Ajuda e Suporte do Windows' pode ler-se que "Os Web sites utilizam cookies para oferecer uma experiência personalizada aos utilizadores e para recolher informações acerca da utilização do Web site. Muitos Web sites também utilizam cookies para armazenar informações que permitem oferecer uma experiência consistente entre as secções do site, tal com um carrinho de compras ou páginas personalizadas. Num Web site fidedigno, os cookies podem enriquecer a experiência permitindo que o site aprenda as preferências ou permitindo evitar o início de sessão de cada vez que visita um Web site. No entanto, alguns cookies, tais como os guardados pelas faixas de anúncios, poderão colocar a privacidade em risco, controlando os sites que são visitados"

[64] Cf. Luís Menezes Leitão, (*Os testemunhos de conexão (cookies)*, p. 763 e 765.

[65] A propósito, confira-se o Parecer 2/2010 sobre publicidade comportamental em linha, do "Grupo de Trabalho do Art.º 29" (órgão consultivo europeu independente em matéria de protecção de dados e de privacidade, instituído pelo artigo 29.º da Directiva 95/46/CE), disponível em *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf*.

Enquanto tratamento de dados, a utilização de *cookies* está sujeita ao regime jurídico da LPDP; nomeadamente no que se refere ao direito à informação e ao consentimento do titular. O regime da protecção da privacidade no sector das comunicações electrónicas (Lei n.º 41/2004) salvaguarda – no seu artigo 5.º – que "o armazenamento de informações e a possibilidade de acesso à informação armazenada no equipamento terminal de um assinante ou utilizador apenas são permitidos se estes tiverem dado o seu *consentimento prévio*, com base em *informações claras e completas* nos termos da Lei de Protecção de Dados Pessoais, nomeadamente quanto aos *objetivos do processamento*."

Como bem aponta Luís Menezes Leitão[66], "a recolha de dados é completamente invisível, pelo que raramente se põe a questão do consentimento do titular", sendo certo que a possibilidade conferida pelo *browser* de rejeitar ou aceitar cookies[67], não poderá equivaler a um consentimento para recolha. Não se cumpre, ademais, o imperativo do artigo 10.º n.º 4 LPDP, de informar o utilizador de que os seus dados podem circular na rede sem condições de segurança.[68]

Na esteira da Directiva europeia – que admite que estes testemunhos de conexão possam ser um "instrumento legítimo e útil, nomeadamente na análise da eficácia da concepção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transacções em linha"[69] – o diploma de transposição admite a utilização de *cookies* quando a finalidade seja meramente *técnica*, ou seja, é permitido o armazenamento ou acesso de informações "que tenha como única finalidade transmitir uma comunicação através de uma rede de comunicações electrónicas" ou "estritamente necessário ao fornecedor para fornecer um serviço da sociedade de informação solicitado expressamente pelo assinante ou utilizador"[70]. Luis Menezes Leitão critica esta abertura, que considera "claramente excessiva"[71], sobretudo se legitimar a prática de um sítio não permitir sequer o acesso aos utilizadores que rejeitem a instalação de *cookies*.

A problemática dos *cookies* é paradigmática do facto de mesmo os utilizadores frequentes de serviços de comunicações electrónicas, desconhecerem muitas das práticas lesivas da sua privacidade, o que impõe a necessidade de uma reflexão crítica (e necessariamente global) em torno da protecção dos dados pessoais em circulação nas redes de comunicação.

Os cookies traduzem operações de recolha de informações pessoais, na maior parte das vezes sem conhecimento ou consentimento do seu titular, permitindo tracar perfis de comportamento, incluindo dados sensíveis.

6. CONSIDERAÇÕES FINAIS

Todas as invenções da humanidade são passíveis de aproveitamento para o bem e para o mal, e as tecnologias informáticas não são excepção. Num mundo que não seria hoje imaginável sem a internet e as suas infindas possibilidades, cada nova oportunidade de evolução representa uma nova ameaça de perturbação do equilíbrio individual e social. As mesmas tecnologias que são sinónimo de progresso e bem-estar, podem representar o enfraquecimento dos direitos de cidadania, entre os quais o direito à privacidade.

Por outro lado, numa sociedade de vertiginoso consumo, a (hiper)vulnerabilidade do consumidor agudiza-se face a práticas comerciais cada vez mais intrincadas e invasivas da sua intimidade, seja no domicílio, nos espaços em que se movimenta, no mundo virtual. O intuito lucrativo não deveria afastar os profissionais da ética e da lealdade que se impõe nas relações de consumo, para que o cidadão-consumidor possa fazer as suas escolhas de forma informada e livre, sem ilegítimos controlos ou pressões.

As mesmas tecnologias que são sinónimo de progresso e bem-estar, podem representar o enfraquecimento dos direitos de cidadania, entre os quais o direito à privacidade.

---

[66] Cf. Luís Menezes Leitão, *Os testemunhos de conexão (cookies)*, p. 768-769.

[67] Para informação relativa à eliminação ou activação/desactivação de cookies, cf. *http://dadus.cnpd.pt/filez/file/apoio/cookies.pdf*. Ademais, é conveniente aos utilizadores de internet a consulta das políticas de privacidade (no que se refere aos cookies) dos sites habitualmente utilizados. A título de exemplo, cf. as políticas do "Facebook" *(http://www.facebook.com/help/cookies/)*, "Almedina" *(http://www.almedina.net/catalog/privacy.php)* e "Priberam" *(http://www.priberam.pt/Informacao-Legal.aspx)*.

[68] Já que apenas surge um texto do género "Um Website '(designação).com' pediu para guardar um ficheiro no seu computador chamado 'cookie'. Este ficheiro pode ser utilizado para rastrear informação de utilização. Deseja permitir isto?".

[69] Cf. Considerando (25) da Directiva 2002/58/CE.

[70] Cf. artigo 5.º n.º 2 da Lei n.º 41/2004, de 18 de Agosto.

[71] Cf. Luís Menezes Leitão, *Os testemunhos de conexão (cookies)*, p. 773-774.

Numa era de "interacção quase instantânea entre a realidade e o direito"[72], são constantes os desafios que se colocam às instâncias político-legislativas.

Em anteriores reflexões sobre o tema[73], cuidamos já da importância de uma política educativa e do rigoroso cumprimento da legislação que disciplina a protecção de dados pessoais, evitando o risco de "banalização" da protecção da privacidade, em nome de lógicas de globalização, segurança ou económicas.

Tendo sempre presente que os sistemas de tratamento de dados devem estar ao *serviço do Homem*[74] e nunca o oposto.

O artigo não está escrito segundo o novo acordo autografico.

[72] Cf. Cunha Rodrigues, *Informática e Reserva da Vida Privada*, p. 288.

[73] Cf. nossas Conclusões-Propostas das III Jornadas de Direito do Consumo de Trás-os-Montes, promovidas pela Associação Portuguesa de Direito do Consumo e pelo Instituto Politécnico de Bragança em 17 de Maio de 2011, disponíveis em *http://www.netconsumo.com/2011/05/iii-jornadas-de-direito-do-consumo-de_70.html*, no seu ponto II, relativo à "Protecção de Dados Pessoais e a Reserva da Privacidade dos Consumidores".

1. Que se exija do Estado e dos Reguladores a promoção de uma activa política educativa em matéria de protecção dos dados pessoais e consciencialização dos cidadãos (em particular as gerações mais jovens) para a importância da "autodeterminação informacional" na preservação da reserva de privacidade, com especial relevo no contexto das redes sociais.

2. Que se garanta a efectividade do direito de oposição do consumidor à utilização dos seus dados pessoais para efeitos de marketing, nomeadamente pela afirmação da lista de pessoas que não desejam receber comunicações publicitárias (designada "lista Robinson") e correspondente sancionamento das entidades infractoras.

3. Que se fiscalize com rigor as práticas de interconexão de dados pessoais, porquanto muitas correspondem a vendas de bases de dados - pouco transparentes e consolidadas em negócios de avultado valor entre empresas - à revelia dos direitos do consumidor e do seu consentimento.

4. Que se precise a responsabilidade pela segurança e confidencialidade dos tratamentos de dados pessoais, por forma a que se não caia na "inimputabilidade" justificada pela globalização, com diluição de condutas passíveis de responsabilidade contra-ordenacional ou criminal num falacioso universo de "crimes sem vítimas e sem culpados".

[74] Cf. Considerando (2) da Directiva 95/46/CE.

CAMPOS, Diogo Leite de: *A Imagem que dá Poder: Privacidade e Informática Jurídica*. In Comunicação e Defesa do Consumidor. Coimbra: Instituto Jurídico da Comunicação, 1996. p. 293-301.
CASTRO, Catarina Sarmento e: Direito da Informática, Privacidade e Dados Pessoais. Coimbra: Almedina, 2005. ISBN 972-40-2424-5.
COSTA, José de Faria: *As Telecomunicações e a privacidade: o olhar (in)discreto de um penalista*. In MONTEIRO, António Pinto (coord.) - As Telecomunicações e o Direito na Sociedade da Informação. Coimbra: Instituto Jurídico da Comunicação, 1999. ISBN 972-98462-0-0. p. 49-78.
COSTA, José de Faria: *O Direito Penal, a Informática e a Reserva da Vida Privada*. In Comunicação e Defesa do Consumidor. Coimbra: Instituto Jurídico da Comunicação, 1996. p. 302-321.
GOMES, Carla Amado: *O direito a privacidade do consumidor – A proposito da Lei 6/99, de 27 de Janeiro*. Revista do Ministério Público. Lisboa. ISSN 0870-6107. N.º 77 - Separata (1999), p. 89-103.
LEITÃO, Luís Menezes: *Comunicações não solicitadas (spam)*. In Lei do Comércio Electrónico Anotada. Coimbra : Coimbra Editora, 2005. ISBN 972-32-1320-6. p. 213-238.
LEITÃO, Luís Menezes: *Os testemunhos de conexão (cookies)*. In Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles – 90 anos. Coimbra: Almedina, 2007. p. 763-774.
LIMBERGER, Têmis: *Da evolução do direito a ser deixado em paz à protecção dos dados pessoais*. Revista da Faculdade de Direito da Universidade do Porto. ISSN 1645-1430. Ano VIII (2011), p. 267-292.
MARQUES, Garcia; MARTINS, Lourenço: Direito da Informática. 2ª edição - refundida e actualizada. Coimbra: Almedina, 2006. ISBN 972-40-2859-3.
NETO, Luísa: *Acórdãos do TC n.os 213/2008 e 486/2009: a prova numa sociedade transparente*. Revista da Faculdade de Direito da Universidade do Porto. ISSN 1645-1430. Ano VIII (2011), p. 315-343.
PINHEIRO, Alexandre Sousa: *Comunicações não solicitadas (spam)*. In Lei do Comércio Electrónico Anotada. Coimbra: Coimbra Editora, 2005. ISBN 972-32-1320-6. p. 239-261.
PINTO, Paulo Mota: *O Direito à Reserva sobre a Intimidade da Vida Privada*. Boletim da Faculdade de Direito da Universidade de Coimbra. Coimbra. ISSN 0303-9773. Vol. LXIX (1993), p. 479-585.
RODRIGUES, Cunha: *Informática e Reserva da Vida Privada*. In Comunicação e Defesa do Consumidor. Coimbra: Instituto Jurídico da Comunicação, 1996. p. 287-291.