Universidade do Minho
Escola de Direito

Emília da Conceição Golim Fontainhas

Dos Testemunhos de Conexão no Quadro Legislativo Europeu da Proteção de Dados - Em particular do consentimento para a sua utilização

outubro de 2013

Dos Testemunhos de Conexão no Quadro Legislativo Europeu da Proteção de Dados - Em particular do consentimento para a sua utilização
Emília da Conceição Golim Fontainhas
UMinho | 2013

Universidade do Minho
Escola de Direito

Emília da Conceição Golim Fontainhas

Dos Testemunhos de Conexão no Quadro Legislativo Europeu da Proteção de Dados - Em particular do consentimento para a sua utilização

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho realizado sob orientação do
Professor Doutor Francisco António Carneiro Pacheco de Andrade
e do
Professor Doutor José Carlos Bacelar Almeida

outubro de 2013

DECLARAÇÃO

Nome: Emília da Conceição Golim Fontainhas

Endereço electrónico: emiliagolim@gmail.com

Número do Bilhete de Identidade: 13223594 3ZY5

Título dissertação: Dos Testemunhos de Conexão no Quadro Legislativo Europeu da Proteção de Dados – Em particular do consentimento para a sua utilização

Orientador(es): Professor Doutor Francisco António Carneiro Pacheco de Andrade e Professor Doutor José Carlos Bacelar Almeida

Ano de conclusão: 2013

Designação do Mestrado:

Mestrado em Direito e Informática

Universidade do Minho, 28 de outubro de 2013

Assinatura: _____

Nome

Emília da Conceição Golim Fontainhas

Titulo

Dos Testemunhos de Conexão no Quadro Legislativo Europeu da Proteção de Dados – Em particular do consentimento para a sua utilização

Designação

Dissertação de Mestrado

Mestrado em Direito e Informática

Orientadores:

Professor Doutor Francisco António Carneiro Pacheco de Andrade

Professor Doutor José Carlos Bacelar Almeida

Mês e anos

Outubro de 2013

Agradecimentos

À Escola de Direito e ao Departamento de Informática da Universidade do Minho, e em especial a todos os que acreditaram e se empenharam na concretização do Mestrado em Direito e Informática.

Ao Professor Doutor Francisco Pacheco Andrade e ao Professor Doutor José Bacelar Almeida, pela orientação desta dissertação, por todos os ensinamentos, apoio e disponibilidade. Sem o seu espírito aberto, sensibilidade e curiosidade este trabalho não teria sido conseguido. O meu sincero obrigada!

Aos meus Pais, por me deixarem sonhar.

Ao Miguel, por tudo.

DOS TESTEMUNHOS DE CONEXÃO NO QUADRO LEGISLATIVO EUROPEU DA PROTEÇÃO DE DADOS – EM PARTICULAR DO CONSENTIMENTO PARA A SUA UTILIZAÇÃO

RESUMO

Esta dissertação estrutura-se em três capítulos.

Os dois primeiros capítulos promovem duas abordagens distintas: primeiro pretendemos perceber o que são os testemunhos de conexão enquanto tecnologia e, depois, procuramos o seu lugar dentro do quadro europeu da proteção de dados. No Capítulo I discutimos a sua história e importância, através da análise das especificações da IETF e da descrição do protocolo HTTP. Fazemos, ainda, uma incursão na atual implementação e utilizações deste mecanismo. O Capítulo II destina-se à análise do quadro legislativo europeu da proteção de dados, onde vamos encontrar a regulação dos testemunhos de conexão. Começamos por traçar a evolução do direito à privacidade e do direito à autodeterminação informativa. Analisamos a Diretiva da Proteção de Dados, que estabelece as obrigações do responsável pelo tratamento de dados e os direitos da pessoa em causa. De seguida, examinamos a Diretiva da Privacidade Eletrónica, comparando a versão de 2002 com as novas disposições resultantes das alterações introduzidas pela Diretiva dos Cidadãos, e fazemos uma primeira abordagem ao artigo 5.º, n.º 3. Finalizando este capítulo, olhamos para o futuro da regulamentação da proteção de dados pessoais na União Europeia.

Por fim, na convergência dos dois primeiros capítulos, o Capítulo III destina-se à análise do requisito do consentimento para a utilização de testemunhos de conexão. Analisamos o âmbito de aplicação do artigo 5.º, n.º 3 da Diretiva da Privacidade Eletrónica, examinamos os requisitos respeitantes ao consentimento e as situações isentas da sua obtenção. Analisamos, ainda, as formas de prestar informações e obter consentimento em linha.

COOKIES IN THE EUROPEAN DATA PROTECTION FRAMEWORK: SPECIALLY THE CONSENT FOR THEIR USE

SUMMARY

This dissertation is structured in three chapters.

The first two chapters provide separated approaches: first we intend to understand what cookies are as a technology and secondly we find their place under the European data protection framework. Therefore, in the Chapter I we discuss the history and importance of the cookies, by the analysis of the IETF's specifications and the description of the HTTP protocol. We also make an incursion in its current implementations and uses. Chapter II is intended to analyse the European data protection framework, where we will find the specific regulation on cookies. We begin by tracing the evolution of the right of privacy and the rise of the right to the informative self-determination. We analyse the Data Protection Directive, which sets the obligations of the data controller and the rights of individuals. Then, we examine the ePrivacy Directive, comparing the 2002 version with the new provisions resulting from the amendments introduced by the Citizens' Directive, and make a first approach to the article 5(3). Closing this chapter, we look at the future of personal data regulation in the European Union.

Finally, at the convergence of the first two chapters, the Chapter III is intended to analyse the requirement of consent for the use of cookies. We analyse the scope of article 5(3) and examine the conditions for valid consent and the situations exempted from the requirement of consent. Also, we analyse the ways to provide information and obtain consent online.

Índice

Abreviaturas

API – Application Programming Interface

AUE – Ato Único Europeu

C.R.P. – Constituição de República Portuguesa

CD – Compact Disc

CD-ROM – Compact Disc Read-Only Memory

CEDH – Convenção Europeia dos Direitos do Homem

CEE – Comunidade Económica Europeia

CERN – Conseil Européen pour la Recherche Nucléaire

Cf. – Confrontar; conferir

Cit. – Citado

CNPD – Comissão Nacional de Proteção de Dados

DMR – Digital Rights Management

DNT – Do Not Track

E.g. – exempli gratia, por exemplo

Et. al. - et alii, e outros

FEDMA - Federation of European Direct and Interactive Markting

HTML – HyperText Markup Language

HTTP – Hypertext Transfer Protocol

HTTPS – HyperText Transfer Protocol Secure

I. e. - isto é, ou seja

IAB - Interactive Advertising Bureau

IETF – Internet Engineering Task Force

IP – Internet Protocol

ISO - International Organization for Standardization

ISP – Internet Service Provider

OCDE – Cooperação e Desenvolvimento Económico

Op. cit. – obra citada

OSI - Open Systems Interconnection

P. – página

P2P – peer-to-peer

P3P – Plataform for Privacy Preferences

pp. – páginas

RDIS - Rede Digital Integrada de Serviços ou Rede Digital com Integração de Serviços

RFC – Request for Comments

RFID – identificação por radiofrequências

RGPD – Regulamento Geral sobre a Proteção de Dados (Proposta da Comissão Europeia de 25 de Janeiro de 2012)

RSE – registos de saúde electrónicos

Ss. – seguintes

SSL – Secure Sockets Layer

TCE – Tratado que institui a Comunidade Europeia

TCP – Transmission Control Protocol

TFUE – Tratado Sobre o Funcionamento da União Europeia

TLS – Transport Layer Security

TUE – Tratado da União Europeia

U.E. – União Europeia

UNICE - Union of Industrial and Employers' Confederation of Europe

URI – Universal Resource Identifier,

URL – Uniform Resource Locator

USB - Universal Serial Bus

W3C – World Wide Web Consortium

Web – World Wide Web

WP – working paper

XSS – Cross-site scripting

Introdução

O n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica estabelece os requisitos para o armazenamento e acesso a informação armazenada no terminal do utilizador ou assinante. Esta norma aplica-se à utilização de testemunhos e conexão, entendidos na aceção da definição dada pela norma RFC 6265 da IETF.

Na sua versão de 2002, o n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica permitia a utilização de testemunhos de conexão, na condição de serem prestadas ao assinante ou utilizador informações claras e completas, nomeadamente sobre as finalidades do processamento e de, cumulativamente, lhe ser garantido o direito de recusar o tratamento. A Diretiva dos Cidadãos promoveu uma alteração a este artigo 5.º n.º 3, passando a exigir o consentimento prévio do utilizador ou assinante, prestado com base em informações claras e completas.

O novo requisito de consentimento veio abalar as práticas correntes no que respeita ao armazenamento e acesso a informações já armazenas no terminal do utilizador ou assinante através de testemunhos de conexão e está na base de um aceso debate sustentado pelas dúvidas acerca da sua interpretação e condições de implementação prática.

Vamos começar por tentar perceber o que são, afinal, os testemunhos de conexão, enquanto tecnologia. Em que contexto tecnológico se inserem, como surgiram, como são implementados e a que finalidades servem.

De seguida, vamos procurar perceber em que contexto é que a União Europeia regula a utilização dos testemunhos de conexão.

Vamos olhar para o quadro europeu da proteção de dados, começando por explicar como surgiu a necessidade de proteger a privacidade das pessoas e os dados pessoais. Vamos traçar a evolução da

proteção do direito à privacidade e do direito à proteção de dados no Direito Internacional e na União Europeia.

Passaremos, então, a explicar as principais linhas da Diretiva da Proteção de Dados, até percebermos o que representa o consentimento neste contexto.

Analisaremos a Diretiva da Privacidade Eletrónica, onde vamos encontrar a regulação específica dos testemunhos de conexão. Vamos traçar as principais diferenças a versão original desta Diretiva e a que resultou das alterações introduzidas pela Diretiva dos Cidadãos.

Finalmente, vamos analisar o artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica que exige o consentimento, prestado com base em informações claras e completas, para a utilização de testemunhos de conexão.

Qual é o objetivo desta norma? Quem é o responsável pelo cumprimento das obrigações dela decorrentes? E quem é que deve prestar o consentimento exigido?

Quais são os requisitos do consentimento para a utilização de testemunhos de conexão?

O consentimento é exigido para a utilização de todos os testemunhos de conexão?

Como é que as informações podem ser prestadas e como é que o consentimento pode ser validamente obtido num ambiente em linha?

Vamos tentar responder a estas questões e perceber se a atual abordagem legislativa ao mecanismo dos testemunhos de conexão é a melhor.

Capítulo I Enquadramento Tecnológico

1. Introdução

A Internet, como hoje a conhecemos, é o resultado "da soma de pequenas conquistas tecnológicas"[1].

Importa que comecemos por enquadrar os testemunhos de conexão no vasto universo da Internet para que os possamos estudar e compreender devidamente.

Os testemunhos de conexão surgem como um complemento ao Protocolo de Transferência de Hipertexto[2], o protocolo que está na base da *World Wide Web*.

A *World Wide Web*, ou simplesmente *Web*, foi a primeira aplicação da Internet a chamar o interesse do público geral.

A Internet, por sua vez, é uma rede que interconecta centenas de milhares de dispositivos por todo o mundo e, ao mesmo tempo, é uma infraestrutura que fornece serviços para aplicações.

1.1. A Internet

A Internet pode ser descrita segundo uma de duas perspetivas, conforme nos propõem James F. Kurose e Keith W. Ross[3].

Segundo os Autores, podemos entender o que é a Internet de acordo com os componentes de *hardware e software* que a compõe ou, então,

[1] MAZZEO, Luzia Maria (coordenadora) *Evolução da Internet no Brasil e no Mundo*, Ministério da Ciência e Tecnologia Secretaria de Política de Informática e Automação, Brasil, abril, 2002

[2] O Protocolo de Transferência de Hipertexto, ou simplesmente "HTTP" (do nome em inglês *Hypertext Transfer Protocol*) é o protocolo em que se baseia a *Web*. É este protocolo, como melhor veremos adiante, que permite que, utilizando um navegador *web*, possamos solicitar páginas *web* aos servidores *web* e que estes no-las possam transferir.

[3] KUROSE, James F. e ROSS, Keith W., *Computer networking a top-down approach,* Pearson Education, Inc., 6ª Edição, 2012, pp. 2 a 7.

podemos entendê-la como uma rede de infraestruturas que fornece serviços para a distribuição de aplicações.

De acordo com a primeira abordagem sugerida – "*Nuts-and-Bolts Description*" –, a Internet é uma rede que interconecta centenas de milhares de dispositivos por todo o mundo – os sistemas terminais (*hosts*) – através das chamadas "ligações" [4] e de dispositivos de comutação, os "encaminhadores" (*packet switches*).

Cada encaminhador tem, no mínimo, duas ligações. Os encaminhadores recebem os dados (organizados em pacotes) através de uma ligação de entrada e reenviam-os por uma ligação de saída.

A Internet usa uma técnica designada por "comutação de pacotes" que permite que múltiplos sistemas terminais partilhem os mesmos caminhos ou partes de caminhos simultaneamente.

Os sistemas terminais ligam-se à rede através dos Fornecedores de Acesso à Internet – *Internet Service Providers* (ISPs). Cada ISP é, normalmente, em si mesmo uma rede de ligações e encaminhadores. A organização hierárquica dos diferentes ISPs, por sua vez, permite que estes estejam interligados.

A ligação eficaz entre sistemas terminais através de encaminhadores deve-se ao facto de tanto uns como outros utilizarem o IP (*Internet* Protocol) e o TCP (*Transmission Control Protocol*).

De acordo com a segunda perspetiva – *Services Description* – a internet é descrita como a infraestrutura que fornece serviços para aplicações.

Estas aplicações envolvem múltiplos sistemas terminais que trocam dados entre si, pelo que são designadas de "aplicações distribuídas".

Os sistemas terminais, nesta perspectiva, são classificados de acordo com duas categorias distintas: clientes ou servidores. Os terminais cliente

[4] As Ligações podem usar diferentes tecnologias e diferentes Meios de Transmissão (e.g. fios de cobre, cabos coaxiais, fibras ápticas, frequências de rádio ou satélite). As diferentes Ligações transmitem os dados a diferentes taxas (bits/s). Ver KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 12 a 22.

executam programas de cliente que permitem o envio de pedidos e a receção de respostas dos terminais servidor, que por sua vez executam programas de servidor que permitem receber e responder a esses pedidos. É o chamado modelo cliente-servidor.

São as ligações e os encaminhadores (as peças que compõem a internet, como vimos na primeira perspetiva) que permitem que se estabeleça a comunicação entre ciente e servidor[5].

Nesta perspetiva, os autores destacam, ainda, o chamado Interface de Programação de Aplicativos – *Application Programming Interface* (API). O API é um conjunto de rotinas e padrões que permite que uma parte de *software* a correr num terminal utilize a infraestrutura da rede de modo a fazer chegar informação a outra parte de software específica que por sua vez corre noutro sistema terminal da rede.

A World Wide Web é uma dessas aplicações, a par, por exemplo, do e-mail, ou da partilha de ficheiros *peer-to-peer* (P2P), entre tantas outras.

É na *Web* que vamos encontrar os testemunhos de conexão[6].

1.1.1. Os Protocolos

Para que duas ou mais entidades possam comunicar remotamente é necessário que corram o(s) mesmo(s) protocolo(s).

São os protocolos que definem o formato e a ordem das mensagens trocadas entre duas os mais entidades, assim como as ações levadas a cabo na transmissão e/ou receção da mensagem ou outro evento[7].

Os protocolos estabelecem as regras semânticas, sintáticas e temporais que vão regular a comunicação remota entre as diferentes entidades.

---

[5] Mas, como veremos no Título 1.1.1. deste Capítulo I, são os protocolos que vão permitir que a comunicação se processe de modo eficaz.

[6] Conforme veremos melhor no Titulo 2 deste Capítulo I.

[7] "A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event." KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., p. 9.

Implementados pelo *software*, *hardware*, ou por ambos, os protocolos são convenções usadas para a comunicação remota conforme o objetivo comunicacional pretendido.

Os terminais, assim como os encaminhadores, correm protocolos.

O Protocolo de Controlo de Transmissão – *Transmission Control Protocol* (TCP) – e o Protocolo de Internet – *Internet Protocol* (IP) – são reconhecidos como os mais importantes protocolos da Internet. Reconhecida a sua incontornável importância para o eficaz processamento das comunicações na rede, o conjunto de protocolos utilizados para a transmissão de informação na internet é referido como o conjunto TCP/IP.

Os protocolos, bem como o *hardware* e o *software* que os implementam, organizam-se de acordo com um modelo estruturado por camadas[8]: a camada física[9], a camada de enlace[10], a camada de rede, a camada de transporte e a camada de aplicação.

O IP é um protocolo da camada de rede. É o responsável pelo endereçamento dos dispositivos na internet e pelo encaminhamento de dados entre os terminais.

A cada dispositivo ligado à rede é atribuído um endereço IP único, que permite a sua identificação perante todos os outros.

Para que a comunicação entre terminais se processe eficazmente, é preciso que a máquina que pretende estabelecer a comunicação saiba o endereço daquela a que pretende dirigir o seu pedido e aquela que o recebe saiba o endereço de onde este proveio para que lhe possa responder.

[8] Adotamos aqui o modelo de internet de cinco camadas ("Five-Layer Internet Protocol Stack") por ser aquele que torna mais simples o enquadramento dos três protocolos a que nos vamos referir (IP, TCP e HTTP). Além deste, existem outros modelos, de que damos como exemplo o famoso "modelo OSI" (*Open Systems Interconnection*) desenvolvido pela *International Organization for Standardization* (ISO) nos anos 70 do século passado, que se divide em sete camadas (a camada física, a camada de enlace, a camada de rede, a camada de transporte, a camada de sessão, a camada de apresentação e a camada de aplicação); ver KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 47 a 53.

[9] E.g.: Modem, RDIS, Bluetooth, USB, entre outros.

[10] E.g.: Ethernet, WiFi, Switch, entre outros.

Assim, aquando do estabelecimento de uma comunicação entre terminais na internet, os dados transferidos são divididos por pacotes que obedecem a um formato próprio. Os dados são, então, precedidos de meta-informação, que vai permitir o seu correto processamento de modo a chegarem eficazmente ao destino. Dessa meta-informação fazem parte os endereços de origem e de destino da mensagem[11].

O protocolo IP, porém, é conhecido por ser um protocolo que não oferece garantias[12] [13].

O TCP, por sua vez, é um protocolo de transporte. É um protocolo dito "orientado à conexão". É aplicado nos sistemas terminais e é o responsável por estabelecer e terminar a conexão entre eles. Este protocolo vai assegurar confiança à comunicação, garantindo que os dados transmitidos são enviados e processados corretamente e pela sua ordem certa[14].

Como exemplo de um protocolo da camada de Aplicação temos o Protocolo de Transferência de hipertexto – *Hypertext Transfer Protocol* (HTTP) –, que analisaremos em maior pormenor[15].

O funcionamento eficaz da rede depende, pois, da concordância da comunidade em relação aos protocolos, tecnologias e práticas.

A *Internet Engineering Task Force* (IETF) desde cedo se assumiu como o organismo responsável pelo desenvolvimento dos *standards* das tecnologias e protocolos da Internet[16] [17].

---

[11] O IP conhece, hoje, duas versões: o IP(v4) e IPv6. O espaço de endereçamento global IP(v4) esgotou em 01 de fevereiro de 2011. Da necessidade que se faz sentir pela iminência deste esgotamento nasceu o IPv6. Entre estas duas versões do Internet Protocol registam-se assinaláveis diferenças. No que respeita ao formato de endereços, no IPv4 estes são compostos por 4 números de 8 bits representados em notação decimal, separados por um ponto (.), em que os primeiros bits identificam a rede onde a máquina em questão se localiza e os seguintes identificam a própria máquina. No IP(v4) tínhamos uma divisão dos endereços por classes, classes essas identificáveis através dos primeiros bits do endereço. No IPv6 temos 8 números de 16 bits representados em notação hexadecimal, separados por dois pontos (:). Aqui, os endereços são compostos por um prefixo de rede de 64 bits e um host adress, igualmente de 64 bits. O IPv6 reflete, ainda, novas preocupações e cuidados, nomeadamente no que respeita à segurança.

[12] "(...) IP makes its "best effort" to deliver segments between communicating hosts, but it makes no guarantees. In particular, it does not guarantee segment delivery, it does not guarantee orderly delivery of segments, and it does not guarantee the integrity of the data in the segments. For these reasons, IP is said to be an unreliable service.", KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., p. 190.

[13] Sobre o IP ver KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 331 e ss..

[14] Sobre o Protocolo TCP ver KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 230 e ss..

[15] Título 1.2.1. deste Capítulo I.

Trata-se de uma comunidade de âmbito internacional aberta a todos aqueles que se preocupem com a evolução e o bom funcionamento da Internet[18] [19].

A IETF tem por missão melhorar o funcionamento da Internet, através da produção de documentos de alta qualidade e tecnologicamente relevantes que influenciem a forma como as pessoas desenham, usam e geram a Internet[20]. Esses documentos, produzidos pela IETF, são chamados RFCs (*Request for Comments*).

Os RFCs podem ser *standards*[21] – documentos normativos aprovados pela IETF –, ou documentos de natureza informativa, e têm sempre início num *Internet Draft* que pode ser submetido por quaisquer interessados.

O trabalho da IETF é desenvolvido no seio dos seus Grupos de Trabalho, dispostos por áreas, que se auto-organizam. Os Grupos desenvolvem o seu trabalho através de *mailing lists* abertas à participação de todos os interessados.

1.2. A *World Wide Web*

Até aos inícios da década de 90 do século passado, a Internet não era mais do que uma ferramenta ao dispor de investigadores e académicos.

---

[16] Cf. KRISTOL, David M., *HTTP Cookies: Standards, privacy, and politics*, em "ACM Transactions on Internet Technology", Vol. 1, Issue 2, novembro de 2001, disponível em http://dl.acm.org/citation.cfm?id=502153&dl=ACM&coll=DL&CFID=286587961&CFTOKEN=78841520, última consulta em 15 de dezembro de 2012.

[17] Existem outras organizações, como por exemplo o *Institute of Electrical and Electronics Engineers* (IEEE) e a *International Organization for Standardization* (ISO) – esta última já por nós mencionada supra a propósito do "modelo OSI" (ver nota de rodapé 8). Dedicamos especial atenção à IETF porque vamos referir-nos, ao longo deste capítulo, a especificações emitidas por esta organização que se revestem de particular relevância para o nosso trabalho.

[18] "The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.", *About the IETF*, Internet Engineering Task Force, disponível em http://www.ietf.org/about/, última consulta em 15 de dezembro de 2012.

[19] "One way to look at the IETF is as the group of people who work together to improve the technology of the Internet on a daily basis." em http://www.ietf.org/newcomers.html, última consulta em 15 de dezembro de 2012.

[20] The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.", *IETF Mission Statement,* Internet Engineering Task Force, disponível em http://www.ietf.org/about/mission.html, última consulta em 15 de dezembro de 2012.

[21] Nos RFCs que são standards lê-se, no início do documento, uma das seguintes expressões: "this document specifies an Internet standards track protocol" ou "this memo documents an Internet Best Current Practice", ou, mais recentemente, "Category: Standards Track" ou "Category: Best Current Practice", cf. *Getting Started in the IETF*, Internet Engineering Task Force, disponível em http://www.ietf.org/newcomers.html#officialdocs, última consulta em 15 de dezembro de 2012.

Tim Berners-Lee, o pai da *World Wide Web*, trabalhava na Organização Europeia para a Investigação Nuclear – *European Organization for Nuclear Research* ou CERN[22] – quando, entre 1989 e 1990, desenvolveu e especificou as três tecnologias que ainda hoje são os pilares da *Web*[23]: Linguagem de Marcação de Hipertexto[24] – *HyperText Markup Language* (HTML) –, o Identificador Uniforme de Recursos[25] – *Uniform Resource Identifier* (URI) – e o Protocolo de Transferência de Hipertexto – *Hypertext Transfer Protocol* (HTTP).

Berners-Lee escreveu o primeiro navegador e editor de páginas *web*, o "*WorlWideWeb*", e o primeiro servidor *web*, o "httpd".[26]

Foi em 30 de abril de 1993, que a CERN anunciou que a *World Wide Web* seria colocada no domínio público, como um *software* livre, sem custos ou outros impedimentos[27].

A *Web* foi a primeira aplicação da internet a captar o interesse do público geral.

Hoje, mais de 2 biliões de pessoas em todo o mundo usam a *Web* para descobrir, trabalhar, partilhar e comunicar[28].

A World Wide Web, ou "Grande Rede Mundial", é em traços simples, o conjunto de páginas *web* a que podemos aceder usando um *navegador web*,

---

[22] Da antiga denominação *Conseil Européen pour la Recherche Nucléaire*.

[23] "The Web relies on three mechanisms to make these resources readily available to the widest possible audience: A uniform naming scheme for locating resources on the Web (e.g., URIs). Protocols, for access to named resources over the Web (e.g., HTTP). Hypertext, for easy navigation among resources (e.g., HTML)", RAGGETT, Dave, HORS, Arnaud Le e JACOBS, Ian Jacobs, *HTML 4.01 Specification*, W3C Recommendation, 24 December 1999, disponível em http://www.w3.org/TR/html401/, última consulta em 15 de dezembro de 2012.

[24] "To publish information for global distribution, one needs a universally understood language, a kind of publishing mother tongue that all computers may potentially understand. The publishing language used by the World Wide Web is HTML (from HyperText Markup Language). HTML gives authors the means to: Publish online documents with headings, text, tables, lists, photos, etc. / Retrieve online information via hypertext links, at the click of a button. / Design forms for conducting transactions with remote services, for use in searching for information, making reservations, ordering products, etc. / Include spread-sheets, video clips, sound clips, and other applications directly in their documents." RAGGETT, Dave, HORS, Arnaud Le e JACOBS, Ian Jacobs, *HTML 4.01 Specification*, cit..

[25] "Every resource available on the Web -- HTML document, image, video clip, program, etc. -- has an address that may be encoded by a Universal Resource Identifier, or "URI". URIs typically consist of three pieces: The naming scheme of the mechanism used to access the resource / The name of the machine hosting the resource / The name of the resource itself, given as a path." RAGGETT, Dave, HORS, Arnaud Le e JACOBS, Ian Jacobs, *HTML 4.01 Specification*, cit..

[26] *Sir Tim Berners-Lee - Web Inventor and Founding Director of the World Wide Web Foundation*, World Wide Web Foundation, disponível em http://www.webfoundation.org/about/sir-tim-berners-lee/, última consulta em 06 de janeiro de 2013.

[27] *Statement Concerning CERN W3 Software Release into Public Domain*, European Organization Nuclear Research, disponível em http://tenyears-www.web.cern.ch/tenyears-www/Declaration/Page1.html e http://tenyears-www.web.cern.ch/tenyears-www/Declaration/Page2.html, últimas consultas em 06 de janeiro de 2013.

[28] "More than 2 billion people around the world use the web to discover, work, share and communicate" in https://www.google.com/intl/en/takeaction/we-are-the-web/, consultada a 14 de dezembro de 2012.

e que se baseia no Protocolo de Transferência de Hipertexto – *Hypertext Transfer Protocol* (HTTP). É uma rede de recursos de informação[29] [30].

Como explicam James F. Kurose, Keith W. Ross[31], as páginas *web* consistem em objetos que, por sua vez, são ficheiros simples (e.g. uma imagem, um ficheiro html, um vídeo). Assim, uma página *web* é, composta por um ficheiro-base html que referencia outros objetos[32].

Os servidores *web* alojam os objetos. Cada um destes objetos (e.g. a imagem, o vídeo, a próprio ficheiro HTML da página) é endereçável por um único *Uniform Resource Locator*[33] (URL).

O *World Wide Web Consortium* (W3C), fundado por Tim Berners-Lee em 1994, é um consórcio de âmbito internacional que tem assumido a responsabilidade de trabalhar no desenvolvimento de protocolos e diretrizes, com a missão expressa de levar a *web* a alcançar o seu potencial máximo[34]. No seu seio desenvolvem-se *standards web*, que resultam do trabalho cooperante das organizações filiadas, uma equipa a tempo integral, bem como o público[35].

O W3C e a IETF têm desenvolvido os seus trabalhos de forma harmoniosa, na convergência dos objetivos comuns de pugnar pelo desenvolvimento da Internet e da *World Wide Web*.

1.2.1. O Protocolo de Transferência de Hipertexto (HTTP)

[29] *HTML 4.01 Specification*, W3C Recommendation, 24 December 1999, disponível em http://www.w3.org/TR/html401/, "The World Wide Web (Web) is a network of information resources.".
[30] "Vem sendo generalizada entre os utilizadores uma – ainda que errada – identificação do termo "Internet" com aquilo que tecnicamente se designa por "World Wide Web", ou "Grande Rede Mundial" e que funciona mediante o uso de uma tecnologia especial, denominada de "hipertexto"", ANDRADE, Francisco, *Da contratação eletrónica – Em particular da contratação inter-sistémica inteligente*, Tese de Doutoramento da Universidade do Minho, 2008, p. 20.
[31] Ver KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 98 e 99.
[32] "A característica essencial do hipertexto é assim a de permitir, através de ligações previamente selecionadas, possibilitar ao usuário saltar de dado em dado, de informação em informação, entre páginas (de texto ou multimédia) ou sítios electrónicos, mediante a utilização de um "browser" ou "programa de leitura de hipertexto.", ANDRADE, Francisco, *Da contratação eletrónica ...* , op. cit., p. 20, nota de rodapé 63.
[33] "URLs form a subset of the more general URI naming scheme.", *HTML 4.01 Specification*, cit..
[34] *W3C Mission*, World Wide Web Consortium*, disponível em* http://www.w3.org/Consortium/mission, última consulta em 3 de março de 2013.
[35] Para mais informações sobre o W3C ver *About W3C*, World Wide Web Consortium*,* disponível em http://www.w3.org/Consortium/, última consulta em 3 de março de 2013.

O HTTP é o protocolo que permite que, utilizando um navegador *web*, possamos solicitar páginas *web* aos servidores *web* e que estes no-las possam transferir. É o protocolo em que se baseia a *Web*, mas pode ser utilizado em qualquer aplicação baseada no modelo cliente-servidor. Trata-se de um protocolo que suporta uma larga variedade de formatos.

Conforme destaca William Stallings[36], o HTTP não é um protocolo para a transferência de hipertexto, mas sim um protocolo que permite a transmissão de informação com a eficiência necessária à navegação baseada em hipertexto.

Encontramos a especificação do protocolo HTTP no RFC 2616[37] da *Internet Engineering Task Force*.

Terminologicamente[38], no contexto do HTTP, dada uma concreta conexão, entendemos por "cliente" o programa que desempenha a função de estabelecer a conexão com o propósito de enviar pedidos ao "servidor" – que é o programa que aceita a conexão tendente a receber pedidos e enviar respostas. O cliente que inicia o pedido, e.g. o navegador, é o chamado "*user agent*".

No entanto, os termos cliente e navegador web são frequentemente usados indistintamente, uma vez que os navegadores *web* são os programas que implementam o HTTP do lado do cliente no contexto da *Web*[39]. Optamos, também nós, por fazer uso dos referidos termos indistintamente, no presente trabalho.

A "conexão" é, nos termos do RFC 2616, a camada de transporte de circuito virtual estabelecida entre dois programas com o propósito de comunicação.

---

[36] STALLINGS, William, *Data and Computer Communications*, 8ª edição, Pearson Education, Inc., 2007, pp 784.
[37] FIELDING, R. [et al], *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616, The Internet Engineering Task Force (IETF), junho, 1999, disponível em http://www.ietf.org/rfc/rfc2616.txt, última consulta em 10 de dezembro de 2012.
[38] Adotamos a terminologia adotada no RFC 2616, FIELDING, R. [et al], *Hypertext ...* RFC 2616, cit..
[39] Encontramos este uso indistinto dos termos cliente e navegador *web* na maioria da bibliografia consultada para este primeiro capítulo, mas quem nos explica com esta simplicidade tal opção são James F. Kurose e Keith W. Ross: KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., p. 99.

A “mensagem” é a unidade básica de comunicação HTTP. Existem dois tipos de mensagem http: a mensagem de pedido e a mensagem de resposta.

O HTTP é, então, implementado num programa para o cliente – navegador *web* – e noutro para o servidor – servidor *web* –, que são executados em terminais diferentes, e comunicam por mensagens HTTP, estruturadas de acordo com o protocolo[40].

Quando um cliente solicita uma página *web*, o navegador envia uma mensagem de pedido HTTP ao servidor. O servidor, recebendo o pedido, responde com uma mensagem de resposta HTTP que contém o objeto solicitado.

A mensagem HTTP compreende:

1) uma linha de pedido ou linha de estado
2) uma ou mais linhas de cabeçalho
3) uma linha em branco
4) o corpo da mensagem / a entidade em si (opcional)

Sem nos delongarmos muito em explicações técnicas[41], importa que dediquemos especial atenção ao campo cabeçalho.

É através do cabeçalho que são trocadas informações adicionais entre o servidor e o navegador.

Na mensagem de pedido, o navegador pode enviar ao servidor várias informações, inseridas no cabeçalho.

Através da introdução na mensagem de pedido de uma linha de cabeçalho *User-agent*, o servidor obtém a descrição do navegador (qual o navegador e a sua versão), bem como informação sobre o sistema operativo

[40] KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 98 e 99.
[41] Para uma análise mais pormenorizada das mensagem http, ver KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 103 a 108 e STALLINGS, William, *Data and Computer ...* , op. cit., pp 788 a 795.

do dispositivo e outras informações adicionais acerca do dispositivo de onde provem o pedido.

Com a introdução da linha de cabeçalho *Accept* na mensagem de pedido HTTP, o navegador faz saber ao servidor com que formatos é que é capaz de lidar, por ordem de preferência.

O navegador pode dar a conhecer ao servidor, através da introdução de uma linha de cabeçalho *Accept-language* na sua mensagem de pedido, qual o idioma em que prefere que lhe seja enviado o objeto solicitado.

A linha de cabeçalho HTTP *referer*, por sua vez, é aquela que permite ao servidor saber de onde veio o pedido. Ou seja, o *site web* a que se destina o pedido fica a saber o URL anteriormente visitado.

Outra linha que pode ser incluída no cabeçalho da mensagem de pedido HTTP é o chamado cabeçalho *cookie*, como veremos com mais atenção no próximo título.

Além destas informações, muitas outras podem ser fornecidas ao servidor através do cabeçalho do pedido HTTP enviado pelo navegador.

Este é um exemplo de uma mensagem de pedido HTTP onde podemos identificar a linha de pedido seguida de alguns dos cabeçalhos supra referidos:

GET /home.aspx HTTP/1.1
Host: alunos.uminho.pt
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:11.0) Gecko/20100101 Firefox/11.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.uminho.pt/estudar/portal-academico
Cookie: __utma=100000205.1000030852.1000004851.1000008782.1000093384.4; __utmz=102000005.1000093384.4.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=uminho; __utmb=102000205.4.10.1000093384; __utmc=100009205

Do mesmo modo, na sua mensagem de resposta a um pedido HTTP, o servidor pode incluir vários cabeçalhos.

Uma das linhas de cabeçalho que o servidor pode optar por inserir na sua mensagem de resposta a um pedido HTTP é o chamado cabeçalho *set-cookie*.

Outra linha de cabeçalho que nos importa considerar é a chamada *Cache-Control*. Esta indica qual o comportamento que os mecanismos de *caching*[42] existentes aos longo da cadeia de comunicação entre o servidor e o cliente devem assumir. Conforme explica Kristol, quando o servidor envie, na sua resposta HTTP, conteúdo personalizado ou conteúdo dependente do tempo, é importante que inclua "ordens" para que a mensagem em causa não possa ser retida.

Assim, podemos ver a mensagem de resposta HTTP ao pedido que usamos no exemplo anterior[43]:

HTTP/1.1 200 OK
Date: Tue, 26 Feb 2013 15:46:56 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=fwxb0or1uuku3eyy4xsk5vjc; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=iso-8859-1
Content-Length: 75886

A informação trocada nas mensagens HTTP é, portanto, texto legível[44], em claro[45], à exceção da entidade em si objeto do pedido e da

[42] Como exemplo de mecanismos de caching temos os *caching proxies.* Um *proxy* é um intermediário que aceita os pedidos dos clientes que lhe estão ligados e os reencaminha para os servidores. Um caching proxy, porém, não se limita a receber e reencaminhar pedidos e respostas entre clientes e servidores; além disso é capaz de reter uma resposta de um servidor ao pedido de um cliente e, mais tarde, enviá-la como resposta ao pedido de um outro cliente sem que necessite de o reencaminhar ao servidor original. O objetivo é diminuir a latência das comunicações. No entanto, o facto de o proxy enviar a mesma resposta a clientes diferentes pode causar alguns problemas, que só se podem evitar impedindo a retenção do conteúdo ou ordenando o proxy a revalidar as respostas com o servidores antes de as reenviar ao cliente. KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., p. 6.

[43] Em ambos os exemplos usados (cabeçalhos das mensagens de pedido e resposta http), apenas os valores das linhas de cabeçalho *cookie* e *set-cookie* são fictícios.

[44] Escritas em ASCII – *American Standard Code for Information Interchange* (Código-Padrão Americano de Intercâmbio de Informação).

[45] A menos que a comunicação se processe por HTTPS.

resposta final pretendida, uma vez que as páginas *web* são codificadas (comummente em HTML) [46].

É através destas mensagens que se estabelece o diálogo entre o cliente o servidor. É através delas que acordam nos pontos essenciais à comunicação de modo a torna-la efetiva.

Para que a comunicação se processe eficazmente, o HTTP assenta nos protocolos TCP e IP.

O HTTP usa o TCP como protocolo para transferência de dados – camada de transporte –, o que lhe confere confiança[47].

A conexão HTTP estabelecida pode ser persistente (HTTP/1.1, por defeito) ou não persistente (HTTP/1.0 e HTTP 1/1), isto é, todos os pares de pedidos e correspondentes respostas podem ser enviados pela mesma conexão TCP ou cada par de pedido e a correspondente resposta é enviado por uma conexão diferente[48] [49].

Como protocolo de rede, o HTTP usa o IP. É este que permite ao servidor saber de onde proveio a mensagem de pedido de modo a saber para onde deve enviar a sua mensagem de resposta. O servidor precisa, portanto, de conhecer o endereço IP do dispositivo de onde provém o pedido.

---

[46] As mensagens HTTP eram, originalmente, apenas texto simples escrito em ASCII – *American Standard Code for Information Interchange* (Código-Padrão Americano de Intercâmbio de Informação). Com o HTTP 1/0 as mensagem passam a ser do tipo MIME – Multipurpose Internet Mail Extension (Extensões de Múltiplos Propósitos do Correio de Internet) –, o que vem permitir a transferência de outros formatos como, por exemplo, imagem ou vídeo.

[47] Sobre o funcionamento do protocolo TCP, KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 230 e ss..

[48] De forma simplificada: o cliente começa sempre por iniciar uma conexão TCP com o servidor. De seguida, através do navegador, o cliente envia uma mensagem de pedido HTTP ao servidor. Recebido o pedido, o servidor envia uma mensagem de resposta HTTP com o objeto. Se estiver na base da ligação uma conexão TCP não persistente, o servidor indica, neste momento, que a conexão TCP pode ser encerrada. O cliente recebe a resposta. Se estiver na base da ligação uma conexão TCP não persistente, é neste momento que ela encerra. Uma ligação TCP não persistente não permite o envio de mais do que um objeto por conexão. Numa conexão TCP persistente, no momento em que envia a reposta, o servidor deixa a ligação TCP aberta, o que vai permitir o envio de mais do que um objeto por cada conexão TCP. KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 98 a 103.

[49] O Grupo de trabalho Hypertext Transfer Protocol Bis (httpbis) da IEFT está a trabalhar na especificação do HTTP/2.0. O Grupo de trabalho tem como presidente Mark Nottingham. Os objetivos propostos preveem, além do mais, a compressão dos cabeçalhos. No entanto, não estão previstas alterações que afetem a abordagem atual do mecanismo dos testemunhos de conexão. A Last Call para o HTTP/2.0 está agendada para abril de 2014. Mais informações disponíveis na página do Grupo de Trabalho em https://datatracker.ietf.org/wg/httpbis/charter/, última consulta em 20 de novembro de 2012.

Quando o cliente se liga à rede através de um *proxy*, a linha de cabeçalho *X-Forwarded-For* incluída na mensagem de pedido HTTP permite ao servidor conhecer o endereço IP da máquina de onde proveio o pedido – caso assim não seja, o servidor apenas conhece o endereço IP do *proxy* de onde proveio a mensagem.

O HTTP quando combinado com o protocolo SSL/TLS (*Secure Sockets Layer/Transport Layer Security*)[50] dá origem ao chamado Protocolo de Transferência de Hipertexto Seguro (HTTPS). Este garante a segurança e a confidencialidade das comunicações com recurso à criptografia[51].

As mensagens HTTP trocadas com base no protocolo HTTPS são, portanto, encriptadas[52].

1.2.1.1. HTTP, um protocolo sem estado

O HTTP é um protocolo sem estado – *statless protocol*. Esta característica deve reter a nossa atenção.

O HTTP não mantém informação de estado e isto quer dizer, numa explicação simplificada, que o servidor não mantém qualquer informação sobre anteriores pedidos do cliente. O servidor não consegue relacionar um pedido atual com pedidos passados ou futuros. O servidor esquece por completo qualquer pedido anterior e trata cada pedido como se do primeiro se tratasse, de modo totalmente independente.

O facto de se tratar de um protocolo sem estado torna mais simples a construção de servidores e navegadores *web*.

[50] O SSL (Secure Sockets Layer) foi desenvolvido em 1994, no seio da *Netscape*, e, mais tarde, passou a assumir a designação de TLS (Transport Layer Security), quando foi transformado em standard da Internet pela IETF.
[51] A confidencialidade das comunicações HTTPS baseia-se em cifras simétricas, com autenticação baseada em criptografia de chave pública e integridade baseada em Message Authentication Codes.
[52] Sobre o HTTPS ver: *HTTPS Everywhere FAQ*, Electronic Frontier Foundation, disponível em https://www.eff.org/https-everywhere/faq, última consulta em 25 de fevereiro de 2013.

No entanto, torna-se muito difícil escrever certas aplicações. Pensemos, desde logo, naquele que é, talvez, o exemplo mais paradigmático do que acabamos de dizer: a implementação dos "cestos de compras"[53] nos *sites web*.

Sem estado, os *sites web* não são capazes de registar e agregar produtos eficazmente numa lista de compras ("cestos de compras"). Simplesmente, a cada novo pedido, o *site web* esquece o pedido anterior e não é capaz de agregar os artigos pretendidos por um cliente para os processar numa única encomenda final. John Schwarz, no seu célebre artigo publicado no New York Times[54], faz a seguinte analogia: fazer compras na *web* era, então, como visitar uma loja em que o balconista tinha amnésia[55] [56].

Sem estado, um utilizador que navegue entre páginas de um mesmo *site* é tratado, a cada pedido, como um novo visitante.

2. Os testemunhos de conexão

Os testemunhos de conexão surgem no contexto da *Web* como um complemento ao HTTP.

Nos primeiros tempos da *World Wide Web*, os navegadores não ofereciam soluções capazes de suprir as dificuldades levantadas pela falta de estado das ligações HTTP.

Com o intuito de superar o problema da falta de estado das ligações HTTP, de modo a permitir o desenvolvimento de aplicações *web* que de outro

[53] Mecanismo também conhecido por "carrinho de compras".
[54] SCHWARZ, John *Giving the Web a Memory Cost Its Users Privacy*, in "The New York Times", 4 de setembro de 2001, disponível em http://www.nytimes.com/2001/09/04/technology/04COOK.html, última consulta em 5 de novembro de 2012.
[55] "it was like visiting a store where the shopkeeper had amnesia." SCHWARZ, John *Giving the Web...* , cit..
[56] No mesmo sentido "*A stateless web is analogous to a vending machine. It has little regard for who you were, what product you are asking for, or how many purchases you have made. It has no memory. Statelessness on the web made commerce difficult. Without a state mechanism, buying goods is analogous to using a vending machine. You could not buy more than one product at a time and there would be no one-click automated shopping feature that remembers your personal information.*" SHAH, Rajiv C. E KESAN, Jay P., *Deconstructing Code,* Illinois Public Law and Legal Theory Research Papers Series, Research Paper No. 04-22, September 29, 2004, p. 298.

modo não seriam viáveis, Lou Montulli desenvolveu, ao serviço da *Netscape*, a ideia daquilo a que veio a chamar *cookies*[57].

Os testemunhos de conexão vieram permitir a manutenção de estado nas conexões HTTP.

O estado numa conexão HTTP implica alguma relação entre primeiro pedido a um servidor e os pedidos anteriores realizados pelo mesmo usuário para aquele servidor.

Uma sessão é uma sequência de pedidos, uma série de troca de mensagens, caracterizada por ter um princípio e um fim, ser relativamente curta e poder ser terminada quer pelo servidor quer pelo cliente[58].

Como explica Kristol[59], há outros mecanismos que permitem conseguir manter o estado numa conexão HTTP.

A informação de estado pode, por exemplo, ser embutida nos URLs ou incorporada em ficheiros escondidos em formulários HTML. Porém, o recurso a estes mecanismos não é considerado eficaz. A informação de estado, nestes casos não faz parte do protocolo. Se o utilizador clicar no botão "retroceder" do seu navegador, o seu estado reverte àquele em que se encontrava na(s) página(s) anterior – para a qual retrocedeu – e a informação de estado entretanto agregada é perdida (por exemplo, o produto selecionado deixa de constar do "cesto de compras").

Além disso, a identificação de sessão embutida no URLs pode trazer outros problemas. O texto URL está visível, acessível e pode ser, por exemplo, copiado pelo utilizador. Imagine-se o caso em que o utilizador partilha o URL com um amigo, por exemplo com o intuito de lhe mostrar o produto que pretende comprar. Pode acontecer que, se o *site* não assumir outros mecanismos de proteção contra este tipo de problemas, o amigo passe a assumir a sessão do utilizador, assumindo a identidade daquele

[57] "*The state object is called a cookie, for no compelling season*", MONTULLI, Lou e GIANNANDREA, John, *Persistent Client State - HTTP Cookies*, Netscape Communications Corporation, 1994.
[58] KRISTOL, David M., *Proposed HTTP State-Info Mechanism*, HTTP Working Group, The Internet Engineering Task Force (IETF), 05 de agosto de 1995, 3. STATE AND SESSIONS, disponível em http://tools.ietf.org/html/draft-kristol-http-state-info-00, última consulta em 20 de novembro de 2012.
[59] KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., pp. 6 e 7.

perante o *site*. Mas se este perigo se regista como consequência involuntária da partilha inconsciente do identificador de sessão, também se pode dar o caso da partilha ser intencional e ter fins maliciosos. Mais, o URL pode ser facilmente alterado, e levar a resultados imprevisíveis.

O recurso ao endereço de IP para identificação de uma sessão não é, também, uma solução eficaz.

O *site* tem facilmente conhecimento do IP através do navegador ou do proxy de onde provém a mensagem de pedido, porém o IP pode facilmente ser partilhado por mais do que um utilizador, o que não garante uma identificação segura do cliente.

Os testemunhos de conexão surgiram da necessidade de ultrapassar o problema da falta de estado das ligações HTTP e hoje são utilizados com várias finalidades.

2.1. Da Especificação Original da *Netscape* ao RFC 6265 da IETF

Com o intuito de capitalizar[60] as potencialidades emergentes da jovem *Web,* Marc Andreessen e Jim Clark fundaram a *Mosaic Communications Corporation*, a 4 de Abril de 1994, que, ainda no ano da sua fundação, foi rebatizada de *Netscape Communications Corporation* (*Netscape*).

A ideia de negócio passava por uma aposta articulada no comércio, segurança e performance de navegadores e servidores web, que seria capaz de atrair aqueles que se iam mostrando interessados em ganhar dinheiro através da internet.

Os testemunhos de conexão são uma das tecnologias desenvolvidas no seio da *Netscape* e surgem da necessidade de ultrapassar o problema da falta de estado das ligações HTTP.

[60] SHAH, Rajiv C. E KESAN, Jay P., *Deconstructing Code*, op. cit., pp. 297 e ss..

Lou Montulli trabalhava ao serviço da *Netscape* quando, em 1994, desenvolveu a ideia dos testemunhos de conexão, adaptando uma tecnologia conhecida por *magic cookie*[61], usada nas plataformas Unix, às necessidades de comunicação entre o computador de um utilizador e um *site web* visitado por aquele, de modo a melhorar a funcionalidade do chamado "cesto de compras", suprindo o problema da falta de estado das ligações HTTP[62].

O "cesto de compras", para ser eficaz precisava de informações de estado de modo a ser capaz de distinguir entre os diferentes compradores ao longo de toda a interação tendente à compra e conseguir registar e agregar os produtos selecionados de modo a serem processados num único momento de compra, no final. Os testemunhos de conexão permitiam ultrapassar o problema da falta de estado das ligações HTTP, possibilitando a implementação eficaz do mecanismo dos "cestos de compra".

A primeira utilização dos testemunhos de conexão foi promovida no próprio *site* da *Netscape* e tinha por finalidade determinar se os visitantes do seu *site web* estavam a aceder-lhe pela primeira vez ou não.

Montulli escreveu, naquele ano de 1994, com o seu colega John Giannandrea, aquela que foi a especificação original dos testemunhos de conexão: "*Persistent Client State HTTP Cookies*"[63].

Conforme explicava a especificação, na sequência da receção de um pedido HTTP, o servidor pode incluir na sua resposta uma informação de estado que vai ser armazenada pelo cliente. Fá-lo através da introdução de um cabeçalho *set-cookie* na sua resposta HTTP. Esse "objeto de estado", enviado pelo servidor, compreende a descrição dos URLs para os quais é válido. Numa próxima ligação (ao mesmo *site web* ou a um URLs para o qual aquela informação de estado seja válida) o cliente vai reenviar essa informação, inalterada, ao servidor, através da introdução de um cabeçalho *cookie*. Foi a essa informação – "objeto de estado" – enviado pelo servidor ao

[61] "Something passed between routines or programs that enables the receiver to perform some operation; a capability ticket or opaque identifier.", *magic cookie*, "The Free On-line Dictionary of Computing", disponível em http://foldoc.org/magic+cookie, última consulta em 28 de março de 2013.
[62] Até então, os mecanismos de cestos de compras implicavam o armazenamento de informação, por exemplo, no URL. Mas este mecanismo levanta muitos problemas, como vimos na inrodução do Título 2. deste Capítulo I.
[63] MONTULLI, Lou e GIANNANDREA, John, *Persistent Client State ...* , cit..

cliente, armazenado e reenviado àquele por este que Montulli chamou *cookie*[64] – testemunhos de conexão.

A especificação conferia uma certa confiança ao mecanismo. Os testemunhos apenas podiam ser enviados de e para as páginas que o utilizador visitava – só estas os podiam escrever e ler. Um *site* não poderia ler ou alterar um testemunho de conexão enviado por outro *site*.

Esta especificação preliminar dos testemunhos de conexão era um documento informal, de apenas quatro páginas, pouco detalhado.

No entanto, a sua simplicidade permitiu que permanecesse como o documento de referência por muito tempo – mais do que, como veremos, seria de esperar.

Em Setembro de 1994, a *Netscape* incorporou o mecanismo dos testemunhos de conexão na versão 0.9 beta do seu navegador *Mosaic Netscape,* que veio a dar origem ao *Netscape Navigator 1.0*, lançado a 15 de Dezembro de 1994.

O *Netscape Navigator* permitia os testemunhos de conexão por defeito. Os testemunhos podiam, então, ser armazenados pelo navegador e reenviados aos servidores visitados sem que o utilizador tivesse conhecimento disso.

A discussão no seio da comunidade científica acerca dos mecanismos de gestão de estado nas ligações HTTP teve início em Abril de 1995, na *mailing list* www-talk da W3C.

---

[64] "The state object is called a cookie, for no compelling reason.", MONTULLI, Lou e GIANNANDREA, John, *Persistent Client State ...* , cit..
"According to an article written by Paul Bonner for Builder.Com on 11/18/1997: "Lou Montulli, currently the protocols manager in Netscape's client product division, wrote the cookies specification for Navigator 1.0, the first browser to use the technology. Montulli says there's nothing particularly amusing about the origin of the name: 'A cookie is a well-known computer science term that is used when describing an opaque piece of data held by an intermediary. The term fits the usage precisely; it's just not a well-known term outside of computer science circles.'" WHALEN, David*, The Unofficial Cookie Faq*, Cookie Central, disponível em http://www.cookiecentral.com/faq/, última consulta em 7 de fevereiro de 2013.
A versão portuguesa da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), adota, segundo apuramos, pela primeira vez a terminologia "testemunhos de conexão" para se referir aos *cookies*. Em França, em março de 1999, foi introduzida oficialmente a expressão "témoin de connexion". O Office de la langue française du Québec já havia proposto, em setembro de 1996, o termo "témoin" como equivalente a *cookie*. Cf. informação disponível no site oficial do Office de la langue française du Québec, disponível em http://www.oqlf.gouv.qc.ca/, última consulta em 25 de fevereiro de 2013.

Em 25 de Agosto de 1995, no Grupo de Trabalho do HTTP da IETF, surgiu uma primeira proposta [65] que visava introduzir estado no HTTP, através da introdução de um novo cabeçalho de pedido e resposta que permitiria que informações de estado fossem transmitidas entre o servidor e o cliente.

Consciente de que um histórico das ações dos utilizadores era útil ou essencial para certas aplicações *web*[66], Kristol propôs uma tecnologia que permitia informação de estado que persistiria unicamente durante cada sessão. Este era um modelo diferente do que vinha a ser adotado e que estava previsto na especificação da *Netscape*.

Larry Masinter presidia, então, ao Grupo de Trabalho do HTTP da IETF e considerou pertinente criar um subgrupo para discutir a questão e chegar a uma abordagem consensual sobre o tema a ser apresentada aos restantes participantes do Grupo de Trabalho [67]. Lui Montulli, autor da especificação original da *Netscape*, foi uma das oito pessoas que constituíram o subgrupo, formado em Dezembro de 1995.

Como explica David M. Kristol[68], a especificação original da *Netscape* foi, então, adotada como modelo para o trabalho que veio a ser desenvolvido pelo subgrupo.

Em Fevereiro de 1996, o subgrupo considerou a possibilidade de, em teoria, os navegador poderem receber, armazenar e reenviar testemunhos de conexão de e para *sites* que o utilizador não visitasse diretamente. Eram as chamadas "transações não verificáveis" [69] ou, como vieram a ficar conhecidas, os testemunhos de terceiros.

Apesar de, desde a especificação da *Netscape*, a tecnologia vedar que um *site* diferente daquele que criou o testemunho para ser armazenado no

[65] KRISTOL, David M., *Proposed HTTP State-Info ..., cit.*.
[66] KRISTOL, David M., *Proposed HTTP State-Info ..., cit.*.
[67] KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., pp. 10 a 12.
[68] KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., pp. 10-12.
[69] Tradução livre da expressão utilizada no RFC 2109 "unverifiable transactions".

terminal do utilizador o lesse, era possível que componentes de terceira parte do *site* visitado enviassem os seus próprios testemunhos.

As preocupações do subgrupo focaram-se, então, no facto de que, se por um lado é expectável que o utilizador possa contar com testemunhos dos *sites web* que deliberadamente visita, por outro não tem porque esperar receber testemunhos de um *site* que não visita deliberadamente, mas a que, por exemplo, o seu navegador acede porque o *site web* que o utilizador deliberadamente visitou carrega uma imagem de um outro *site* que lhe vai enviar um testemunho.

A especificação foi publicada como RFC 2109 – "*HTTP State Management*" – sob a autoria de D. Kristol e L. Montulli, em Fevereiro de 1997[70].

Mas continuavam a registar-se problemas de compatibilidade. Os navegadores *Netscape Navigator* e *Internet Explorer* comportavam-se de modo diferente perante atributos que não lhes fossem familiares[71].

O RFC 2109 tentou promover alterações que não foram bem sucedidas[72].

No que respeitava às "transações não verificáveis", a especificação determinava a proibição de os navegadores *web* aceitarem testemunhos de terceiro ou só, em alternativa, permitia que os aceitassem com a condição de estes poderem ser controlados pelo utilizador através de uma opção que, por defeito, os rejeitaria.

Muitos modelos de negócio assentavam, já, nos testemunhos de terceira parte e as críticas à especificação não se fizeram esperar.

---

[70] KRISTOL, D. e MONTULLI, L., *HTTP State Management Mechanism*, RFC 2109, The Internet Engineering Task Force (IETF), fevereiro de 1997, disponível em http://www.ietf.org/rfc/rfc2109.txt, última consulta em 10 de dezembro de 2012.

[71] Cf. KRISTOL, David M., *HTTP Cookies: Standards,...* , op. cit. pp. 12 e 13.

[72] Neste sentido ZALEWSKI, Michael, *HTTP cookies, or how not to design protocols*, em "lcamtuf's blog", 28 de outubro de 2010, disponível em *http://lcamtuf.blogspot.pt/2010/10/http-cookies-or-how-not-to-design.html*, última consulta em 4 de novembro de 2012.

A discussão para a revisão do RFC foi longa.

Conforme explica Kristol, a discussão em torno de questões relacionadas com as "transações não verificáveis" fez com que o trabalho tendente à revisão da especificação entrasse num impasse e, de modo a conseguir progredir nos trabalhos, foi decidido afastar a parte respeitante às "transações não verificáveis" até à obtenção de um consenso na parte tecnológica[73].

Obtido o ambicionado consenso e reintroduzida a questão das "transações não verificáveis" não surgiram mais comentários sobre o anteriormente tão debatido tema e o novo RFC 2965[74], publicado em outubro de 2000, não viria a diferir materialmente do seu antecessor neste tocante[75].

De modo a superar as incompatibilidades verificadas, a especificação descrevia três cabeçalhos: o cabeçalho *cookie*, o cabeçalho *set-cookie2* e o cabeçalho *cookie2*.

As especificações dos testemunhos de conexão eram documentos que não refletiam a realidade da implementação da tecnologia do mecanismo[76].

O RFC 2965, irrealista no seu esforço de tentar redesenhar o mecanismo dos testemunhos de conexão, foi considerado um falhanço[77].

Com especificações desadequadas, as compatibilidades com os diferentes navegadores tinha de ser atestada por tentativas.

---

[73] A discussão levantada em torno dos testemunhos de terceira parte levou à proposta de "testemunhos certificados", apresentada Dan Jaye. A ideia, pressupunha a existência de uma entidade certificadora independente que atestaria e auditaria o nível de confiança dos *sites*, atendendo às suas politicas de privacidade, permitindo aos utilizadores optar por permitir ou não os testemunhos de acordo com a sua utilização. O cabeçalho http *Set-Cookie-Certifiers* permitiria o envio do certificado juntamente com o testemunho, que serviria para o navegador aferir da compatibilidade das finalidades de uso dos testemunhos em causa com as definições do navegador por que o utilizador teria optado.
"The intent is to provide a mechanism that allows user agents to determine the privacy policies of a server and to accept or reject cookies based on that policy. Allowing the user to decide whether to accept cookies based on how the server uses them provides far better control over privacy than just distinguishing between servers the users directly accesses (verified transactions) and those to which the user agent was redirected (unverified transaction.)", JAYE, Dan, *HTTP State Management Proposal foi Certified Cookies*, 30 de março de 1997, disponível em http://lists.w3.org/Archives/Public/ietf-http-wg-old/1997JanApr/0742.html, última consulta em 20 de novembro de 2012.

[74] KRISTOL, D. e MONTULLI, L., *HTTP State Management Mechanism*, RFC 2965, The Internet Engineering Task Force (IETF), outubro de 2000, disponível em http://www.ietf.org/rfc/rfc2965.txt última consulta em 10 de dezembro de 2012.

[75] Para uma descrição mais pormenorizada sobre a história dos RFC 2109 e RFC 2965, ver KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., pp. 24 e ss..

[76] Sendo o RFC 2956 o que mais se afastava da implementação real do mecanismo.

[77] Neste sentido ZALEWSKI, Michael, *HTTP cookies, or...* , cit..

A descrição realista da implementação deste mecanismo só veio a ser feita no RFC 6265 – "HTTP State Management Mechanism"[78], publicado em Abril de 2011, da autoria de A. Barth.

Em inícios de 2009, a IETF iniciou uma *mailinglist* para discutir os problemas relacionados com os testemunhos de conexão, que culminou com a criação, em dezembro daquele ano, do Grupo de Trabalho *HTTP State Management Mechanism*, que teve por presidente Jeff Hodges.

O Grupo de Trabalho tinha por objetivo especificar aquilo que eram as implementações comuns do mecanismo e documentar as variações existentes procurando um consenso dentro destas.

Assim, ficou desde logo assente[79], que o Grupo de Trabalho não criaria nada de novo.

O Grupo propôs-se, tão-somente, a descrever como implementar os testemunhos e conexão de modo a que interagissem eficazmente com as infraestruturas existentes.

O RFC 6265 especifica os cabeçalhos *set-cookie* e *cookie* como eles são realmente usados na Internet.

2.2. Funcionamento

Na resposta a um pedido HTTP, o servidor pode incluir informações[80] que vão permitir suprir a falta de estado das ligações HTTP. Fá-lo através da introdução de um cabeçalho *set-cookie* na resposta HTTP.

---

[78] BARTH, A., *HTTP State Management Mechanism*, RFC 6265, The Internet Engineering Task Force (IETF), abril 2011, disponível em http://tools.ietf.org/html/rfc6265, última consulta em 4 de novembro de 2012, "This document specifies the syntax and semantics of these headers as they are actually used on the Internet", p. 4.

[79] "The working group must not introduce any new syntax or new semantics not already in common use", cfr descrição do Grupo de Trabalho, disponível em http://datatracker.ietf.org/wg/httpstate/charter/, última consulta em 04 de novembro de 2012.

[80] Utilizamos, neste primeiro capítulo, os termos "dados" e "informações" indistintamente. Usamos "informações" para nos referirmos aos dados compreendidos nos testemunhos de conexão por ser essa a terminologia usada nas especificações da IETF.
Na literatura sobre gestão e representação do conhecimento, é comum encontrarmos a distinção entre os conceitos de dados, informação e conhecimento. Os dados serão, então, os elementos mais básicos, os factos em bruto, sem significado, relações ou contexto. Da contextualização – organização – dos dados surge a informação. A informação resulta da interpretação dos factos, que são relacionados entre si de modo a obterem significado. Mais difícil de definir é a noção de conhecimento. O conhecimento é obtido a partir dos dados e da informação. Para uma abordagem conceptual mais aprofundada ver ZINS, Chaim, *Conceptual Approaches for Defining Data, Information,*

O cliente recebe esta informação e armazena-a no terminal do utilizador. Aquando de uma nova ligação ao servidor, reenvia inalterada[81] a informação previamente recebida através da introdução do chamado cabeçalho *cookie* no seu pedido.

Esta é a descrição básica dos testemunhos de conexão.

Os testemunhos de conexão permitem ao servidor reconhecer o navegador, até que a validade do testemunho expire.

A informação compreendida nos testemunhos de conexão está na discricionariedade do servidor.

Os testemunhos de conexão são simples linhas de texto, legíveis, enviadas pelo servidor ao navegador, no cabeçalho *set-cookie* da resposta ao pedido HTTP que, uma vez recebidas por um navegador cooperante, são armazenadas como um arquivo de texto por este no terminal do utilizador e, aquando de um novo pedido ao *site*, são reenviados inalterados, no cabeçalho *cookie* do pedido HTTP.

Assim, o cabeçalho *set-cooki* pode ser o seguinte:

Set-Cookie: example = one; path=/; expires Fri, 15-Feb-2013 15:50:00 GMT

O servidor dá, desta forma, ordem ao navegador para armazenar o testemunho e reenviá-lo aquando de uma nova solicitação.

O navegador, cooperante e com permissão para tal, armazena o testemunho juntamente com os seus atributos, com o nome ***example***, como um ficheiro de texto numa pasta ou subpasta no terminal do utilizador e, se este não tiver expirado ou sido apagado, reenvia-a na nova solicitação, introduzindo o cabeçalho *cookie:*

---

and Knowledge, Journal of the American Society for Information science and Technology, 15 de fevereiro, 2007, disponível em http://www.success.co.il/is/zins_definitions_dik.pdf, última consulta em 04 de novembro de 2012.

[81] Como veremos, ainda sob este título, o cabeçalho *cookie* é diferente do cabeçalho *set-cookie*, mas a informação que contém foi a que o *site* previamente definiu naquele cabeçalho *set-cookie*.

Cookie: example = one

O servidor pode enviar múltiplos cabeçalhos *set-cookie* na mesma resposta.

Cada cabeçalho *set-cookie*, por sua vez, conforme explica a especificação[82], compreende obrigatoriamente o atributo nome=valor – no nosso exemplo, o nome será ***example*** e o valor ***one*** – seguido de nenhum ou vários atributos.

Os atributos “data de expiração” (*Expires Attribute*) e “idade-máxima” (*Max-Age Attribute*) indicam a longevidade do testemunho.

O atributo “data de expiração” indica a data em que o testemunho de conexão expira – e é eliminado.

O atributo “idade-máxima” indica, não a data em que o testemunho expira, mas os segundos que faltam até que este expire.

Se ambos os atributos estiverem definidos (“data de expiração” e “idade-máxima”), é o atributo “idade-máxima” que deve prevalecer. Quando nenhum dos dois esteja definido, por defeito o navegador deve apagar o testemunho quando a sessão para que foi gerado expirar.

De todo o modo, o utilizador sempre pode apagar o testemunho de conexão por iniciativa própria, a qualquer momento.

O atributo “domínio” (*Domain Attribute*) é particularmente importante nos casos – tão comuns – em que o *site* conta com vários servidores para suportar a sua atividade na rede. Assim, com este atributo o *site* consegue que o testemunho seja acessível a todas as suas páginas. Se o valor do atributo domínio for "example.com"[83], o navegador vai reenviar o testemunho num futuro pedido dirigido a “example.com”, “www.example.com” e “www.corp.example.com”.

Se este atributo não for definido, o cliente dele apenas deve reenviar o testemunho aquando de um pedido ao servidor de origem.

[82] Cf. BARTH, A., *HTTP ...* RFC 6265, cit., pp. 10 e ss..
[83] Utilizamos aqui, sem alterações, o exemplo dado no RFC 6265, BARTH, A., *HTTP ...* RFC 6265, cit., p. 11.

Ademais, o servidor que envia o testemunho tem de pertencer ao domínio que define, ou seja, "example.com" não pode enviar um testemunho com o atributo de domínio definido para “instance.com”.

Testemunhos de conexão que tenham definido unicamente um domínio público (.com ou .pt, por exemplo) são conhecidos por *supercookies*. Os navegadores estão configurados para bloquear este tipo de testemunhos.

O atributo “caminho” (*Path Attribute*) define os caminhos (URLs) para os quais o testemunho é válido. Só as páginas compreendidas nos caminhos definidos podem ler o testemunho. Se este atributo não estiver definido, por defeito será somente considerado o URL que enviou o testemunho.

O atributo “segurança” (*Secure Attribute*) não tem um valor associado. Quando este atributo conste, o testemunho só deve ser enviado através de uma ligação segura. Assim, o testemunho só será usado através de uma ligação HTTPS, que vai garantir que o testemunho (como parte que é da mensagem HTTP) seja transmitido cifrado – e não em claro.

O atributo “*HttpOnly*”, também, não tem um valor associado[84]. Este atributo dá indicação ao navegador de que o testemunho apenas pode ser usado em pedidos HTTP. Deste modo, pretende-se impedir que seja dado acesso ao testemunho às chamadas Interfaces de Programação de Aplicativos (*Application Programming Interface* – APIs)[85].

[84] Os atributos “segurança” e “HttpOnly”, por não terem valores associados, são referidos como “bandeiras” (*flags*).

[85] O Interface de Programação de Aplicativos (API) permite que uma parte de *software* a correr num terminal utilize a infraestrutura da rede de modo a fazer chegar informação a outra parte de software específica que, por sua vez, corre noutro sistema terminal da rede.
O *JavaScript* é um exemplo dessas APIs. Trata-se de um *script* que é executado no lado do cliente, no próprio navegador. O *JavaScript* tem, geralmente, permissão para aceder aos testemunhos de conexão, a menos que a bandeira HttpOnly esteja definida e, então, impeça este acesso.
O *Cross-site scripting* (XSS) é um ataque que se serve desta possibilidade de executar linguagens no lado do cliente. Um utilizador mal intencionado pode procura vulnerabilidades num *site* que lhe permita injetar código que depois vai correr nos navegadores que acederem à ligação do *site* onde está alojado. O XSS pode, pois, ser utilizado para ganhar acesso ao testemunho de conexão que o *site* onde o código malicioso está inserido armazenou no terminal do utilizador (vitima do ataque), e que são enviados ao atacante quando o utilizador enviar um novo pedido ao *site* original. Uma vez que só o *site* que cria o testemunho é que pode ter acesso a ele (ou o conjunto de *sites* do mesmo domínio), o atacante precisa de injetar o código malicioso no *site* que instalou os testemunhos a que pretende aceder.

O navegador pode, porém, estar configurado para ignorar completamente o cabeçalho *set-cookie*[86]. Caso contrário, recebido um cabeçalho *set-cookie*, o navegador armazena o testemunho no terminal do utilizador como pares atributo-valor.

O espaço de armazenamento disponível para os testemunhos de conexão não é, geralmente, muito grande. A especificação[87] recomenda os navegadores a fornecer as capacidades de, pelo menos: 4096 bytes por testemunho, 50 testemunhos por domínio e 3000 testemunhos no total.

Cada navegador instalado em cada computador tem a sua área de armazenamento de testemunhos de conexão.

Num novo pedido ao mesmo servidor (ou a domínios pertencentes ao mesmo servidor) – por exemplo, no pedido de outra página do *site* – o navegador envia aquelas informações que recebeu, que vão permitir ao *site* reconhecer o navegador e associar o presente pedido ao anterior.

As informações são reenviadas pelo navegador ao servidor no cabeçalho *cookie*. O cliente reenvia ao servidor, apenas, o par nome-valor do testemunho.

Assim, os testemunhos de conexão são:

1) Informações enviadas pelo servidor ao cliente, numa linha de cabeçalho da resposta HTTP,

2) Informações armazenadas pelo cliente no terminal do utilizador como um arquivo de texto

3) E informações que são reenviados pelo cliente, inalterados, ao servidor aquando de um novo pedido.

Mas a tecnologia dos testemunhos de conexão, geralmente, contempla outra componente: uma base de dados do *site web*.

[86] É o que acontece quando são bloqueados por defeito pelo navegador ou por opção do utilizador os testemunhos de terceiros, cf. BARTH, A., *HTTP ...* RFC 6265, cit., p.17.
[87] BARTH, A., *HTTP ...* RFC 6265, cit., p. 27.

É comum que os testemunhos de conexão se limitam a fazer o reconhecimento do navegador ou se associam a dados anónimos.

Como tão bem explica Marshall Brain[88], os testemunhos de conexão muitas vezes não são mais do que um número de identificação, gerado aleatoriamente pelo *site web*.

O espaço de armazenamento disponível para os testemunhos de conexão não é, como vimos, muito grande. Daí tratarem-se de (e serem persistentemente referidos como) "pequenos" ficheiros.

Assim, muitas vezes, recorrendo ao exemplo dos cestos de compras, os produtos selecionados são armazenados numa base de dados do *site web* e não no testemunho de conexão, no terminal do utilizador[89].

2.3. Classificação dos Testemunhos de Conexão

2.3.1. Os testemunhos de sessão e os testemunhos permanentes

A primeira grande distinção entre testemunhos de conexão é entre testemunhos de sessão e testemunhos permanentes.

Os testemunhos de sessão[90] são ficheiros temporários, armazenados na memória temporária enquanto o utilizador navega no *site* que lho(s) criou, de onde são apagados assim que o utilizador desliga o navegador.

Se o testemunho não tiver definido o atributo data de expiração, por defeito é, geralmente, suprimido assim que o utilizador encerra o navegador.

---

[88] BRAIN, Marchall, *How Internet Cookies Work*, HowStuffWorks, disponível em http://www.howstuffworks.com/cookie.htm, última consulta em 6 de setembro de 2012.

[89] O W3C está a desenvolver o "DOM Storage". Este mecanismo permitirá o armazenamento local de um elevado volume de dados no computador do utilizador através de scripts, com uma diferença substancial em relação aos testemunhos de conexão: as informações só serão transmitidas ao servidor por iniciativa do utilizador, em vez de o serem em todos os pedidos dirigidos ao servidor de origem.
Para mais informações sobre o Dom Storage, ver *Web Storage W3C Candidate Recommendation*, World Wide Web Consortium, de 8 de dezembro de 2011, disponível em http://www.w3.org/TR/webstorage/, última consulta em 4 de novembro de 2012.

[90] Também designados de *transient cookie* ou *in-memory cookie*.

Os testemunhos de sessão permitem que o servidor recorde os passos do utilizador durante a sua navegação entre as páginas do *site*, sem ter de solicitar informações que foram previamente dadas ou pedir a repetição de passos já dados: permite que o utilizador seja identificado durante aquela concreta visita e evitam que a cada página, a cada pedido ao servidor, o utilizador seja considerado sempre um novo e distinto visitante.

Se o testemunho tiver definida uma data de expiração – maior do que a que dura uma sessão – o testemunho é armazenado pelo navegador no disco rígido do utilizador e é reenviado ao servidor em todas as subsequentes visitas, até que a data definida seja atingida e, então, o testemunho de conexão é suprimido: é o chamado testemunho de conexão permanente[91].

Os navegadores mais recentes suportam as chamadas sessões de navegação "privadas" ou "anónimas" que não armazenam testemunhos que durem além da sessão – que são apagados assim que o utilizador fechar o navegador[92].

2.3.2. Os testemunhos de origem e os testemunhos de terceiros

Os testemunhos de origem são aqueles que são enviados pelos *sites* diretamente visitados pelo utilizador. O domínio (ou subdomínio) definido no testemunho corresponde àquele visível na barra de endereços do navegador.

---

[91] Também referido como *stored cookie* ("testemunho armazenado", em tradução livre).

[92] O Professor Menezes Leitão distingue entre *cookies passivos* e *cookies ativos*: "Os *cookies* passivos são opcionais e específicos de uma tarefa, destinando-se exclusivamente a reconhecer as páginas mais usadas do sítio e não transmitem dados que o utilizador não autoriza. Já os *cookies* activos são executados clandestinamente para obtenção de informações do utilizador, sem o seu consentimento. Entre estes são especialmente lesivos os *cookies* activos de transferência bruta, como no caso de instalação de *Applets Java* e controlos *Activex* no disco rígido do computador, que passam a acompanhar futuras visitas a *sites* que o utilizador realiza, ao mesmo tempo que verificam os dados pessoais existentes no computador, bem como outros *cookies* instalados, que revelam os gostos e preferencias do mesmo. Neste aspecto é normalmente referida a empresa *Doubleclick* que usa a tecnologia dos *cookies* para determinar o perfil comercial dos cibernautas, armazenando e comercializando os dados assim recolhidos.
Os *cookies* passivos não permitem retirar informações dos computadores, apenas podendo ser usados para armazenar informações que o utilizador forneceu de alguma maneira. (...)", MENEZES LEITÃO, Luís Manuel Teles de, *Os Testemunhos de Conexão (Cookies)*, Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles, 90 Anos, Almedina, 2007, p. 765.
Esta classificação, pela explicação avançada, não nos parece adequada. Mais, entendemos que induz em erro, já que não é verdade que os testemunhos de conexão sejam mecanismos capazes de "verificar os dados pessoais existentes no computador" ou de "retirar informações dos computadores".

Já os testemunhos de terceiros são, na perspetiva dos programas de navegação [93], aqueles que são enviados por domínio (ou subdomínio) diferente daquele que é visitado pelo utilizador e que aparece na barra de endereços do navegador.

Pode, pois, acontecer que a página *web* visitada pelo utilizador exiba conteúdos de um outro *site*, e.g. imagens ou anúncios publicitários.

O mecanismo dos testemunhos de terceiros vai permitir que um *site* que exiba conteúdos num outro envie testemunhos ao utilizador que não tem consciência de estar a ligar-se a este *site* terceiro, já que o pedido que deliberadamente fez não foi a esse *site*. Ou seja, o utilizador vai receber testemunhos com origem num *site* que não visitou diretamente.

O *site* que envia testemunhos é sempre visitado pelo navegador. Não é possível receber testemunhos de conexão de um *site* a que não se aceda. No entanto, o utilizador, no caso dos testemunhos de terceiros, não promove esse acesso e este só acontece porque estão incorporados conteúdo de *site*s terceiros em *site*s deliberadamente visitados.

Do mesmo modo que pode receber testemunhos de um *site* que não visita diretamente, o utilizador pode enviá-los em visitas subsequentes que tampouco promove deliberadamente. Essas visitas subsequentes ao *site* terceiro podem dar-se a partir de outro qualquer *site* que exiba conteúdo seu.

Imaginemos que o utilizador visita o *site* ***www.site1.com*** que, por sua vez, exibe uma imagem do *site* ***www.imagem.com***. O navegador envia um pedido ao ***www.site1.com*** e outro ao ***www.imagem.com***. Como resposta, o navegador vai receber duas mensagens, uma com origem em cada um dos *sites*. Ora, as respostas podem conter testemunhos de conexão (cabeçalhos *set-cookie*), que o navegador vai armazenar. Se o utilizador visitar o *site* ***www.site2.com*** que, por sua vez, também exibe uma imagem do *site*

[93] O Grupo do Artigo 29.º distingue o conceito de "testemunho de terceiros" no contexto da proteção de dados a nível europeu e na perspectiva dos programas de navegação, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão* (WP 194), de 7 de junho de 2012, p. 2, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_pt.pdf, última consulta em 30 de agosto de 2013.
Neste ponto do nosso trabalho, adotamos a noção de "testemunhos de terceiro" na perspectiva dos programas de navegação, por ser esta que melhor se enquadra na abordagem tecnológica por que optamos neste primeiro Capítulo. No Capítulo III vamos ver que a noção de testemunho de origem e testemunhos de terceiros adotada pelo Grupo do Artigo 29.º é a que decorre do contexto da proteção de dados a nível europeu.

www.imagem.com, na mensagem de pedido dirigida ao *site* ***www.imagem.com*** o navegador vai incluir o cabeçalho *cookie* com o testemunho que tinha armazenado pertencente àquele domínio. Nos dois casos, o utilizador não promoveu deliberadamente a visita ao *site* ***www.imagem.com***; o navegador só o visitou porque exibia conteúdo nos *sites* ***www.site1.com*** e ***www.site2.com***.

Os navegadores podem, pois, permitir que o utilizador bloqueie os testemunhos de terceiros. Podem faze-lo recusando o envio de cabeçalhos *cookie* em pedido a terceiros ou não processando um cabeçalho *set-cookie* recebido de terceiros[94].

2.4. Utilizações dos Testemunhos de Conexão

Os testemunhos de conexão melhoraram, inquestionavelmente, a experiencia dos utilizadores na *Web*. Com eles, a navegação é mais rápida e simples.

Não é uma coincidência que os testemunhos de conexão tenham estado presentes durante o crescimento exponencial da Grande Rede Mundial.

As vantagens conseguidas com a implementação deste mecanismo são inegáveis, não só para o servidor, mas também para o utilizador.

O mecanismo dos testemunhos de conexão, além do mais, permite a não repetição de mensagens e de passos, que prejudica a fluência da navegação, bem como a personalização da navegação.

Os testemunhos de conexão vêm sendo utilizados com variadas finalidades e servem distintos propósitos.[95]

[94] BARTH, A., *HTTP ...* RFC 6265, cit., p. 28. A especificação explica, ainda, que as politicas de bloqueio a testemunhos de terceiro são ineficientes porque os servidores podem contorná-las e monitorizar os utilizadores sem recorrer ao mecanismo dos testemunhos de conexão; e dá o exemplo de dois servidores colaborantes que podem monitorizar os seus utilizadores através de informação embutida nos URLs.

[95] Neste título, adotamos a sistematização e os cenários de utilização descritos no Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão: GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit..

Apesar de podermos individualizar as diferentes utilizações dos testemunhos de conexão, importa reter que o mesmo testemunho pode servir a diversas finalidades – "testemunhos polivalentes"[96].

Os testemunhos de conexão que permitem a identificação do utilizador ao longo de uma sessão que tenha iniciado são designados de "testemunhos de autenticação"[97]. Estes podem ser testemunhos de sessão ou testemunhos permanentes.

Quando um *site web* permite o acesso a conteúdos autorizados através da autenticação dos utilizadores, o recurso aos testemunhos de autenticação torna possível que o utilizador possa navegar pelas páginas do *site* sem que tenha de reinserir os dados da sua conta em cada nova página por que navegue no *site*, a cada solicitação ao *site*.

É o que acontece quando o utilizador se autentica, por exemplo, através do sistema *login-password*. Num primeiro momento, o utilizador autentica-se, o *site* identifica de que utilizador se trata e envia um testemunho que contém um identificador de sessão que o *site* passa a associar àquele utilizador e que lhe vai ser reenviado pelo navegador em todos os pedidos subsequentes ao *site* – isto no caso de o testemunho de autenticação ser um testemunho de sessão.

No caso dos testemunhos de autenticação permanentes, pode mesmo acontecer que testemunho previamente armazenado no terminal do utilizador seja enviado pelo navegador ao *site* no primeiro pedido que dá inicio à sessão e se substitua ao sistema de autenticação, ou seja, que as credenciais de acesso não sejam solicitadas para aceder a um conteúdo autorizado e o acesso seja permitido com base na receção da informação de testemunho que o *site* tinha previamente associado a uma conta – as informações contidas no testemunho podem mesmo ser as próprias credenciais de acesso. [98]

[96] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 6.
[97] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 7.
[98] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 7 e 8.

Por sua vez, os "testemunhos alimentados pelo utilizador" [99] são aqueles que visam conservar os dados inseridos pelo utilizador ao longo da sessão e não são, comummente, mais do que um número de identificação gerado aleatoriamente pelo *site*. (Os testemunhos alimentados pelo utilizador permitem que os artigos selecionados sejam memorizados no mecanismo do "cesto de compras".) [100]

Os testemunhos de conexão podem ser utilizados para finalidades de reforço da segurança da navegação na *web*. Os "testemunhos de segurança centrados no utilizador"[101] são testemunhos permanentes que se destinam a proteger os sistemas de início de sessão. Com recurso a este mecanismo, é possível ao *site* reagir contra uma sequência registada de tentativas de início de sessão sem sucesso. [102]

Os dados técnicos necessários à reprodução de conteúdos vídeo ou áudio são armazenados nos chamados "*flash cookies*"[103].

Trata-se de testemunhos que não devem ter tempo de vida superior ao necessário para a reprodução do conteúdo a que servem.

No entanto, a utilização deste tipo de testemunhos de conexão tem ido muito para além deste propósito de permitir a reprodução de conteúdos.

O Flash corre no cliente e dispõe de espaço de armazenamento no terminal do utilizador que é usado como uma "porta dos fundos" para a implementação de testemunhos de conexão. Os *flash cookies* são, assim, muitas vezes usados para contornar políticas de privacidade que imponham ou permitam restrições à monitorização dos utilizadores.

---

[99] Ou *user input cookies*.
GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 7.
[100] Sobre os "testemunhos alimentados pelo utilizador" ver GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 7.
[101] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.
[102] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.
[103] *Flash cookies* por referência à tecnologia *Adobe Flash*. É a tecnologia utilizada, ainda, por muitos fornecedores de jogos on-line de que se destacam os massivamente presentes nas redes sociais.
O Grupo de Trabalho do Artigo 29.º para a Proteção de dados designa este tipo de testemunhos de "testemunhos de sessão criados por um leitor multimédia", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.
Sobre os "testemunhos de sessão criados por um leitor multimédia" ver GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.

É possível que os sites armazenem uma cópia do testemunho nesse espaço destinado ao Flash que será utilizada para recriar o testemunho caso seja apagado. São os chamados "testemunhos zombie".

Os testemunhos de conexão podem, também, ser utilizados com a finalidade de equilibrar a carga entre os servidores. Trata-se de testemunhos de sessão que permitem ao *site web* distribuir o tratamento dos pedidos pelos seus servidores. Assim, o testemunho vai identificar o servidor em que teve origem e para o qual deve ser reenviado, estabelecendo que aquela sessão daquele cliente se processará com aquele concreto servidor do *site*. O objetivo da informação contida no testemunho é permitir identificar as extremidades da comunicação.[104]

Os "testemunhos de personalização da interface do utilizador"[105], que podem ser de sessão ou permanente, permitem armazenar as preferências reveladas por este, como a língua[106], a cor de fundo, o tamanho da letra, o número de resultados, entre tantos outros. Trata-se de preferências manifestadas ativamente pelo utilizador (através de um *click* num botão ou da validação de uma opção expressando a sua preferência).[107]

Os "testemunhos relativos a módulos de extensão (plug-in) para partilha de conteúdos em redes sociais"[108] são aqueles que permitem a partilha de conteúdos disponibilizados em diferentes *sites* na *web* ou a identificação perante estes *sites* com recurso à conta que o utilizador já tem na rede social[109], que lhe vai permitir, por exemplo, comentar o conteúdo do *site*. Para isto, os *sites* optam pela integração dos chamados "módulos de extensão para partilha de conteúdos" que dão acesso aos testemunhos

[104] Sobre os "testemunhos de sessão para equilibrar a carga" ver GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.
[105] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 9.
[106] Importa reter que os *sites* conhecem o IP das maquinas de onde provêm os pedidos e podem definir a língua em que o site (multilíngue) é apresentado com base na localização do utilizador, sem necessitar de recorrer ao mecanismo dos testemunhos de conexão.
[107] Sobre os "testemunhos de personalização da interface do utilizador" ver GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 9.
[108] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 9.
[109] A utilização de um sistema de autenticação centralizado permite o aceder a uma diversidade de *websites* a partir de uma única conta já existente.

armazenados no terminal do utilizador que vão permitir à rede social identificar os utilizadores.

Mais uma vez, podem estar em causa testemunhos de sessão ou testemunhos permanentes.[110]

Os testemunhos de conexão são, também, utilizados para a obtenção de indicadores importantes sobre e para a estratégia em linha. É a chamada "analítica"[111].

Recorrendo aos testemunhos, os *sites* conseguem medidores estatísticos que lhes permitem analisar tendências. Os *sites* podem recorrer aos testemunhos para contabilizar o número de visitantes e perceber, por exemplo, as páginas mais visitadas dentro do *site*, em que páginas os visitantes passam mais tempo, entre tantos outros indicadores. A analítica pode ser "de origem"[112] ou "de terceiros", consoante o domínio de onde provenham os testemunhos.

Os testemunhos de conexão são massivamente usados para a monitorização da atividades dos utilizadores em linha. São os chamados "*tracking cookies*".

As empresas viram, desde cedo, nos testemunhos de conexão um meio eficaz de obter indicadores importantes sobre e para a sua estratégia em linha. Assim, recorrendo aos testemunhos, os *sites* podem analisar tendências, contabilizar visitantes, descobrir preferências. Com recurso aos testemunhos, os *sites web* conseguem dados estatísticos relevantes sobre a atividade e os hábitos de navegação dos seus utilizadores.

Os testemunhos de terceiros vêm permitir a monitorização da atividade levada a cabo não dentro do mesmo *site web* mas através de diferentes *sites web*[113].

---

[110] Sobre os "testemunhos relativos a módulos de extensão (plug-in) para partilha de conteúdos em redes sociais" ver GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 9 e 10.
[111] Na terminologia do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 11 e 12.
[112] Sobre os testemunhos de conexão utilizados para "analítica de origem" ver GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 11 e 12.
[113] "Tracking is the collection and correlation of data about the Internet activities of a particular user, computer, or device, over time and across non-commonly branded websites, for any purpose other than fraud prevention or

Ao permitirem a monitorização da atividade dos utilizadores ao longo do tempo, os testemunhos de conexão vêm permitir a criação de perfis dos utilizadores[114].

Os perfis criados podem ser implícitos os explícitos[115]. Os primeiros são criados por inferência a partir da observação dos comportamentos individuais e coletivos ao longo do tempo e os segundos recorrem aos dados pessoais que os próprios utilizadores fornecem aos serviços *web*. As duas técnicas podem ser combinadas.

O recurso a testemunhos de terceiros permite monitorizar a atividade dos utilizadores através de diferentes *sites web* e criar perfis muito mais pormenorizados.

Os testemunhos de conexão não são um mecanismo imprescindível ou exclusivo da monitorização ou da criação de perfis on-line. No entanto, permitem fazê-lo com maior facilidade e mais pormenor[116].

Os testemunhos de conexão são, ainda, utilizados para a publicidade em linha. Esta representa uma das principais fontes de rendimento em linha, contribuindo para o crescimento e expansão da economia da Internet, e pode ser contextual, segmentada ou comportamental.

A publicidade contextual limita-se à seleção de anúncios com base no conteúdo que o utilizador está a visualizar ou a pesquisar no momento em que aqueles lhe são apresentados.

A publicidade segmentada tem por base características do utilizador, que ele mesmo fornece, como a idade ou o sexo.

Por sua vez, a publicidade comportamental baseia-se no comportamento assumido pelo utilizador e que é monitorizado.[117]

---

compliance with law enforcement requests", CORRY, Bil Corry e STEINGRUEBL, Andy, *Where is the Comprehensive Online Privacy Framework?*, Position Paper for W3C Workshop on Web Tracking and User Privacy, Princeton, NJ, abril de 2011.

[114] Definição de perfis, ou *profiling*.

[115] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental em linha* (WP 171) , de 22 de Junho de 2010, p. 8, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf, última consulta em 30 de agosto de 2013.

[116] "Although cookies are not the only mechanism servers can use to track users across HTTP requests, cookies facilitate tracking because they are persistent across user agent sessions and can be shared between hosts.", BARTH, A., *HTTP ...* RFC 6265, cit., p. 28

Os anunciantes recorrem à possibilidade de monitorizar a atividade dos utilizadores na *web* para criar perfis dos utilizadores (*profiling*) e dirigir-lhes publicidade extremamente incisiva. A forma mais comum de o fazer é com recurso a testemunhos persistentes de terceiros.

Assim, é possível que quando um utilizador visita um *site web* que exiba um conteúdo (publicidade) de um terceiro, este *site* terceiro envia um testemunho de conexão que o navegador vai armazenar e reenviar numa próxima visita. A próxima visita ao *site* terceiro pode, porém, dar-se não só a partir do mesmo *site*, mas de um qualquer *site* que exiba conteúdo seu.

Isto vai permitir ao *site* terceiro monitorizar a atividade dos utilizadores através de diferentes *sites web*.

No entanto, a publicidade comportamental em linha processa-se, ainda, com recurso às chamadas redes de publicidade. Estas envolvem anunciantes (aqueles que pretendem promover um produto ou serviço), editores (os proprietários de *sites web* que procuram obter receitas com a venda de espaços publicitários nas suas páginas) os fornecedores de redes de publicidade (que estabelecem a ligação entre os anunciantes e os editores e controlam os critérios que vão estar na base do endereçamento personalizado da publicidade).[118]

No contexto das redes de publicidade, o fornecedor da rede é o *site* terceiro que vai alojar conteúdos (publicidade dos produtos dos anunciantes) no(s) site(s) que o utilizador diretamente visita (editores). Os fornecedores de redes de publicidade conseguem, desta forma, traçar perfis dos utilizadores muito mais pormenorizados do que seria possível a um anunciante isolado.[119]

---

[117] GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* … , cit., pp. 4 e 5.

[118] Adotamos a terminologia proposta pelo Grupo do Artigo 29: GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., p. 5.

[119] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., p. 5.
O Grupo de Trabalho do Artigo 29.º para a Proteção de Dados refere a colaboração que as grandes redes de publicidade mantêm com muitas outras redes secundarias e dá como exemplo a lista de parceiros do *Google Adsense*, (disponível em http://www.google.com/support/adsense/bin/answer.py?answer=94149) e a lista de parceiros do *Yahoo!*, (disponível em http://info.yahoo.com/privacy/us/yahoo/thirdparties/), GRUPO DO ARTIGO 29.º

A publicidade na *web* compreende duas partes: a escolha do anúncio a enviar na resposta a um pedido e o próprio envio do anúncio[120]. É a escolha do anúncio que depende da definição de perfis[121].

A publicidade baseia-se, então, no comportamento assumido pelo utilizador e que é monitorizado. Os anúncios exibidos são personalizados, de acordo com os interesses, hábitos e preferências de cada utilizador.

2.5. Os testemunhos de conexão e a privacidade online

Os testemunhos de conexão são, portanto, uma tecnologia que permite não apenas manter o estado nas conexões HTTP, mas que é, também, utilizada com várias outras finalidades, muito distintas.

Apesar de se tratar de um mecanismo, por si só, inócuo, as utilizações que dele podem ser feitas levantam sérios problemas, de entre os quais se destacam os relacionados com a violação do direito à privacidade dos utilizadores da *web*[122].

Desde logo, o mecanismo dos testemunhos de conexão foi largamente utilizado sem que fosse dado ao utilizador conhecimento disso, sem que este fosse notificado de que os testemunhos estavam a ser armazenados no seu terminal pelo seu navegador *web*, sem que fosse chamado a dar o seu consentimento para tal.

PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 6, nota de rodapé n.º 6.

[120] KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., pp. 14 e 15.

[121] *Profiling*.

[122] "Cookies are inherently neither good nor bad. They can enhance web applications, and they can be used to invade privacy; technology alone cannot distinguish good uses from bad. In fact, just labeling a use as "bad" is highly subjective.", KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., p. 18.
"The HTTP State Management mechanism is both useful and controversial. It is useful because numerous applications of HTTP benefit from the ability to save state between HTTP transactions, without encoding such state in URLs. It is controversial because the mechanism has been used to accomplish things for which it was not designed and is not well-suited. Some of these uses have attracted a great deal of public criticism because they threaten to violate the privacy of web.". MOORE, K. E FREED, N., *Use of HTTP State Management, RFC 2964*, The Internet Engineering Task Force (IETF), de outubro de 2000, p. 1, disponível em https://tools.ietf.org/html/rfc2964 , última consulta em 20 de novembro de 2012.

Os testemunhos estavam desenhados para ser transmitidos e armazenados discretamente, sem alertar o utilizador – sem que a sua intervenção fosse necessária ou reclamada em qualquer momento.

Os testemunhos de conexão vieram permitir uma monitorização muito pormenorizada dos utilizadores na *web*.

Como vimos, os testemunhos de conexão surgiram em 1994, no seio da *Netscape*.

Apesar de terem sido desenvolvidos para manter o estado nas conexões HTTP de modo a tornar eficiente o mecanismo do cesto de compras na *web*, Lou Montulli desde cedo admitiu que estes poderiam ter outras utilizações[123].

Como escreveu John Schwartz, Lou Montulli sentou-se ao seu teclado para resolver um dos maiores problemas da *World Wide Web*, mas acabou por criar outro[124].

A existência dos testemunhos de conexão, e a capacidade de monitorização que este mecanismo permitia da atividade dos utilizadores em linha, só foi exposta à consciência pública, em 1996, como realçam Rajiv C. Shah e Jay P. Kesan[125]. Em 12 de Fevereiro de 1996, o *Financial Times* publicou aquele que é apontado como o primeiro artigo a expor publica e mediaticamente os testemunhos de conexão, da autoria de Tim Jackson, sob o título "*This Bug in Your PC is a Smart Cookie*"[126]. No dia seguinte, Lee Gomes publicava um artigo de conteúdo semelhante no *San Jose Mercury News*, com o título "*Web cookies May Be Spying on You*"[127].

[123] SCHWARZ, John *Giving the Web...* , cit..
[124] "One day in June 1994, Lou Montulli sat down at his keyboard to fix one of the biggest problems facing the fledgling World Wide Web — and, as so often happens in the world of technology, he created another one." SCHWARZ, John *Giving the Web...* , cit..
[125] SHAH, Rajiv C. E KESAN, Jay P., *Deconstructing Code*, op. cit., pp. 300 e ss..
[126] "Este *bug* no seu Computador é um Testemunho de Conexão", em tradução livre.
[127] "Os Testemunhos de Conexão podem estar a espiá-lo", em tradução livre.

David M. Kristol [128] conta que os participantes da discussão da especificação dos testemunhos de conexão inesperadamente se viram na interceção da tecnologia com a política, à medida que as questões relacionadas com a privacidade despertavam inquietações no seio do grupo e iam levantando vozes na opinião pública e nos centros de decisão política.

Koen Holtman, participou no Grupo de Trabalho do HTTP onde começou a discussão tendente à especificação da IETF dos testemunhos de conexão. Holtman, holandês, foi o principal responsável pelas questões levantadas a propósito das implicações do mecanismo na privacidade dos utilizadores da *web*. As suas inquietações transmitiam a posição dos europeus, que esperavam que o seu direito à privacidade não fosse posto em causa na *web*[129].

Foi Holtman quem chamou a atenção, desta feita já no entretanto formado subgrupo, para a possibilidade de, por acordo entre diferentes *sites*, poderem ser enviados testemunhos por terceiros.

Sobre as chamadas "transações não verificáveis" o utilizador não teria qualquer controlo. O utilizador teria controlo sobre os *sites* que deliberadamente visita – no limite tem a opção de os visitar ou não. Mas não teria qualquer controlo sobre as transações registadas entre o seu navegador e os *sites* terceiros que exibem conteúdos naqueles que deliberadamente visita.

Em 1996, a *Netscape* programou o seu navegador para distinguir entre testemunhos de origem e testemunhos de terceiros. Os utilizadores podiam, agora, recusar que o seu navegador *Netscape* armazenasse testemunhos de conexão no seu terminal ou recusar apenas que armazenasse testemunhos de terceiros.

Estes mecanismos de controlo foram incorporados, também, nos navegadores que entretanto surgiram, já que todos eles suportavam o mecanismo dos testemunhos de conexão.

[128] KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., p. 13.
[129] KRISTOL, David M., *HTTP Cookies: Standards,...* , cit., p. 25 e SCHWARZ, John *Giving the Web...* , cit..

O RFC 2109 veio recomendar os navegadores *web* a recusar testemunhos de terceiro (ou, como então eram chamados, as "transações não verificadas") ou, se os permitissem, que pudessem ser controlados pelo utilizador através de uma opção que, por defeito, os rejeitaria.

No entanto, já eram muitos os modelos de negócio que assentavam nas potencialidades permitidas pelos testemunhos de terceiro e, na prática, as recomendações do RFC 2109 e, depois e no mesmo sentido, do RFC 2965 acabaram por não ter implementação na prática.

Por defeito, os navegadores continuaram a permitir todos os testemunhos de conexão.

Os testemunhos de conexão já se tinham afirmado como uma realidade incontornável na *web*.

As empresas de publicidade descobriram as potencialidades dos testemunhos de conexão.

Como relata Schwartz[130], a DoubleClick e a Engage puseram em prática uma técnica que a comunidade científica já tinha teorizado: através da exibição de anúncios em diferentes *sites*, estas empresas conseguiam utilizar os mesmos testemunhos de conexão em diferentes *sites* da rede, o que lhes permitia reconhecer o mesmo visitante[131] em todos eles. Esta técnica da introdução dos chamados testemunhos de terceiro para a publicidade em linha veio permitir a criação de perfis muito mais detalhados e abrangentes da atividade dos utilizadores na rede.

A monitorização dos utilizadores na *web* estava longe de ser um objetivo abrangido pela ambição de Montulli. O pai dos testemunhos de conexão, aquando do desenvolvimento do mecanismo, recusou a hipótese da atribuição de um número de identificação único a cada computador que permitisse manter o estado nas conexões HTTP, precisamente para salvaguardar a privacidade dos utilizadores da *web*.

[130] SCHWARZ, John *Giving the Web...* , cit..
[131] I.e., identificar o navegador.

Como explicam James F. Kurose, Keith W. Ross[132], os testemunhos de conexão muitas vezes não são mais do que um número de identificação, que permite ao *site web* reconhecer o navegador que já o visitou.

Através de um número de identificação o servidor pode, de facto, monitorizar a atividade dos seus utilizadores. O *site* facilmente sabe por que ordem o utilizador a que foi atribuído determinado número de identificação navegou entre as suas páginas, e a que horas o fez.

Os testemunhos de conexão permitem a associação eficaz de vários dados, recolhidos de diversas formas.

Como vimos, a mensagem de pedido HTTP pode conter outros cabeçalhos com informações que o cliente fornece ao servidor[133].

O HTTP *referer*, por exemplo, é um cabeçalho que permite ao servidor saber de onde veio o pedido. Ou seja, o *site web* a que se destina o pedido fica a saber o URL anteriormente visitado.

A combinação desta informação com a utilização dos testemunhos de conexão permite a monitorização da atividade dos utilizadores muito para além da que é realizada no próprio *site*.

Os anunciantes podem, então, associar e armazenar dados sobre os utilizadores, ainda que anonimamente.

Com base num testemunho de conexão permanente, o anunciante consegue associar todos os *site*s da rede que o utilizador com o número de identificação "ID=user1" visitou e determinar quais os seus hábitos e preferências. [134]

Os testemunhos de conexão funcionam sem que se conheça a identidade do visitante, bastando a atribuição de um número de identificação único e anónimo.

[132] Ver KUROSE, James F. e ROSS, Keith W., *Computer networking a ...*, op. cit., pp. 108 a 110.
[133] Título 1.2.1. deste Capítulo I.
[134] Na prática, estas operações costumam ser contratadas pelos anunciantes a prestadores de redes de publicidade.

O servidor não tem como saber, usando o mecanismo dos testemunhos sem mais, a identidade do utilizador.

Contudo, se o utilizado se registar no *site*, preenchendo um formulário onde indica o seu nome e outras informações, o *site* pode, então, associar o número de identificação atribuído com esses dados.

A combinação do mecanismo dos testemunhos com outras informações é pode possibilitar a associação da identidade atribuída com a identidade real do utilizador.

(Convém fazer um parênteses para realçar que o testemunho de conexão identifica a seguinte combinação: computador, navegador e, se for o caso, conta de utilizador. Um utilizador pode ter vários computadores e/ou navegadores e/ou várias contas de utilizador e terá, por isso, diferentes testemunhos de conexão atribuídos e armazenados a cada um dos navegadores instalados nos diferentes computadores e cada conta. Do mesmo modo, quando não exista conta de utilizador, o mesmo navegador pode ser utilizado por várias pessoas que, devido ao reenvio pelo navegador ao *site* do mesmo testemunho armazenado, vão ser reconhecidas por este como tratando-se do mesmo utilizador.)

A combinação de todas as informações recolhidas (que o utilizador forneceu; que o servidor conhece por necessidades imperiosas à comunicação [135]; que foram fornecidas como informações adicionais no cabeçalho HTTP) com os testemunhos de conexão torna-os um poderosíssimo mecanismo de monitorização, que levanta sérias e preocupantes questões relacionadas com a privacidade dos utilizadores da *web*[136].

[135] Como o endereço de IP, que o site precisa de conhecer para saber a quem enviar a sua resposta.

[136] Um caso que mereceu a atenção mediática e despertou a preocupação geral foi a anunciada compra da Abacus Direct pela DoubleClick, em 1999. A Abacus possuía uma vasta base de dados com os hábitos de compra de milhares de pessoas identificadas (nome, morada, telefone, etc.). A possibilidade de a DoubleClick cruzar os dados resultantes da sua monitorização dos utilizadores anónimos feita através da publicidade que exibia na *web* com esses dados gerou uma onda de consternação e críticas generalizada. O cruzamento das informações das duas bases de dados acabou por não acontecer.
Apesar de os testemunhos de conexão facilitarem a monitorização dos utilizadores da *web*, a combinação de informações a este nível já sai do domínio do nosso trabalho, mas não podíamos deixar de chamar a atenção para os alarmantes perigos potenciais do cruzamento de informações obtidas por diferentes meios, quando algum desses meios se recorre do mecanismo dos testemunhos de conexão.
Sobre o caso referido da anunciada compra da Abacus Direct pela DoubleClick, ver HEMPHILL, Thomas A., *DoubleClick and Consumer Online Privacy: An E-Commerce Lesson Learned*, em *Business and Society Review,* Volume 105, Issue 3, pp 361 a 372, 2000.

O RFC 6265, na linha do seu proposto objetivo de se limitar a descrever aquela que era a real implementação dos testemunhos de conexão na prática, constata que as políticas dos diferentes navegadores variam significativamente no que aos testemunhos de terceiros concerne e opta por expressamente não adotar uma política sobre testemunhos de terceiros. Afastou-se, assim, da posição firme – e falhada – dos documentos anteriores.

A especificação mostra-se consciente de que uma política proibitiva pode dificultar a monitorização, mas não a pode impedir – já que esta não depende exclusivamente do uso dos mecanismos de conexão.

Recomenda, no entanto que os navegadores permitam aos utilizadores gerir os testemunhos de conexão armazenados no seu terminal, o que inclui apaga-los e rejeitá-los (o que implica o não processamento dos cabeçalhos *set-cookie* e a não inclusão de cabeçalhos cookie nos pedidos HTTP). Recomenda, ainda, que seja dada aos utilizadores a opção de não armazenar testemunhos entre sessões, i.e. testemunhos persistentes[137].

A privacidade dos utilizadores na *web* é, incontornavelmente, uma questão associada à utilização do mecanismo dos testemunhos de conexão[138].

A abordagem da comunidade científica no sentido de proteger a privacidade[139] dos utilizadores da *web* que pode ver-se ameaçada pela utilização de mecanismos como o dos testemunhos de conexão, não se tem limitado às recomendações expressas nas especificações dos testemunhos de conexão.

Preocupado com as questões que envolvem a privacidade na *web*, o W3C desenvolveu a *Plataform for Privacy Preferences* (P3P).

[137] Esta faculdade é concedida, na prática, por funcionalidades de navegação privada ou anónima.
[138] Não vamos analisar os ataques informáticos que têm por objetivo aceder, alterar ou eliminar as informações compreendidas nos testemunhos de conexão por se tratar de questões que fogem ao âmbito do nosso trabalho.
[139] E, muito importante e diretamente relacionada com a privacidade dos utilizadores da web, é a sua confiança na plataforma. A web é uma plataforma de negócios. As empresas – inclusivamente as de publicidade – não podem arriscar pôr em causa a confiança que os utilizadores ainda demonstram ao fazer uso de muitos dos serviços disponíveis na rede.

O P3P é uma especificação que permite aos *sites* expressar as suas políticas de privacidade de uma forma que pode ser automaticamente interpretada pelos navegadores, de modo a dispensar-se os utilizadores da necessidade de ler a política de privacidade de cada *site*. As políticas de privacidade dos *sites* – em particular, as informações que recolhem e os usos que lhes dão – devem, de acordo com o P3P, ser expressadas não só em linguagem compreensível aos utilizadores mas, também, às máquinas – aos navegadores –, que através de interfaces ajudam o utilizador a melhor compreender esses políticas e a tomar decisões automatizadas sobre elas.

Mais, de acordo com o W3C, a imprevisibilidade dos atuais mecanismos de bloqueio de testemunhos de conexão é um problema para os que desenvolvem serviços dependentes da manutenção de estado nas ligações HTTP. Com o P3P os comportamentos dos navegadores perante estas tecnologias devem tornar-se previsíveis e os efeitos da implementação do P3P podem mesmo servir como um incentivo à alteração da abordagem feita até aqui pelos *sites* de publicidade e de comércio eletrónico[140].

Mas, a especificação[141], datada de Abril de 2002, resultou demasiado complexa e, na prática, o P3P não conhece significativa implementação.

Uma tecnologia mais simples e já suportada pela maioria dos navegadores é o cabeçalho HTTP "Do Not Track" (DNT). Trata-se de linha de cabeçalho introduzida pelo navegador no pedido HTTP que indica ao servidor que o utilizador se opõe a ser monitorizado. O Grupo de Trabalho "Tracking Protection" do W3C, formado em setembro de 2011, está a trabalhar na especificação deste cabeçalho.

---

[140] Platform for Privacy Preferences (P3P) Project - *Enabling smarter Privacy Tools for the Web*, disponível em http://www.w3.org/P3P/, última consulta em 3 de março de 213.

[141] CRANOR, Lorrie, LANGHEINRICH, Marc, MARCHIORI, Massimo, PRESLER-MARSHALL, Martin e REAGLE, Joseph, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C Recommendation, 16 April 2002 http://www.w3.org/TR/P3P/, última consulta em 3 de março de 213.
O Grupo de Trabalho para o P3P publicou, em 13 de novembro de 2006, a The "Platform for Privacy Preferences 1.1 (P3P1.1) Specification", incluindo as alterações entretanto discutidas mas que não foi suficiente para que, na prática, a tecnologia conhecesse significativa implementação. CRANOR, Lorrie, HOGBEN, Giles, LANGHEINRICH, Marc, MARCHIORI, Massimo, PRESLER-MARSHALL, Martin, REAGLE, Joseph e SCHUNTER, Maltthias, *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*, W3C Working Group Note 13, novembro, 2006, disponível em http://www.w3.org/TR/P3P11/, última consulta em 3 de março de 2013.

A privacidade na *Web* não é uma questão exclusivamente tecnológica. Como vimos, os testemunhos de conexão são discutidos na convergência dos campos tecnológico e político.

Por poderem pôr em causa a privacidade dos cidadãos, os testemunhos de conexão são, hoje, objeto de regulação jurídica.

Capítulo II O Quadro Legislativo Europeu da Proteção de Dados

1. Da Proteção da Privacidade à regulação do Tratamento de Dados Pessoais

Para melhor compreendermos as opções legislativas que vêm regular a utilização de testemunhos de conexão, devemos começar por perceber como surgiu a necessidade de proteger juridicamente a privacidade das pessoas e regular a matéria dos dados pessoais, uma vez que é neste contexto que se insere aquela matéria.

O direito à proteção de dados pessoais evoluiu da ideia de privacidade.

O desenvolvimento tecnológico, que confrontou a sociedade ocidental do século XX com novos e complexos desafios, contribuiu de modo decisivo para a evolução e conformação deste direito.

A privacidade é reconhecida pelas diversas sociedades humanas, desde as civilizações mais antigas. Representa, porém, um valor dinâmico, com um objeto tão amplo e abrangente quanto vago[142].

Como tão bem sistematiza Teresa Coelho Moreira [143], podemos analisar a evolução da privacidade sob duas perspetivas: uma historicista e outra racionalista.

A aproximação historicista foca-se na possibilidade de estudar e perceber a privacidade em diferentes épocas e sociedades[144], enquanto que

[142] Neste sentido, MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo eletrônico do empregador*, Almedina, 2010, pp. 106 e ss..

[143] MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos Trabalhadores ...* ,op. cit., pp. 105 e ss..

[144] "Em relação ao percurso histórico da privacidade distinguiram-se diversos momentos: em primeiro lugar, o fenómeno da propensão do ser humano para procurar um espaço próprio longe dos demais e sem o olhar indiscreto dos restantes cidadãos; depois, o aparecimento da necessidade de privacidade e, consequentemente, a gestação da ideia e reivindicação teórica; e, por último, a formulação técnico-jurídica do direito à privacidade, primeiro ligado ao direito de propriedade e, depois, como um direito fundamental autónomo com legislação própria – é a passagem da *privacy property* para a *privacy personality*", MOREIRA, Teresa Alexandra Coelho, A Privacidade dos ..., op. cit., p. 109.

a aproximação racionalista situa o surgimento do direito à privacidade num determinado contexto histórico.

A ideia da privacidade, do direito ao espaço próprio inviolável de cada um – de um tempo ou um espaço para si distante de todos os outros –, pode ser encontrada ao longo da história da humanidade como uma evolução lógica da salvaguarda da individualidade no seio da coletividade.

Como nos ensina a Ilustre Professora, "numa perspetiva historicista, a privacidade é um fenómeno constante que aparece em todas as sociedades humanas ligadas ao sentimento de territorialidade" [145] . A perspetiva historicista, "pretende encontrar vestígios de privacidade, tentando demonstrar a aspiração humana à sua proteção"[146].

Referências à privacidade são, pois, encontradas ao longo da história da humanidade, desde a Antiguidade, nas mais diferentes sociedades e institutos.

A procura do isolamento, do espaço e do tempo longe dos outros, é uma característica transversal a todos os homens, em todas as sociedades.

É esta procura que vai resultar na necessidade da privacidade, necessidade essa que, uma vez reconhecida, lança a base para a formulação jurídica do direito à privacidade[147].

Por sua vez, a abordagem realista, "permite determinar com precisão o momento em que numa sociedade baseada numa determinada classe social – no caso a classe burguesa – se produz a conjuntura para que aqueles fenómenos isolados de demonstrações de privacidade se concretizem na formulação jurídica de um direito com vocação de generalidade"[148].

[145] MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 109.
[146] MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 114.
[147] Sobre a evolução histórica da privacidade ver MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., pp. 105 e ss..
[148] "Parece ser possível a convivência das duas teorias já que não se afigura discutível defender que a ideia de privacidade pode estar presente em modelos sociais muito diferentes – desde a Antiguidade até aos nossos dias – e considerar que a época concreta em que, na história do Ocidente, surgiu o conceito jurídico deste direito coincide com a ascendência da burguesia. Parece, pois, que a teoria racionalista permite determinar com precisão o momento em que numa sociedade baseada numa determinada classe social – no caso a classe burguesa – se produz a conjuntura para que aqueles fenómenos isolados de demonstrações de privacidade se concretizem na formulação jurídica de um direito com vocação de generalidade.", MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., pp. 118 e 119.

A formulação jurídico-doutrinal do direito à privacidade acontece em 1890, no famoso artigo "*The right to privacy*"[149], da autoria dos advogados Samuel Warren e Louis Brandeis. Este artigo marca o início da autonomização do direito à privacidade[150].

Como sintetiza Catarina Sarmento e Castro[151], Warren e Brandeis batizaram como "«*right to be let alone*»[152] aquilo que seria "um «*right against the world*», destinado a proteger da «curiosidade popular» variadas dimensões da personalidade". Os autores adotaram a expressão utilizada pelo juiz Thomas Cooley, nesse mesmo ano de 1980, que referiu "a right of complete immunity: to be let alone"[153], identificando-lhe o conteúdo[154].

O direito à privacidade, até então, era protegido mediante o recurso à violação do direito da propriedade privada[155], à violação da confidencialidade, da confiança, ou de uma obrigação de tipo contratual.

Dá-se a "passagem da *privacy property* para a *privacy personality*" [156]. A formulação técnico-jurídica do direito à privacidade desprende-se do direito de propriedade [157] e consagra-se como um direito autónomo, ligado à personalidade.

---

[149] WARREN, Samuel e BRANDEIS, Louis, *The right to privacy*, em "Harvard Law Review", Vol. IV, n.º 5, 15 de dezembro de 1890, disponível em http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm, última consulta em 3 de março de 2013.

[150] Neste sentido, MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., pp. 117 e ss., e CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005, p. 17, e MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*, 2ª Edição Refundida e Atualizada, Almedina, Coimbra, 2006, pp. 140 e 141.

[151] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 17 e 18.

[152] "O direito a estar só ou a ser deixado só", MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 114.

[153] GLENN, Ricard A., *The right to privacy: rights and liberties under the law*, ABC-Clio, Inc. Santa Bárbara, Califórnia, 2003, p. 4.

[154] No entanto, a perspectiva de Warren e Brandeis apenas veio a ser acolhida pelo tribunais americanos em 1905, no processo Pavasich v New England Live Insurace Co., em que o Georgia Supreme Court reconheceu a existência de um direito à privacidade; cf. CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 18.
A autora refere, ainda, outras importantes decisões jurisprudências que se inserem no contexto histórico da autonomização do direito à privacidade CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 17 a 19.

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

[156] MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 109.

[157] Mas a defesa daquilo que hoje reconhecemos como direito à privacidade não se fazia apenas com recurso à violação ao direito de propriedade. "(...) a proteção do Direito para aspectos da personalidade humana que até aí [até à publicação do artigo de Warren e Brandeis, WARREN, Samuel e BRANDEIS, Louis, *The right to privacy*, Harvard Law Review, Vol. IV, n.º 5, 15 de dezembro de 1890], apenas haviam sido jurisprudencialmente protegidos mediante o recurso à violação do direito da propriedade privada, à violação da confidencialidade, da confiança, ou de uma obrigação de tipo contratual.", CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 17.

Com o desenvolvimento tecnológico, o direito à privacidade conhece novos desafios.

O século XX veio consagrar a esfera privada na organização da vida social, por oposição à esfera pública. Dá-se a democratização da privacidade[158].

As novas ameaças, que nos finais do século XIX e inícios do século XX se prendiam com o crescimento da imprensa escrita, associada à imagem fotográfica, impunham como objetivo a criação de um sistema que defendesse a privacidade das pessoas[159].

O direito à privacidade consolidava-se como direito de exclusão dos demais da vida privada de cada um. Era um direito de aceção negativa[160]. Visava garantir a não ingerência de todos os outros na vida privada de cada indivíduo.

Estava lançado o gérmen daquilo que viria a ser o direito à autodeterminação informativa[161]. A faculdade de um individuo se negar ou opor à recolha e difusão de informações que lhe digam respeito, apresentava-se como uma garantia do direito à privacidade.

A privacidade impôs-se como um direito fundamental, ligado à dignidade da pessoa humana. A sua relevância afirma-se tanto na esfera

[158] BOTTMANN, Denise e BRUCHARD, Dorothée de, *História da Vida Privada*, Da Primeira Guerra a nossos dias, Editora Schwarcz, Lda., São Paulo, 2009, pp. 16 e 17. (Uma tradução para português da obra PROST, Antoine e VINCENT, Gérard, *Histoire de la vie privée*, sob a direção de Philippe Ariès e Georges Duby, Editions du Seuil, volume 5)

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

[160] "Este direito goza de um duplo âmbito de poder. Por um lado, traduz-se na faculdade de impedir a tomada de conhecimento injustificado ou intrusivo e, por outro, o direito a opor-se à instrumentalização do seu conhecimento mediante a divulgação ilegítima.", MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. citada, p. 123.

[161] Sobre o direito à autodeterminação informativa, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., 22 a 29.

privada, de cada um, como na estrutura político-social da coletividade, sendo imprescindível na consolidação das sociedades democráticas[162].

Eleni Kosta explica que foi com o final da Segunda Guerra Mundial e sob o impacto dos regimes totalitários que se fez sentir uma maior necessidade de sistematizar a proteção da vida privada dos cidadãos[163] [164].

É neste contexto histórico que surge a Declaração Universal dos Direitos do Homem, das Nações Unidas, de 10 de Dezembro de 1948. O artigo 12.º deste documento de direito internacional, de incontornável importância histórica[165], é consagra o seguinte:

> *Artigo 12.º*
>
> *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.*

Dois anos mais tarde, mas ainda no rescaldo da segunda Grande Guerra, outro documento de direito internacional se assume na defesa do direito da vida privada. Falamos da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (ou, abreviadamente, "Convenção Europeia dos Direitos do Homem" – CEDH), do Conselho da Europa, de 4 de Novembro de 1950, que, ao contrário da Declaração Universal dos Direitos do Homem, tem carácter vinculativo.

Apesar de não dar uma definição clara de privacidade, a Convenção consagra o direito ao respeito pela vida privada e familiar e regista um importante avanço ao distinguir a vida privada da honra[166]:

---

[162] "Uma sociedade que protege a privacidade e encoraja a autonomia e a diversidade de escolhas individuais é mais facilmente mais tolerante e pluralista do que outra em que as escolhas individuais sejam cerceadas.", MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., pp. 108 e 109.

[163] KOSTA, Eleni, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, Países Baixos, 2013, p. 12.

[164] Neste sentido, também MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., pp. 125 e ss..

[165] Não é esta, porém, a primeira formulação do direito à privacidade no Direito Internacional. Teresa Coelho Moreira chama a nossa atenção para a Declaração Americana dos Direitos e Deveres do Homem, de 2 de maio de 1948, aprovada em Bogotá, na IX Conferência Internacional Americana, cujo artigo 5.º declara que "Toda a pessoa tem direito à proteção da Lei contra ataques abusivos à sua honra, reputação e à vida privada e familiar", MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 126.

[166] Neste sentido, MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 167.

Artigo 8.º

(Direito ao respeito pela vida privada e familiar)

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.

A Convenção Europeia dos Direitos do Homem criou o Tribunal Europeu dos Direitos do Homem, com missão de apreciar as queixas relativas à violação dos direitos e liberdades previstos na Convenção, pelos Estados partes da mesma.

Mais tarde, em 16 de Dezembro de 1966, a Assembleia Geral das Nações Unidas aprova, em Nova Iorque, o Pacto Internacional sobre Direitos Civis e Políticos[167], que no seu artigo 17.º estabelece o seguinte:

Artigo 17.º

1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação.

2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados.

A proteção da privacidade estava consagrada pelo Direito Internacional.

[167] Portugal subscreveu o Pacto Internacional sobre Direitos Civis e Políticos em 7 de outubro de 1976.

A Declaração Universal dos Direitos do Homem, das Nações Unidas, e a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, do Conselho da Europa, foram adotados num contexto histórico muito específico. Os regimes totalitários tinham-se apresentado como reais ameaças à privacidade dos indivíduos[168].

Ambos os documentos visavam, portanto, garantir a defesa dos direitos e liberdades do cidadão face ao Estado.

A privacidade era um valor há muito reconhecido e reclamado na sociedade ocidental do pós-guerra; uma ideia que evoluía desde a mais longínqua memória da humanidade.

Mas a privacidade, enquanto sentimento resultante do balanceamento entre esfera pública e privada, partilhado pelos indivíduos organizados em sociedade, não deixou de evoluir como ideia e valor.

É com o desenvolvimento dos computadores e a proliferação das bases de dados e sistemas automatizados, que vamos assistir ao surgimento de uma ideia de privacidade como uma realidade verdadeiramente incontornável da vida em sociedade.

O surgimento do tratamento automatizado de dados vem gerar um novo contexto que apresenta novos desafios e impõe novas considerações na abordagem da privacidade.

"A tecnologia contribui para o surgimento de uma nova esfera privada que, embora mais rica, também se apresenta mais frágil, por estar mais

[168] "The mentioning of home and correspondence could build on constitutional traditions in many countries around the world, as a common heritage of a long development, sometimes during many centuries, but the focus on privacy and private life was new, and an obvious reaction to what happened in the Second World War.", HUSTINX, Peter, *EU Data Protection Law - Current State and Future Perspectives*, em "Ethical Dimensions of Data Protection and Privacy" Centre for Ethics, University of Tartu / Data Protection Inspectorate Tallinn, Estónia, 9 de janeiro de 2013, disponível em https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_EN.pdf, última consulta em 30 de agosto de 2013.

exposta a terceiros, o que origina a necessidade de um reforço da proteção jurídica e de um alargamento das fronteiras do conceito de privacidade"[169].

A utilização de sistemas automatizados pela administração pública, que se começou a sentir fortemente nos anos 60 do século passado[170], gerou um sentimento de desconfiança dos cidadãos em relação aos poderes públicos que passavam a recolher, tratar e trocar dados relativos à vida privada daqueles com extrema facilidade. Os novos sistemas, opacos ao cidadão, tornam-no cada vez mais transparente aos olhos dos que detêm o seu poder. A descontextualização apresenta-se como um perigo iminente, capaz de culminar em resultados imprevisíveis.

A reconhecida dimensão negativa do direito à privacidade[171], que visava garantir a não ingerência dos demais na vida privada de cada um, e do direito à autodeterminação informativa, que permitia ao individuo negar-se ou opor-se à recolha e difusão de informações que lhe digam respeito[172], mostrou-se insuficiente perante a nova realidade.

O direito à autodeterminação informativa passa, então, a ser considerado numa nova e revolucionaria perspetiva, desta feita, positiva.

Consolidando-se como um direito fundamental, o direito à autodeterminação informativa reconhece a cada cidadão o poder de decidir "até onde vai a sobra que deseja que paire sobre as informações que lhe respeitem"[173].

A proteção de dados pessoais aparece, assim, como garante do direito à privacidade. Apesar de surgir como uma "antítese" entre o direito à

[169] MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 120.
[170] Entre nós, refira-se o projeto do Registo Nacional de Identificação, instituído no anos 70 do século passado. Ver MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 131 a 133.
[171] Que "goza de um duplo âmbito de poder. Por um lado, traduz-se na faculdade de impedir a tomada de conhecimento injustificado ou intrusivo e, por outro, o direito a opor-se à instrumentalização do seu conhecimento mediante a divulgação ilegítima." MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...*, op. cit., p. 123.
[172] Neste sentido, CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 27.
[173] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 28.

privacidade e os computadores, acabou por evoluir para ser considerada uma "síntese" entre ambos[174].

Como explica Catarina Sarmento e Castro [175], a construção de princípios de proteção de dados pessoais foi influenciada pela própria jurisprudência do Tribunal Europeu dos Direitos do Homem, a partir da ideia geral da proteção da privacidade do artigo 8.º da Convenção Europeia dos Direitos do Homem[176] [177]. Este Tribunal considerou o uso de informações acerca da vida de um individuo, bem como o acesso de cada um aos dados que lhe digam respeito, elementos delimitadores do conceito de vida privada[178].

A Convenção Europeia para a Proteção dos Direitos do Homem não se aplica diretamente entre privados. Como vimos, surge num contexto que prioriza a proteção dos cidadãos perante os Estados.

É neste contexto de mudança e de constatação das insuficiências do direito positivado que surgem no quadro internacional novos documentos que visam garantir o direito à privacidade, através da consagração da perspetiva positiva do direito à autodeterminação informativa, regulando a proteção de dados pessoais.

A Organização para a Cooperação e Desenvolvimento Económico (OCDE)[179] aprova, em 23 de Setembro de 1980, as *Guidelines*, ou Linhas

[174] KOSTA, Eleni, *Consent in European...* , op. citada, p. 14.
[175] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp.. 25 e 26.
[176] No entanto, fê-lo sem nunca se debruçar diretamente sobre a proteção de dados pessoais per se. Neste sentido, KOSTA, Eleni, *Consent in European ...* , op. citada, p. 18.
[177] O Tribunal Europeu dos Diretos do Homem considerou, por um lado, que nem todos os aspectos do tratamento de dados pessoais estão a coberto do artigo 8.º da Convenção Europeia dos Direitos do Homem, e, por outro, que nem todos os dados pessoais cabem no âmbito desse mesmo artigo 8.º. Neste sentido, *Eleni, Consent in...* , op. citada, pp. 18 e 19 e GUTWIRTH, Serge, DE HERT, Paul, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitucionalization in Action*, em "Reinventing Data Protection?", Springer, 2009, pp. 20 a 22.
[178] Sobre a análise do artigo 8.º da CEDH pela jurisprudência do Tribunal Europeu dos Direitos do Homem, ver MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...* , op. cit., pp. 123 e ss..
[179] Sobre a OCDE, ver o *site* oficial, disponível em http://www.oecd.org/about/, última consulta em 21 de maio de 2013.
Portugal aderiu à OCDE em 4 de agosto de 1961.

Diretrizes Regulamentadoras da OCDE da Proteção da Vida Privada e dos Fluxos de Dados Pessoais[180].

Apesar de não ser um documento vinculativo, as Linhas Diretrizes Regulamentadoras da OCDE da Proteção da Vida Privada e dos Fluxos de Dados Pessoais, vêm reconhecer a proteção da privacidade como uma necessidade prioritária da política internacional, consagrando a privacidade como um direito fundamental. Deste documento constam referências a princípios que se vêm a confirmar tão importantes na proteção de dados pessoais, como o da qualidade dos dados e da finalidade.

Mas não foi só a OCDE que desenvolveu esforços no sentido de regular o tratamento de dados pessoais.

O Conselho da Europa[181] adotou, em 1980, a Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, conhecida como "Convenção n.º 108"[182], aberta à assinatura em 28 de janeiro de 1981, em Estrasburgo[183].

A Convenção n.º 108, vinculativa para os Estados ratificadores, consagra no artigo 8.º da Convenção n.º 108 a dimensão positiva do direito à autodeterminação informativa, reconhecendo que a pessoa a quem os dados respeitam pode exercer o controlo sobre os mesmos.

A Convenção n.º 108 definiu, ainda, o conceito de "dados de carácter pessoal" como "qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação («titular dos dados»)"[184].

---

[180] Sobre os trabalhos no seio da OCDE que antecederam à adoção das Guidelines, ou Linhas Diretrizes Regulamentadoras da OCDE da Proteção da Vida Privada e dos Fluxos de Dados Pessoais, KOSTA, Eleni, *Consent in European ...* , op. citada, 2013, pp. 26 e ss..

[181] O Conselho da Europa conta, hoje, com 47 Estados membros.
Portugal aderiu a esta organização em setembro de 1976.
Sobre o Conselho da Europa, ver o *site* oficial, disponível em http://hub.coe.int/, última consulta, 21 de maio de 2013.

[182] A Convenção encontra-se atualmente em processo de revisão.
Através da emenda introduzida em 1999, a Convenção n.º 108 veio a permitir a adesão das Comunidades Europeias e, em 2001 foi aprovado o Protocolo Adicional à Convenção, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados.
A lista dos atuais Estados signatários da Convenção n.º 108 pode ser consultada em http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG.

[183] Sobre o percurso do Conselho da Europa na tutela do direito privacidade, ver MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...* , op. cit., pp. 165 e ss..

[184] Artigo 2.º, alínea a), da Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção n.º 108º).

Não é qualquer tratamento de dados que é considerado uma violação da privacidade, nos termos da Convenção n.º 108. A perspetiva adotada exige, porém, que os tratamentos levados a cabo obedeçam a certos requisitos legais.

Da Convenção n.º 108 decorrem, então, princípios informadores do tratamento de dados pessoais, como o da qualidade dos dados, desdobrado nos princípios do tratamento leal e lícito; da finalidade; da adequação, pertinência e proporcionalidade; da exatidão e adequação dos dados e da conservação por tempo limitado [185].

Estavam lançados os alicerces daquele que viria a ser o atual quadro legislativo europeu da proteção dos dados pessoais[186].

A Convenção n.º 108 do Conselho da Europa, ao contrário das Linhas Diretrizes Regulamentadoras da OCDE da Proteção da Vida Privada e dos Fluxos de Dados Pessoais, que estendia a sua área de influência direta a 4 continentes [187], cinge-se às fronteiras do velho continente. Distingue-se, ainda, daquela por se ocupar concretamente do tratamento de dados pessoais automatizado.

Como faz notar Teresa Coelho Moreira, "a Convenção (108) é o primeiro documento internacional destinado a garantir o direito à liberdade informática ou direito à autodeterminação informacional e ficou estabelecido o marco genérico de proteção da pessoa perante possíveis intromissões na sua privacidade, ou lesão de outros direitos de personalidade, através da informática"[188].

O direito à privacidade e o direito à proteção de dados pessoais são, assim, expressões de uma mesma ideia universal de dignidade, autonomia e

[185] Artigo 5.º da Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção n.º 108º)
[186] De destacar, ainda, a Recomendação n.º R (87) 15 do Comité de Ministros, do Conselho da Europa, de 17 de setembro de 1987, que veio regular a utilização de dados pessoais no sector da polícia.
[187] Nos anos 70 do século passado, a OCDE contava não só com a participação de 19 países europeus, como também dos Estados Unidos da América, Canadá, Japão e Austrália.
Hoje, esta organização conta com 34 Estados membros.
[188] MOREIRA, Teresa Alexandra Coelho, *A Privacitdade dos ...* , op. cit., pp. 171 e 172.

valor único de cada ser humano, que implica o direito de todo o individuo desenvolver a sua personalidade e ter controlo sobre os assuntos que diretamente o afetem[189].[190]

Não podemos, no entanto, pensar estes dois direitos como sendo as duas faces de uma mesma moeda. A verdade é que o direito à proteção de dados pessoais é, por um lado, mais amplo do que o direito à privacidade, na medida em que assumiu a proteção de informações pessoais, independentemente da relação destas com o direito à privacidade. Por outro, é mais limitado, pois desconsidera os aspetos do direito à privacidade que extravasam o tratamento de informações pessoais[191].

2. O Quadro Legislativo Europeu da Proteção de Dados

A União Europeia tem assumido um papel muito importante na regulação do tratamento de dados pessoais.

Se hoje na União, que é de Direito [192], vemos expressa e autonomamente reconhecido o direito à proteção de dados de caráter pessoal a par do direito à privacidade, enquanto direitos fundamentais, sabemos que nem sempre foi assim.

Comecemos, pois, por ver o caminho percorrido por estes direitos na União Europeia, até à sua confirmação no topo da hierarquia normativa.

Paralelamente, vamos ver como a União foi tomando iniciativas no sentido de regular a matéria da proteção de dados pessoais.

2.1. Evolução histórica do direito à privacidade e da proteção de dados pessoais no direito da União Europeia

[189] Neste sentido, HUSTINX, Peter, *EU Data Protection ...* , cit., p. 2.
[190] Sobre a Convenção n.º 108 do Conselho da Europa ver, ainda, MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 265 a 271.
[191] Neste sentido, HUSTINX, Peter, *EU Data Protection ...* , cit., p. 3.
[192] A União Europeia cria normas jurídicas que vinculam diretamente os Estados-Membros e os seus cidadãos.

A Comunidade Económica Europeia foi criada em 25 de março de 1957, pelo Tratado de Roma (Tratado CEE), no rescaldo da Segunda Guerra Mundial, com o intuito de incentivar a cooperação económica na Europa[193].

A nova organização não gozava de um catálogo de direitos fundamentais, expresso e autónomo.

O Tribunal de Justiça das Comunidades Europeias (hoje, Tribunal de Justiça da União Europeia – autoridade judiciária da União, que vela pela aplicação e a interpretação uniformes do direito, em colaboração com os órgãos jurisdicionais dos Estados-Membros[194])[195] – desde cedo foi chamado a pronunciar-se sobre a defesa dos direitos fundamentais.

Começou por faze-lo, no final da década de 60 do século XX[196], através do reconhecimento de um elenco de direitos fundamentais que vieram a tornar-se num verdadeiro catálogo com valor de princípios gerais de Direito comunitário[197], colmatando a lacuna quanto a estes nos Tratados constitutivos. O Tribunal reconheceu, por esta via e entre outros, o direito à vida privada.

Em 1979, no Acórdão *Hauer*, o Tribunal adota expressamente a Convenção Europeia dos Direitos do Homem, do Conselho da Europa, referindo que a mesma "será examinada e aplicada pelo Tribunal sempre que as Partes lhe façam referência"[198].

---

[193] Sobre a história da União Europeia, ver o *site* oficial da organização, disponível em http://europa.eu/index_pt.htm (ultima consulta, 21 de maio de 2013).

[194] A estrutura judiciaria europeia é constituída pelos tribunais organicamente Europeus (o Tribunal de Justiça da União Europeia, com sede no Luxemburgo, que é composto por três jurisdições: o Tribunal de Justiça, o Tribunal Geral, criado em 1988, e o Tribunal da Função Pública, criado em 2004) e pelos tribunais funcionalmente europeus, ou seja, os tribunais dos Estados-Membros que aplicam, em primeira linha, o direito da União Europeia.

[195] O Tribunal de Justiça das Comunidades Europeias foi instituído pelo Tratado de Paris, assinado em 18 de abril de 1951, que criou a Comunidade Europeia do Carvão e do Aço (entretanto extinta, em 2002),
A Comunidade Europeia do Carvão e do Aço, a Comunidade Europeia da Energia Atómica (criada em Roma no mesmo dia 25 de março de 1957) e a Comunidade Económica Europeia formavam as Comunidades Europeias.

[196] No acórdão Stauder, de 12 de novembro de 1969, o Tribunal de Justiça das Comunidades Europeias (hoje, Tribunal de Justiça da União Europeia) consagrou que "o respeito pelos direitos fundamentais faz parte integrante dos princípios gerais do Direito que o Tribunal de Justiça assegura". Acórdão do Tribunal de Justiça, *Erich Stauder contra Cidade de Ulm – Sozialamt*, Processo 29-69, de 12 de novembro de 1969.

[197] Neste sentido, MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...* , op. cit., pp. 188.

[198] A Convenção Europeia dos Direitos do Homem, do Conselho da Europa já tinha sido é expressamente referida como "fonte de inspiração" para o Tribunal de Justiça das Comunidades Europeias, no Acórdão Rutili, de 28 de outubro de 1975. Acórdão do Tribunal de Justiça, *Roland Rutili*, residente em Gennevilliers, e Ministro do Interior, Processo 36/75.

À medida que o reconhecimento do direito à privacidade se consolidava na jurisprudência do Tribunal de Justiça, a produção legislativa internacional e europeia tendente a regular o tratamento de dados pessoais aumentava e reforçava a importância desta matéria, que a Comunidade não podia desconsiderar[199].

Em 29 de julho de 1981, a então CEE adotou uma recomendação através da qual aconselhava os Estados-Membros a subscrever a

[199] Nos anos 70 do século XX surgem as primeiras leis nacionais de proteção de dados. O Land alemão do Hesse aprova a primeira lei de proteção de dados pessoais em 1970. Seguiu-se a Suécia em 1973, a promulgar uma lei de proteção de dados pessoais.
Em 1976, a Constituição da República Portuguesa veio proteger expressamente o tratamento de dados pessoais, através do seu artigo 35.º. Esta disposição foi, entretanto, aletrada pela revisões constitucionais de 1982, 1989 e 1997. Sobre a evolução registada entre o texto original do artigo 35.º da CRP e o resultante das revisões constitucionais ver MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 281 a 299.
O artigo 35.º da Constituição da República Portuguesa consagra um direito "especial de personalidade que protege os cidadãos dos perigos que pode causar o uso da informática para a sua privacidade", CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 32.
Assim como o artigo 35.º, também os artigos 34.º (Inviolabilidade do domicílio e da correspondência) e o artigo 32.º n.º 8 (que respeita às Garantias de processo criminal), visam garantir o direito à reserva da intimidade da vida privada consagrado no artigo 26.º, todos da CRP., neste sentido, CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 39.
Luís Silveira refere-se à relevância estática, de eficácia negativa, e à relevância dinâmica, enquanto impulso legislativo dirigido ao legislador ordinário, da consagração constitucional do direito à proteção de dados, SILVEIRA, Luís Novais Lingnau da, *O Direito à Proteção de Dados Pessoais (Tentativa de caracterização)*, em "Sociedade da Informação - O Percurso Português" - Parte I, APDSI, 2007, disponível http://www.apdsi.pt/index.php/news/545/82/Livro-Sociedade-da-Informacao---O-Percurso-Portugues-Parte-I, última consulta em 30 de agosto de 2013.
A dignidade constitucional conferida a este direito, não só o blinda contra uma eventual descaracterização promovida por lei ordinária, como a incumbe de regular questões essenciais ao exercício efetivo do direito à proteção de dados.
Desde logo, o legislador constitucional remeteu para a lei a regulamentação do exercício dos direitos reconhecidos a todos os cidadãos de acesso aos dados que lhes digam respeito, de retificação e de atualização, bem como do direito a conhecer a finalidade a que se destinam, nos termos do n.º 1 do artigo 35.º.
O legislador ordinário foi, igualmente, incumbido de definir o conceito de dados pessoais, as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e de garantir a sua proteção, designadamente através de entidade administrativa independente – n.º 2 do artigo 35.º.
Esta entidade administrativa independente, inscrita no n.º 2 do artigo 35.º na revisão constitucional de 1997, veio a ser criada em 1991 e instituída em 1994. Falamos da Comissão Nacional de Proteção de Dados (originalmente Comissão Nacional de Proteção de Dados Pessoais Informatizados).
O n.º 3 do artigo 35.º proíbe o tratamento de categorias de dados "sensíveis": dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica. No entanto, a revisão constitucional de 1997 vem permitir que a proibição em causa seja afastada mediante consentimento expresso do titular, mediante autorização prevista por lei com garantias de não discriminação ou para finalidades estatísticas desde que os dados não possam ser individualmente identificáveis.
O n.º 4 resultou da revisão constitucional de 1982 e proíbe o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei, imprimindo uma delimitação negativa ao direito da proteção de dados em complemento da perspectiva positiva do direito de acesso, SILVEIRA, Luís Novais Lingnau da, *O Direito à...* , cit..
Já presente desde o texto original, a proibição da atribuição de um número nacional único aos cidadãos, agora constante do n.º 5, visa proteger as pessoas contra a possibilidade da criação de perfis dos cidadão com base num número único.
O n.º 6 do artigo 35.º consagra o princípio do livre acesso às redes informáticas de uso público (neste sentido, SILVEIRA, Luís Novais Lingnau da, *O Direito à* ..., cit..
Incumbe à lei ordinária, como resulta, ainda, deste n.º 6, a definição do regime aplicável aos fluxos de dados transfronteiras e das formas adequadas de proteção de dados pessoais, bem como de outros cuja salvaguarda se justifique por razões de interesse nacional.
Por fim, o n.º 7 do artigo 35.º, introduzido na revisão constitucional de 1997, vem estender a proteção aos dados pessoais contidos em ficheiros manuais.

Convenção n.º 108 do Conselho da Europa[200]. A Comunidade Europeia reconheceu esta Convenção como "adequada para introduzir à escala europeia um nível uniforme em matéria de proteção de dados"[201].

Contudo, a Comissão Europeia reservou-se o direito de adotar um instrumento legislativo próprio, se todos os Estados-Membros não assinassem e ratificassem esta Convenção num prazo razoável[202].

Os Estados-Membros da Comunidade que ainda não tivessem aderido à Convenção deviam, então, assiná-la durante o ano de 1981, e ratifica-la antes do final do ano de 1982[203].

Em 17 de fevereiro de 1986, é assinado, no Luxemburgo, o Ato Único Europeu (AUE), com o objetivo de relançar a integração europeia e concluir a realização do mercado interno. O chamado "Mercado Único", vem a ser concluído em 1993, e contempla as chamadas "quatro liberdades": a livre circulação de mercadorias, de serviços, de pessoas e de capitais.

Os Estados-Membros, através deste documento, declaram-se "decididos a promover conjuntamente a democracia, com base nos direitos fundamentais reconhecidos nas Constituições e legislações dos Estados-Membros, na Convenção de Proteção dos Direitos do Homem e das Liberdades Fundamentais e na Carta Social Europeia, nomeadamente a liberdade, a igualdade e a justiça social"[204].

A concretização do projeto de relançar a integração europeia e concluir a realização do mercado interno culminou com a assinatura do Tratado de Maastricht, em 1992, que institui a União Europeia (Tratado da União Europeia – TUE), caracterizou-se pela passagem de uma união económica para uma união política.

---

[200] COMISSÃO EUROPEIA, *Recomendação da Comissão relativa a uma convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal*, de 29 de Julho de 1981, (81/679/CEE), Jornal Oficial nº L 246 de 29/08/1981 p. 0031 – 0031, Edição especial portuguesa: Capítulo 16 Fascículo 1 p. 0077, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31981H0679:PT:HTML, última consulta em 30 de agosto de 2013.
[201] COMISSÃO EUROPEIA, *Recomendação da Comissão relativa a uma ...* , cit.., Parágrafo I, ponto 5.
[202] COMISSÃO EUROPEIA, *Recomendação da Comissão relativa a uma ...* , cit.., Parágrafo I, ponto 5.
[203] COMISSÃO EUROPEIA, *Recomendação da Comissão relativa a uma ...* , cit.., Parágrafo II, ponto 1.
[204] AUE, preâmbulo.

O TUE veio permitir o lançamento da integração política.

O Tratado que institui a Comunidade Económica Europeia é alterado em vista à instituição da Comunidade Europeia.

A União Europeia passa a basear-se em três pilares: as Comunidades Europeias, a Política Externa e de Segurança Comum e a cooperação policial e judiciária em matéria penal.

O Tratado firma a jurisprudência do Tribunal de Justiça, incorporando no seu texto que a União "respeitará os direitos fundamentais tal como os garante a Convenção Europeia de Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais, assinada em Roma em 4 de Novembro de 1950, e tal como resultam das tradições constitucionais comuns aos Estados-Membros, enquanto princípios gerais do direito comunitário".[205]

A harmonização da matéria da proteção de dados no seio da Comunidade através da Convenção n.º 108 do Conselho da Europa não se mostrou eficaz.

Nos no início dos anos 90 do século passado, já eram muitos os Estados-Membros que haviam tomado a iniciativa de regular a nível interno o tratamento de dados pessoais [206] . Ao mesmo tempo, outros países permaneciam sem quaisquer normas sobre a matéria, já que alguns Estados-Membros permaneciam sem sequer aderir à Convenção.

A Comunidade não ignorou que as diferenças entre as legislações nacionais, e entre estas e a ausência total de regulamentação noutros Estados-Membros, poderiam levantar entraves ao funcionamento do Mercado Único, causando sérias distorções.

A Comissão Europeia, incitada pelo Parlamento Europeu, deu início aos trabalhos tendentes à adoção de uma Diretiva sobre o tratamento de dados pessoais.

[205] Artigo F do TUE.

[206] Em 1991, Dinamarca, França, Alemanha, Irlanda, Luxemburgo, Países Baixos, Reino Unido e Portugal já tinham leis de proteção de dados pessoais, cf. KOSTA, Eleni, *Consent in European ...* , op. citada, p. 84, nota de rodapé 288.

O processo legislativo culminou na adoção da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[207], fortemente inspirada pela Convenção n.º 108 do Conselho da Europa.

Se, os anos 60 do século passado ficaram marcados pelo sentimento de desconfiança e pelos consequentes desafios que a utilização de sistemas automatizados e complexas bases de dados informáticas pela administração pública levantaram; os anos 90 confirmaram a ubiquidade da informática, presente em todos os sectores sociais, e em possante expansão, impulsionada pelo surgimento da *World Wide Web*. A rede das redes trazia consigo um universo inimaginável de novas oportunidades e, consequentemente, de imprevisíveis riscos apresentados sob a forma de complexos desafios.

Em 1997, foi assinado o Tratado de Amesterdão que alterou o Tratado da União Europeia e os Tratados que instituem as Comunidades Europeias[208].

No TUE, é inserido o considerado através do qual a União confirma "o seu apego aos direitos sociais fundamentais, tal como definidos na Carta Social Europeia, assinada em Turim, em 18 de Outubro de 1961, e na Carta Comunitária dos Direitos Sociais Fundamentais dos Trabalhadores, de 1989". O n.º 1 do artigo F, é alterado, e passa a consagrar que "a União assenta nos princípios da liberdade, da democracia, do respeito pelos direitos do Homem

[207] A Diretiva 95/46/CE do Parlamento e do Conselho, de 24 de outubro de 1995, foi transposta para a ordem jurídica portuguesa através da Lei n.º 67/98, de 26 de outubro, que revogou a Lei nº 10/91.
Sobre a Lei 10/91, de 29 de abril ver MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 300 a 313.
Sobre a Lei n.º 67/98, de 26 de outubro ver MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 340 a 374; CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit.; e GUERRA, Amadeu, *A Lei da Proteção de Dados Pessoais*, em "Direito da Sociedade da Informação", Volume II, Coimbra Editora, fevereiro de 2001, pp. 145 e ss..
Analisaremos com maior pormenor a Diretiva 95/46/CE no Título 2.2. deste Capítulo II.

[208] O Tratado da Comunidade Econômica Europeia, o Tratado da Comunidade Europeia do Carvão e do Aço e o Tratado da Comunidade Europeia da Energia Atômica.

e pelas liberdades fundamentais, bem como do Estado de direito, princípios que são comuns aos Estados-Membros".

Ao TCE[209] é aditado o artigo que consagra que "os atos comunitários relativos à proteção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados serão aplicáveis às Instituições e órgãos instituídos pelo presente Tratado, ou com base nele e que antes da data prevista, o Conselho criará um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados atos comunitários às Instituições e órgãos da Comunidade e adotará as demais disposições que se afigurem adequadas."[210].

Longe de configurar a consagração de um direito fundamental à proteção de dados pessoais, o artigo 286.º do TCE representa a afirmação da importância desta matéria para a União, que lhe confere lugar no topo de hierárquica legislativa comunitária[211].

Nesse mesmo ano de 1997, é aprovada a Diretiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações[212].

Em 2000 surge a 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[213].

---

[209] Tratado que institui a Comunidade Europeia – Tratado de Roma de 1957.
[210] Artigo 286.º do TCE.
[211] De destacar, ainda, a inserção no TUE, no titulo relativo à cooperação policial e judiciária em matéria penal, da alínea b) do n.º 1 do artigo 30.º que acautela que a ação em comum no domínio da cooperação policial abrange "a recolha, armazenamento, tratamento, análise e intercâmbio de informações pertinentes, incluindo informações em poder de serviços responsáveis pela aplicação da lei respeitantes a transações financeiras suspeitas, em especial através da Europol, sob reserva das disposições adequadas relativas à proteção dos dados de carácter pessoal.", entretanto revogado pela v. 3 da Ata de Ratificação do Tratado de Lisboa (JO, C 290, de 30.11.2009, pág.1).
[212] Transposta para a ordem jurídica nacional pela Lei n.º 69/98, de 28 de outubro.
[213] Transposta para a ordem jurídica nacional pelo Decreto-Lei nº 7/2004, de 7 de janeiro (Lei do Comércio Electrónico).
Sobre o Decreto-Lei nº 7/2004, de 7 de janeiro ver AUTORES VÁRIOS, *Lei do Comércio Electrónico Anotada*, Ministério da Justiça, Coimbra Editora, 2005, anotação ao artigo 22.º, p. 84.

Em 7 de dezembro de 2000, o ordenamento jurídico europeu ganha um catálogo de direitos fundamentais.

A Carta dos Direitos Fundamentais da União Europeia[214], formalmente adotada em Nice, pelo Parlamento Europeu, pelo Conselho Europeu e pela Comissão Europeia, vem consagrar o respeito pela reserva da vida privada no seu artigo 7.º, do capítulo dedicado às liberdades.

No entanto, a Carta não se limita a este reconhecimento geral do direito à privacidade, autonomizando, no artigo 8.º, o direito à proteção de dados pessoais[215] [216].

> ***Artigo 8.º***
>
> ***Proteção de dados pessoais***
>
> ***1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal 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 rectificação.***
>
> ***3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.***

Protegem-se, com a autonomização deste direito à proteção de dados, não apenas os dados pessoais íntimos e privados, mas todos os que sejam relativos a uma pessoa.

---

[214] "(...) é uma «Carta para a Europa mas não uma carta para os Europeus», já que estes não são os únicos beneficiários. Os direitos nela previstos aplicam-se a quase todos – cidadãos dos Estados-Membros, residentes legais ou ilegais, ou, simplesmente, pessoas que estão de passagem. O que está em jogo é o princípio da universalidade dos direitos do homem.", MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...* , op. cit., op. citada, p. 193.

[215] Este artigo é inspirado pelo 8.º da Convenção Europeia dos Direitos do Homem e na Convenção n.º 108 do Conselho da Europa, assim como no artigo 286.º do Tratado que institui a Comunidade Europeia, (hoje, artigo 16.º do Tratado Sobre o Funcionamento da União Europeia) e na própria Diretiva 95/46/CE do Parlamento Europeu e do Conselho, relativa á proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[216] Não podemos deixar de reproduzir a seguinte consideração da Ilustre Professora Teresa Coelho Moreira: "Neste art. 8.º, diferentemente do que sucede com outros direitos deste Documento, opta-se por identificar um certo conteúdo do mesmo: o princípio da licitude, o princípio da finalidade, o princípio do consentimento e o do fundamento legal do tratamento, o direito de acesso e o de retificação. Mas, por outro lado, não se referem outros princípios ou direitos também reconhecidos noutros textos europeus, como o direito à informação, o princípio da qualidade dos dados, o direito de cancelamento ou o princípio da segurança, nem se aludindo à proteção dos dados sensíveis. Por isso, talvez tivesse sido preferível limitar-se a proclamar este direito.", MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos ...* , op. cit., p. 196 e 197.

A Carta dos Direitos Fundamentais da União Europeia reconhece expressamente o consentimento enquanto fundamento legitimador do tratamento de dados pessoais sem, no entanto, excluir a possibilidade da previsão de outros.

Em 2002, é revogada a Diretiva 97/66/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações, pela Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)[217].

É nesta Diretiva que, pela primeira vez, é expressamente regulada a utilização dos testemunhos de conexão enquanto mecanismo de armazenamento e acesso a informações no terminal do utilizador.

Quatro anos mais tarde, é aprovada a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações[218], e que altera a Diretiva 2002/58/CE.

Em dezembro de 2008 foi assinado o Tratado de Lisboa, que veio atribuir à Carta dos Direitos Fundamentais da União Europeia o mesmo valor jurídico que os Tratados[219].

Assim, o direito à proteção de dados pessoais, consagrado no artigo 8.º da Carta, assume-se como um direito fundamental, juridicamente vinculativo para as Instituições da UE e para os Estados-Membros, que tem de ser respeitado e promovido sempre que apliquem o direito da União.

[217] Que desenvolveremos com mais atenção no Título 2.3. deste Capítulo II.
A Diretiva 2002/58/CE foi transposta para a ordem jurídica nacional pela Lei n.º 41/2004, de 18 de agosto.
Sobre a Lei n.º 41/2004, de 18 de agosto ver MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 385 a 391.
[218] Transposta para a ordem jurídica nacional pela Lei nº 32/2008, de 17 de julho.
[219] Ex vi artigo 6.º TUE.

As disposições da Carta não alargam as competências da União[220] – que são as que estão contempladas nos Tratados. No entanto, o exercício dessas mesmas competências passa a ser orientado pela consideração e promoção dos direitos fundamentais consagrados.

Do artigo 6.º do TUE, que atribui força vinculativa à Carta, decorre que o bloco de jusfundamentalidade da União consagra direitos fundamentais decorrentes de normas internacionais, europeias e nacionais[221], que nos conduz ao chamado princípio do nível de proteção mais elevado[222]. Segundo este princípio, nenhuma disposição da Carta deve ser "interpretada no sentido de restringir ou lesar os direitos do Homem e as liberdades fundamentais reconhecidos, nos respetivos âmbitos de aplicação, pelo direito da União, o direito internacional e as Convenções internacionais em que são Partes a União ou todos os Estados-Membros, nomeadamente a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, bem como pelas Constituições dos Estados-Membros"[223]. Ou seja, numa situação de concorrência entre diferentes níveis de proteção, aplica-se aquele que for mais elevado quanto ao direito fundamental em causa. Nenhum patamar de proteção atingido por qualquer dos ordenamentos deve retroceder.

O Tratado de Lisboa, que entrou em vigor em 2009, promoveu, igualmente, a reforma do TUE e do Tratado que institui a Comunidade Europeia, sendo que este último passa a adotar a designação de Tratado Sobre o Funcionamento da União Europeia (TFUE).

O atual artigo 16.º Tratado Sobre o Funcionamento da União Europeia, que substitui o antigo artigo 286.º do Tratado que institui a Comunidade Europeia, consagra o direito de todas as pessoas à proteção dos dados de carácter pessoal que lhes digam respeito, adotando uma abordagem

[220] Artigo 6.º TUE.
[221] "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.", artigo 6.º, n.º 3 do TUE.
[222] Artigo 53.º da CDFUE.
[223] Artigo 53.º da CDFUE.

moderna e global sobre a proteção de dados e a livre circulação de dados pessoais[224], que cobre igualmente o domínio da cooperação policial e judiciária em matéria penal.

> ***"1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.***
> ***2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário[225], 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."***

Este é um artigo intimamente ligado ao bom funcionamento do mercado interno.

A proteção de dados pessoais é, assim, um domínio ao qual o Tratado atribui à União competência partilhada com os Estados-Membros, o que quer dizer que estes exercem a sua competência na medida em que a União não tenha exercido a sua[226]. Uma vez que a UE exerceu a sua competência, através da adoção da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, ficou inibida a iniciativa legislativa dos Estados-Membros sobre esta matéria.

No TUE é inserido o atual artigo 39.º, no Capítulo II relativo à política externa e de segurança comum, do Título V, que estipula o seguinte:

---

[224] Neste sentido, COMISSÃO EUROPEIA, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Proteção da privacidade num mundo interligado Um quadro europeu de proteção de dados para o século XXI*, /* COM/2012/09 final */, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:PT:HTML, última consulta em 20 de junho de 2013.
[225] Sobre o processo legislativo ordinário, artigo 289.º e artigo 294.º do TFUE.
[226] Artigo 2.º n.º 2 e artigo 4.º, n.º 2, alínea a), do TFUE.

> ***"Em conformidade com o artigo 16 do Tratado sobre o Funcionamento da União Europeia e em derrogação do n.º 2 do mesmo artigo, o Conselho adota uma decisão que estabeleça as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação do presente capítulo, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes."***

Assim, no contexto da política externa e de segurança comum, as normas são adotadas pelo Conselho, por unanimidade dos Estados-Membros.

Em 2009, a Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro, conhecida como "Diretiva dos Cidadãos"[227], veio alterar a Diretiva 2002/58/CE [228] relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, nomeadamente na parte em que regula o armazenamento e acesso de informações no terminal do utilizador, ou seja, o regime jurídico aplicável à utilização de testemunhos de conexão.

A União Europeia está, presentemente, a desenvolver uma profunda reforma na área da proteção de dados pessoais[229].

Do novo pacote legislativo de proteção de dados pessoais previsto destaca-se o Regulamento de Proteção de Dados Pessoais que substituirá a Diretiva 95/46/CE.

[227] Transposta para a ordem jurídica nacional pela Lei n.º 46/2012, de 29 de agosto.
[228] Além de alterar a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, alterou a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidores.
[229] Que desenvolveremos com mais atenção no Título 2.4. deste Capítulo II.

2.2. A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 04 de Outubro de 1995

Após quatro anos de negociações, foi aprovada a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, decorrente da necessidade de fazer circular informações pessoais no mercado interno.

A Diretiva 95/46/CE [230] – que ficou conhecida como "Diretiva da Proteção de Dados" – surge da necessidade de harmonizar[231] a proteção conferida aos dados pessoais nos Estados-Membros, com vista ao bom funcionamento do mercado interno, dado o fluxo transfronteiriço de dados que acompanha a circulação de pessoais, mercadorias, capitais e serviços[232].

A Diretiva da Proteção de Dados contempla um duplo objetivo. Assim, considerando, além do mais, que "os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos

[230] A Diretiva 95/46/CE entrou em vigor em 13 de dezembro de 1995 e o seu prazo de transposição nos Estados-Membros terminou em 24 de outubro de 1998. Foi modificada, uma única vez, pelo Regulamento (CE) n. ° 1882/2003 do Parlamento Europeu e do Conselho de 29 de setembro de 2003 que adapta à Decisão 1999/468/CE do Conselho, as disposições relativas aos comités que assistem a Comissão no exercício das suas competências de execução previstas em atos sujeitos ao artigo 251.º do Tratado, que deu uma nova redação ao artigo 31.º.

[231] É através das Diretivas que a União procura a harmonização do direito nos diferentes Estados-Membros. Estas vinculam os Estados-Membros destinatários quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios.
Os Regulamentos, por sua vez, são instrumentos legislativos que visam a uniformização, uma vez que tem carácter geral. O Regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.
Sobre os atos jurídicos da União Europeia ver o artigo 288.º do Tratado sobre o Funcionamento da União Europeia.

[232] Neste sentido, considerandos 7, 8 e 9 primeira parte, da Diretiva 95/46/CE:
"(7) Considerando que as diferenças entre os Estados-membros quanto ao nível de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domínio do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro; que estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício de uma série de atividades económicas à escala comunitária, falsear a concorrência e entravar o exercício pelas administrações das funções que lhes incumbem nos termos do direito comunitário; que esta diferença de níveis de proteção resulta da disparidade das disposições legislativas, regulamentares e administrativas nacionais;
(8) Considerando que, para eliminar os obstáculos à circulação de dados pessoais, o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-membros; que a realização deste objetivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-membros, tendo especialmente em conta a dimensão das divergências que se verificam atualmente a nível das legislações nacionais aplicáveis na matéria e a necessidade do coordenar as legislações dos Estados-membros para assegurar que a circulação transfronteiras de dados pessoais seja regulada de forma coerente e em conformidade com o objetivo do mercado interno nos termos do artigo 7º A do Tratado; que é portanto necessária uma ação comunitária com vista à aproximação das legislações;
(9) Considerando que, devido à proteção equivalente resultante da aproximação das legislações nacionais, os Estados-membros deixarão de poder levantar obstáculos à livre circulação entre si de dados pessoais por razões de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada (...)."

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"[233] e que "o estabelecimento e o funcionamento do mercado interno no qual é assegurada a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exigem não só que os dados pessoais possam circular livremente de um Estado-Membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais das pessoas"[234], a Diretiva visa que 1) os Estados-Membros assegurem "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" [235] sem 2) "restringir ou proibir a livre circulação de dados pessoais entre Estados-Membros"[236].[237]

A Diretiva abarca a realidade tecnológica de forma ampla, aplicando-se tanto ao tratamento de dados por meios total ou parcialmente

[233] Considerando 2 da Diretiva 95/46/CE.
[234] Considerando 3 da Diretiva 95/46/CE.
[235] No sentido da margem de conformação deixada aos Estados-Membros aquando da aplicação da Diretiva, que devem, porém, salvaguardar o nível de proteção mais elevado, destacamos os considerandos 9, 10 e 11 da Diretiva 95/46/CE:
"(9) Considerando que (...) é deixada aos Estadas-membros uma margem de manobra que, no contexto da aplicação da diretiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; que, ao fazê-lo, os Estados-membros se esforçarão por melhorar a proteção atualmente assegurada na respectiva legislação nacional; que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verificar-se disparidades na aplicação da diretiva, o que poderá refletir-se na circulação de dados quer no interior de um Estado-membro, quer na Comunidade;
(10) Considerando que o objetivo das legislações nacionais relativas ao tratamento de dados pessoais é assegurar o respeito dos direitos e liberdades fundamentais, nomeadamente do direito à vida privada, reconhecido não só no artigo 8º da Convenção europeia para a proteção dos direitos do Homem e das liberdades fundamentais como nos princípios gerais do direito comunitário; que, por este motivo, a aproximação das referidas legislações não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na Comunidade."
E, ainda, os considerandos 22 e 23:
"(22) Considerando que os Estados-membros precisarão, na sua legislação ou nas regras de execução adotadas nos termos das presente diretiva, as condições gerais em que o tratamento de dados é lícito; que, nomeadamente, o artigo 5º, conjugado com os artigos 7º e 8º, permite que os Estados-membros estabeleçam, independentemente das regras gerais, condições especiais para o tratamento de dados em sectores específicos e para as diferentes categorias de dados referidas no artigo 8º;
(23) Considerando que os Estados-membros podem assegurar a concretização da proteção das pessoas tanto por uma lei geral relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais, como por leis setoriais, por exemplo as relativas aos institutos de estatística."
[236] Artigo 1.º da Diretiva 95/46/CE.
[237] Teresa Coelho Moreira considera mesmo que "esta Diretiva, contrariamente à Convenção n.º 108 do Conselho da Europa, não é diretamente um instrumento de proteção dos direitos das pessoas, mas antes, uma ferramenta para impedir os entraves à livre circulação de informação pessoal no contexto do mercado interno. Esta Diretiva prossegue dois objetivos fundamentais: tutelar a privacidade e os restantes direitos fundamentais e garantir o fluxo de dados entre os Estados membros. Trata-se, desta forma, de impedir que as diferenças entre os níveis de proteção dos direitos e liberdades das pessoas e, em particular, da privacidade, garantidos pelos Estados membros no que concerne ao tratamento de dados pessoais, afete o funcionamento regular do mercado único.", MOREIRA, Teresa Alexandra Coelho, A Privacidade dos ..., op. cit., pp. 199 e 200.

automatizados[238] como ao tratamento manual[239] e abrangendo qualquer tipo de informação pessoal[240].

O legislador comunitário não ignorou que progresso tecnológico veio facilitar o tratamento de dados pessoais[241], ao mesmo tempo que as redes de telecomunicações proporcionavam a circulação desses dados[242] com rapidez e eficácia sem precedentes[243].

A Diretiva aplica-se, assim, "ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados"[244].

Está, porém, fora do seu âmbito de aplicação o tratamento de dados pessoais "efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário", assim como o que "tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal" [245]. A

[238] "Considerando que, tendo em conta a importância do desenvolvimento que, no âmbito da sociedade de informação, sofrem atualmente as técnicas de captação, transmissão, manipulação, gravação, conservação ou comunicação de dados de som e de imagem relativos às pessoas singulares, há que aplicar a presente diretiva ao tratamento desses dados", no entanto "o tratamento desses dados só é abrangido pela presente diretiva se for automatizado ou se os dados tratados estiverem contidos ou se destinarem a ficheiros estruturados segundo critérios específicos relativos às pessoas, a fim de permitir um acesso fácil aos dados pessoais em causa", considerandos 14 e 15 da Diretiva 95/46/CE.

[239] "Considerando que a proteção das pessoas se deve aplicar tanto ao tratamento automatizado de dados como ao tratamento manual; que o âmbito desta proteção não deve, na prática, depender das técnicas utilizadas, sob pena de se correr o sério risco de a proteção poder ser contornada; que, em todo o caso, no que respeita ao tratamento manual, a presente diretiva apenas abrange os ficheiros e não as pastas não estruturadas; que, em particular, o conteúdo de um ficheiro deve ser estruturado de acordo com critérios específicos relativos às pessoas que permitam um acesso fácil aos dados pessoais; que, em conformidade com a definição da alínea c) do artigo 2º, os diferentes critérios que permitem determinar os elementos de um conjunto estruturado de dados pessoais e os diferentes critérios que regem o acesso a esse conjunto de dados podem ser definidos por cada Estado-membro; que as pastas ou conjuntos de pastas, bem como as suas capas, que não estejam estruturadas de acordo com critérios específicos, de modo algum se incluem no âmbito de aplicação da presente diretiva", Considerando 27 e artigo 3.º da Diretiva 95/46/CE.

[240] Considerando 26 da Diretiva 95/46/CE.

[241] Considerando 4 da Diretiva 95/46/CE.

[242] Considerando 6 da Diretiva 95/46/CE.

[243] No entanto, a Diretiva Diretiva 95/46/CE surgiu num contexto tecnológico já significativamente diferente daquele em que nos achamos hoje. A capacidade de processamento e memória dos computadores também aumentou consideravelmente. Em 1995 a *World Wide Web* dava os primeiros passos. A Internet estava ainda longe de ter a dimensão que hoje apresenta, quer no que respeita ao número de utilizadores, quer quando à diversidade de serviços prestados "em linha". As relações económicas, sociais e laborais não conheciam, então, a influência determinante que hoje lhes é impressa pelos novos meios de interação – e controle – proporcionados pela evolução tecnológica.

[244] Artigo 3.º, n.º 1, da Diretiva 95/46/CE.

[245] Artigo 3.º, n.º 2, primeiro parágrafo, da Diretiva 95/46/CE.

Diretiva da Proteção de Dados não se aplica, ainda ao tratamento "efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas"[246].

No que respeita ao âmbito territorial, a Diretiva da Proteção de Dados[247] é aplicável ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento situado no território de um Estado-Membro[248]. Assim, o local onde o tratamento em si tem lugar não é relevante.

No caso de o responsável pelo tratamento não estar estabelecido no território da União, a Diretiva é aplicável quando este recorrer a meios, automatizados ou não, situados no território de um Estado-Membro, para tratamento de dados pessoais; a salvo se esses meios só forem utilizados para trânsito no território da Comunidade[249].

Se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-Membros, fica obrigado a tomar as medidas necessárias para garantir que cada um desses seus estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável[250].

Para efeitos da Diretiva em análise, a noção de "estabelecimento no território de um Estado-Membro" pressupõe o "exercício efetivo e real de uma atividade mediante uma instalação estável; que, para o efeito, a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, não é determinante"[251].

---

[246] Artigo 3.º, n.º 2, segundo parágrafo, da Diretiva 95/46/CE.
O Tribunal de Justiça pronunciou-se sobre esta exceção, no Acórdão Lindqvist: "a segunda exceção prevista, no segundo travessão do mesmo n.º 2, visa unicamente as atividades que se inserem no âmbito da vida privada ou familiar dos particulares, o que não é manifestamente o caso do tratamento de dados de carácter pessoal que consiste na sua publicação na Internet de maneira que esses dados sejam disponibilizados a um número infinito de pessoas". Acórdão do Tribunal de Justiça, *Bodil Lindqvist*, Processo C-101/01, de 6 de novembro de 2003.
[247] Em rigor, referimo-nos à aplicação da legislação nacional de transposição da Diretiva 95/46/CE.
[248] Artigo 4.º, n.º 1, alínea a), da Diretiva 95/46/CE.
[249] Artigo 4.º, n.º 1, alínea c), da Diretiva 95/46/CE.
[250] Artigo 4.º, n.º 1, alínea b), da Diretiva 95/46/CE.
[251] Considerando 19 da Diretiva 95/46/CE.

O artigo 2.º da Diretiva 95/46/CE define aqueles que são alguns dos conceitos essenciais à compreensão do quadro legislativo europeu da proteção de dados.

Desde logo, para efeitos da Diretiva, entende-se por "dados pessoais" "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»)", sendo que "é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"[252].[253]

Uma pessoa é considerada identificável quando, no âmbito de um grupo de pessoas, pode ser distinguida dos outros membros do grupo e, por isso, ser tratada de forma diferente[254].

"Para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa"[255].

Assim, dados pessoais não são exclusivamente aqueles através dos quais é possível identificar diretamente uma pessoa, mas também todos aqueles que indiretamente o permitam, através da associação de conceitos ou conteúdos.

A Diretiva refere-se, no artigo 8.º, a "categorias específicas de dados". Estes dados, são aqueles que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual". São os chamados

[252] Artigo 2.º, alínea a), da Diretiva 95/46/CE.
[253] Sobre o conceito de "dados pessoais" no contexto da n.º Lei 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 70 e ss.
[254] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007 sobre o conceito de dados pessoais* (WP 136), de 20 de junho de 2007, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf, última consulta em 30 de agosto de 2013.
[255] Considerando 26 da Diretiva 95/46/CE.

"dados pessoais sensíveis"[256]; que impõem condições mais estritas para legitimar o seu tratamento.

Por "tratamento de dados pessoais" a Diretiva entende "qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição" [257], independentemente da tecnologia ou técnica utilizada ou formato[258].

O tratamento dos dados pessoais é definido pelo "responsável pelo tratamento".

Por "Responsável pelo tratamento" deve entender-se "a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais"[259]. É sobre este que impende, em primeira linha, a responsabilidade pelo respeito e garantia dos direitos relativos ao tratamento de dados pessoais[260].

A Diretiva adota princípios orientadores que determinam a legitimidade dos tratamentos de dados pessoais.

---

[256] Entre nós, sobre o tratamento de dados pessoais sensíveis ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 88 a 99 e pp. 215 a 227, e MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 247 e ss..

[257] Artigo 2.º, alínea b), da Diretiva 95/46/CE.

[258]"Constituirão dados pessoais toda a informação, seja ela numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo, relativa a uma pessoa identificada ou identificável", CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 71.

[259] Artigo 2.º, alínea d), da Diretiva 95/46/CE, que acrescenta que "sempre que as finalidades e os meios do tratamento sejam determinadas por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário.

[260] "Quando uma mensagem que contém dados pessoais é transmitida através de um serviço de telecomunicações ou de correio electrónico cujo único objetivo é a transmissão de mensagens deste tipo, será a pessoa de quem emana a mensagem, e não quem propõe o serviço de transmissão, que será em regra considerada responsável pelo tratamento dos dados pessoais contidos na mensagem; que, contudo, as pessoas que propõe esses serviços serão em regra consideradas responsáveis pelo tratamento dos dados pessoais suplementares necessários ao funcionamento do serviço.", considerando 47 da Diretiva 95/46/CE.

A licitude do tratamento de dados depende da observância dos princípios relativos à qualidade dos dados[261], assim como dos princípios relativos à legitimidade do tratamento de dados[262].

Os princípios aplicáveis ao tratamento de dados pessoais efetivam-se em obrigações impostas ao responsável pelo tratamento, por um lado e, por outro, em direitos reconhecidos ao titular daqueles[263].

A Diretiva 95/46/CE impõe aos Estados-Membros a obrigação de estabelecer que qualquer pessoa possa recorrer aos tribunais em caso de violação dos direitos que lhe são garantidos pelas disposições nacionais aplicáveis ao tratamento de dados pessoais. Mais prevê que qualquer pessoa que tenha sofrido um prejuízo devido a um tratamento ilícito de dados pessoais que lhe digam respeito tem o direito de obter a correspondente reparação[264].[265]

A proteção das pessoas garantida pela Diretiva não obsta às transferências de dados pessoais para países terceiros que assegurem um "nível de proteção adequado", que deve ser apreciado em função de todas as circunstâncias associadas à transferência ou ao conjunto de transferências. Assim, devem ser tidos em consideração, de acordo com o nº 2 do artigo 25.º, a natureza dos dados, a finalidade e a duração do tratamento; os países de origem e destino final; as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa; as regras profissionais e as medidas de segurança que são respeitadas nesse país.

Estão, portanto, impedidas as transferências dados pessoais de Estados-Membros para países terceiros que não disponham desse "nível de

[261] Artigo 6.º da Diretiva 95/46/CE, que desenvolveremos com mais atenção no Título 2.2.1. deste Capítulo II. Entre nós, sobre os princípios fundamentais para o tratamento de dados pessoais, ver CASTRO, Catarina Sarmento e, *Direito da Informática …* , op. cit., pp. 229 a 237.

[262] Artigo 7.º da Diretiva 95/46/CE, que desenvolveremos com mais atenção no Título 2.2.2. deste Capítulo II. Entre nós, sobre os fundamentos do tratamento de dados pessoais, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 205 a 213, e MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 247 e ss..

[263] Que desenvolveremos com mais atenção no Título 2.2.2. deste Capítulo II.

[264] Artigos 22.º e 23.º da Diretiva 95/46/CE.

[265] Entre nós, sobre o incumprimento das disposições sobre proteção de dados ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 303 a 321, e GUERRA, Amadeu, A Lei de ..., cit, pp. 166 a 169.

proteção adequado", salvo derrogações exaustivamente enumeradas no artigo 26.º da Diretiva[266] [267].[268]

O artigo 27.º da Diretiva visa a promoção a elaboração de códigos de conduta nacionais e comunitários destinados a contribuir, em função das características de cada sector, para a boa execução das disposições nacionais e comunitárias.

Os Estados-Membros foram incumbidos de estabelecer uma ou mais autoridades públicas independentes responsáveis pelo controlo da aplicação das disposições adotadas em execução da Diretiva, no seu território[269].[270]

O Grupo de Trabalho de Proteção de Dados foi criado na sequência da aprovação da Diretiva. Previsto no artigo 29.º e também conhecido por "Grupo do Artigo 2.º para a Proteção de Dados" ou, simplesmente, "Grupo de Trabalho do Artigo 29"[271], trata-se de um grupo de trabalho independente, com caráter consultivo, composto pelas autoridades de proteção de dados dos Estados-Membros, por um representante das autoridades criadas para os organismos comunitários e por um representante da Comissão Europeia.

[266] Como veremos no Título 2.2.2.1. deste Capítulo II, o consentimento da pessoa em causa pode legitimar a transferência de dados para um país terceiro que não assegure um "nível de proteção adequado", de acordo com o n. 2º do artigo 25.º da Diretiva 95/46/CE.

[267] No Acórdão do Tribunal de Justiça de 6 de novembro de 2003, proferido no âmbito do Processo C-101/01 (Caso Lindqvist), ficou negativamente delimitado o conceito de "transferência para países terceiros", vingando o entendimento de que "não existe uma «transferência para um país terceiro de dados» na acepção do artigo 25.° da Diretiva 95/46, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados quando uma pessoa que se encontra num Estado-Membro insere numa página a Internet, de uma pessoa singular ou coletiva que alberga o sítio Internet no qual a página pode ser consultada e que está estabelecida nesse mesmo Estado ou noutro Estado-Membro, dados de carácter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontrem em países terceiros". O Tribunal atendeu "por um lado, ao estádio de evolução da Internet à época da elaboração da Diretiva 95/46/CE e, por outro, à ausência de critérios aplicáveis à utilização da Internet, no seu capítulo IV, no qual se insere o referido artigo 25.°, que visa assegurar o controlo, pelos Estados- -Membros, das transferências de dados de carácter pessoal para países terceiros e proibir estas transferências quando estes não ofereçam um nível de proteção adequado", e concluiu que "não se pode presumir que o legislador comunitário tinha a intenção de incluir prospectivamente no conceito de «transferência para um país terceiro de dados» tal inserção de dados numa página Internet, mesmo que estes se tornem deste modo acessíveis às pessoas de países terceiros que possuam os meios técnicos para aceder a esses dados". Acórdão do Tribunal de Justiça, *Bodil Lindqvist*, Processo C-101/01, de 6 de novembro de 2003.

[268] Entre nós, sobre a transferência de dados pessoais para países terceiros, CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 275 a 301.

[269] Artigo 28.º da Diretiva 95/46/CE.

[270] Em Portugal, a Comissão Nacional de Proteção de Dados (CNPD) é a entidade administrativa independente, com poderes de autoridade, que tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei. Sobre a Comissão Nacional de Proteção de Dados ver *site* oficial disponível em http://www.cnpd.pt/, última consulta em 20 de outubro de 2013.

[271] Doravante "Grupo de Trabalho", "Grupo do Artigo 29.º" ou, simplesmente, "Grupo".

Tem como principais atribuições analisar as questões relativas à aplicação da Diretiva 95/46/CE, contribuindo para a sua maior uniformização; elaborar sobre o nível de proteção na comunidade e nos países terceiros; aconselhar a Comissão sobre medidas a tomar para proteção de direitos e liberdades das pessoas; elaborar parecer sobre códigos de conduta elaborados a nível comunitário e fazer recomendações sobre quaisquer questões de proteção de dados pessoais.

O trabalho desenvolvido pelo Grupo do Artigo 29.º tem-se mostrado de essencial importância na aplicação das regras de proteção de dados na União bem como se tem revelado crucial na evolução deste direito na sua conformação com a evolução tecnológica.

2.2.1. Os Princípios relativos à qualidade dos dados e os direitos da pessoa em causa

A Diretiva 95/46/CE consagra aqueles que são os princípios fundamentais aplicáveis ao tratamento de dados pessoais.[272]

Os "princípios da proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada", contidos na Diretiva da Proteção de Dados, "precisam e ampliam os princípios contidos na Convenção n.º 108, do Conselho da Europa, relativa à proteção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais"[273].

Os princípios aplicáveis ao tratamento de dados pessoais, implementam-se através da observância cumulativa, por um lado, das obrigações que impendem sobre os "responsáveis pelo tratamento de dados, em especial no que respeita à qualidade dos dados, à segurança técnica, à notificação à autoridade de controlo, às circunstâncias em que o tratamento

[272] Sobre os princípios fundamentais para o tratamento de dados pessoais, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 229 a 237.
[273] Considerando 11 da Diretiva 95/46/CE.

pode ser efetuado"[274], e, por outro, do respeito pelos "direitos das pessoas cujos dados são tratados serem informadas sobre esse tratamento, poderem ter acesso aos dados, poderem solicitar a sua retificação e mesmo, em certas circunstâncias, poderem opor-se ao tratamento" [275].

A Diretiva reconhece, assim, um conjunto de direitos ao titular dos dados[276], que vêm aflorar o princípio geral da transparência[277]. Este princípio impõe que o titular dos dados seja informado da recolha e tratamento daqueles, de modo que lhe permita ter completa consciência do processamento levado a cabo e dos seus fins.

Assim como o titular dos dados se apresenta transparente ao responsável pelo tratamento – que passa a conhecer informações pessoais daquele – não deve este poder, legitimamente, proceder a um tratamento de dados que se mostre opaco ao sujeito e, o impeça de posteriormente à recolha exercer quaisquer direitos sobre os dados que lhe dizem respeito[278].

Neste sentido, é consagrado o direito à informação do titular dos dados[279]. Este concretiza-se no direito a ser informado sobre a finalidade da recolha e do tratamento dos seus dados; sobre a eventual comunicação (transmissão) dos seus dados, sobre a identidade quer do responsável pelo tratamento, quer de eventuais destinatários dos seus dados e,

---

[274] "These principles are implemented through obligations that data controllers should comply with in order to protect the data they hold, reflecting both their interests and those of the data subjects.", KOSTA, Eleni, DUMORTIER, Jos, GRAUX, Hans, TIRTEA, Rodica and IKONOMOU, Demosthenes, *Study on data collection and storage in the EU*, ENISA – European Network and Information Security Agency, 23 de fevereiro de 2012, p. 7, disponível em http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection, ultima consulta em 30 de maio de 2013.

[275] Considerando 25 da Diretiva 95/46/CE.

[276] Sobre os direitos dos titulares dos dados consagrados na Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 239 a 262, e MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 356 a 358.

[277] O princípio geral da transparência não é, contudo, expressamente consagrado na Diretiva 95/46/CR. Apenas o considerando 63, respeitante ao papel das autoridades de controlo, se refere expressamente à transparência do tratamento.
Sobre o princípio geral da transparência, entre nós expressamente consagrado no artigo 2.º da Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 229.

[278] "(...) a transparência do tratamento de dados é igualmente uma condição de lealdade, que assume um valor em si mesma também após a informação inicial ter sido prestada.'', GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição de consentimento* (WP 194), de 13 de julho de 2011, p. 11, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_pt.pdf, última consulta em 30 de agosto de 2013..

[279] Sobre o direito de informação do titular dos dados na Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 242 a 247.

eventualmente, dos representantes destes; e sobre as condições do tratamento dos dados.

O titular dos dados deve, ainda, ser informado do carácter obrigatório ou facultativo da resposta e possíveis consequências no caso de não responder[280].

O titular dos dados tem o direito de se opor ao tratamento[281] e, não se opondo, mantém sempre o direito de acesso aos mesmos[282] – livre e sem restrições, com periodicidade razoável e sem demora ou custos excessivos –; bem como o direito a exigir do responsável pelo tratamento a sua retificação (e atualização), bloqueio e apagamento[283] [284].

O direito ao apagamento, consagrado no artigo 12.º, alínea b), da Diretiva 95/46/CE configura-se numa garantia do direito ao esquecimento[285].

Finalmente, o titular dos dados tem o direito de não ficar sujeito a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento[286] [287]; e o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido devido ao tratamento ilícito de dados ou a qualquer outro ato incompatível com as disposições nacionais de execução da Diretiva[288].

Os direitos dos titulares dos dados têm de ser garantidos pelo responsável pelo tratamento. Sobre este impendem as obrigações de prestar

[280] Artigo 10.º da Diretiva 95/46/CE.
[281] Artigo 14.º da Diretiva 95/46/CE.
[282] Artigo 12.º da Diretiva 95/46/CE.
[283] Artigo 12.º, alínea b), da Diretiva 95/46/CE.
[284] Sobre os direitos de acesso, retificação, atualização, bloqueio e apagamento do titular dos dados na Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 247 a 257.
[285] O direito ao esquecimento também se encontra presente na previsão que impõe que os dados devem ser conservados apenas pelo período necessário às finalidades do tratamento, em conformidade com a alínea e) do n.º 1 do artigo 6.º da Diretiva 95/46/CE. Neste sentido, CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 239 e ss..
[286] Artigo 15.º da Diretiva 95/46/CE.
[287] Sobre o direito do titular dos dados de não ficar sujeito a uma decisão individual automatizada na Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 261 e 262.
[288] Artigo 23.º da Diretiva 95/46/CE.

as informações[289] ao titular dos dados e de garantir o exercício dos direitos de acesso, retificação (e atualização), bloqueio e apagamento dos dados, livre e sem restrições, com periodicidade razoável e sem demora ou custos excessivos[290].

Além destas obrigações, outras resultam da aplicação da Diretiva para o responsável do tratamento.

A Diretiva estipula que o tratamento de dados pessoais só poderá ser tido como lícito se forem respeitados os chamados "princípios relativos à qualidade dos dados" – que se traduzem nas condições gerais de licitude do tratamento de dados pessoais – vertidos no seu artigo 6.º [291] [292].

O responsável pelo tratamento de dados está obrigado a respeitar estes princípios, aquando de qualquer tratamento de dados pessoais.

Assim, e de acordo com a alínea a) do n.º 1 do artigo 6.º da Diretiva, os Estados-Membros devem estabelecer que os dados pessoais serão "objeto de um tratamento leal e lícito"[293].

Como explica Catarina Sarmento e Castro[294], a lealdade do tratamento relaciona-se com o princípio geral da transparência que, como vimos, tem como afloramentos os direitos reconhecidos ao titular dos dados.

Por sua vez, a licitude do tratamento afere-se pela verificação do cumprimento das regras nacionais, comunitárias, europeias e internacionais, a que o tratamento de dados em causa está sujeito[295].

Da alínea b) do n.º 1 do artigo 6.º [296] decorre o princípio da finalidade[297], que consagra que os Estados-Membros devem estabelecer que

[289] Artigo 10.º da Diretiva 95/46/CE.
[290] Artigo 12.º da Diretiva 95/46/CE.
[291] Sobre os direitos de acesso, retificação e atualização do titular dos dados na Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 247 a 251.
[292] Sobre os princípios fundamentais para o tratamento de dados pessoais consagrados na Lei n.º 67/98, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 229 a 237.
[293] Artigo 6.º, n.º 1, alínea a), da Diretiva 95/46/CE.
[294] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 235.
[295] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 235.
[296] Este artigo tem inspiração no artigo 5.º, n.º 1, alínea b) da Convenção n.º 108 do Conselho da Europa, que consagra que os dados de carácter pessoal que sejam objeto de um tratamento automatizado devem ser "registados para finalidades determinadas e legítimas, não podendo ser utilizados de modo incompatível com essas finalidades".

os dados pessoais serão "recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades", ressalvando que "o tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-Membros estabeleçam garantias adequadas".

Assim, os dados pessoais em causa só podem ser utilizados para finalidade(s) determinada(s), e legítima(s). A(s) finalidade(s) têm de ser conhecidas antes do início da recolha dos dados, têm de estar claramente determinadas e ser conhecidas do seu titular ("pessoa em causa"), e não podem ser contrárias à lei.

Estes requisitos têm de ser preenchidos por todas as finalidades a que o tratamento se propuser, sob pena de ilicitude do tratamento. Os dados não podem ser tratados para finalidade distinta da definida na recolha, mas apenas para finalidades "compatíveis" com esta. [298]

Cataria Sarmento e Castro ajuda-nos a perceber o que deve entender-se por finalidade "compatível"[299], esclarecendo que a finalidade do tratamento será compatível com a finalidade da recolha nos casos em que o titular dos dados (a "pessoa em causa") pudesse antecipar que os dados poderiam ser tratados para aquela finalidade, ou quando o tratamento se mostre necessário para cumprimento de requisitos de proteção de dados resultantes da Lei. Em todo o caso, é exigido um juízo de proporcionalidade[300].

A utilização de dados para fins não determinados na recolha pode, no entanto, não ser considerado incompatível com as finalidades da recolha nos

[297] Sobre o princípio da finalidade na Lei n.º 67/98, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 229 a 235.
[298] O artigo 6.º, n.º 4, da proposta de Regulamento Geral de Proteção de Dados introduz a possibilidade do tratamento posterior dos dados para fins incompatíveis, no caso de poder ser encontrado outro fundamento jurídico (com exceção do interesse
legítimo do responsável pelo tratamento). O Grupo do Artigo 29.º para a Proteção de Dados manifestou a sua preocupação em relação a esta norma, e "embora não ponha em causa a necessidade de deixar em aberto a possibilidade de os dados serem tratados posteriormente para outros fins", " considera que esta disposição é contrária ao princípio geral da limitação das finalidades que é um dos principais conceitos de proteção de dados na Europa", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 01/2012 sobre as propostas de reforma em matéria de proteção de dados* (WP 191), de 23 de março de 2012, p. 12, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_pt.pdf, última consulta em 30 de agosto de 2013.
[299] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 231.
[300] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 231.

termos da segunda parte da alínea b) do n.º 1 do artigo 6.º da Diretiva 95/46/CE, segundo o qual compete aos Estados-Membros estabelecer garantias adequadas a essa exceção[301].

Assim, do princípio da finalidade são indissociáveis os princípios da adequação, pertinência e proporcionalidade[302], consagrados no artigo 6.º, n.º 1, alínea c) da Diretiva 95/46/CE.

De acordo com estes princípios, os dados pessoais recolhidos têm de ser adequados às finalidades definidas, pertinentes em função delas e cingir-se ao estritamente necessário às mesmas.

Por sua vez, a alínea d) do n.º 1 do artigo 6.º da Diretiva 95/46/CE remete-nos para os princípios da exatidão e atualização[303] dos dados, que impõe ao responsável pelo tratamento o dever de garantir os direitos de acesso e retificação do titular dos dados.

Os dados devem, ainda, ser conservados apenas pelo período necessário às finalidades do tratamento, em conformidade com a alínea e) do n.º 1 do artigo 6.º da Diretiva, que nos remete para o princípio da proporcionalidade da conservação dos dados.

O responsável pelo tratamento tem, ainda, as obrigações de garantir a confidencialidade[304] e a segurança do tratamento[305], bem como de assegurar que, quando ocorra uma transferência de dados para países exteriores à UE, esses países garantam um nível de proteção adequado.

Os princípios relativos à qualidade dos dados, assim como o direito à informação e o direito de acesso da pessoa em causa podem, porém, sofrer

[301] Entre nós, o tratamento de dados pessoais para finalidades diferentes das definidas na recolha carece de autorização da Comissão Nacional de Proteção de Dados, nos termos do artigo 28.º da Lei 67/98, de 28 de outubro, que transpõe para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE.
[302] Sobre o princípio da adequação, pertinência e proporcionalidade na Lei n.º 67/98, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 236 e 237.
[303] Sobre o princípio da exatidão e da atualização dos dados na Lei n.º 67/98, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 237.
[304] Artigo 16.º da Diretiva 95/46/CE.
[305] Artigo 17.º da Diretiva 95/46/CE.

derrogações e restrições a fim de salvaguardar a segurança do Estado, a defesa, a segurança pública, a repressão de infrações penais, um interesse económico ou financeiro importante de um Estado-Membro ou da UE, ou a própria proteção da pessoa em causa ou de outrem[306].

2.2.2. Os fundamentos de legitimidade do tratamento de dados pessoais – em particular, o consentimento

A licitude do tratamento não se basta com a observância dos princípios relativos à qualidade dos dados. [307]

A Diretiva n.º 95/46/CE estabelece os fundamentos – princípios – relativos à legitimidade do tratamento de Dados Pessoais, no seu artigo 7.º[308].[309]

Como explica Catarina Sarmento e Castro, a doutrina considera que a licitude do tratamento de dados depende de um duplo teste: o teste da qualidade dos dados (que se prende com os princípios que vimos no ponto anterior) e o teste da fundamentação do tratamento.[310]

Para que o tratamento de dados pessoais seja lícito é necessário que se verifique um dos fundamentos de legitimidade previstos do artigo 7.º.

[306] Artigo 13.º da Diretiva 95/46/CE.
[307] Neste sentido, CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 205 e 206.
[308] A Convenção n.º 108 "introduziu os conceitos de «tratamento leal e lícito» e de «finalidades legitimas» (artigo 5.º). No entanto, ao contrário da Diretiva 95/46/CE, não forneceu uma lista de critérios para aferir a legitimidade do tratamento de dados.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., nota de rodapé 6, p. 5.
[309] Sobre os fundamentos do tratamento de dados pessoais previstos na Lei n.º 67/98, CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 205 a 213.
[310] CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 205 e 206.

Diretamente ligado à ideia de autodeterminação informativa[311], o consentimento da pessoa em causa apresenta-se como um conceito-chave no que respeita à proteção de dados pessoais.[312]

A Diretiva da Proteção de Dados reconhece o consentimento inequívoco da pessoa em causa como uma das condições legitimadoras do tratamento de dados, na alínea a) do artigo 7.º.

Como pressuposto geral de licitude do tratamento de dados, o consentimento tem sempre de ser, simultaneamente, livre, específico, informado e, ainda, inequívoco[313].

O artigo 2.º alínea h), da Diretiva define "consentimento da pessoa em causa" 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".

Para que possa ser considerado livre, o consentimento tem de ser prestado sem qualquer pressão, coação, intimidação, ou sob a ameaça ou risco de que a sua recusa resulte em prejuízos ou quaisquer consequências negativas para a pessoa em causa[314]. As consequências do consentimento ou não consentimento não podem comprometer a liberdade de escolha, sob pena de a opção de o prestar não ser livre.

[311] Sobre o direito à autodeterminação informativa, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 22 a 29.
[312] "O consentimento está relacionado com o conceito de autodeterminação informativa. A autonomia da pessoa em causa é simultaneamente uma condição prévia e uma consequência do consentimento: dá à pessoa em causa influência sobre o tratamento de dados.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 10.
[313] Artigo 7.º, alínea a), da Diretiva 95/46/CE.
[314] "Entende-se por "livre" consentimento uma decisão voluntária, tomada por uma pessoa na posse de todas as suas faculdades, sem qualquer tipo de coerção, de carácter social, financeiro, psicológico ou outro. Num contexto médico, o consentimento sob a ameaça de não tratamento ou de tratamento de menor qualidade não pode ser considerado "livre". 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.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE)* (WP 131), de 15 de fevereiro de 2007, p. 9, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_pt.pdf, última consulta em 30 de agosto de 2013.

O consentimento será específico quando à pessoa em causa tenham sido dadas, de modo inteligível, informações específicas sobre a finalidade do tratamento, que não pode ser vaga ou genérica.

É no momento da recolha, assim como em qualquer momento posterior em que se observe alguma alteração à finalidade do tratamento, que o consentimento deve ser prestado, sob pena de ser considerado ilícito.

O consentimento é informado quando se baseia "numa apreciação e compreensão dos factos e implicações de uma ação", devendo a pessoa em causa "receber, de forma clara e compreensível, informações exatas e completas sobre todas as questões pertinentes, designadamente as especificadas nos artigos 10.° e 11.° da Diretiva, como a natureza dos dados tratados, as finalidades do tratamento, os destinatários das eventuais transferências e os seus direitos. Isto implica igualmente a consciência das consequências do não consentimento do tratamento em questão"[315].

O titular dos dados deve, pois, ser informado sobre a finalidade da recolha e do tratamento dos seus dados; sobre a eventual comunicação (transmissão) dos seus dados, sobre a identidade quer do responsável pelo tratamento, quer de eventuais destinatários dos seus dados e, eventualmente, dos representantes destes; sobre as condições do tratamento dos dados, sobre o carácter obrigatório ou facultativo da resposta e possíveis consequências no caso de não responder; sobre a existência do direito ao acesso aos dados que lhe digam respeito e do direito de os ratificar[316].

O consentimento será inequívoco quando se basear em declarações ou atos que manifestem aceitação. Desta definição decorre que o consentimento se tem de traduzir numa ação, não podendo ser inferido de uma omissão[317]. Tem de ser, necessariamente "uma manifestação de vontade", "inequívoca", "pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento".

[315] ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento ... saúde electrónicos (RSE)*, cit. p. 9.
[316] Artigo 10.º da Diretiva 95/46/CE.
[317] Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 13.

Para ser considerado inequívoco, o consentimento tem de ser obtido a partir de um procedimento que não pode dar espaço a qualquer dúvida quando à intenção da pessoa[318].

No entanto, o consentimento não é o único fundamento previsto para o tratamento de dados pessoais.

Podem, ainda, legitimar o tratamento outros cinco fundamentos legais sujeitos, porém, a um "teste de necessidade", que limita o seu âmbito de aplicação[319].

Assim, o tratamento de dados pode igualmente ser lícito se for necessário: para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa [320]; ou para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito [321]; ou para a proteção de interesses vitais da pessoa em causa[322]; ou para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados[323]; ou para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa[324].

Atendendo ao caso concreto, pode acontecer que mais do que fundamento sejam chamados a legitimar um tratamento de dados.

---

[318] Neste sentido, Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 23.
"Dito de outro modo, a manifestação pela qual a pessoa aceita que os seus dados sejam objeto de tratamento deve ser inequívoca quanto à sua intenção. Se existir uma dúvida razoável quanto à intenção da pessoa, existirá ambiguidade.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 23.
[319] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 8.
[320] Artigo 7.º, alínea b), da Diretiva 95/46/CE.
[321] Artigo 7.º, alínea c), da Diretiva 95/46/CE.
[322] Artigo 7.º, alínea d), da Diretiva 95/46/CE.
[323] Artigo 7.º, alínea e), da Diretiva 95/46/CE.
[324] Artigo 7.º, alínea f), da Diretiva 95/46/CE.

O Grupo do Artigo 29.º oferece-nos um exemplo elucidativo da aplicação simultânea de vários fundamentos: numa situação em que está em causa a aquisição de um automóvel, os dados necessários para comprar o automóvel seriam licitamente tratados ao abrigo da alínea b) do artigo 7.º, enquanto que os dados necessários para tratar dos documentos do automóvel sê-lo-iam ao abrigo da alínea c), os dados necessário para serviços de gestão de clientes, ao abrigo da alínea f) e os dados necessário para transferir os dados a terceiros para as suas próprias cativídades de comercialização, ao abrigo da alínea a)[325].

Como vemos, o teste da necessidade limita o responsável ao tratamento estritamente indispensável, sendo que em tudo que o exceda deve obter outro fundamento legitimante.

Para que o tratamento de dados pessoais seja lícito é, portanto, necessário que encontre preenchido, pelo menos, um dos fundamentos de legitimidade. Não obstante, importa reter que nenhum desses fundamentos – nem sequer o consentimento[326] – exonera o responsável pelo tratamento das obrigações relativas à qualidade dos dados, elencadas no artigo 6.º da Diretiva da Proteção de Dados.

2.2.2.1. O Consentimento como fundamento específico para tratamento de dados pessoais sensíveis e para a transferência de dados para países terceiros que não assegurem um nível de proteção adequado

Além de fundamento geral de licitude, o consentimento aparece ainda como um fundamento específico no caso do tratamento de dados pessoais

[325] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 9.
[326] "Por principio, o consentimento não devia ser visto como uma derrogação aos outros princípios de proteção de dados, mas sim como uma salvaguarda. O consentimento é, antes de mais, um fundamento de licitude, não afastando a aplicação de outros princípios.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 9.

sensíveis[327] – em que o consentimento da pessoa em causa tem de ser explícito[328] – e no caso da transferência de dados para países terceiros que não assegurem um nível de proteção considerado adequado pelo direito da União[329].

O tratamento de certas categorias específicas de dados – ou dados pessoais sensíveis, como comummente são referidos – é, em princípio, proibido.

Excecionalmente, o tratamento de dados pessoais sensíveis é permitido quando a pessoa em causa para tal dê o seu consentimento explícito. Esta é a única situação em que a Diretiva expressamente requer que o consentimento prestado seja explícito[330].

O consentimento é explícito quando é manifestado de forma expressa. Ou seja, no caso do tratamento de dados sensíveis, o consentimento da pessoa em causa não pode ser inferido de um ato tendente a expressar a sua manifestação de aceitação, sem mais. Deve, sim, resultar da resposta ativa à questão que lhe apresenta a oportunidade de dar ou não o seu acordo para um uso especial ou divulgação da informação pessoal que lhes diz respeito.

[327] Sobre o consentimento enquanto fundamento específico para o tratamento de dados pessoais sensíveis na Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 88 a 99 e pp. 215 a 222.
[328] Artigo 8.º, n.º 2, alínea a), da Diretiva 95/46/CE.
[329] Artigo 26.º, n.º 1, alínea a), da Diretiva 95/46/CE.
[330] Como analisaremos melhor no Título 2.4. deste Capítulo II, a Proposta de Regulamento Geral de Proteção de Dados da Comissão Europeia introduz na definição de consentimento o requisito de que este tem de ser explícito. Assim, a ser aprovado o texto avançado, o consentimento explícito será exigido não só para o tratamento de dados pessoais sensíveis mas para todos os tratamentos de dados pessoais legitimados pelo consentimento da pessoa em causa. COMISSÃO EUROPEIA, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)*, COM(2012) 11 final 2012/0011 (COD), disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf*, última consulta em 21 de outubro de 2013.*

O consentimento explícito é prestado verbalmente ou por escrito, através de um ato pelo qual o titular expressa a sua opção de aceitar uma forma de tratamento de dados pessoais que lhe dizem respeito[331].

A Diretiva 95/46/CE prevê, no entanto, outras situações excecionais que podem legitimar o tratamento de certas categorias específicas de dados. Assim será quando o tratamento for necessário para o cumprimento das obrigações e dos direitos do responsável pelo tratamento no domínio da legislação do trabalho, desde que o mesmo seja autorizado por legislação nacional que estabeleça garantias adequadas[332]; ou quando a pessoa em causa se encontre física ou legalmente incapaz de prestar o seu consentimento e o tratamento for necessário para proteger interesses vitais desta ou de uma outra pessoa[333]; ou quando o tratamento for efetuado por uma fundação, uma associação ou qualquer outro organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas atividades legítimas e com as garantias adequadas, na condição de o tratamento dizer unicamente respeito aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem o consentimento das pessoas em causa[334]; ou o tratamento disser respeito a dados manifestamente tornados públicos pela pessoa em causa ou for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial[335]. O tratamento de dados pessoais sensíveis é, ainda possível quando for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços da saúde e quando o tratamento desses dados for efetuado por um profissional da saúde obrigado ao segredo profissional pelo direito nacional ou por regras estabelecidas pelos organismos nacionais

[331] "Num ambiente on-line, o consentimento explícito pode ser dado através de assinaturas eletrónicas ou digitais. Contudo, pode também ser dado clicando num botão, dependendo do contexto, enviando mensagens de correio electrónico de confirmação, clicando em ícones, etc.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 29.
[332] Artigo 8.º, n.º 2, alínea b), da Diretiva 95/46/CE.
[333] Artigo 8.º, n.º 2, alínea c), da Diretiva 95/46/CE.
[334] Artigo 8.º, n.º 2, alínea d), da Diretiva 95/46/CE.
[335] Artigo 8.º, n.º 2, alínea e), da Diretiva 95/46/CE.

competentes, ou por outra pessoa igualmente sujeita a uma obrigação de segredo equivalente[336].

As derrogações à proibição geral, podem, ainda, ser outras além das previstas na Diretiva. Aos Estados-membros é permitido estabelecer, por motivos de interesse público importante, outras derrogações através de disposições legislativas nacionais ou de decisões da autoridade de controlo, desde que prestadas as garantias adequadas[337].

É permitido, ainda, sob reserva das derrogações que poderão ser concedidas pelo Estado-membro com base em disposições nacionais que prevejam garantias específicas e adequadas, o tratamento de dados relativos a infrações, condenações penais ou medidas de segurança se efetuado sob o controlo das autoridades públicas ou se o direito nacional estabelecer garantias adequadas e específicas. O registo completo das condenações penais deve, no entanto, ser mantido sob o controlo das autoridades públicas[338].

O consentimento enquanto fundamento específico para a transferência de dados para países terceiros que não assegurem um nível de proteção considerado adequado[339] pelo direito da União tem de ser inequívoco[340]. O alcance deste requisito é o mesmo que encontramos no artigo 7.º, alínea a), da Diretiva.

Os fundamentos alternativos ao consentimento que podem legitimar a transferência de dados para países que não assegurem um nível de proteção adequado[341] são semelhantes às condições que legitimam o tratamento de dados pessoais[342].

---

[336] Artigo 8.º, n.º 3, da Diretiva 95/46/CE.
[337] Artigo 8.º, n.º 4, da Diretiva 95/46/CE.
[338] Artigo 8.º, n.º 5, da Diretiva 95/46/CE.
[339] A Comissão Europeia reconheceu que asseguram um nível de proteção adequado a Andorra, a Argentina, a Austrália, o Canadá, a Suíça, as Ilhas Faroé, Guernsey, o Estado de Israel, a Ilha de Man, Jersey, os Princípios da Privacidade em Porto Seguro (Safe Harbor) do Departamento de Comércio dos Estados Unidos, e a transferência de registo de nomes de passageiros aéreos para o Bureau of Customs and Border Protection dos Estados Unidos. Cf. COMISSÃO EUROPEIA, *Commission decisions on the adequacy of the protection of personal data in third countries*, disponível em http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm, última consulta em 15 de outubro de 2013.
[340] Artigo 26.º, n.º 1, alínea a), da Diretiva 95/46/CE.
[341] "Em derrogação ao disposto no artigo 25º e sob reserva de disposições em contrário do seu direito nacional em casos específicos, os Estados-membros estabelecerão que a transferência de dados pessoais para um país terceiro que não assegure um nível de proteção adequado na acepção do nº 2 do artigo 25º poderá ter lugar desde que: a) A pessoa em causa tenha dado de forma inequívoca o seu consentimento à transferência; ou b) A transferência seja

A particularidade é que o consentimento – ou alguma das situações alternativas sujeitas ao teste da necessidade – tem de se verificar em relação à transferência para o país terceiro que não assegurem um nível de proteção considerado adequado.

Assim, o consentimento prestado nos termos do artigo 7.º, alínea a), para o tratamento não legitima, por si só, a transferência. É necessário que além de uma condição legitimante do tratamento se verifique, cumulativamente, uma condição legitimante para a transferência [343]. O consentimento livre, específico, informado e inequívoco da pessoa em causa é uma dessas condições[344].

2.3. A Proteção da Privacidade no Sector das Comunicações Eletrónicas

A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) – Diretiva da Privacidade Eletrónica – veio substituir a Diretiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações, que transpôs os princípios estabelecidos na Diretiva 95/46/CE em regras específicas para o sector das telecomunicações[345].

---

necessária para a execução de um contrato entre a pessoa em causa e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou c) A transferência seja necessária à execução ou celebração de um contrato celebrado ou a celebrar, no interesse da pessoa em causa, entre o responsável pelo tratamento e um terceiro; ou d) A transferência seja necessária ou legalmente exigida para a proteção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial; ou e) A transferência seja necessária para proteger os interesses vitais da pessoa em causa; ou f) A transferência seja realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta pelo público em geral ou por qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.", Artigo 26.º, n.º 1, da Diretiva 95/46/CE.

[342] Condições elencadas no artigo 7.º da Diretiva 2002/58/CE.

[343] Artigo 26.º, n.º 1, da Diretiva 95/46/CE.

[344] Artigo 26.º, n.º 1, alínea a), da Diretiva 95/46/CE.

[345] Considerando 4 da Diretiva 2002/58/CE.

Com um enfoque direcionado aos serviços de telefónicos fixos[346], Diretiva 97/66/CE mostrava-se desadequada a proteger eficazmente a privacidade das pessoas na realidade imposta pela Sociedade da Informação para que irreversivelmente transitava a Europa.

As transformações registadas no mercado das comunicações promovidas pelo progresso tecnológico, pelo crescimento e diversificação das ofertas dos serviços, pela convergência dos sectores das telecomunicações, da radiodifusão e das tecnologias da informação, tornavam desadequado o regime em vigor e impunham a necessidade de regular a proteção dos dados pessoais e da privacidade aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas[347] [348].

A Diretiva 2002/58/CE, entretanto alterada pela Diretiva 2009/136/CE Parlamento Europeu e do Conselho, de 25 de Novembro[349], estabelece um regime específico para a privacidade no sector das comunicações eletrónicas.

Trata-se, portanto, de legislação especial face à Diretiva da Proteção de Dados[350].

Assim, "no sector das comunicações eletrónicas, é aplicável a Diretiva 95/46/CE, especialmente no que se refere a todas as questões relacionadas

---

[346] KOSTA, Eleni, *Consent in European ...* , op. citada, p. 263.

[347] Neste sentido, COMISSÃO EUROPEIA, *Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões, de 10 de novembro de 1999 - Para um novo quadro das infraestruturas das comunicações eletrónicas e serviços conexos* - Análise das comunicações - 1999 [COM(1999) 539 final, 10.11.1999 - Não publicado no Jornal Oficial], disponível em http://europa.eu/legislation_summaries/internal_market/single_market_services/l24216_pt.htm, última consulta em 20 de junho de 2013.

[348] Remetemo-nos aqui para o princípio da neutralidade tecnológica, que serve de base a todo o quadro regulamentar das redes e serviços de comunicações eletrónicas de 2002, e que consiste em "não impor nem favorecer de modo discriminatório a utilização de um dado tipo de tecnologia, mas garantir que o mesmo serviço seja regulamentado de modo equivalente, independentemente dos meios utilizados no seu fornecimento", COMISSÃO EUROPEIA, *Comunicação ... serviços conexos*, cit..

[349] Esta é, na verdade, a segunda alteração à Diretiva 2002/58/CE, tendo a primeira sido levada a cabo pela Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

A Diretiva 2006/24/CE teve por objetivo harmonizar as disposições dos Estado-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves (artigo 1.º, n.º 1). Nesse sentido, foi aditado o n.º 1-A ao artigo 15.º da Diretiva 2002/58/CE.

[350] Diretiva 95/46/CE.

com a proteção dos direitos e liberdades fundamentais não abrangidos especificamente pelas disposições da presente diretiva (Diretiva 2002/58/CE), incluindo as obrigações que incumbem à entidade que exerce o controlo e os direitos das pessoas singulares"[351].

A Diretiva 2002/58/CE representa, pois, um complemento da Diretiva 95/46/CE, com vista à proteção da privacidade num sector específico e particularmente importante no que respeita ao tratamento de dados.

A Diretiva da Privacidade Eletrónica forma o quadro regulamentar das redes e serviços de comunicações eletrónicas conjuntamente com a Diretiva 2002/19/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos (Diretiva «Acesso») [352] , a Diretiva 2002/20/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa à autorização de redes e serviços de comunicações eletrónicas (Diretiva «Autorização») [353] , a Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de marco de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (Diretiva-Quadro)[354] e a Diretiva 2002/22/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas (Diretiva «Serviço Universal»)[355].

Este quadro regulamentar tem em vista a criação de um mercado interno das comunicações eletrónicas na Comunidade, e garantir ao mesmo tempo um elevado nível de investimento, inovação e proteção dos consumidores através do reforço da concorrência. Aplica-se todos os tipos de redes e serviços de comunicações eletrónicas e já não apenas às

[351] Considerando 10 da Diretiva 2002/58/CE.
[352] Alterada pela Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009.
[353] Alterada pela Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009.
[354] Modificada pelo Regulamento (CE) n. o 717/2007 do Parlamento Europeu e do Conselho, de 27 de junho de 2007, relativo à itinerância nas redes telefónicas móveis públicas da Comunidade, pelo Regulamento (CE) n. o 544/2009 do Parlamento Europeu e do Conselho, de 18 de junho de 2009 e pela Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009. Este regulamento
[355] Alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009.

telecomunicações e consagra o princípio da neutralidade tecnológica, que consiste em "não impor nem favorecer de modo discriminatório a utilização de um dado tipo de tecnologia, mas garantir que o mesmo serviço seja regulamentado de modo equivalente, independentemente dos meios utilizados no seu fornecimento"[356]

"Os serviços de comunicações eletrónicas publicamente disponíveis através da Internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais e à sua privacidade"[357].

As redes de comunicações eletrónicas, acessíveis a um vasto público, com capacidade crescente em termos de armazenamento e de processamento informático de dados, bem como o desenvolvimento transfronteiriço de serviços, impunham o surgimento de regulamentação específica do sector das comunicações eletrónicas.

A confiança dos utilizadores nestas redes foi um importante fator do seu sucesso e rápida expansão.

A Diretiva 2002/58/CE tem um duplo objetivo, como acontece com a Diretiva geral da Proteção de Dados. O diploma vem harmonizar as disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no sector das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade"[358].

As disposições desta Diretiva, em complemento do que acontece com a Diretiva da Proteção de Dados, vieram assegurar a proteção dos legítimos

[356] COMISSÃO EUROPEIA, *Comunicação ... serviços conexos*, cit..
[357] Considerando 6 da Diretiva 2002/58/CE.
[358] Artigo 1.º, n.º 1, da Diretiva 2002/58/CE, com a redação que lhe foi dada pela Diretiva 2009/136/CE.

interesses das pessoas coletivas, enquanto assinantes de um de um serviço de comunicações eletrónicas[359].

A Diretiva da Privacidade Eletrónica é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas publicamente disponíveis nas redes públicas de comunicações da Comunidade[360].

Ora, para efeitos de aplicação da Diretiva, o termo "comunicação" é definido como "qualquer informação trocada ou enviada entre um número finito de partes, através de um serviço de comunicações eletrónicas publicamente disponível", sendo que não se incluem no conceito "as informações enviadas no âmbito de um serviço de difusão ao público em geral, através de uma rede de comunicações eletrónicas, exceto na medida em que a informação possa ser relacionada com o assinante ou utilizador identificável que recebe a informação"[361].

A Diretiva 2002/58/CE, define "assinante" como "a pessoa singular ou coletiva que é parte num contrato com um prestador de serviços de comunicações eletrónicas acessíveis ao público para o fornecimento desses serviços"[362].

Como "utilizador" define-se "qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço"[363].

---

[359] Artigo 1.º, n.º 2, da Diretiva 2002/58/CE.

[360] A Diretiva 2002/58/CE é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrônicas acessíveis ao público em redes de comunicações públicas na Comunidade, nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação, de acordo com o artigo 3.º da Diretiva 2002/58/CE, com a redação que lhe foi dada pela Diretiva 2009/136/CE.
Como ficou expressamente esclarecido com a Diretiva 2009/136/CE (Considerando 55), os grupos fechados de utilizadores, bem como as redes empresariais, estão excluídos do âmbito de aplicação da Diretiva da Privacidade Eletrónica.

[361] Artigo 2.º, alínea d), e Considerando 16 da Diretiva 2002/58/CE.

[362] Artigo 2.º, alínea k), da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), por remissão do artigo 2.º da Diretiva 2002/58/CE.

[363] Artigo 2.º, alínea a), da Diretiva 2002/58/CE.

No que respeita à clarificação do conceito de "serviço de comunicações eletrónicas" a Diretiva define-o como um "serviço oferecido em geral mediante remuneração, que consiste total ou principalmente no envio de sinais através de redes de comunicações eletrónicas, incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão, excluindo os serviços que prestem ou exerçam controlo editorial sobre conteúdos transmitidos através de redes e serviços de comunicações eletrónicas; excluem-se igualmente os serviços da sociedade da informação[364], tal como definidos no artigo 1.º da Diretiva 98/34/CE[365], que não consistam total ou principalmente no envio de sinais através de redes de comunicações eletrónicas"[366] [367].

São "rede de comunicações eletrónicas" os "sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos, nomeadamente elementos da rede que não se encontrem ativos, que permitem o envio de sinais por cabo, feixes hertzianos, meios óticos, ou por outros meios eletromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de eletricidade, na medida em que são utilizados para a transmissão de sinais, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida."[368].

[364] Sobre o conceito de sérvios da sociedade da informação ver AUTORES VÁRIOS, *Lei do Comércio ...* , op. cit., anotação ao artigo 3.º, pp. 24 e ss..
[365] Diretiva 98/34/CE, do Parlamento Europeu e do Conselho, de 22 de junho de 1998, alterada pela Diretiva 98/48/CE do Parlamento Europeu e do Conselho, de 20 de julho de 1998.
[366] Artigo 2.º, alínea c), da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), por remissão do artigo 2.º da Diretiva 2002/58/CE.
[367] Os serviços de comunicações eletrónicas são serviços na acepção do artigo 57.º do Tratado Sobre o Funcionamento da União Europeia.
[368] Artigo 2.º, alínea a), da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), com a redação que lhe foi dada pela Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, por remissão do artigo 2.º da Diretiva 2002/58/CE.
A alínea m) do Artigo 2.º da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho define "oferta de rede de comunicações eletrónicas" como o "estabelecimento, operação, controlo ou disponibilização da referida rede".

Mas o âmbito de aplicação da Diretiva da Privacidade Eletrónica limita-se aos serviços de comunicações eletrónicas que sejam publicamente disponíveis nas redes de comunicações públicas.

Ora, são públicas as redes de comunicações utilizadas "total ou principalmente para o fornecimento de serviços de comunicações eletrónicas acessíveis ao público e que serve de suporte à transferência de informações entre os pontos terminais da rede"[369].

Assim, uma rede de comunicação é pública para efeitos da Diretiva se for utilizada para o fornecimento de serviços de comunicações eletrónicas acessíveis ao público.

Por sua vez, os serviços de comunicações eletrónicas acessíveis ao público implicam a utilização de redes de comunicação públicas[370] [371].

A questão de saber quando é que uma rede de comunicações ou um serviço são públicos não é de resposta fácil. Desde logo, imagine-se, por exemplo, os casos de acesso à internet nos cibercafés ou outros estabelecimentos abertos ao público em que o serviço de comunicações em causa (acesso à internet), é disponibilizado ao público, não através de uma rede pública, mas antes de uma rede que se pode considerar privada.

A Autoridade Europeia para a Proteção de Dados, no seu segundo parecer da sobre a revisão da Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, deu o seu contributo para a clarificação da questão propondo que "se a rede for intencionalmente tornada acessível ao público para o fornecimento de um serviço público de comunicações (...) o serviço/rede em causa ficará abrangido pela Diretiva de Privacidade e Comunicações Eletrónicas".[372]

---

[369] Artigo 2.º, alínea d), da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), com a redação que lhe foi dada pela Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, por remissão do artigo 2.º da Diretiva 2002/58/CE.

[370] Neste sentido, KOSTA, Eleni, *Consent in European ...* , op. citada, p. 274.

[371] Só encontramos uma definição de "serviços de comunicações eletrónicas públicas" na alínea 4) do artigo 1.º da Diretiva 2002/77/CE da Comissão, de 16 de setembro de 2002, relativa à concorrência nos mercados de redes e serviços de comunicações eletrónicas. Porém, a definição avançada por esta Diretiva não particularmente esclarecedora, já que de acordo a mesma são serviços de comunicações eletrónicas públicas os "serviços de comunicações eletrónicas publicamente disponíveis".

[372] Sobre a inexistência de uma interpretação consistente do termo "público" no contexto de serviços e redes de comunicação, ver KOSTA, Eleni, *Consent in European ...* , op. citada, p. 275.

2.3.1. Alguns dos principais aspectos regulados pela Diretiva 2002/58/CE

Sem nos demoramos numa análise exaustiva da Diretiva 2002/58/CE – que extravasaria os limites do nosso trabalho –, façamos uma rápida incursão em alguns dos aspetos regulados por esta, atendendo, num primeiro momento, ao regime jurídico estabelecido pela sua versão original.

A Diretiva 2002/58/CE impõe obrigações ao prestador de serviço de comunicações eletrónicas publicamente disponível. Desde logo, impõe-lhe deveres com vista à segurança dos serviços.

Estipula o artigo 4.º que o prestador do serviço tem o dever de adotar as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, impondo-lhe, ademais, em caso de risco especial de violação da segurança da rede, o dever de fornecer informação aos assinantes, completadas com indicações adicionais quando o risco se situe fora do âmbito das medidas que lhe compete tomar.

O diploma em apreço dispõe, igualmente, sobre os chamados "dados de tráfego", por que faz entender "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma"[373].

O artigo 6.º da Diretiva 2002/58/CE determina que estes dados devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação, podendo, no entanto, ser tratados licitamente os que forem necessários para efeitos de faturação dos assinantes e de pagamento de interligações até final do período durante o qual a fartura pode ser legalmente contestada ou o pagamento reclamado.

[373] Artigo 2.º, alínea b), da Diretiva 2002/58/CE.

Neste último caso, o prestador de serviços tem a obrigação de informar o assinante ou utilizador dos tipos de dados de tráfego que são tratados.

Para efeitos de comercialização dos serviços de comunicações eletrónicas ou para o fornecimento de serviços de valor acrescentado, o prestador de serviço podia tratar os dados de tráfego na medida do necessário e pelo tempo necessário para a prestação desses serviços ou dessa comercialização, se o assinante ou utilizador a quem os dados dissessem respeito tivesse dado o seu consentimento.

Ou seja, ao teste da necessidade a que se sujeita a conservação dos dados cumulava-se a exigência do consentimento da pessoa em causa quando a finalidade fosse a comercialização de serviços de comunicações ou o fornecimento de serviços de valor acrescentado. Neste caso, o prestador do serviço tem, além da obrigação de prestar informações sobre o tipo de dados de tráfego tratados, a de garantir ao utilizador ou assinante o direito de retirar a qualquer momento o seu consentimento para o tratamento dos dados de tráfego.

Já os dados, além dos dados de tráfego, que indiquem a posição geográfica do equipamento terminal de um utilizador (dados de localização)[374] só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado, nos termos do estipulado no artigo 9.º da Diretiva 2002/58/CE. O prestador de serviços tem a obrigação de informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado e de garantir o direito destes de retirar em qualquer momento o seu consentimento e recusar temporariamente o tratamento desses dados para cada ligação à rede ou para cada transmissão de uma comunicação.

[374] Artigo 2.º, alínea c), da Diretiva 2002/58/CE.

No que respeita às listas de assinantes, prevê o artigo 12.º da Diretiva, que estes devem ser informados dos fins a que aquelas se destinam, bem como de quaisquer outras possibilidades de utilização baseadas em funções de procura incorporadas em versões eletrónicas da lista. Estas informações devem ser disponibilizadas ao assinante gratuitamente, e antes de os seus dados serem incluídos naquelas.

Aos assinantes deve ser dada a "possibilidade de decidir da inclusão dos seus dados pessoais numa lista pública e, em caso afirmativo, de quais os dados a incluir, na medida em que esses dados sejam pertinentes para os fins a que se destinam as listas, como estipulado pelo fornecedor das listas, bem como de verificar, corrigir ou retirar esses dados"[375].

O legislador comunitário veio permitir aos Estados-Membros, aquando da transposição, optar pela exigência de que o "consentimento adicional dos assinantes seja solicitado para qualquer utilização de uma lista pública que não a busca de coordenadas das pessoas com base no nome e, se necessário, num mínimo de outros elementos de identificação"[376].

A Diretiva da Privacidade Eletrónica regula, também, e pela primeira vez, no seu artigo 13.º, as comunicações não solicitadas (*spam*), estabelecendo a necessidade de consentimento prévio do assinante como fundamento da legalidade da utilização de sistemas de chamada automatizados sem intervenção humana, de aparelhos de fax ou correio eletrónico para fins de comercialização direta.

No entanto, se "uma pessoa singular ou coletiva obtiver dos seus clientes coordenadas eletrónicas de contacto para correio eletrónico, no contexto da venda de um produto ou serviço" pode usá-las "para fins de comercialização direta dos seus próprios produtos ou serviços análogos, desde que aos clientes tenha sido dada clara e distintamente a possibilidade de recusarem, de forma gratuita e fácil, a utilização dessas coordenadas eletrónicas de contacto quando são recolhidos e por ocasião de cada

[375] Artigo 12.º, n.º 2, da Diretiva 2002/58/CE.
[376] Artigo 12.º, n.º 3, da Diretiva 2002/58/CE.

mensagem, quando o cliente não tenha inicialmente recusado essa utilização"[377].

Em qualquer caso, é "proibida a prática do envio de correio eletrónico para fins de comercialização direta, dissimulando ou escondendo a identidade da pessoa em nome da qual é efetuada a comunicação, ou sem um endereço válido para o qual o destinatário possa enviar um pedido para pôr termo a essas comunicações"[378].

A confidencialidade das comunicações e respetivos dados de tráfego é, igualmente, tratada pela Diretiva da Privacidade Eletrónica.

O artigo 5.º n.º 1 impõe a obrigação de assegurar a confidencialidade das comunicações "independentemente da natureza da rede e do facto de elas envolverem ou não a travessia das fronteiras com Estados não pertencentes à UE"[379].

2.3.1.1. Os testemunhos de conexão na versão original da Diretiva 2002/58/CE

A Diretiva 2002/58/CE vem, pela primeira vez, regular especialmente[380] a utilização dos testemunhos de conexão.

Expressamente referenciados no considerando 25, a utilização de testemunhos de conexão na União Europeia passa a estar sujeita às condições plasmadas no n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica. Estas aplicam-se a todos as técnicas de armazenamento e

[377] Artigo 13.º, n.º 2, da Diretiva 2002/58/CE.
[378] Artigo 13.º, n.º 4, da Diretiva 2002/58/CE.
[379] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2008 sobre a revisão da Diretiva 2002/58/CE relativa à privacidade no sector das comunicações eletrónicas (Diretiva Privacidade Eletrónica)* (WP 150), de 15 de maio de 2008, p. 7, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_pt.pdf, última consulta em 30 de agosto de 2013.
[380] A Diretiva 2002/58/CE é lei especial face à Diretiva da Proteção de Dados. O artigo 5.º, n.º 3 da Diretiva 2002/58/CE, que disciplina a utilização de testemunhos de conexão, conferindo-lhe um regime especial, não pode, no nosso entender, ser visto como a sua primeira regulação. A verdade é que enquanto mecanismo que serve à recolha e tratamento de dados pessoais, a sua utilização neste contexto cabe no âmbito da Diretiva 95/46/CE, conforme veremos melhor no Título 3.1.1.1. do Capítulo III.

acesso a informações previamente armazenadas no equipamento terminal do utilizador, e não apenas aos testemunhos de conexão.

No entanto, atendendo ao âmbito do nosso trabalho, é ao impacto da previsão plasmada no n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica na utilização dos testemunhos de conexão que dedicamos especial atenção[381].

Considerado um instrumento que pode ser "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" [382].

O equipamento terminal dos utilizadores de redes de comunicações eletrónicas e todas as informações armazenadas nesse equipamento são considerados parte integrante da esfera privada dos utilizadores e que devem ser protegidos ao abrigo da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais[383].

Os testemunhos de conexão são regulados enquanto "dispositivos" que "podem entrar nos terminais dos utilizadores sem o seu conhecimento a fim de obter acesso a informações, armazenar informações escondidas ou permitir a rastreabilidade das atividades do utilizador", análogos aos "denominados «gráficos espiões», «programas-espiões», («spyware»), «gráficos-espiões» («web bugs») e «identificadores ocultos» («hidden identifiers»)", que "podem constituir uma grave intrusão na privacidade desses utilizadores", pelo que a sua utilização deverá ser autorizada "unicamente para fins legítimos, com o conhecimento dos utilizadores em causa.[384].

[381] Neste ponto do nosso trabalho, porém, limitando-nos a uma primeira abordagem contextualizante, que desenvolveremos no Capítulo III.
[382] Considerando 25 da Diretiva 2002/58/CE.
[383] Considerando 24 da Diretiva 2002/58/CE.
[384] Considerandos 24 e 25 da Diretiva 2002/58/CE.

O n.º 3 do artigo 5.º da Diretiva 2002/58/CE, na sua versão original, permitia a utilização de redes de comunicações eletrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador, desde que fossem prestadas ao assinante ou utilizador informações claras e completas, nomeadamente sobre as finalidades do processamento e, cumulativamente, lhe fosse garantido o direito de recusar o tratamento[385] [386].

A utilização de redes de comunicações eletrónicas para o armazenamento de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador era, deste modo, permitida por defeito.

Ressalvadas ficavam as situações em que o armazenamento técnico ou o acesso visava como finalidade exclusiva efetuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação que tenha sido explicitamente solicitado pelo assinante ou pelo utilizador[387].

2.3.2 As principais alterações introduzidas pela Diretiva 2009/136/CE

Em 2009, o quadro regulamentar comunitário das redes e serviços de comunicações eletrónicas foi objeto de uma reforma com vista a completar o mercado interno das comunicações eletrónicas.

---

[385] Direito de *opt-out*.
Os designados sistemas de *opting out* e de *opting in* conheceram particular destaque no contexto das comunicações não solicitadas (spam), reguladas através do artigo 13.º da Diretiva da Privacidade Eletrónica. Trata-se, respectivamente, de um sistema de opção negativa, de acordo com o qual a difusão de mensagens não solicitadas é permitida, a menos que o destinatário se oponha a recebê-las, e de um sistema de opção positiva, que garante que só recebe estas mensagens quem se manifestar interessado em recebê-las. AUTORES VÁRIOS, Lei do Comércio ..., op. cit., anotação ao artigo 22.º, p. 84.
Entre nós, as comunicações não solicitadas eram reguladas pelo artigo 22.º da Lei do Comércio Electrónico (Decreto-Lei n.º 7/2004, de 7 de janeiro); com a Lei n.º 46/2012, o regime das comunicações não solicitadas transitou para o novo artigo 13.º-A da Lei n.º 41/2004 (que transpôs a Diretiva dos Cidadãos).
Sobre os sistemas de *opting out* e de *opting in*, ainda MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 397 a 402.
[386] Artigo 5.º, n.º 3, da Diretiva 2002/58/CE.
[387] Artigo 5.º, n.º 3, da Diretiva 2002/58/CE.

A Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, conhecida por "Diretiva dos Cidadãos", alterou a Diretiva 2002/22/CE e a Diretiva 2002/58/CE[388]. Por sua vez, a Diretiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, também conhecida por "Diretiva legislar melhor", veio alterar a Diretiva 2002/19/CE, a Diretiva 2002/20/CE e a Diretiva 2002/21/CE.

Dado o tema do nosso trabalho, vamos limitar a nossa atenção às alterações promovidas pela Diretiva dos Cidadãos à Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

A Diretiva dos Cidadãos reforça que a Diretiva 2002/58/CE visa a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos fundamentais à privacidade e à confidencialidade no que respeita ao tratamento de dados pessoais no sector das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade[389], e esclarece que se centra nas redes de comunicações públicas e serviços e comunicações eletrónicas acessíveis ao público e não se aplica a grupos fechados de utilizadores nem a redes empresariais[390].

O artigo 3.º, referente aos serviços abrangidos, adota uma nova redação que vem clarificar que as redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação se inserem no âmbito da Diretiva da Privacidade Eletrónica[391].

[388] A Diretiva 2009/136/CE alterou, ainda, o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor.
[389] Considerando 51 da Diretiva 2009/136/CE.
[390] Considerando 55 da Diretiva 2009/136/CE.
[391] Passam, desta forma, a estar indubitavelmente incluídos no âmbito de aplicação da Diretiva os dispositivos de identificação por radiofrequências (RFID) quando "ligados a redes de comunicações eletrónicas acessíveis ao público ou utilizam serviços de comunicações eletrónicas como infraestrutura de base", caso em que deverão aplicar-se as disposições da Diretiva Privacidade e Comunicações Eletrónicas, "nomeadamente as respeitantes aos dados sobre segurança, tráfego e localização e à confidencialidade" (Considerando 56 da Diretiva 2009/136/CE).

A disposição relativa à segurança do processamento (artigo 4.º) é reforçada passando a impor mais obrigações ao prestador do serviço.

São-lhe impostas, medidas técnicas e organizativas mínimas com vista a garantir segurança dos seus serviços, que passam por assegurar que somente o pessoal autorizado possa ter acesso aos dados pessoais, e apenas para fins legalmente autorizados; proteger os dados pessoais transmitidos, armazenados ou de outro modo tratados, contra a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado; e assegurar a aplicação de uma política de segurança no tratamento dos dados pessoais.

O prestador de serviços passa a estar obrigado a notificar, sem demora injustificada, a autoridade nacional competente, sempre que tenha lugar a violação de dados pessoais[392].

Por "violação de dados pessoais" passa a entender-se, de acordo com a aditada alínea h) do artigo 2.º, "uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmiti- dos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público na Comunidade".

No caso de a violação em causa afetar negativamente os dados pessoais do assinante ou utilizador, o prestador do serviço deve, ainda, notificar a violação ao assinante ou utilizador para que este possa tomar as precauções necessárias. Esta notificação não é, porém, exigida se a autoridade competente considerar que foram adotadas as medidas tecnológicas de proteção adequadas e que essas medidas foram aplicadas aos dados a que respeita a violação.

"A notificação ao assinante ou ao indivíduo indica, pelo menos, a natureza da violação de dados pessoais e os pontos de contacto onde podem

[392] O Grupo do Artigo 29.º emitiu um parecer com vista a chamar a atenção da Comissão sobre alguns pontos a serem clarificados no que respeita à obrigação notificação no caso de violação de dados pessoais: GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications* (WP 197), de 12 de julho de 2012, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp197_en.pdf, última consulta em 30 de agosto de 2013.

ser obtidas informações complementares e recomendará medidas destinadas a limitar eventuais efeitos adversos da violação dos dados pessoais" e a notificação à autoridade nacional competente "indica ainda as consequências da violação de dados pessoais e as medidas propostas ou tomadas pelo prestador para fazer face a essa violação"[393].

As autoridades competentes devem poder verificar se os prestadores cumpriram as suas obrigações de notificação e aplicar sanções adequadas em caso de não cumprimento.

Os prestadores devem, ainda, "manter um registo das violações de dados pessoais, com a indicação dos factos que lhes dizem respeito, dos seus efeitos e das medidas de reparação tomadas" que inclua apenas a informação necessária para que as autoridades nacionais competentes possam verificar o cumprimento das obrigações de notificação e comunicação impostas[394].

Apesar do reforço impresso à matéria da segurança, a obrigação de notificar violações de dados pessoais não foi estendida aos serviços da sociedade da informação[395], conforme sugeriam o parecer da Autoridade Europeia para a Proteção de Dados, as alterações do Parlamento[396] e como defendia o Grupo do Artigo 29.º.º[397].

O Grupo chamou, em tempo, a atenção para o facto de a limitação desta obrigação aos prestadores dos serviços de comunicações eletrónicas acessíveis ao público reduzir significativamente o impacto do dever de notificar violações de dados pessoais como meio de proteção dos

[393] Artigo 4.º, n.º 3, da Diretiva 2002/58/CE, aditado pela Diretiva 2009/136/CE.
[394] Artigo 4.º, n.º 4, da Diretiva 2002/58/CE, aditado pela Diretiva 2009/136/CE.
[395] "Qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços", cf. Artigo 1.º, n.º 2, da Diretiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas, alterada pela Diretiva 98/48/CE do Parlamento Europeu e do Conselho, de 20 de Julho de 1998.
Sobre o conceito de sérvios da sociedade da informação AUTORES VÁRIOS, *Lei do Comércio ...* , op. cit., anotação ao artigo 3.º, pp. 24 e ss..
[396] Alterações 187/rev e 184 do Parlamento.
[397] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2008 sobre a revisão ...* , cit., p. 3, e GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *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 sector das comunicações eletrónicas (diretiva da privacidade eletrónica)* (WP 159), de 10 de fevereiro de 2009, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_pt.pdf, última consulta em 20 de outubro de 2013.

particulares “contra os riscos de roubo de identidade, prejuízos financeiros, perda de oportunidades de negócio ou de emprego e danos físicos, entre outros”[398]. Entendendo, ainda, que o alargamento do âmbito de modo a incluir de forma geral os serviços da sociedade da informação “implicaria uma sua maior responsabilização e contribuiria para sensibilizar melhor o público, o que contribuiria indubitavelmente para limitar os riscos de segurança”[399].

No que respeita ao tratamento de dados de tráfego, passa a ser exigido que o consentimento prestado pelo assinante ou utilizador seja prévio ao tratamento[400].

Quanto às comunicações não solicitadas, às pessoas singulares ou coletivas prejudicadas por infrações às disposições nacionais aprovadas nos termos do artigo 13.º da Diretiva, que tenham um interesse legítimo na cessação ou proibição dessas infrações, deve ser garantida a possibilidade de intentar ações judiciais contra tais infrações, sem prejuízo de eventuais recursos administrativos.

Aos Estados-Membros é deixada, ainda, a possibilidade de estabelecer regras específicas sobre as sanções aplicáveis a prestadores de serviços de comunicações eletrónicas que pela sua negligência contribuam para essas infrações[401].

2.3.2.1 A alteração à regulação dos testemunhos de conexão

O n.º 3 do Artigo 5.º da Diretiva 2002/58/CE, que estabelece as condições de armazenamento e acesso a informação armazenada no equipamento terminal do utilizador, foi alterado pela Diretiva dos Cidadãos.

[398] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 1/2009 sobre as propostas ...* , cit., p. 4.
[399] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2008 sobre a revisão ...* , cit., p. 3.
[400] Artigo 6.º, n.º 3, da Diretiva 2002/58/CE, com a redação que lhe foi dada pela Diretiva 2009/136/CE.
[401] Artigo 13.º, n.º 6, da Diretiva 2002/58/CE, com a redação que lhe foi dada pela Diretiva 2009/136/CE-

As alterações começam por se fazer notar no âmbito de aplicação do artigo. A disposição original referia-se à "utilização de redes de comunicações eletrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador". Na nova redação é adotada a mais abrangente referência ao "armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador".

Mas a principal diferença introduzida pela Diretiva dos Cidadãos no que respeita à regulação dos testemunhos de conexão reside no facto de o armazenamento ou acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador deixar de ser permitido por defeito e passar a depender de consentimento prévio.

A Diretiva dos Cidadãos estabelece o consentimento prévio do assinante ou utilizador como condição legitimante do armazenamento ou acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador; consentimento esse que deve ser prestado com base em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento[402].

Mantém-se, assim, a obrigação de prestação de informações claras e completas, nos termos da Diretiva 95/46/CE, conforme já decorria da versão original da Diretiva relativa à privacidade e às comunicações eletrónicas.

A nova exigência de consentimento prévio do assinante ou utilizador prestado com base em informações claras e completas não impede 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 que tenha sido expressamente

[402] Artigo 5.º, n.º 3, da Diretiva 2002/58/CE, com a redação que lhe foi dada pela Diretiva 2009/136/CE.

solicitado pelo assinante ou pelo utilizador[403], que continuam expressamente ressalvados, como já acontecia na versão original da disposição.

2.4. A Reforma do Quadro Legislativo da UE de Proteção de Dados

Dezoito anos passaram desde a adoção da Diretiva 95/46/CE.

A realidade quotidiana dos cidadãos europeus é muito diferente daquela em que se formularam as regras que até hoje disciplinam o tratamento de dados pessoais na União. O próprio quadro institucional da União mudou. A Diretiva foi transposta pelos Estados-Membros e, hoje, a sua disciplina é aplicada através de 27 regimes nacionais.

O progresso tecnológico e a globalização transformaram profundamente o modo como os dados pessoais são recolhidos, consultados, utilizados e transferidos[404].

A Internet faz hoje parte do dia-a-dia dos cidadãos europeus[405]. Mais do que um instrumento de trabalho, a rede das redes afirmou-se como um meio privilegiado de interação social e plataforma de transações económicas variadas.

As redes sociais, a computação em nuvem, assim como os serviços baseados na localização geográfica do utilizador e os cartões inteligentes contribuem para que hoje nos achemos neste "admirável mundo novo dos dados"[406].

---

[403] Artigo 5.º, n.º 3, da Diretiva 2002/58/CE, com a redação que lhe foi dada pela Diretiva 2009/136/CE.

[404] *Em que medida irá a reforma da UE adaptar as regras de proteção de dados aos novos progressos tecnológicos?*, Comissão Europeia, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_pt.pdf, última consulta em 20 de agosto de 2012.

[405] 250 milhões de pessoas que utilizam diariamente a Internet na Europa, cf. COMISSÃO EUROPEIA, *Comunicação (...) século XXI*, cit., E *Em que medida ...* , cit..

[406] *Porque precisamos de uma reforma da proteção de dados na UE?*, Comissão Europeia, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_pt.pdf, última consulta em 20 de agosto de 2012.

A transposição da Diretiva 95/46/CE pelos 27 Estados-Membros da UE originou regras de proteção de dados divergentes que no atual contexto digital não asseguram o grau de harmonização que se exige nem a eficácia necessária para garantir o direito à proteção dos dados pessoais[407].

As obrigações administrativas que impendem sobre os responsáveis são excessivamente burocráticas e dispendiosas[408] sem que isso se reflita num proporcional reforço da proteção das pessoas.

O novo quadro institucional da União, introduzido com o Tratado de Lisboa, em 2009, reforçou o direito fundamental à proteção de dados.

O direito à proteção de dados goza hoje de reconhecimento autónomo no artigo 8.º da vinculativa Carta dos Direitos Fundamentais da União Europeia. O novo artigo 16.º do TFUE introduz uma nova base jurídica horizontal, com vista a uma abordagem moderna e global sobre a proteção de dados e a livre circulação de dados pessoais, que se aplica não só às áreas respeitantes ao funcionamento do mercado interno, mas também o domínio da cooperação policial e judiciária em matéria penal[409].

Em 25 de janeiro de 2012, a Comissão Europeia, consciente da necessidade de um regime mais moderno, eficiente e consistente, propôs uma reforma das regras de proteção de dados em vigor, com vista a reforçar a proteção da privacidade em linha e impulsionar a economia digital europeia[410].

A Comissão pretende atualizar as regras que garantem a proteção de um direito que já se havia conformado como fundamental e, ao mesmo tempo, de um bem comum, a livre circulação de dados, que se veio afirmar

[407] Neste sentido, HUSTINX, Peter, *EU Data Protection ...* , cit., e COMISSÃO EUROPEIA, *Comunicação (...) século XXI*, cit..
[408] A atual obrigação de notificar todas as operações de tratamento de dados, custa às empresas aproximadamente 130 milhões de euros por ano. Cf. *Em que medida ...* , cit..
[409] COMISSÃO EUROPEIA, *Comunicação (...) século XXI*, cit..
[410] *Commission proposes a comprehensive reform of the data protection rules*, disponível em http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm, última consulta em 30 de agosto de 2013.

não só como uma realidade incontornável mas essencial à economia europeia.

Com vista a reforçar os direitos das pessoas e a fortalecer o mercado interno, a Comissão propões a adoção de um conjunto de regras neutras do ponto de vista tecnológico e preparadas para o futuro, aplicáveis em toda a União Europeia[411].

O pacote legislativo avançado para a proteção dos dados pessoais na União Europeia consiste de duas propostas legislativas: uma Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)[412], que substitui a Diretiva 95/46/CE, e uma Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados[413], que substitui a Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008[414].

A opção legislativa por um Regulamento Geral sobre a Proteção de Dados (RGPD), diretamente aplicável aos Estados-Membros, permitirá a uniformização das normas nesta matéria.

---

[411] *Em que medida ...* , cit..
[412] COMISSÃO EUROPEIA, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)*, COM(2012) 11 final 2012/0011 (COD), disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf, última consulta em 20 de outubro de 2013.
[413] COMISSÃO EUROPEIA, *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados*, COM/2012/010 final - 2012/0010 (COD), disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:PT:HTML.
[414] Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal.

Pela Proposta de RGPD avançada pela Comissão passará a Reforma do regime da proteção de dados na União Europeia, pelo que lhe vamos dedicar alguma atenção neste ponto do nosso trabalho[415].

A proposta avançada não promove uma rutura com o regime atual, mas antes respeita uma linha de continuidade.

A verdade é que os princípios consagrados na Diretiva 95/46/CE são tão válidos hoje como eram em 1995[416].

Na Proposta de RGPD é expressamente consagrado o princípio da transparência.

Os responsáveis pelo tratamento ficam obrigados a fornecer "informações transparentes, de fácil acesso e compreensão"[417], bem como a prever "procedimentos e mecanismos para o exercício dos direitos pelo titular dos dados, incluindo meios para pedidos por via eletrónica que requeiram resposta à pessoa em causa dentro de um prazo fixado e os motivos da recusa"[418].

É introduzido o princípio geral da proteção da privacidade desde a conceção (*privacy by design*), que reforça significativamente as obrigações do responsável pelo tratamento, na medida em que lhe impõe o dever de assegurar que as garantias em matéria de proteção de dados são tomadas em consideração desde a fase de planeamento dos procedimentos e dos sistemas de tratamento[419]. A proteção de dados deve, ainda, ser garantida por defeito[420].

---

[415] Desde a Proposta inicial da Comissão, de 25 de janeiro de 2005, e até ao momento em que escrevemos este título não tinham sido alcançados acordos significativos sobre alterações entretanto propostas àquele texto, pelo que optamos por nos limitar à Proposta da Comissão: Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), de 25 de janeiro de 2005, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf.
No entanto, a Comissão Parlamentar das Liberdades Cívicas, Justiça e Assuntos Internos votou a reforma legislativa no dia 21 de outubro de 2013. Alterações entretanto debatidas foram aprovadas. Com esta votação iniciaram-se as negociações entre os eurodeputados e os governos nacionais da União Europeia.
Conforme informação disponível no *site* oficial do Parlamento Europeu (http://www.europarl.europa.eu/), "o objetivo é adotar a legislação antes das próximas eleições europeias na primavera de 2014".

[416] Neste sentido, COMISSÃO EUROPEIA, *Comunicação (...) século XXI*, cit., e ... , cit..

[417] Artigo 11.º da Proposta de RGPD, que se inspira na Resolução de Madrid sobre as normas internacionais em matéria de proteção de dados pessoais e da vida privada, cf. Exposição de Motivos, p. 9.

[418] Artigo 12.º da Proposta de RGPD e Exposição de Motivos, p. 9.

[419] COMISSÃO EUROPEIA, Comunicação (...) século XXI, cit., e Artigo 23.º da Proposta de RGPD.

[420] Artigo 23.º da Proposta de RGPD.

Assim, ao responsável pelo tratamento é imposto o dever de aplicar mecanismos que garantam, por defeito, que apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento e, especialmente, que não são recolhidos ou conservados para além do mínimo necessário para essas finalidades, tanto em termos da quantidade de dados, como da duração da sua conservação.

A definição de consentimento é clarificada.

Com o intuito de garantir que o titular de dados dá o seu consentimento com todo o conhecimento de causa, a manifestação de vontade pela qual a pessoa em causa aceita que os dados pessoais que lhe dizem respeito sejam objeto de tratamento além de livre, específica e informada passa a exigir-se explícita, mediante uma declaração ou um ato positivo inequívoco.

Neste sentido, o silêncio ou a omissão não constituem um consentimento[421].

A Proposta de Regulamento avança, ainda, no sentido de fazer recair sobre o responsável pelo tratamento o ónus de provar o consentimento da pessoa em causa, sempre que o tratamento for realizado com base nesse fundamento[422].

Quando à pessoa em causa não for dada uma verdadeira liberdade de escolha, o consentimento prestado não constitui um fundamento jurídico válido[423].

Do mesmo modo, o consentimento não deve constituir um fundamento jurídico válido para o tratamento de dados pessoais se existir um desequilíbrio manifesto entre o titular dos dados e o responsável pelo tratamento[424] [425].

[421] Considerando 25 da Proposta de RGPD.
[422] Considerando 32 da Proposta de RGPD.
[423] Considerando 33 da Proposta de RGPD.
[424] Considerando 34 da Proposta de RGPD.
[425] O artigo 7.º da Proposta de RGPD clarifica as condições para que o consentimento seja válido enquanto fundamento jurídico para o tratamento lícito.

O Regulamento proposto visa, também, simplificar procedimentos e reduzir custos relacionados com o cumprimento das obrigações que impendem sobre os responsáveis pelo tratamento.

Atualmente, uma empresa que proceda ao tratamento de dados pessoais em mais do que um Estado-Membro tem de consultar a autoridade competente de cada um deles, para confirmar se está a agir em conformidade com a legislação nacional.

A Proposta de Regulamento avança com um sistema de "balcão único". Os responsáveis pelo tratamento de dados na União passam a ter apenas como interlocutor a autoridade do Estado-Membro onde está situado o estabelecimento principal da empresa. A autoridade principal atuará em estreita colaboração com todas as restantes autoridades competentes.

Num esforço tendente à desburocratização, a obrigação geral de notificar a autoridade competente previamente ao tratamento é substituída por uma reforço da obrigação dos responsáveis pelo tratamento e os subcontratantes de conservarem a documentação respeitante aos tratamentos de dados sob a sua responsabilidade[426].

As obrigações do responsável pelo tratamento são significativamente reforçadas.

Além das já referidas obrigações de incorporar, na sua atividade, os conceitos de privacidade desde a conceção e a privacidade por defeito, têm o dever de realizar avaliações de impacto sobre a proteção de dados previamente a operações de tratamento de dados de risco[427]. O responsável pelo tratamento deve, ainda, designar um delegado para a proteção de dados. Esta obrigação existe para o sector público e, no sector privado, para as grandes empresas (empresas com 250 assalariados ou mais) ou sempre que as atividades de base do responsável pelo tratamento ou do

[426] Artigo 28.º da Proposta de RGPD.
A autorização prévia da autoridade competente é, porém, necessária nos alguns casos especialmente previstos no artigo 34.º da Proposta de RGPD.
[427] Artigo 33.º da Proposta de RGPD.

subcontratante consistam em operações de tratamento de dados que exijam um controlo regular e sistemático[428].

Em caso de violação de dados pessoais, o responsável pelo tratamento passa a estar obrigado a notificar esse facto à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo máximo de 24 horas após ter tido conhecimento da mesma[429].

As infrações administrativas previstas pelo Regulamento sujeitam o responsável pelo tratamento a coimas a aplicar pela autoridade de controlo[430].

A Proposta de Regulamento prevê o reforço do poder de controlo do titular dos dados.

Remetendo ao caso do estudante austríaco Max Schrems, que na primavera de 2011 solicitou à rede social *Facebook* o registo das informações que este serviço tinha a seu respeito, com base no direito de acesso consagrado no artigo 12.º da Diretiva 95/46/CE, e em resposta recebeu um documento de 1 222 páginas com registos da sua atividade naquele *site*, a Comunicação da Comissão[431] destaca a necessidade de reforço do direito ao esquecimento – ou "direito a ser esquecido"[432].

A constatação de que a "rede social recolhe muitos mais dados do que (a pessoa em causa) pensava e que alguns dados pessoais que (a pessoa em causa) julgou terem sido apagados ainda estavam conservados" levou a Comissão a procurar garantir "que esta situação não se volte a reproduzir no futuro"[433].

[428] Artigo 35.º da Proposta de RGPD.
[429] Artigo 31.º da Proposta de RGPD.
[430] Artigo 79.º da Proposta de RGPD.
[431] COMISSÃO EUROPEIA, *Comunicação (...) século XXI*, cit..
[432] "The right to be forgotten is of course not an absolute right. There are cases where there is a legitimate reason to keep data in a data base. The archives of a newspaper are a good example. It is clear that the right to be forgotten cannot amount to a right to re-write or erase history. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media. The right to be forgotten includes an explicit provision that ensures it does not encroach on the freedom of expression and information." COMISSÃO EUROPEIA, *MEMO/13/923*, de 22 de outubro de 2013, disponível em http://europa.eu/rapid/press-release_MEMO-13-923_en.htm, última consulta em 23 de outubro de 2013.
[433] COMISSÃO EUROPEIA, Comunicação (...) século XXI, cit..

O artigo 17.º da proposta de Regulamento, inserido no Capitulo III referente aos direitos do titular dos dados, prevê as condições do direito a ser esquecido. Este artigo, "desenvolve e especifica mais detalhadamente o direito de apagamento consagrado no artigo 12.º, alínea b), da Diretiva 95/46/CE, e prevê as condições do direito a ser esquecido, incluindo a obrigação do responsável pelo tratamento que tornou públicos os dados pessoais de informar os terceiros sobre o pedido da pessoa em causa de apagamento de quaisquer ligações para esses dados, ou cópias ou reproduções que tenham sido efetuadas" [434].

Ao titular dos dados é, pois, reconhecido o direito de obter do responsável pelo tratamento o apagamento de dados pessoais que lhe digam respeito e a cessação da comunicação ulterior desses dados, sempre os dados deixaram de ser necessários em relação à finalidade que motivou a sua recolha ou tratamento [435] ; ou o titular dos dados se opuser ao tratamento[436]; ou o tratamento dos dados não respeitar o Regulamento por outros motivos[437]; ou o titular dos dados retirar o consentimento sobre o qual é baseado o tratamento, ou se o período de conservação consentido tiver terminado e não existir outro fundamento jurídico para o tratamento dos dados[438].

O direito ao esquecimento não é, portanto, uma novidade, mas um reforço do atual direito ao apagamento.[439]

---

[434] Proposta de RGPD, Exposição de Motivos, p. 9.
[435] Artigo 17.º, n.º 1, alínea a) da Proposta de RGPD,
[436] Artigo 17.º, n.º 1, alínea c) da Proposta de RGPD,.
[437] Artigo 17.º, n.º 1, alínea d) da Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados).
[438] Artigo 17.º, n.º 1, alínea b) da Proposta de RGPD,
[439] O Parlamento Europeu, entretanto, considerou ilusória a previsão de um "direito ao esquecimento" e alterou o artigo 17.º proposto pela Comissão. O direito ao esquecimento, deu lugar ao "direito ao apagamento".
"The 'right to be forgotten' is a right that is not provided for by this Regulation. By using this term, data subjects are promised a right they in practice do not have. The right to erasure must be as strong as possible and take into account the possible difficulties to remove personal data on the Internet. This should be done by strengthening the right to erasure instead of promising non-existing rights through misleading titles." PARLAMENTO EUROPEU, Comissão das Liberdades Cívicas, Justiça e Assuntos Internos, *AMENDMENTS (4) 1189 - 1492 on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Proposal for a regulation* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Draft report Jan Philipp Albrecht (PE501.927v04-00), 8 de março de 2013, alteração 1381.
"The 'right to be forgotten' is a right that is not provided for by this Regulation. By using this term, data subjects are promised a right they in practice do not have. The right to erasure must be as strong as possible and take into account the possible difficulties to remove personal data on the Internet. This should be done by strengthening the right to erasure instead of promising non-existing rights through misleading titles." PARLAMENTO EUROPEU, Comissão das Liberdades Cívicas, Justiça e Assuntos Internos, *AMENDMENTS (4) 1189 - 1492 on the proposal ...* , cit., alteração 1381.

É consagrado, também, o direito à portabilidade dos dados. Este consiste no direito de o titular transferir dados de um sistema de tratamento eletrónico para outro, sem que o responsável pelo tratamento se possa opor[440]. Este direito permite ao titular dos dados transferi-los mais facilmente para o novo prestador de serviços, promovendo-se, desta forma, a concorrência entre estes.

No que respeita ao âmbito de aplicação, a Proposta de RGPD amplia a incidência territorial da proteção de dados em relação à atual Diretiva, passando a ficar sujeitas às obrigações decorrentes do Regulamento todas as empresas que ofereçam bens e/ou serviços e/ou que monitorizem os comportamentos de cidadãos europeus, independentemente de estarem ou não estabelecidas na União Europeia[441].

A Proposta de Regulamento prevê, ainda, a substituição do Grupo do Artigo 29.º para a Proteção de Dados por um Comité Europeu para a Proteção de Dados. Este Comité, a ser composto por um diretor da autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados, deve contar com a participação da Comissão nas suas atividades e ser independente nas suas funções. O Comité Europeu para a Proteção de Dados deve contribuir para a aplicação coerente do presente regulamento em toda a União, nomeadamente no aconselhamento da Comissão e na promoção da cooperação das autoridades de controlo no conjunto da União[442].

[440] Artigo 18.º da Proposta de RGPD,
[441] Sobre a excessiva extensão do âmbito de aplicação das normas de proteção de dados da União Europeia, TENE, Omer Tene e WOLF Christopher Wolf, White Paper - *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, The Future of Privacy Forum, Washington, DC, 2013, disponível em http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf, última consulta em 3 de julho de 2013.
[442] Considerando 110 e artigos 64.º e ss. da Proposta de RGPD,

A Proposta apresentada pela Comissão prevê, portanto, o reforço da posição dos titulares dos dados, da responsabilização dos responsáveis pelo tratamento dos dados e da posição das autoridades de controlo.

Capítulo III O consentimento como fundamento para a utilização de testemunhos de conexão

1. Introdução

A Internet, acessível a um número cada vez maior de pessoas, faz parte do dia-a-dia dos cidadãos europeus[443], não só como um instrumento de trabalho, mas como um meio privilegiado de interação social e plataforma de numerosas transações económicas.

O tratamento de dados pessoais, desde logo a sua recolha, através da *World Wide Web* resulta, tantas vezes, de operações já rotineiras introduzidas na vida dos cidadãos.

Como vimos [444] , os testemunhos de conexão consistem em informações que são enviadas pelo servidor *web* do *site* que visitamos[445] ao nosso navegador e que, uma vez recebidas (sendo o navegador cooperante) são armazenadas no nosso equipamento terminal e, aquando de um novo pedido ao *site*, são acedidas pelo navegador (cooperante) que lhas reenvia inalteradas.

O *site web* recorrendo-se da tecnologia dos testemunhos de conexão consegue, portanto, armazenar e aceder a informação previamente armazenada no terminal do utilizador ou assinante.

O artigo 5.º, n.º 1, da Diretiva da Privacidade Eletrónica[446] protege a confidencialidade das comunicações em geral e o n.º 3 do mesmo artigo 5.º regula a proteção da confidencialidade no caso concreto do armazenamento e acesso a informação armazenada no terminal do utilizador ou assinante.

[443] COMISSÃO EUROPEIA, *Comunicação (...) século XXI*, cit., e *Em que medida irá a reforma da proteção de dados reforçar os direitos dos cidadãos?*, Comissão Europeia, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_pt.pdf, última consulta em 30 de agosto.
[444] Capítulo I.
[445] Ou que é acedido a partir do nosso navegador *web*.
[446] Salvo indicação em contrário, neste Capitulo III, por "Diretiva da Privacidade Eletrónica" deve entender-se a Diretiva 2002/58/CE com a redação que lhe foi dada pela Diretiva 2009/136/CE.

Esta norma aplica-se, portanto, à utilização de testemunhos e conexão, bem como a outras tecnologias semelhantes.

O considerando 25 da Diretiva 2002/58/CE, refere-se expressamente aos testemunhos de conexão, que reporta como um instrumento que pode ser "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".

Na versão de 2002 da Diretiva da Privacidade Eletrónica, o n.º 3 do artigo 5.º permitia a utilização de redes de comunicações eletrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador, na condição de serem prestadas ao assinante ou utilizador informações claras e completas, nomeadamente sobre as finalidades do processamento e de, cumulativamente, lhe ser garantido o direito de recusar o tratamento[447].

A Diretiva dos Cidadãos promoveu uma alteração ao artigo 5.º n.º 3 da Diretiva 2002/58/CE, que passa a exigir o consentimento prévio, com base em informações claras e completas, do utilizador ou assinante como condição para o armazenamento ou acesso a informações já armazenadas no seu equipamento terminal. "Esta exigência aplica-se a todos os tipos de informações armazenadas ou acessíveis no equipamento terminal do utilizador, embora a questão essencial do debate se centre na utilização de testemunhos de conexão (cookies), entendidos na aceção da definição dada pela norma RFC 6265[448]„[449].

O novo requisito de consentimento[450] veio abalar as práticas correntes no que respeita ao armazenamento e acesso a informações já armazenas no terminal do utilizador ou assinante através de testemunhos de conexão.

[447] Direito de autoexclusão ou direito de *opt-out*.
[448] Sobre a especificação RFC 6265 da IETF ver Título 2.1. e Título 2.2. do Capítulo I.
[449] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p.2.
[450] "Esta exigência do consentimento reflete a crescente preocupação por parte dos cidadãos, políticos, autoridades responsáveis pela proteção de dados, organizações de defesa dos consumidores e decisores políticos em relação à rápida proliferação das tecnologias que monitorizam o comportamento individual na Internet ao longo do tempo e em diferentes sítios Web. Além disso, os meios à disposição dos cidadãos para proteger a sua vida privada e os seus dados pessoais contra este tipo de monitorização não estavam a acompanhar este crescimento. Em 2009, os

O direito de recusar o tratamento configurava um direito da pessoa em causa, um direito de oposição[451] específico e especial, porque legitimante do tratamento através do armazenamento e acesso a informações previamente armazenadas no equipamento terminal do utilizador. Já o consentimento é, em si mesmo, um princípio legitimante do tratamento, que passa a assumir-se como fundamento específico para a utilização de testemunhos de conexão, e tecnologias similares.

Assim, era legítimo à entidade responsável proceder ao tratamento de informações através da utilização de testemunhos de conexão, desde que fornecesse informações claras e completas à pessoa em causa e esta não recusasse o tratamento, estando-lhe efetivamente garantida a possibilidade de o fazer.

Com a alteração introduzida pela Diretiva dos Cidadãos, a utilização de testemunhos de conexão depende da prévia obtenção do consentimento da pessoa em causa.

O debate a respeito da implementação das novas regras previstas para a utilização de testemunhos de conexão, pela Diretiva 2009/136/CE, é sustentado pelas dúvidas acerca da interpretação deste requisito, da sua implementação prática e da sua efetiva necessidade.

Tendo em conta tudo quando deixamos exposto nos dois capítulos anteriores, vamos agora analisar a opção legislativa vertida neste artigo 5.º

decisores políticos tinham fortes dúvidas sobre a possibilidade de depender do sector da publicidade para aumentar a sensibilização do público e a possibilidade de escolha dos utilizadores em matéria de publicidade comportamental em linha. Diversos inquéritos públicos demonstraram, e continuam a demonstrar, que o utilizador médio da Internet não tem consciência de que o seu comportamento está a ser monitorizado com a ajuda de testemunhos ou identificadores únicos, nem de quem o faz ou para que fins o fazem. Esta falta de sensibilização contrasta fortemente com a crescente dependência de muitos cidadãos europeus do acesso à Internet para desenvolver atividades quotidianas, tais como fazer compras, ler, comunicar com os amigos e pesquisar informações. Além disso, a Internet está rapidamente a substituir diversas atividades «fora de linha», tais como o acesso a determinados serviços públicos. A rápida substituição do acesso fixo à Internet pelo acesso móvel veio dificultar ainda mais a possibilidade de os utilizadores da Internet se protegerem recorrendo a meios técnicos.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 16/2011 sobre a recomendação da EASA/IAB relativa às melhores práticas em matéria de publicidade comportamental em linha* (WP 188), de 8 de dezembro de 2011, p. 3, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_pl.pdf, última consulta em 30 de agosto de 2013.

[451] Artigo 14.º, da Diretiva 95/46/CE.

n.º 3 da Diretiva da Privacidade Eletrónica, dedicando especial atenção ao requisito de consentimento do utilizador ou assinante enquanto condição legitimante da utilização de testemunhos de conexão, introduzido pela Diretiva dos Cidadãos.

2. Objetivo do artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica

A Diretiva da Privacidade Eletrónica visa tem por objetivo a proteção do direito à privacidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas[452].

O considerando 24 da Diretiva 2002/58/CE refere que "o equipamento terminal dos utilizadores de redes de comunicações eletrónicas e todas as informações armazenadas nesse equipamento constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos ao abrigo da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais".

Com a entrada em vigor do Tratado Lisboa, a Carta dos Direitos Fundamentais da União Europeia tornou-se vinculativa. Nela, a União consagrou autonomamente o direito ao respeito pela vida privada e familiar[453] e o direito à proteção de dados pessoais[454], que o Tribunal de Justiça já há muito vinha conformando como fundamentais[455].

O artigo 5.º, n.º 3 é um complemento ao artigo 5.º, n.º 1 da Diretiva da Privacidade Eletrónica.

Assim como conteúdo das comunicações e os respetivos dados de tráfego são passíveis de conter informações do âmbito da esfera privada dos

[452] Artigo 1.º da Diretiva da Privacidade Eletrónica.
A proteção da privacidade não é, porém, o único objetivo da Diretiva da Privacidade Eletrónica, como vimos no Título 2.3. do Capítulo II.
[453] Artigo 7.º da Carta dos Direitos Fundamentais da União Europeia.
[454] Artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.
[455] Título 2.1. do Capítulo II.

utilizadores, também o equipamento terminal o é, pelo que deve ser protegido.

A confidencialidade das comunicações passa, então, pela sua proteção no momento em que estão a ser entregues pelo equipamento terminal do utilizador ao serviço de comunicações, quando são recebidas pelo terminal do serviço, e quando são postas à disposição do utilizador ou armazenadas no seu equipamento terminal.[456]

Assim, o principal objetivo do artigo 5.º, n.º 3 é a proteção do equipamento terminal do utilizador e de quaisquer informações aí armazenadas, enquanto parte da esfera privada dos utilizadores[457], no que respeita ao tratamento de dados pessoais[458].

3. Âmbito de aplicação do artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica

A utilização legítima dos testemunhos de conexão, enquanto informações armazenadas e acedidas no equipamento terminal do utilizador ou assinante, depende do cumprimento do disposto nº 3 do artigo 5.º da Diretiva da Privacidade Eletrónica. É isso mesmo, aliás, que decorre referência expressa a esta tecnologia no considerando 25 da Diretiva 2002/58/CE, e que temos vindo a referir.

Mas, antes de procedermos à análise das características do consentimento exigido enquanto fundamento legitimante para a utilização de testemunhos de conexão, importa dedicar alguma atenção ao âmbito de aplicação da norma em causa.

---

[456] COMMUNICATIONS COMMITTEE (EUROPEAN COMMISSION Information Society and Media Directorate-General Electronic Communications Policy Implementation of Regulatory Framework), *Working Document Implementation of the revised Framework– Article 5(3) of the ePrivacy Directive*, COCOM10-34, Bruxelas, 20 de outubro de 2010, p. 3., disponível em http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-35-guidance-implementation-telecoms-rules-privacy, última consula em 20 de agosto de 2013.
[457] Considerando 24 da Diretiva 2002/38/CE.
[458] Artigo 1.º da Diretiva da Privacidade Eletrónica.

3.1 Âmbito de aplicação material

O artigo 3.º da Diretiva da Privacidade Eletrónica dispõe que esta "é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na Comunidade, nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação"[459].

Considerando, no entanto, que o equipamento terminal dos utilizadores e todas as informações armazenadas nesse equipamento constituem parte integrante da sua esfera privada[460] e que terceiros podem armazenar informações no[461] equipamento de um utilizador, ou ter acesso a informação já armazenada, para diferentes fins, que vão desde os legítimos (em que se incluem certos tipos de testemunhos de conexão), até aos que envolvem a intromissão indevida na esfera privada (como software espião ou vírus)[462]; o n.º 3 do artigo 5.° tem um âmbito de aplicação material mais abrangente do que a generalidade das disposições da Diretiva em que se inclui.

Em primeiro lugar, porque não se limita à proteção de informações compreendidas no conceito de dados pessoais.

Depois, porque não se aplica apenas aos serviços de comunicações eletrónicas.

Por último, porque extravasa o contexto das redes de comunicações eletrónicas.

[459] Conforme analisamos mais pormenorizadamente no Título 2.3. do Capítulo II.
[460] Considerando 24, da Diretiva 2002/58/CE
[461] Na versão portuguesa, da Diretiva 2009/136/CE lê-se "terceiros podem desejar armazenar informações sobre o equipamento de um utilizador (...)". Entendemos tratar-se de um lapso. Na versão em inglês da mesma lê-se "Third parties may wish to store information on the equip- ment of a user (...)".
[462] Considerando 66, da Diretiva 2009/136/CE.

3.1.1. Informações abrangidas

Ao contrário do que estabelece a norma geral vertida no artigo 3.º da Diretiva da Privacidade Eletrónica, a disposição que ora analisamos não se limita a ser aplicada ao tratamento de dados pessoais.

O n.º 3 do artigo 5.º, em questão, refere-se ao "armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador".

O legislador comunitário abraçou o entendimento de que toda a informação contida no terminal de um utilizador faz parte da sua esfera privada e, por isso, merece proteção [463] – independentemente da sua qualificação como dados pessoais.

O Grupo do Artigo 29.º, no seu parecer sobre publicidade comportamental em linha, confirmou que "o artigo 5.º, n.º 3, é aplicável ao armazenamento e/ou acesso a «informações», qualquer que seja o seu tipo. Não é um requisito para a aplicação desta disposição que estas informações sejam dados pessoais na aceção da Diretiva 95/46/CE"[464].

Assim, a opção terminológica do n.º 3 do artigo 5.º visa estender o âmbito da previsão a todos os casos de armazenamento ao acesso a informação armazenada no terminal de um utilizador ou assinante [465]. A disposição não se aplica, portanto, apenas quando em causa estejam informações compreendidas no conceito de dados pessoais, mas sempre que haja armazenamento ou acesso a informações já armazenadas no terminal do utilizador, por tal representar uma imiscuição na sua esfera privada.

[463] Considerando 24, da Diretiva 2002/58/CE.
[464] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p-10.
[465] KOSTA, Eleni, *Consent in European...* , op. cit., p. 297, e KOSTA, Eleni, *Handling cookies within the european union: making the cookies crumble?*, em "VIII Congreso Internet, Derecho y Política 2012 Retos y oportunidades del entretenimiento en línea", Barcelona, 2012, p. 403.

3.1.1.1. Aplicação da Diretiva 95/46/CE

A verdade é que a utilização de testemunhos de conexão frequentemente envolve o tratamento de dados pessoais.

Como vimos[466], é considerado dado pessoal "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»)", sendo que "é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social"[467].

No Parecer 1/2008 sobre questões de proteção de dados ligadas aos motores de pesquisa, adotado em 4 de Abril de 2008, o Grupo de Artigo 29.º confirmou que, na maioria dos casos, os testemunhos devem ser considerados dados pessoais[468].

"Se um testemunho contiver um identificador único do utilizador, esse identificador constitui claramente [469] um dado pessoal. A utilização de testemunhos persistentes ou de meios análogos com um identificador único do utilizador permite acompanhar os utilizadores de um determinado computador mesmo que sejam utilizados endereços I.P. dinâmicos"[470][471].

[466] Título 2.2. do Capítulo II.
[467] Artigo 2.º, alínea a), da Diretiva 95/46/CE.
[468] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 1/2008 sobre questões de proteção de dados ligadas aos motores de pesquisa* (WP 148), de 4 de Abril de 2008, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_pt.pdf#h2-6, última consulta em 30 de agosto de 2013.
[469] Não somos, contudo, da opinião de que um testemunho que contenha um identificador único permita "claramente" identificar as pessoas em causa. A verdade é que pode ser instalado um testemunho com um identificado único num equipamento terminal a partir do qual várias pessoas, utilizando o mesmo navegador, acedam ao mesmo *site*. O número único permite identificar o navegador mas pode não permitir a identificação, ainda que indireta, de cada uma ou alguma das pessoas.
[470] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 1/2008 sobre questões de proteção ...* , cit., p. 9.
[471] O Tribunal de Justiça, através do Acórdão de 24 de novembro de 2011, considerou os endereços de IP dados pessoais. Acórdão do Tribunal de Justiça, *Scarlet Extended SA contra Société belge des auteurs*, compositeurs et éditeurs SCRL (SABAM), Processo C-70/10, de 24 de novembro de 2011.

Assim, é possível monitorizar os utilizadores e identificar as pessoas em causa.[472]

Decorre do considerando 10 da Diretiva da Privacidade Eletrónica que "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 abrangidas especificamente pelas disposições da presente diretiva, incluindo as obrigações que incumbem à entidade que exerce o controlo e os direitos das pessoas singulares".

Conforme confirmou o Grupo do Artigo 29.º, "trata-se de um caso de aplicação do critério da especialidade, segundo o qual a lei especial (*lex specialis*) prevalece sobre a lei geral (*lex generalis*). Assim sendo, o artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica, que diz respeito ao consentimento informado, será diretamente aplicável. A Diretiva 95/46/CE será plenamente aplicável, excerto em relação às disposições expressamente previstas na Diretiva da Privacidade Eletrónica, que correspondem essencialmente ao artigo 7.º da Diretiva 95/46/CE sobre os fundamentos legais do tratamento de dados. As restantes disposições da Diretiva 95/46/CE, incluindo os princípios relacionados com a qualidade dos dados, os direitos da pessoa em causa (tais como os direitos de acesso, apagamento e oposição), a confidencialidade e segurança do tratamento e as transferências internacionais de dados, serão plenamente aplicáveis"[473].

Assim, sempre que as informações abrangidas por um testemunho de conexão sejam dados pessoais, além das regras estabelecidas no artigo 5.º, n.º 3 da Diretiva da Privacidade Eletrónica, são aplicáveis as disposições da Diretiva 95/46/CE.[474]

---

[472] O Grupo do Artigo 29.º chama, ainda, a atenção para o facto de que "outras situações que podem levar à identificabilidade são as fusões, as perdas de dados e a crescente disponibilidade de dados pessoais na Internet em combinação com endereços IP", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 10.

[473] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 11.

[474] Entre nós, sobre a aplicação da Lei n.º 67/98, de 26 de outubro, à utilização de testemunhos de conexão ver MENEZES LEITÃO, Luís Manuel Teles de, *Os Testemunhos de ...* , cit., pp. 767 e ss..

Desde logo, os responsáveis pelo tratamento, têm de respeitar os princípios relativos à qualidade dos dados, previstos no artigo 6.º da Diretiva 95/46/CE, bem como os direitos das pessoas em causa estabelecidos nos artigos 12.º e 14.º [475].

O tratamento de dados pessoais sensíveis é, em princípio, proibido pelo artigo 8.º da Diretiva 95/46/CE. Para que através do mecanismo dos testemunho de conexão se possa proceder ao tratamentos desta categoria de dados, para além do consentimento obtido para o tratamento de dados em geral, a pessoa em causa tem de prestar o seu consentimento explícito, específico e prévio, conforme resulta do artigo 8.º, n.º 2, alínea a).

Nos termos do artigo 17.º da Diretiva 95/46/CE, os responsáveis pelo tratamento e os subcontratantes têm, ainda, a obrigação de aplicar medidas técnicas e organizativas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a divulgação não autorizada e outras formas de tratamento ilícito.

Os responsáveis pelo tratamento estão, igualmente, obrigados a notificar o tratamento de dados pessoais às autoridades responsáveis pela proteção de dados, se tal estiver previsto na legislação nacional, em conformidade com o artigo 18.º da Diretiva 95/46/CE.

No caso da transferência de dados para fora da UE, os responsáveis pelo tratamento devem observar o disposto nos artigos 25.º e 26.º da Diretiva 95/46/CE.

3.1.2. Serviços da sociedade de informação

[475] Que analisamos no Título 2.2.1. do Capítulo II.

O n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica, afasta-se da norma geral do artigo 3.º, ainda, na medida em que não se aplica apenas aos serviços de comunicações eletrónicas.

Esta disposição abarca a realidade mais ampla compreendida na noção de serviços da sociedade de informação, conforme salientou o Grupo do Artigo 29.º no Parecer 1/2008 sobre questões de proteção dos dados ligadas aos motores de pesquisa[476].

Por "serviço da sociedade da Informação" entende-se qualquer serviço prestado, normalmente mediante remuneração, à distância (sem que as partes estejam simultaneamente presentes), por via eletrónica (enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos) e mediante pedido individual de um destinatário de serviços[477].

O conceito de remuneração tem um significado amplo, conforme a concretização que lhe foi sendo dada pelo Tribunal de Justiça. Para que se possa entender que o serviço é prestado mediante remuneração, essencial é que o prestador receba uma contrapartida-económica por aquele, que não tem necessariamente de provir do beneficiário do mesmo[478].

Assim, estão incluídos nos serviços oferecidos mediante remuneração aqueles que obtêm contrapartida económica através de publicidade. [479]

[476] Do Parecer resulta que o n.º 3 do artigo 5.° (testemunhos de conexão e programas de espionagem) e o artigo 13.° (comunicações não solicitadas), da Diretiva da Privacidade Eletrónica "são disposições gerais aplicáveis não só aos serviços de comunicação eletrónicas mas também a quaisquer outros serviços se estas técnicas forem utilizadas", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 1/2008 sobre questões de proteção ...* , cit., p. 13.

[477] Artigo 1.º, da Diretiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas, alterada pela Diretiva 98/48/CE do Parlamento Europeu e do Conselho, de 20 de julho de 1998.

[478] Acórdão do Tribunal de Justiça, *Estado Belga Contra Rene Humbel e Marie-Therese Edel*, Processo 263/86, de 27 de setembro de 1988, e Acórdão do Tribunal de Justiça, *Bond van Adverteerders e outros contra Estado neerlandês*, Processo 352/85, de 26 de abril de 1988.

[479] Entre nós, o artigo 3.º do Decreto-Lei n.º 7/2004, de 7 de janeiro define "serviço da sociedade da informação" como "qualquer serviço prestado a distância por via eletrónica, mediante remuneração ou pelo menos no âmbito de uma atividade económica na sequência de pedido individual do destinatário". Assim, "não é, pois, necessário que o serviço seja prestado mediante remuneração; basta que seja prestado no âmbito de uma atividade económica, ainda que não esteja envolvida uma contraprestação", AUTORES VÁRIOS, *Lei do Comércio ...*, op. cit., anotação ao artigo 3.º, p. 25.

3.1.3. Suportes externos

A Diretiva dos Cidadãos promoveu o alargamento do já amplo âmbito de aplicação da norma aplicável à utilização de testemunhos de conexão.

A disposição original da Diretiva 2002/58/CE referia-se à "utilização de redes de comunicações eletrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador".

A proteção conferida extravasava, já na versão original, o âmbito geral de aplicação da Diretiva, não só por não se limitar à proteção de informações compreendidas no conceito de dados pessoais, nem se aplicar apenas aos serviços de comunicações eletrónicas, como vimos supra.

A disposição era aplicável ao armazenamento ou acesso a informações no terminal do utilizador ou assinante através da utilização de redes de comunicações eletrónicas – sendo elas classificadas como públicas, ou não[480].

Com a Diretiva dos Cidadãos, cai o pressuposto de aplicação respeitante à utilização de redes de comunicações eletrónicas.

Adotando uma redação ainda mais abrangente, a norma é agora aplicável ao "armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador".

Conforme esclarece o considerando 65 da Diretiva dos Cidadãos, "a utilização de *software* que monitoriza sub-repticiamente as ações do utilizador ou subverte o funcionamento do equipamento terminal do utilizador em benefício de terceiros (software espião) constitui uma séria ameaça à privacidade dos utilizadores tal como os vírus".

[480] Conceitos que analisamos no Título 2.3. do Capítulo II.

Atendendo ao considerando 24 da Diretiva 2002/58/CE cuja interpretação em conformidade com as alterações promovidas pela Diretiva dos Cidadãos defendemos, o equipamento terminal dos utilizadores (já não apenas nas redes de comunicações eletrónicas) e todas as informações armazenadas nesse equipamento merecem proteção porque constituem parte integrante da sua esfera privada.

Assim "é necessário assegurar um nível de proteção elevado e equitativo da esfera privada dos utilizadores, independentemente do facto de o *software* espião ou dos vírus serem inadvertidamente telecarregados através de redes de comunicação eletrónicas ou entregues e instalados furtivamente em software distribuído através de outros suportes externos de armazenamento de dados, como CD, CD-ROM e chaves USB"[481].

A opção de alargar o âmbito de aplicação da norma em apreço surge como resposta ao caso reportado pelo UK National Consumer Council em 2006. A Sony/BMG tinha introduzido uma ferramenta anti pirataria (*Digital Rights Management* – DMR) chamada "MediaMax" num CD do grupo musical Van Zant, que não se limitava a restringir o número de cópias permitidas a partir do CD e instalava no computador em que fosse inserido, de modo imperceptível ao utilizador, um programa capaz de obter ou manter privilégios de administrador[482].

O equipamento terminal e as informações aí armazenadas fazem parte integrante da esfera privada do utilizador e, por isso, merecem proteção contra qualquer acesso indesejado. Neste sentido, o âmbito de aplicação do n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica foi alargado de modo a abranger o armazenamento ou acesso a informações previamente armazenadas no terminal do utilizador, tanto com recurso a redes de comunicações eletrónicas, como a programas instalados em *software* distribuído através de suportes externos, como CDs, CD-ROMs ou chaves USB.

[481] Considerando 65, da Diretiva 2009/136/CE.
[482] Como explica com maior detalhe KOSTA, Eleni, *Consent in European ...* , op. cit., 294 e 295.

3.2. Âmbito de aplicação territorial

O âmbito de aplicação da Diretiva da Privacidade Eletrónica é estabelecido no seu artigo 3.º, n.º 1, nos termos do qual o artigo 5.º, 3.º, é aplicável ao armazenamento de informações ou à possibilidade de acesso a informações armazenadas no equipamento terminal das pessoas em causa que utilizem redes públicas de comunicações na União Europeia.

Com vimos[483], com a Diretiva dos Cidadãos, caiu o pressuposto de aplicação do artigo 5.º, n.º 3 da Diretiva da Diretiva da Privacidade Eletrónica respeitante à utilização de redes de comunicações eletrónicas. A norma em causa é, agora, aplicável ao armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador, independentemente deste se processar com recuso a uma rede de comunicações eletrónicas ou a outros suportes externos.

Essencial para a determinação do âmbito de aplicação territorial do artigo 5.º, n.º 3, é a localização do equipamento terminal no território da União.

Sendo as informações em causa dados pessoais, aplica-se a Diretiva 95/46/CE quando o tratamento for efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento situado num Estado-Membro, ou quando o responsável pelo tratamento não esteja estabelecido no território da União e recorrera a meios, automatizados ou não, situados no seu território, para tratamento de dados pessoais (salvo se esses meios forem apenas utilizados para o trânsito no território da União).[484]

[483] Título 3.1.3. deste Capítulo III.
[484] Título 2.2. do Capítulo II.

Vimos [485] que para efeitos da Diretiva em análise, a noção de "estabelecimento no território de um Estado-Membro" pressupõe o "exercício efetivo e real de uma atividade mediante uma instalação estável; que, para o efeito, a forma jurídica de tal estabelecimento, quer se trate de uma simples sucursal ou de uma filial com personalidade jurídica, não é determinante"[486].

Assim, quando o testemunho de conexão for utilizado no contexto das atividades de um estabelecimento do responsável no território de um Estado-Membro, aplica-se-lhe a legislação de proteção dos dados desse Estado-Membro. No caso de o responsável pelo tratamento estar estabelecido em mais do que um Estado-Membro, todos os estabelecimentos devem cumprir as obrigações decorrentes das legislações de cada um desses Estados.

Em relação aos casos em que o responsável pelo tratamento não está estabelecido no território da União Europeia, o Parlamento Europeu e o Conselho decidiram recorrer à relação física entre a ação e um sistema jurídico. Assim, a Diretiva da Proteção de Dados aplica-se quando o responsável pelo tratamento não estiver estabelecido no território da União, mas optar por "tratar dados pessoais para fins específicos e utilizar os meios, automatizados ou não, situados no território de um Estado-Membro"[487].

O considerando 20 da Diretiva 95/46/CE explica que "o facto de o tratamento de dados ser da responsabilidade de uma pessoa estabelecida num país terceiro não deve constituir obstáculo à proteção das pessoas assegurada pela presente diretiva; que, nesses casos, o tratamento deverá ser regido pela legislação do Estado-Membro onde se encontram os meios utilizados para o tratamento de dados em causa e que deverão oferecer-se garantias de que os direitos e as obrigações estabelecidos na presente diretiva serão efetivamente respeitados".

---

[485] Artigo 4.º, n.º 1, alíneas a) e c), da Diretiva 95/46/CE, que já tivemos oportunidade de analisar sucintamente no Título 2.2. do Capítulo II.
[486] Considerando 19, da Diretiva 95/46/CE.
[487] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de proteção de dados ao tratamento de dados pessoais na Internet efectuado por sites não-europeus* (WP 56), de 30 de Maio de 2002, p. 7, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp156_pt.pdf, última consulta em 30 de agosto de 2013.

O Grupo do Artigo 29.º para a Proteção de Dados faz notar que não é necessário que o indivíduo seja cidadão, esteja fisicamente presente, ou seja residente na União Europeia para que a Diretiva da Proteção de Dados se aplique. A Diretiva "harmoniza as leis dos Estados-Membros relativas aos direitos fundamentais concedidos a todos os seres humanos, independentemente da sua nacionalidade" [488]. O que releva para efeitos de aplicação das Diretiva [489] é a localização dos meios utilizados para o tratamento.[490]

Assim, quando estejam em causa dados pessoais tratados com recurso a meios localizados no território da União Europeia o responsável pelo tratamento deve cumprir com as obrigações decorrentes da Diretiva 95/46/CE, a menos que esses meios sejam utilizados para trânsito da informação no território da Comunidade. O Grupo do Artigo 29.º esclarece que "um caso típico em que os meios são utilizados apenas para trânsito são as redes de telecomunicações (estruturas, cabos, etc.) [491] que constituem parte da Internet e pelas quais as comunicações da Internet circulam, desde o ponto de envio até ao ponto de destino"[492].

Para concretizar o conceito de "meios", o Grupo do Artigo 29.º recorre-se do dicionário de inglês Collins, que faz entender por "equipment" (meios) um conjunto de instrumentos ou dispositivos reunidos para um fim específico, e esclarece que os computadores, terminais e servidores, são "meios" na aceção do artigo 4.º, n.º 1, alínea c), da Diretiva 95/46/CE.[493] [494]

---

[488] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre a determinação ...*, op. cit, p. 8.
[489] Ou, em rigor, das legislações nacionais de transposição.
[490] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre a determinação ...*, op. cit, pp. 7 e 8.
[491] Entre nós, sobre as redes de telecomunicações, GONÇALVES, Pedro, *Direito das Telecomunicações*, Almedina, Coimbra, 1999, pp. 133 e ss..
[492] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre a determinação ...*, op. cit, p. 9.
[493] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre a determinação ...*, op. cit, p. 9.
[494] Não era este, no entanto, entre nós, o entendimento da Comissão Nacional de Proteção de Dados, que através da deliberação n.º 28/2000 entendeu que "quando a lei fala no recurso a «meios situados em território português» deve entender-se que estão em causa, tão só, "meios próprios do responsável" ou, ainda, de um seu "representante", "prestador de serviços" ou de um "subcontratante" que atue em nome, sob a supervisão ou por conta do responsável. Não se pode aplicar a lei portuguesa quando o meio que serve de recolha de dados é um PC pertencente ao utilizador, titular dos dados, que os envia para um país terceiro e para utilização por empresa ou entidade não estabelecida em território onde a lei portuguesa não seja aplicável". COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, Relatório 2000, Parte II – Orientações da CNPD, 2000, disponível em http://www.cnpd.pt/bin/relatorios/anos/relat00.htm, última consulta em 30 de junho de 2013.

Por sua vez, o conceito de "recurso" (aos meios) pressupõe algum tipo de atividade levada a cabo pelo responsável pelo tratamento com intenção de proceder ao tratamento de dados pessoais. O responsável pelo tratamento determina os dados que são tratados, os procedimentos e as finalidades.[495]

No caso dos testemunhos de conexão, o responsável pelo tratamento utiliza o computador (equipamento terminal) do utilizador, localizado no território de um Estado-Membro, para o tratamento de dados pessoais, determinando as informações abrangidas, os procedimentos e as finalidades.

Assim, para efeitos da utilização de testemunhos de conexão, o computador do utilizador representa um meio, na aceção do artigo 4.º, n.º 1, alínea c), da Diretiva 95/46/CE a que o responsável pelo tratamento recorre para o tratamento de dados pessoais. [496]

4. A pessoa em causa

O artigo 5.º, n.º 3, em análise, exige que sejam prestadas informações claras e completas e que seja obtido o consentimento do utilizador ou assinante. A formulação adotada é alternativa, ao contrário do que acontece, noutras disposições da Diretiva da Privacidade Eletrónica, nomeadamente no n.º 1 do mesmo artigo.

Como tivemos oportunidade de ver [497] , enquanto "utilizador" é "qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço" [498] , "assinante" é "a pessoa singular ou coletiva que é parte num contrato com um prestador de serviços

[495] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre a determinação ...*, op. cit, p. 10.
[496] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre a determinação ...*, op. cit, pp. 11 e 12.
[497] Título 2.3. do Capítulo II.
[498] Artigo 2.º, alínea a), da Diretiva 2002/58/CE.
Ou seja, a pessoa que acede ao(s) *site(s)*.

de comunicações eletrónicas acessíveis ao público para o fornecimento desses serviços".[499]

Se, muitas vezes, assinante e utilizador são a mesma pessoa, nem sempre assim é.

A Diretiva não esclarece a quem compete a escolha nem qual a vontade que deve prevalecer no caso de divergência.

Eleni Kosta questiona se a escolha estará a cargo da entidade que utiliza o testemunho e conclui, em respeito pelo direito à autodeterminação informativa, que se deve procurar o consentimento do utilizador[500].

Parece ser esse, também, o sentido do considerando 66 da Diretiva dos Cidadãos que se refere, unicamente, ao utilizador.

No entanto, o *Information Commissioner's Office* (ICO) – entidade pública independente do Reino Unido, criada para promover o acesso à informação oficial e proteger informações pessoais – refere-se a casos em que, por exemplo, um empregador fornece a um empregado um terminal com acesso a determinados serviços para a realização de uma tarefa concreta cuja execução depende da utilização de testemunhos de conexão. O ICO entende que pode ter precedência a vontade do empregador ressalvando, porém, os casos que envolvam a recolha de informações pessoais do empregador/utilizador em que só o consentimento deste pode ser considerado válido para a instalação do testemunho em causa.[501]

A verdade é que esta é uma questão muito complexa.

---

[499] Artigo 2.º, alínea k), da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002 relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), por remissão do artigo 2.º, da Diretiva 2002/58/CE.
Ou seja, a pessoa que é titular do contrato com o fornecedor do serviço de internet.

[500] KOSTA, Eleni, *Consent in European ...* , op. cit., p. 313, e KOSTA, Eleni, *Handling cookies within* ..., cit., p. 409.

[501] UK INFORMATION COMISSIONER'S OFFICE (ICO), Guidance on the rules on use of cookies and similar technologies, VV.3, maio de 2012, 10 e ss., disponível em http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookiespp, última consulta em 30 de agosto de 2013.

Atendendo ao considerando 24 da Diretiva 2002/58/CE, ao texto e ao próprio objetivo do artigo 5.º n.º 3, entendemos que a resposta a esta questão também deve passar pela titularidade do equipamento terminal.

O artigo em análise [502] exige o consentimento do utilizador ou assinante em cujo terminal se pretendam armazenar ou aceder a informações.

Como vimos[503], o principal objetivo do artigo 5.º, n.º 3 é a proteção do equipamento terminal do utilizador e de quaisquer informações aí armazenadas, enquanto parte da esfera privada dos utilizadores[504], no que respeita ao tratamento de dados pessoais[505].[506]

Mas, a verdade é que através dos testemunhos de conexão podem ser armazenadas informações relativas à navegação de vários utilizadores num mesmo equipamento terminal (que, por sua vez, pode ter vários titulares).

Os utilizadores, em relação a quem são "gerados" os testemunhos de conexão, serão os titulares dos dados tratados através deste mecanismo, enquanto que os titulares dos equipamentos terminais são as pessoas cuja esfera privada se visa proteger especialmente com esta norma. Porém, estes só são chamados a dar o seu consentimento quando sejam assinantes ou utilizadores.

Assim, quando o utilizador seja o titular do equipamento terminal, é o consentimento deste que é exigido.

Quando o titular do equipamento terminal seja o assinante, é o consentimento deste que se exige – pense-se no suprarreferido exemplo do empregador, que será o assinante e o titular do equipamento terminal utilizado pelo trabalhador.

[502] Artigo 5.º, n.º 3, da Diretiva 2002/58/CE com a redação que lhe foi dada pela Diretiva 2009/136/CE.
[503] Título 2. deste Capítulo III.
[504] Considerando 24 da Diretiva 2002/38/CE.
[505] Artigo 1.º da Diretiva da Privacidade Eletrónica.
[506] Como vimos no Título 2. deste Capitulo III.

O consentimento em análise é o fundamento de legitimidade específico para o armazenamento de informações[507]. Quando as informações em causa forem dados pessoais do utilizador, ou seja, quando através dos testemunhos de conexão instalados no terminal de um assinante, titular do equipamento terminal, se recolham dados pessoais do utilizador, este sempre estará protegido pelas regras da Diretiva da Proteção de Dados. O responsável pelo tratamento está obrigado a cumprir todas essas regras, que passam pela verificação de um fundamento legitimante, quando o consentimento especialmente obtido pela instalação de testemunhos de conexão não se revele, no caso concreto, válido para de legitimar o tratamento de dados pessoais de um titular diferente da pessoa a quem competia prestar o consentimento especial.

Situação mais complicada será quando o assinante, utilizador e titular do equipamento terminal sejam pessoas diferentes.

É em relação a esta situação não prevista, em que o titular do equipamento terminal não pode ser chamado a dar o seu consentimento – em desconformidade com o objetivo da própria norma –, que entendemos que o consentimento do utilizador deve prevalecer sobre o do assinante, em respeito pelo direito à autodeterminação informativa.

Chamamos a atenção para o facto de, na prática, não ser fácil à entidade responsável pelo *site* saber se em causa está o titular do equipamento terminal ou, sequer, a pessoa que é parte no contrato com um prestador de serviço de comunicações eletrónicas. A entidade responsável pelo *site* pode nem ser capaz de distinguir entre vários utilizadores.

Quando várias pessoas utilizem o mesmo equipamento terminal e o mesmo navegador para aceder ao mesmo *site* podem facilmente ser confundidas e tratadas por aquele como se do mesmo utilizador se tratasse.

[507] Qualquer tipo de informações, independentemente de serem ou não dados pessoais.

Pode, porém, acontecer que o grau de imiscuição dos dados pessoais de cada uma delas seja tal que impeça a sua identificação ou as torne não identificáveis. Não deixarão, no entanto, de ser informações dependentes de consentimento para serem tratadas. O consentimento prestado por uma dessas pessoas pode, formalmente, legitimar o tratamento de informações relativas a outras[508]. É outro problema de aplicação desta norma[509] para o qual se chama a atenção.

5. A entidade responsável

Como consequência do alargado âmbito de aplicação conferido ao n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica, as obrigações impostas nesta norma impendem diretamente sobre qualquer entidade que pretenda armazenar ou aceder a informações no terminal do utilizador ou assinante, sendo irrelevante que se trate de um responsável pelo tratamento ou de um subcontratante[510] [511].

A entidade responsável pelo cumprimento das obrigações decorrentes do artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica é, então, aquela que instala e lê os testemunhos de conexão. Mais concretamente, o responsável é o titular do *site* visitado, que instala e acede a testemunhos[512].

Assim, no caso dos testemunhos de terceiros, é sobre o titular do *site* terceiro que impende a obrigação de obter o consentimento prévio, com base

[508] Principalmente atendendo à possibilidade decorrente do considerando 25 da Diretiva 2002/58/CE de o consentimento prestado para a instalação dos testemunhos legitimar os acessos posteriores ao mesmo.
[509] Artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica.
[510] Por "subcontratante" deve entender-se a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que trata os dados pessoais por conta do responsável pelo tratamento, artigo 2.º, alínea e), da Diretiva 2002/58/CE.
[511] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., p. 10.
[512] Catarina Sarmento e Castro identifica os titulares dos *sites web*, a par dos operadores de telecomunicações, dos fornecedores de acesso à internet, dos fornecedores de serviços Internet e dos utilizadores, como "atores que interagem na *Internet*, por eles passando o respeito, ou o desrespeito, de regras de proteção de dados pessoais", CASTRO, Catarina Sarmento e, *Direito da Informática* ... , op. cit., pp. 154 a 156.

em informações claras e completas, de acordo com o n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica. O *site* terceiro é o responsável pelo cumprimento das obrigações decorrentes da utilização do testemunho, já que é ele quem o envia e lê.

No entanto, o Grupo do Artigo 29.º é da opinião[513] que os titulares dos *sites* que alojam conteúdos de *terceiros* e, nessa medida, são responsáveis pelo direcionamento dos seus visitantes para estes domínios, são corresponsáveis pelos testemunhos de conexão por eles instalados, na medida da sua colaboração. Esta responsabilidade deve ser aferida caso a caso.

O titular do *site* diretamente visitado é responsável por codeterminar as finalidades dos testemunhos a instalar pelo *site* terceiro, na medida em que define os critérios subjacentes aos conteúdos que aceita alojar[514].

O Grupo do Artigo 29.º realça, no entanto, que a responsabilidade do titular do *site* diretamente visitado pela instalação de testemunhos de terceiros é limitada e não o obriga a cumprir com a maioria das obrigações previstas para os responsáveis pelo tratamento, na medida em que a sua colaboração se cinja ao reencaminhamento do visitante para aquele outro domínio. Desde logo, será comum ficarem excluídos da obrigação de garantir o direito de acesso, uma vez que os dados não estão em seu poder. Já não será assim quando além de redirecionar, o *site* diretamente visitado forneça ao terceiro informações que tenha em sua posse sobre o utilizador, nomeadamente dados pessoais recolhidos através do preenchimento de um formulário. Neste último exemplo, o titular do *site* diretamente visitado é um verdadeiro responsável pelo tratamento e, por isso, sujeito a todas as obrigações que da lei decorrem.[515]

[513] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., pp. 12 e 13.
[514] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., pp. 12 e 13.
[515] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., pp. 12 e 13.

Quando as informações armazenadas ou acedidas através do testemunho sejam dados pessoais, a entidade que os instala ou lê desempenha o papel de responsável pelo tratamento e, além das obrigações decorrentes do artigo 5.º, n.º 3 da Diretiva da Privacidade Eletrónica, tem de cumprir com as que resultam da Diretiva 95/46/CE.

6. A confirmação do consentimento como fundamento legitimante da utilização de testemunhos de conexão

A Comissão Europeia apresentou a sua Proposta de diretiva relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas[516], em 25 de agosto de 2000. Deste texto, não constava qualquer previsão relativa ao armazenamento e acesso a informação previamente armazenada no equipamento terminal do utilizador ou assinante.

O Parlamento Europeu, no âmbito da primeira leitura do processo de codecisão, introduziu pela primeira vez uma previsão respeitante ao armazenamento ou acesso a informação previamente armazenada no terminal do utilizador. A alteração 26 à proposta da Comissão previa o seguinte:

> ***Os Estados-membros proibirão a utilização de redes de comunicações eletrónicas para a armazenagem de informação ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador sem o consentimento prévio e explícito do assinante ou do utilizador em causa. Esta proibição não impedirá qualquer armazenamento técnico ou acesso que tenham como finalidade efetuar ou facilitar a transmissão de uma***

[516] COMISSÃO DAS COMUNIDADES EUROPEIAS, *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas*, COM(2000) 385 final – 2000/0189(COD), Bruxelas, 12 de julo de 2000.

> ***comunicação através de uma rede de comunicações eletrónicas.*** [517]

O Parlamento Europeu avançou, então, com a regulamentação do armazenamento e acesso a informação no equipamento terminal do utilizador, estabelecendo o consentimento prévio e explícito do utilizador ou assinante como condição legitimante[518]. Esta opção, no entanto, não foi bem recebida por organizações como a IAB (Interactive Advertising Bureau) Europe, a UNICE (Union of Industrial and Employers' Confederation of Europe) – hoje, BUSINESSEUROPE, the Confederation of European Business – e a FEDMA (Federation of European Direct and Interactive Markting), que exerceram forte pressão contra a alteração proposta pelo Parlamento Europeu, alegando que o requisito de consentimento prévio e explícito do utilizador ou assinante como condição legitimante para o armazenamento e acesso a informação no equipamento terminal criaria barreiras desnecessárias na internet e teria um impacto devastador no comércio eletrónico[519].

O texto final da Diretiva acabou por acolher a alteração proposta pelo Conselho da União Europeia, através da Posição Comum N.º 26/2002[520], que substituiu a proibição geral de armazenamento ou acesso a informação no equipamento terminal do utilizador ou assinante, pela sua permissão, por defeito. Assim, o n.º 3 do artigo 5.º da Diretiva 2002/58/CE veio estabelecer que:

> ***Os Estados-Membros velarão por que a utilização de redes de comunicações eletrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador só seja permitida na condição de serem fornecidas ao assinante ou ao***

[517] PARLAMENTO EUROPEU, *Processo de co-decisão: primeira leitura, Proposta de diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrônicas* (COM(2000) 385 – C5-0439/2000 – 2000/0189(COD)), de 12 de julho de 2000.
[518] Direito de *opt-in*.
[519] Cf. KOSTA, Eleni, *Consent in European ...* , op. cit., p. 299.
[520] CONSELHO DA UNIÃO EUROPEIA, *Posição Comum n.º 26/2002 adotada pelo Conselho em 28 de Janeiro de 2002 tendo em vista a adopção, da Diretiva 2002/. . ./CE do Parlamento Europeu e do Conselho, de . . ., relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrônicas* (2002/C 113 E/03).

utilizador em causa informações claras e completas, nomeadamente sobre os objetivos do processamento, em conformidade com a Diretiva 95/46/CE, e de lhe ter sido dado, pelo controlador dos dados [521]***, o direito de recusar esse processamento. Tal não impedirá qualquer armazenamento técnico ou acesso que tenham como finalidade exclusiva efetuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação que tenha sido explicitamente solicitado pelo assinante ou pelo utilizador.*** [522]

O requisito de consentimento prévio e explícito foi, assim, substituído pela imposição ao responsável pelo tratamento das obrigações de prestar ao utilizador ou assinante informações claras e completas e reconhecer direito deste a recusar o tratamento.

Considerados como instrumentos que podem ser legítimos e úteis, "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" [523], os testemunhos de conexão vêm expressamente referidos no considerando 25 da Diretiva 2002/58/CE. A sua utilização, na União Europeia, está sujeita às condições plasmadas no n.º 3 do artigo 5.º.

O n.º 3 do artigo 5.º da Diretiva 2002/58/CE, permitia a utilização de redes de comunicações eletrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador, desde que fossem prestadas ao assinante ou utilizador informações claras e completas, nomeadamente sobre as finalidades do processamento e, cumulativamente, lhe fosse garantido o direito de recusar o tratamento[524].

[521] O n.º 3 do artigo 5.º, da Diretiva 2002/58/CE refere-se a "controlador dos dados", que mais não é do que o responsável pelo tratamento ("data controller", na versão inglesa).
[522] CONSELHO DA UNIÃO EUROPEIA, Posição Comum n.º 26/2002, cit..
[523] Considerando 25, da Diretiva 2002/58/CE.
[524] Direito de *opt-out*.

Ressalvadas ficavam as situações em que o armazenamento técnico ou o acesso visava como finalidade exclusiva efetuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação que tenha sido explicitamente solicitado pelo assinante ou pelo utilizador. [525]

A revisão da Diretiva 2002/58/CE no âmbito da reforma do quadro europeu das comunicações eletrónicas reacendeu o debate em torno dos requisitos para o armazenamento e aceso a informação previamente armazenada no equipamento terminal do utilizador ou assinante.

A proposta da Comissão[526] previa, unicamente, a alteração do n.º 3 do artigo 5.º no sentido de excluir o requisito da utilização de redes de comunicação eletrónicas, alargando o seu âmbito de aplicação.

O Parlamento Europeu, aquando da primeira leitura[527], insistiu na exigência de um requisito apertado de consentimento prévio do assinante ou utilizador, que ficara frustrada aquando da aprovação da Diretiva 2002/58/CE, entendendo que as implementações práticas das regras do artigo 5.º, n.º 3 então em vigor, não conferiam uma proteção suficiente dos direitos do utilizador, particularmente no que respeita à transparência e ao direito de

[525] Artigo 5.º, n.º 3, da Diretiva 2002/58/CE.
[526] COMISSÃO DAS COMUNIDADES EUROPEIAS, *Proposta de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor*, {SEC(2007) 1472} {SEC(2007) 1473}, COM(2007) 698 final 2007/0248 (COD), Bruxelas, 13 de novembro de 2007, Bruxelas, 13 de novembro de 2007, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0698:FIN:pt:PDF, última consulta em 20 de agosto de 2013.
[527] PARLAMENTO EUROPEU, *I Resolução legislativa do Parlamento Europeu, de 24 de Setembro de 2008 , sobre uma proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n. °2006/2004 relativo à cooperação no domínio da defesa do consumidor* (COM(2007)0698 — C6-0420/2007 — 2007/0248(COD)) - P6_TC1-COD(2007)0248 Posição do Parlamento Europeu aprovada em primeira leitura em 24 de setembro de 2008.

escolha. Assim, introduziu a alteração 128, passando o n.º 3 do artigo 5.º a ter a seguinte redação:

> ***Os Estados-Membros asseguram que o armazenamento de informações ou o acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador, direta ou indiretamente através de qualquer dispositivo de armazenamento, seja proibido, salvo em caso de consentimento prévio do assinante ou do utilizador em causa, sendo que a configuração do programa de navegação constitui consentimento prévio, e desde que lhe sejam prestadas informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento, e lhe seja dado, pelo controlador dos dados, o direito de recusar o processamento. Esse facto não impede 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 em termos estritamente necessários para prestar um serviço no âmbito da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.*** [528]

No entanto, o Parlamento voltou a encontrar resistência.

A Comissão não aceitou o requisito de consentimento do assinante ou utilizador[529].

Mas o Parlamento não desistiu da intenção de introduzir o requisito de consentimento e, na segunda leitura, reformulou a redação do artigo:

---

[528] PARLAMENTO EUROPEU, *I Resolução legislativa do Parlamento Europeu, de 24 de Setembro de 2008 , sobre uma proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n. °2006/2004 relativo à cooperação no domínio da defesa do consumidor* (COM(2007)0698 — C6-0420/2007 — 2007/0248(COD)) - P6_TC1-COD(2007)0248 Posição do Parlamento Europeu aprovada em primeira leitura em 24 de setembro de 2008.

[529] COMISSÃO DAS COMUNIDADES EUROPEIAS, Proposta alterada de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor, COM(2008)723 final 2007/0248 (COD), Bruxelas, 6 de novembro de 2008, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0723:FIN:pt:PDF, última consulta em 20 de agosto de 2013.

No artigo 5.º, o n.º 3 passa a ter a seguinte redação:

«3. Os Estados-Membros assegurarão que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só seja permitido, se este tiver dado o seu consentimento prévio, que foi concedido com base em informações claras e completas, em conformidade com a Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento ▌. Tal não impedirá 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 que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.» [530]

Esta alteração foi aceite pela Comissão Europeia[531] e pelo Conselho da União Europeia[532].[533]

A assinatura final da Diretiva dos Cidadãos pelo Parlamento Europeu e pelo Conselho[534], teve lugar em 25 de novembro de 2009.

---

[530] PARLAMENTO EUROPEU, *Resolução legislativa do Parlamento Europeu, de 6 de Maio de 2009, referente à posição comum aprovada pelo Conselho tendo em vista a aprovação de uma diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor* (16497/1/2008 – C6-0068/2009 – 2007/0248(COD)), 6 de maio de 2009.

[531] COMISSÃO DAS COMUNIDADES EUROPEIAS, *Parecer da Comissão nos termos do artigo 251.º, n.º 2, terceiro parágrafo, alínea c), do Tratado CE, sobre as alterações do Parlamento Europeu à posição comum do Conselho respeitante à proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor QUE ALTERA A PROPOSTA DA COMISSÃO nos termos do n° 2 do artigo 250° do Tratado CE*, COM(2009) 421 final 2007/0248 (COD), Bruxelas, 29 de julho de 2009, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0421:FIN:PT:PDF, última consulta em 20 de agosto de 2013.

[532] CONSELHO DA UNIÃO EUROPEIA, *Adenda ao Projeto de Ata, 2970.ª* reunião do Conselho da União Europeia (Assuntos Gerias e Relações Externas), realizada no Luxemburgo, em 26 de outubro de 2009, Bruxelas, 17 de novembro de 2009 (OR. fr) 14985/09 ADD 1 PV/CONS 55, p. 7.

[533] Sobre os trabalhos preparatórios, da Diretiva 2002/58/CE e, da Diretiva 2009/136/CE no que respeita ao artigo 5.º, n.º 3, KOSTA, Eleni, *Consent in European ...* , op. cit., pp. 298 a 303.

[534] PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA, *Diretiva do Parlamento Europeu e do Conselho que Altera a Diretiva 2002/22/CE Relativa ao Serviço Universal e aos Direitos dos Utilizadores em Matéria de Redes e Serviços de Comunicações Eletrónicas, a Diretiva 2002/58/CE Relativa ao Tratamento de Dados Pessoais a e à Proteção da Privacidade no Sector das Comunicações Eletrónicas e o Regulamento (CE) N.º*

Culminado o processo legislativo, o artigo 5.º n.º 3 da Diretiva da Privacidade Eletrónica, com a redação que lhe foi dada pela Diretiva dos Cidadãos, passa a exigir o consentimento do utilizador ou assinante, prestado com base em informações claras e completas nos termos da Diretiva 95/46/CE, como condição para o armazenamento ou acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador.

7. Requisitos relativos ao Consentimento

O armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador está dependente do seu consentimento prévio, com base em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento, nos termos do n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica. São estes, portanto, os fundamentos relativos à legitimidade da utilização de testemunhos de conexão.

A Diretiva da Privacidade Eletrónica define consentimento por parte do utilizador ou assinante por remissão para a definição de consentimento dado pela pessoa a quem dizem respeito os dados, previsto na Diretiva da Proteção de Dados[535].

Assim por consentimento deve entender-se "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"[536].

2006/2004 Relativo à Cooperação entre as Autoridades Nacionais Responsáveis pela Aplicação da Legislação de Defesa do Consumidor, 2007/0248 (COD) LEX 1102, PE-CONS 3674/1/09 REV 1, Estrasburgo, 25 de novembro de 2009.

[535] Artigo 2.º, alínea f), da Diretiva da Privacidade Eletrónica.

[536] Artigo 2.º, alínea h), da Diretiva 95/46/CE.

Como tivemos oportunidade de ver[537], o consentimento surge na Diretiva 95/46/CE como um de entre vários fundamentos legais para o tratamento de dados pessoais.

Nos termos da alínea a) do artigo 7.º da Diretiva 95/46/CE, o consentimento, enquanto fundamento de legitimidade deve, ainda, ser prestado de forma inequívoca.

O consentimento deve ser utilizado de modo a conferir à pessoa em causa controlo sobre o tratamento dos seus dados – no caso, das suas informações e sobre o acesso ao seu equipamento terminal. Se utilizado incorretamente, o consentimento não pode constituir um fundamento legitimante do tratamento, já que o controlo dado à pessoa em causa se torna meramente ilusório[538].

Sintetizando, o consentimento enquanto fundamento de legitimidade específico para a utilização de testemunhos de conexão tem de ser prévio, prestado com base em informações claras e completas (informado), livre, específico e inequívoco.

Porém, dada a diversidade das informações que podem estar em causa, a utilização de testemunhos de conexão pode envolver o tratamento de dados pessoais sensíveis. Neste caso, o consentimento deve ainda ser explícito[539].

Em todas as situações, para ser válido o consentimento prestado tem, ainda, de poder ser revogável a todo o tempo.

O direito de revogar o consentimento prestado decorre diretamente do direito à autodeterminação informativa e não se confunde com o direito de oposição[540] previsto no artigo 14.º da Diretiva 95/46/CE. Enquanto aquele

[537] Título 2.2.2. do Capítulo II.
[538] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 2.
[539] Artigo 8.º, n.º 2, alínea a), da Diretiva 95/46/CE.
[540] Entre nós, sobre o direito de oposição previsto no artigo 14.º, da Diretiva 95/46/CE e transposto através do artigo 12.º da Lei n.º 67/98, de 26 de outubro, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 254 a 261, e MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., p. 359.

pressupõe o prévio consentimento da pessoa em causa para o tratamento de dados que lhe digam respeito, este aplica-se a tratamentos de dados com um fundamento legitimante diferente do consentimento. [541]

O direito de revogar o consentimento prestado é um direito indisponível, a que a pessoa em causa não pode renunciar, e que pode exercer a qualquer momento.[542] [543]

Atendendo ao facto de que o mesmo testemunho pode servir a diversas finalidades – "testemunhos polivalentes" [544] – o consentimento prestado tem, ainda, de preencher todos os requisitos em relação a cada uma delas, para que a sua utilização seja legítima.

A propósito da Diretiva da Proteção de Dados [545], já tivemos oportunidade de avançar com descrições sucintas das diferentes características do consentimento em matéria de tratamento de dados pessoais. Regressemos a elas num esforço de lhes apreender melhor o alcance no contexto específico da utilização de testemunhos de conexão.

7.1. O Consentimento Informado

Através da Internet podem ser levados a cabo quer tratamentos visíveis, quer tratamentos invisíveis de dados pessoais. Enquanto os primeiros são realizados com o conhecimento da pessoa em causa, ou segundos não e, portanto, são-lhe "invisíveis"[546]. [547]

[541] Neste sentido, KOSTA, Eleni, *Consent in European ...* , op. cit., 251.
[542] Neste sentido, KOSTA, Eleni, *Consent in European ...* , op. cit., p. 251.
[543] Entre nós, o consentimento prestado pode sempre ser revogável nos termos do artigo 81.º, n.º 2, do Código Civil. "A revogação do consentimento deve dar lugar à imediata destruição dos dados e é ilícita, embora possa fazer incorrer o titular na obrigação de indemnizar os danos causados pela revogação", Cf. VASCONCELOS, Pedro Pais de, *Proteção de Dados Pessoais e Direito à Privacidade*, em "Direito da Sociedade da Informação", Volume I, Coimbra Editora, outubro 1999, p. 252.
[544] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 6.
[545] Título 2.2. do Capítulo II.
[546] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Recomendação 1/99 sobre o tratamento invisível e automatizado de dados pessoais na Internet realizado por software e hardware* (WP17), de 23 de Fevereiro de 1999, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17_pt.pdf, última consulta em 30 de agosto de 2013.

A utilização de testemunhos de conexão representa um exemplo típico de tratamento invisível de dados[548].

Este mecanismo veio sendo largamente utilizado sem que fosse dado ao utilizador conhecimento de que estavam a ser armazenadas acedidas informações previamente armazenadas no seu equipamento terminal. Este não era notificado da intromissão externa no seu equipamento terminal promovida por esta via e, muito menos, era chamado a dar o seu consentimento para tal.[549]

As práticas comuns passavam pela armazenagem e acesso discretos, sem qualquer alerta ao utilizador – sem que a sua intervenção fosse necessária ou reclamada em qualquer momento[550].

O Grupo do Artigo 29.º cedo chamou a atenção para a necessidade de prestar informações ao utilizador sobre "quando o software da Internet tenciona receber, armazenar ou enviar um cookie", devendo a mensagem "especificar, numa linguagem compreensível a nível geral, qual a informação

---

[547] Entre nós, sobre os tratamentos visíveis e invisíveis de dados pessoais, com especial referência aos testemunhos de conexão, ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 156 a 160, e MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática ...* , op. cit., pp. 432 a 441.

[548] "Atualmente, é quase impossível utilizar a Internet sem se ser confrontado com propriedades invasoras da privacidade que levam a cabo 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. Um exemplo deste tipo de técnica é o chamado cookie, que pode ser definido como um registo informático de informações enviadas de um servidor *web* para o computador de um utilizador, com o objetivo de identificar futuramente esse computador aquando de visitas posteriores ao mesmo sítio *web*." GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Recomendação 1/99 sobre o tratamento ...* , cit., p. 4.

[549] "Research into consumers' understanding of the internet and cookies demonstrates that current levels of awareness of the way cookies are used and the options available to manage them is limited. The Department for Culture, Media and Sport commissioned PricewaterhouseCoopers LLP (PWC) to conduct research into the potential impact of cookies regulation. PWC conducted an online survey of over 1000 individuals in February 2011. Despite the report acknowledging that the most intensive internet users are overrepresented in the sample, the results illustrate that significant percentages of these more 'internet savvy' consumers have limited understanding of cookies and how to manage them: 41% of those surveyed were unaware of any of the different types of cookies (first party, third party, Flash / Local Storage). Only 50% were aware of first party cookies. Only 13% of respondents indicated that they fully understood how cookies work, 37% had heard of internet cookies but did not understand how they work and 2% of people had not heard of internet cookies before participating in the survey. 37% said they did not know how to manage cookies on their computer. The survey tested respondents' knowledge of cookies, asking them to confirm if a number of statements about cookies were correct or not. Out of the sixteen statements only one was answered correctly by the majority of respondents. Those who use the internet less regularly, or have a generally lower level of technical awareness, are even less likely to understand the way cookies work and how to manage them. The report concluded that 'broader consumer education about basic online privacy fundamentals could go a long way toward making users feel more comfortable online and also enable them to take more control of their privacy while online' and that 'online businesses will need to evolve their data collection and usage transparency in order to illustrate to consumers the benefits of opting-in.'" UK INFORMATION COMISSIONER'S OFFICE (ICO), *Guidance on the* ... , cit., p. 3

[550] Como vimos melhor ao longo do Título 2. do Capítulo I.

que se tenciona armazenar no cookie, com que objetivo e, também, qual o seu prazo de validade"[551].

O artigo 5.º n.º 3 da Diretiva da Privacidade Eletrónica, com a redação que lhe foi dada pela Diretiva dos Cidadãos, veio estabelecer como requisito legitimante para armazenamento e acesso a informações previamente armazenadas no equipamento terminal o consentimento prévio do utilizador ou assinante prestado com base em informações claras e completas.

Já na versão de 2002 desta norma, além de ter que dar ao utilizador ou assinante o direito de recusar o tratamento, o responsável estava obrigado a fornecer-lhe em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento.

A obrigação de prestar informações relativas ao tratamento levado a cabo está, portanto, presente nas duas versões da norma em apreço. Com a Diretiva dos Cidadãos, esta obrigação não se altera na sua substância mas passa a ser exigida num momento prévio à obtenção do consentimento do utilizador ou assinante para o armazenamento de informações ou acesso a informações previamente armazenadas no seu equipamento terminal.

Assim, a legitima utilização de testemunhos de conexão, nos termos do n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica depende do fornecimento de informações claras e completas ao utilizador, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do tratamento, e da obtenção o consentimento do utilizador ou assinante, depois de lhe terem sido fornecidas aquelas informações.

Justifica-se, portanto, começarmos por nos ocupar desta obrigação de prestar informações à pessoa em causa, nos termos da Diretiva 95/46/CE,

[551] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Recomendação 1/99 sobre o tratamento ...* , cit., p. 3.

nomeadamente sobre os objetivos do processamento[552], que impende sobre a entidade responsável.

Como já tivemos oportunidade de referir[553], para ser tido como informado, o consentimento deve basear-se "numa apreciação e compreensão dos factos e implicações de uma ação"[554].

As disposições da Diretiva 95/46/CE aplicam-se a matérias que não sejam especialmente previstas pela Diretiva da Privacidade Eletrónica, quando esteja em causa o tratamento de dados pessoais[555].

O artigo 10.º da Diretiva 95/46/CE dispõe sobre as informações que o responsável pelo tratamento – ou o seu representante – está obrigado a prestar à pessoa em causa junto da qual recolha dados que lhe digam respeito.

A remissão expressa incluída no artigo 5.º n.º 3 da Diretiva da Privacidade Eletrónica seria, portanto, escusada não fosse o seu amplo âmbito de aplicação[556]. Como vimos[557], esta norma não se limita ao tratamento de dados pessoais, mas aplica-se ao armazenamento ou acesso de quaisquer informações – independentemente de serem ou não dados pessoais – no equipamento terminal do utilizador ou assinante.

---

[552] Por "objetivos do processamento" devemos entender "finalidades do tratamento", nos termos, da Diretiva 95/46/CE.
Lamentamos as incoerências terminológicas nas versões portuguesas das Diretivas do quadro legislativo europeu da proteção de dados.
[553] Título 2.2.2. do Capítulo II.
[554] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE)* (WP 131), de 15 de fevereiro de 2007, p. 9, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_pt.pdf, última consulta em 30 de agosto de 2013.
Entre nós, o artigo 2.º da Lei 67/98, de 26 de outubro reconhece o princípio geral da transparência. Sobre este princípio ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 229.
[555] Como vimos no Título 2.3 do Capítulo II.
[556] Neste sentido KOSTA, Eleni, *Consent in European ...* , op. cit., p. 309, e KOSTA, Eleni, *Handling cookies within* ..., cit., p. 406.
[557] Título 3.1.1. deste Capítulo III.

Desta forma, a obrigação do responsável pelo tratamento ou do seu representante fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as informações especificadas no artigo 10.º da Diretiva da Proteção de Dados, é estendida à recolha de todas as informações armazenadas ou acedidas no equipamento terminal do utilizador ou assinante.

Quando esteja em causa a instalação de testemunhos de terceiros, como vimos[558], é sobre o titular do *site* terceiro que impende a obrigação de prestar informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento, que decorre do n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica, por ser este quem o envia e lê.

No entanto, o Grupo do Artigo 29.º é da opinião[559] que os titulares dos *sites* que alojam conteúdos de *terceiros* são corresponsáveis pelos testemunhos de conexão por eles instalados, na medida da sua colaboração.

No que respeita à obrigação de prestar informações em apreço, a coordenação entre o *site* diretamente visitado e o site terceiro deve atender à finalidade visada pela imposição da obrigação de prestar informações. O que releva é a capacidade das informações chegarem de modo eficaz, claro e completo ao utilizador para que este, com base nelas, possa tomar uma decisão válida.[560]

Independentemente da medida em que partilhe das obrigações decorrentes do n.º 3 do artigo 5.º com o titular do *site* terceiro, o titular do *site* diretamente visitado tem obrigações para com o utilizador que decorrem diretamente da Diretiva 95/45/CE. A verdade é que este é responsável pelo

[558] Título 5. Deste Capítulo III.
[559] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., pp. 12 e 13.
[560] Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 22.

redireccionamento do utilizador para o *site web* terceiro, nomeadamente através da transferência do seu endereço IP[561].[562]

O titular do *site* diretamente visitado está obrigado a informar o utilizador sobre o tratamento de dados levado a cabo pela operação de redireccionamento com recurso ao navegador do utilizador, sobre a instalação de um testemunho de terceiros no seu equipamento terminal que aquele tratamento visa permitir, sobre a identidade da entidade terceira e sobre os objetivos do tratamento a levar a cabo por esta através daqueles testemunhos[563].[564]

As informações prestadas serão, então, completas se compreenderem as finalidades do testemunho; a eventual comunicação (transmissão) das informações, a identidade quer da entidade responsável, quer de eventuais destinatários dos seus dados e dos representantes destes; as condições do tratamento e a duração do testemunho[565]; a necessidade de aceitar a instalação e/ou o acesso e as possíveis consequências no caso de não aceitar[566]; a existência do direito ao acesso aos dados e do direito de os retificar[567]; e, se for caso disso, a possibilidade de instalação de testemunhos de terceiros, respetivas finalidades e identidade da entidade terceira.[568]

O Grupo do Artigo 29.º destaca que é, ainda, essencial que ao utilizador ou assinante seja dada informação relativa ao modo como pode

[561] A transferência do endereço IP processa-se com recurso ao navegador. GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 21.
[562] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 21.
[563] Sem prejuízo de outras informações devidas pelo reencaminhamento de outros dados pessoais dos seus utilizadores a terceiros.
[564] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., pp. 20 e 21.
[565] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on obtaining consent for cookies* (WP 208), p. 3, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf, última consulta em 20 de outubro de 2013.
[566] No que respeita à informação a respeito das consequências no caso de não responder (aceitar a instalação ou acesso), defendemos, que estas devem ser objetivas e não compreender conclusões qualitativas. Ou seja, devem ser preferidas expressões como *navegação mais rápida/lenta***,** *experiência mais/menos personalizada* a expressões como *melhor/pior navegação* ou *melhor/pior experiencia***.**
[567] Artigo 10.º, da Diretiva 95/46/CE.
[568] Sobre o fornecimento de informações prévio à recolha de dados pessoais de um indivíduo através de um *site* ver, ainda, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Recomendação 2/2001 sobre determinados requisitos mínimos para a recolha de dados pessoais em linha na União Europeia* (WP 43), de 17 de maio de 2001, pp. 5 a 8, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp43_pt.pdf, última consulta em 30 de agosto de 2013.

expressar o seu consentimento em relação a todos, alguns ou nenhum dos testemunhos, e à forma de alterar as suas preferências no futuro.[569]

Contudo, para cumprir com o requisito respeitante ao consentimento informado, não chega que as informações prestadas sejam completas. Devem, ao mesmo tempo, ser claras, ou seja, "tão conviviais quanto possível" [570].

O Grupo do Artigo 2.º refere-se a dois tipos de exigências com vista a assegurar a adequação da informação, um respeitante à qualidade e outro à acessibilidade e visibilidade da informação. [571]

A respeito da qualidade da informação o Grupo refere[572] que esta se deve ser suscetível de ser entendida por um utilizador médio. Assim, para que possa ser considerada compreensível, é importante ter em atenção não só o idioma em que a informação é prestada mas, também, a linguagem que deve ser acessível ao utilizador comum[573]. A forma de prestar a informação devida depende sempre do contexto.

No que respeita à acessibilidade e visibilidade da informação, esta deve ser prestada diretamente às pessoas, "deve ser claramente visível (tipo e tamanho das letras), proeminente e completa.". [574]

7.2. O Consentimento Prévio

[569] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on …* , cit., pp. 3 e 4.
[570] Considerando 25, da Diretiva 2002/58/CE.
[571] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição …* , cit., p. 22.
[572] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição …* , cit., p. 22.
[573] Como vimos no Título 2.5. do Capítulo I, de acordo com o P3P, as políticas de privacidade dos *sites* devem ser ser expressadas não só em linguagem compreensível aos utilizadores mas, também, às máquinas – aos navegadores –, de modo a que estes, de interfaces, ajudem o utilizador a melhor compreender esses politicas e a tomar decisões automatizadas sobre elas.
[574] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição …* , cit., p. 22.

Apesar de a versão portuguesa da Resolução legislativa do Parlamento Europeu, de 6 de Maio de 2009 (segunda leitura) ter mantido a referência ao consentimento prévio, como resultava da alteração prevista na primeira leitura, o mesmo não aconteceu nas versões inglesa e francesa que apenas se referem à exigência de consentimento prestado com informações claras e completas[575] [576].

A interpretação do requisito de consentimento viu-se, assim, obscurecida.

A redação do considerando 66, respeitante ao armazenamento e acesso a informações previamente armazenadas no terminal do utilizador ou assinante, contribuiu para a dispersão de interpretações, afastando-se do novo requisito de consentimento e referindo-se à prestação de informações e ao direito de recusar o tratamento, na senda da versão de 2002 do artigo 5.º, n.º 3[577].

[575] "Article 5(3) shall be replaced by the following:
«3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing ▌. This shall not prevent any technical storage or access for the sole purpose of carrying out ▌the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.»" e
"À l'article 5, le paragraphe 3 est remplacé par le texte suivant:
«3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement ▌. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ▌la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. » ".

[576] "(...) the principle that all language versions are equally authentic means that no single version is authentic. (...) Linguistic discrepancies can rarely be resolved just by comparison of different versions.", Cf. JACOBS, Francis, *SEMINARS ON QUALITY OF LEGISLATION How to interpret legislation which is equally authentic in twenty languages - Summary report*, Comissão Europeia, Lecture by Advocate General, Bruxelas, 20 de outubro de 2003, disponível em http://ec.europa.eu/dgs/legal_service/seminars/agjacobs_summary.pdf, ultimo acesso em 30 de agosto de 2013.
"As diferentes versões linguísticas de um texto comunitário devem ser objeto de interpretação uniforme e, portanto, quando exista uma divergência entre essas versões, a disposição em causa deve ser interpretada em função da economia geral e da finalidade da regulamentação de que constitui um elemento.", Acórdão do Tribunal de Justiça, Regina (A Rainha) e Pierre Bouchereau, Processo 30/77, de 27 de outubro de 1977. No mesmo sentido, o Acórdão do Tribunal de Justiça, *Erich Stauder e Cidadede Ulm — Sozialamt*, Processo 29/69, de 12 de Novembro de 1969.

[577] Apesar de a versão portuguesa do considerando 66, da Diretiva 2009/136/CE ter mantido uma referência às formas de prestação de pedir consentimento, como já decorria do considerando 25, da Diretiva 2002/58/CE, ("As formas de prestação de informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão simples quanto possível."), as versões inglesa e francesa do considerando 66, da Diretiva 2009/136/CE referem-se apenas a formas de prestação de informações e de proporcionar o direito de recusar: "The methods of providing information and offering the right to refuse should be as user-friendly as possible" e "Les méthodes retenues pour fournir des informations et offrir le droit de refus devraient être les plus conviviales possibles".

Foi com base no considerando 66 que a Áustria, a Bélgica, a Estónia, a Finlândia, a Alemanha, a Irlanda, a Letónia, a Malta, a Polónia, a Roménia, a Eslováquia, a Espanha e o Reino Unido declararam entender que o consentimento exigido no novo n.º 3 do artigo 5.º deve, na prática, ser exercido como direito de recusar o armazenamento ou o posterior acesso[578]:

> ***O artigo 5.º, n.º 3, da Diretiva 2002/58/CE diz respeito às condições em que a informação, incluindo software espião ou outros tipos de programas malévolos indesejados, pode ser colocada no equipamento terminal dos cidadãos. É igualmente aplicável aos testemunhos de conexão ("cookies") e a tecnologias similares, cuja utilização pode ser legítima em numerosas circunstâncias. O texto alterado do artigo 5.º, n.º 3, esclarece que a atual exigência de consentimento para a utilização de tais tecnologias é aplicável independentemente de serem disponibilizadas através das redes de comunicações eletrónicas ou de outros meios técnicos. Esses Estados-Membros reconhecem que tal clarificação é suscetível de exigir a alteração de algumas legislações nacionais. Todavia, tal como indicado no considerando 66, o artigo 5.º, n.º 3 alterado não se destina a alterar o requisito em vigor segundo o qual tal consentimento deve ser exercido como direito de recusar a utilização de testemunhos de conexão ou tecnologias similares para fins legítimos. Esses Estados-Membros sublinham igualmente que os métodos para prestar informações e proporcionar o direito de recusar deverão ser tão simples quanto possível.[579]***

O texto final do novo artigo 5.º n.º 3 da Diretiva da Privacidade Eletrónica, assume a redação dada pela Resolução legislativa do Parlamento Europeu, de 6 de Maio de 2009 (segunda leitura), mantendo-se a desconformidade entre as versões das várias línguas da União.

---

[578] Cf. KOSTA, Eleni, Consent in European Data Protection Law, Martinus Nijhoff Publishers, Países Baixos, 2013, pp. 303 e 304, e KOSTA, Eleni, *Handling cookies within* ..., cit., p. 404 e 405.

[579] CONSELHO DA UNIÃO EUROPEIA, *Adenda à nota Ponto "I/A" Proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, a Diretiva 2002/19/CE relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos e a Diretiva 2002/20/CE relativa à autorização de redes e serviços de comunicações eletrónicas* (AL + D) (terceira leitura), Declarações 15864/09 ADD 1 REV 1 Bruxelas, 18 de novembro de 2009.

O Grupo Artigo 29.º para a Proteção de Dados, através do seu Parecer 2/2010 sobre publicidade comportamental em linha, adotado em 22 de Junho de 2010, defendeu que o consentimento exigido no n.º 3 do artigo 5.º "tem de ser obtido antes do testemunho ser instalado e/ou as informações armazenadas no equipamento terminal do utilizador serem recolhidas, o que habitualmente se designa por «consentimento prévio»"[580] [581].

Apesar da posição assumida pelo Grupo do Artigo 29.º[582], algumas entidades responsáveis mantêm-se resistentes a tal interpretação[583].

A Comissão Europeia, não assumiu uma posição oficial sobre esta querela[584].

7.3. O Consentimento Livre

[580] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 14.
GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on ...* , cit., p. 4.
[581] O Grupo do Artigo 29.º esclareceu, ademais, que "a possibilidade de iniciar o tratamento sem obtenção de consentimento prévio apenas é lícita quando a Diretiva da Proteção de Dados Pessoais ou a Diretiva da Privacidade Eletrónica, em vez de exigirem o consentimento, preverem um fundamento alternativo e remeterem para o direito de oposição ou de recusar o tratamento. Estes mecanismos distinguem-se claramente do consentimento. Nestes casos, o tratamento pode já ter-se iniciado e a pessoa tem o direito de se opor ou de o recusar." GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 34.
[582] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 14.
[583] Apenas em Portugal, na Áustria, na Bulgária, no Chipre, na França, na Grécia, na Itália, na Letónia, na Lituânia, no Luxemburgo, nos Países Baixos, na Polónia, na Roménia, na Eslováquia, na Espanha, na Suécia, e no Reino Unido se entende que o consentimento exigido para a utilização de testemunhos de conexão tem de ser prestado num momento anterior à sua instalação – "consentimento prévio". Na Alemanha o entendimento é de que o consentimento só tem de ser prévio quando em causa esteja o tratamento de dados pessoais. DLA PIPER, *How the EU has implemented the new law on Cookies*, updated, 8 de outubro de 2012, p. 22, disponível em http://www.dlapiper.com/files/Publication/c12bf543-f878-420b-b05d-90a25022df07/Presentation/PublicationAttachment/8384fccd-731f-4c7b-ac70-95ca52e0fb68/EU_cookies_update_October_2012.pdf, última consulta em 30 de agosto de 2013 e *Cookie Laws Across Europe*, Cookipedia, disponível em http://cookiepedia.co.uk/cookie-laws-across-europe, última consulta em 15 de Outubro de 2013.
[584] A Comissão Europeia, sem assumir uma posição oficial sobre a questão, remeteu para a indústria a missão de desenvolver soluções tecnológicas com vista ao cumprimento dos requisitos legais, minimizando os custos da sua implementação. COMMUNICATIONS COMMITTEE (EUROPEAN COMMISSION Information Society and Media Directorate-General Electronic Communications Policy Implementation of Regulatory Framework), *Working Document Implementation of the revised Framework– Article 5(3) of the ePrivacy Directive*, COCOM10-34, Bruxelas, 20 de outubro de 2010, p. 6.; KOSTA, Eleni, *Consent in European ...* , op. cit., pp. 318 e 319, e KOSTA, Eleni, Handling cookies ... , cit., pp. 412 e 413

"O consentimento apenas será válido se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado. Se as consequências do consentimento comprometerem a liberdade de escolha da pessoa, o consentimento não será livre."[585]

O consentimento livre garante o exercício do direito de autodeterminação informativa[586], que é uma liberdade fundamental.[587]

O Grupo do Artigo 29.º esclarece que se entende por "livre" consentimento "uma decisão voluntária, tomada por uma pessoa na posse de todas as suas faculdades, sem qualquer tipo de coerção, de carácter social, financeiro, psicológico ou outro", realçando que "o recurso ao consentimento deve limitar-se a casos em que a pessoa em causa tenha uma liberdade de escolha genuína e possa subsequentemente retirar o consentimento sem correr riscos" [588].

Entendemos, desde logo, que o consentimento dado na sequência de informações prestadas com base em expressões qualitativas, porque confrontam o utilizador ou assinante com uma consequência negativa não objetiva, não será livre[589].

A propósito do carácter obrigatório ou facultativo da resposta, o considerando 25 da Diretiva 2002/58/CE refere que "os utilizadores deveriam ter a oportunidade de recusarem que um testemunho de conexão («cookie») ou um dispositivo análogo seja armazenado no seu equipamento terminal" realçando que "tal é particularmente importante nos casos em que outros

[585] Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 14.
[586] Sobre o direito à autodeterminação informativa ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 22 a 29.
[587] KOSTA, Eleni, *Consent in European ...* , op. cit., p. 171.
[588] Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., pp. 14 e 15.
[589] Pelo que devem ser preferidas expressões como *navegação mais rápida/lenta***,** *experiência mais/menos personalizada* a expressões como *melhor/pior navegação* ou *melhor/pior experiencia***.**

utilizadores para além do próprio têm acesso ao equipamento terminal e, consequentemente, a quaisquer dados que contenham informações sensíveis sobre a privacidade armazenadas no referido equipamento". Porém, no último período do considerando admite-se que o acesso ao conteúdo de um *site web* específico pode depender da aceitação de um testemunho de conexão (ou dispositivo análogo), caso seja utilizado para um fim legítimo.

Ora, a liberdade de aceitar ou não o testemunho de conexão é restringida perante a consequência de o utilizador ou assinante ver limitado o acesso ao conteúdo em causa; a verdade é que neste caso não existe uma verdadeira escolha[590].

Aquando da revisão da Diretiva 2002/58/CE, o Grupo do Artigo 29.º chamou a atenção para o facto de este último período do considerando 25 contradizer a posição de que os utilizadores devem ter a possibilidade de recusar a instalação de um testemunho de conexão nos seus computadores e para a necessidade de clarificação ou revisão do mesmo[591], o que não veio a acontecer.

Assim, quando o testemunho de conexão seja utilizado para um fim legítimo é permitida uma limitação à liberdade do consentimento, nos termos supra referidos[592].

7.4. O Consentimento Específico

O consentimento, para ser válido, tem de ser prestado em relação à finalidade exata do tratamento, tem de se aplicar a um contexto limitado, não

[590] Neste sentido, KOSTA, Eleni, *Consent in European ...* , op. cit., p. 312.
[591] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 8/2006 sobre a revisão do quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, com destaque para a Diretiva relativa à privacidade e às comunicações eletrónicas* (WP 126), de 26 de Setembro de 2006, p. 3, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp126_pt.pdf, última consulta em 30 de agosto de 2013.
[592] Conforme decorre do considerando 25, da Diretiva 2002/58/CE.

podendo ser genérico. Trata-se de um requisito em estreita conexão com a obrigação da entidade responsável de prestar informações. [593]

O consentimento deve ser prestado em relação aos diferentes aspetos do tratamento, nomeadamente em relação às informações recolhidas e às finalidades do tratamento[594].

O Grupo do Artigo 29.º entende que devem ser consideradas as "expectativas razoáveis das partes"[595][596]. Se os tratamentos subsequentes estiverem abrangidos pelas expectativas razoáveis da pessoa em causa, o Grupo entende que, em princípio, bastará aos responsáveis pelo tratamento obter o consentimento uma vez[597].

Em relação ao caso concreto da utilização de testemunhos de conexão, o considerando 25 da Diretiva 2002/58/CE esclarece que "a informação e o direito a recusar poderão ser propostos uma vez em relação aos diversos dispositivos a instalar no equipamento terminal do utente durante a mesma ligação e deverá também contemplar quaisquer outras futuras utilizações do dispositivo durante posteriores ligações". Recorrendo-se desta previsão, o Grupo do Artigo 29.º, consciente dos problemas práticos relativos à obrigação de obtenção de consentimento prévio, é da opinião que o consentimento para instalar o testemunho abrange os acessos posteriores ao mesmo, que têm lugar sempre que o utilizador visita um *site web* que

[593] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 19.
[594] A propósito do princípio da finalidade ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 229 a 237.
[595] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 19.
[596] "As it ["reasonable expectation of privacy"] makes privacy protection dependent on contextual factors, it could imply that the factual evolution and introduction of new technologies will determine what privacy level can be reasonably expected, inducing a weakening of privacy protection. Is it reasonable to expect any privacy when everything we do can be constantly monitored? The development of monitoring technologies and the increasing concern for public safety and security certainly lead to the erosion of privacy: the reasonable expectation of privacy turns into an expectation of being monitored." HERT, Paul De, GUTWIRTH, Serge, MOSCIBRODA, Anna, WRIGHT, e GONZALEZ-FUSTER, Gloria, *Legal Safeguards for Privacy and Data Protection in Ambient Intelligence*, From the SelectedWorks of Serge Gutwirth, outubro 2008, p. 5 , disponível em http://works.bepress.com/serge_gutwirth/4/, última consulta em 30 de agosto de 2013.
[597] A este propósito o Grupo do Artigo 29.º refere o do Tribunal de Justiça, Deutsche Telekom AG, Processo C-543/09, de 5 de Maio de 2011, que a propósito do artigo 12.º, n.º 2, da Diretiva da Privacidade Eletrónica, entendeu que, "tendo um assinante sido informado da possibilidade da transmissão de dados de caráter pessoal que lhe dizem respeito a uma empresa terceira, e tendo esse assinante dado o seu consentimento para a publicação de tais dados nessa lista, a transmissão desses mesmos dados à outra empresa não deve ser objeto de um novo consentimento pelo assinante, se existir a garantia de que os dados em causa não serão utilizados para fins diferentes daqueles para os quais foram recolhidos com vista à sua primeira publicação", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., pp. 19. e 20.

instalou o testemunho ou, no caso dos testemunhos de terceiros, outro *site* parceiro da mesma rede de publicidade[598] a que pertence aquele que instalou o testemunho.[599]

Assim, o consentimento não tem de ser prestado previamente a cada acesso às informações contidas num testemunho cuja instalação foi consentida com base em informações claras e completas. No entanto, para que o consentimento prestado nestes termos, para o futuro, preencha o requisito da especificidade em relação a cada acesso e, consequentemente, seja válido é necessário que as utilizações futuras sejam compatíveis com as finalidades iniciais em que o utilizador ou assinante consentiu[600].

7.5. O Consentimento Inequívoco

O consentimento é inequívoco quando se baseia em declarações ou atos que manifestem aceitação.

Este requisito adicional do artigo 7.º, alínea a), da Diretiva 95/46/CE reforça o sentido do requisito que se prende com a manifestação de vontade do artigo 2.º, alínea h), do mesmo diploma. A verdade é que o conceito de "manifestação" é muito amplo, já para admite qualquer meio ou forma, mas tem de ser "pela qual" a pessoa "aceita" o tratamento.

Para ser considerado inequívoco, o consentimento não pode dar espaço a qualquer dúvida quanto à intenção da pessoa em causa[601].

---

[598] Como vimos no Título 2.4. do Capítulo I, no contexto da publicidade comportamental em linha, podem estar em causa vários sites terceiros que colaboram entre si, formando uma rede de publicidade, na qual são parceiros.

[599] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 19.

[600] Ou, pelo menos, possam ser reconduzidas às "expectativas razoáveis" da pessoa em causa, cf. GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 19.

[601] Neste sentido, Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 23.
"Dito de outro modo, a manifestação pela qual a pessoa aceita que os seus dados sejam objeto de tratamento deve ser inequívoca quanto à sua intenção. Se existir uma dúvida razoável quanto à intenção da pessoa, existirá ambiguidade.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 23.

Relacionado com esta característica surge a questão da prova do consentimento. O consentimento deve ser suscetível de verificação.

O Grupo do Artigo 29.º defende que os responsáveis pelo tratamento de dados devem ter em conta que a prova do consentimento pode ser exigida no contexto de medidas de aplicação coerciva e, por uma questão de boa prática, devem gerar e conservar provas do mesmo.[602]

No entanto, o consentimento inequívoco não se confunde com o consentimento explícito.

Quando esteja em causa o tratamento de dados pessoais sensíveis através de testemunhos de conexão, o consentimento exigido pelo artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica, não é suficiente e, nos termos do artigo 8.º, n.º 2, alínea a), da Diretiva 95/46/CE, este tem ainda de ser explícito. Ou seja, tem de ser manifestado de forma expressa.

O consentimento explícito depende da resposta ativa do utilizador à questão que lhe apresenta a alternativa de aceitar ou não a instalação de testemunho(s) de conexão.

Mas o requisito de consentimento explícito não está expressamente previsto para o tratamento de informações que não sejam dados pessoais sensíveis, através de testemunhos de conexão.

Por entender que no contexto da Internet "o consentimento tácito nem sempre conduz a um consentimento inequívoco" [603], o Grupo do Artigo 29.º

[602] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 28.
[603] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 18.

defende que as pessoas em causa devem manifestar a sua vontade, prestando o seu consentimento de modo explícito.[604]

Por sua vez, o Information Commissioner's Office (ICO) – entidade independente do Reino Unido, criada para promover o acesso à informação oficial e proteger informações pessoais – nas suas Linhas Diretrizes sobre as regras sobre a utilização de testemunhos de conexão e tecnologias similares[605] dedicou especial atenção à validade do consentimento tácito para a utilização de testemunhos de conexão.

O ICO concluiu que o consentimento tácito, assim como o explícito, tem de configurar uma indicação livre, específica e informada da vontade do utilizador. Para ser válido, o consentimento tácito tem de resultar de ações do utilizador que permitam inferir o seu consentimento. Trata-se de uma série de ações que, no seu conjunto e contexto, constituem uma indicação suficientemente forte sobre a concordância do utilizador em relação à instalação do testemunho. Para que se possa concluir pela existência de uma indicação suficientemente forte, é necessário que ao levar a cabo essas ações o individuo esteja consciente e compreenda razoavelmente que, ao faze-lo, está a aceitar a instalação de testemunhos de conexão no seu equipamento terminal.[606] [607]

As diferentes autoridades nacionais competentes assumiram posições divergentes sobre a necessidade do consentimento ser expresso no contexto da utilização de testemunhos de conexão[608].

Numa clara tentativa de dirimir estas diferenças, omitindo as classificações de explícito ou tácito, o Grupo do Artigo 29.º defendeu, mais

[604] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., p. 18.
[605] UK INFORMATION COMISSIONER'S OFFICE (ICO), *Guidance on the* ... , cit..
[606] UK INFORMATION COMISSIONER'S OFFICE (ICO), *Guidance on the* ... , cit., pp. 6 e ss..
[607] Em Portugal, a lei Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto não requer que o consentimento seja expresso mas, uma vez que tem de ser prévio e baseado em informações completas, há quem defenda que o consentimento tácito não será suficiente. DLA Piper, *How the EU* …, cit.
[608] Na Bélgica, na Dinamarca, em Espanha, a Finlândia, na Hungria, na Irlanda, na Polónia, na Roménia e no Reino Unido entende-se que o consentimento pode ser tácito. DLA Piper*, How the EU* …, cit., e *Cookie Laws Across Europe*, Cookipedia, disponível em http://cookiepedia.co.uk/cookie-laws-across-europe, última consulta em 15 de Outubro de 2013.

recentemente que os utilizadores podem manifestar o seu consentimento para instalação de testemunhos de conexão através de uma "ação positiva ou outro comportamento ativo, desde que completamente informados do que essa ação representa"[609]. Esta ação positiva ou comportamento ativo não tem, pois, necessariamente de ser a resposta a uma questão que confronta o utilizador ou assinante com a escolha de permitir ou não a instalação de testemunhos.

8. O consentimento prestado por pessoas sem capacidade jurídica plena

A questão do consentimento prestado por pessoas sem capacidade jurídica plena, em que se incluem os menores, é regulada a nível nacional pela legislação cada Estado-membro.

A Diretiva 95/46/CE não dispõe sobre condições especiais de obtenção do consentimento das pessoas sem capacidade jurídica plena.

Assim, em relação a esta matéria regista-se uma abordagem fragmentada dentro do território da União Europeia, desde logo na definição da idade a partir da qual o menor é considerado capaz de prestar o seu consentimento para o tratamento de dados que lhe digam respeito. A falta de harmonização compromete a segurança jurídica.

A Proposta de Regulamento Geral de Proteção de Dados da Comissão pretende dar um passo no sentido da uniformização desta matéria, estabelecendo que o tratamento de dados pessoais que digam respeito a menores com menos de 13 anos de idade no contexto da prestação de

[609] "The users could signify their consent for cookies would be through a positive action or other active behaviour, provided they have been fully informed of what that action represents", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on ...* , cit., p. 4.

serviços da sociedade da informação depende da autorização dos seus pais ou tutores[610].

O Grupo do Artigo 29.º já havia chamado a atenção para a importância da consideração desta matéria no contexto da revisão da Diretiva da Proteção de Dados Pessoais, realçando que os interesses dos menores e de outras pessoas sem capacidade jurídica plena seriam melhor protegidos se a diretiva contemplasse disposições adicionais que regulassem especialmente a recolha e tratamento dos seus dados, atendendo à sua situação de especial vulnerabilidade.

O Grupo sugeriu que as futuras disposições possam prever as circunstâncias nas quais é exigido o consentimento do representante legal, simultaneamente ou em substituição do consentimento da pessoa incapaz, bem como as circunstâncias em que não seria possível invocar o consentimento para legitimar o tratamento de dados pessoais. [611]

Concordamos com Eleni Kosta na medida em que defende que o fundamento para o tratamento de dados pessoais que digam respeito a menores deve ser outro que não o consentimento. A autora sugere que o tratamento de dados pessoais de menores se deve legitimar na prossecução dos seus legítimos interesses. [612]

9. As exceções à obrigação de obter consentimento

A exigência de consentimento prévio, com base em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento, para o armazenamento de informações ou acesso a informações previamente armazenadas no equipamento terminal do utilizador ou assinante, é uma regra que conhece exceções.

[610] Artigo 13.º da Proposta de RGPG.
[611] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., pp. 31 e 32.
[612] KOSTA, Eleni, *Consent in European ...* , op. cit., pp 385 e 386.

Nos termos do n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica, estão isentas da obtenção de consentimento as situações em que o testemunho de conexão tem como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, e aquelas em que a utilização do testemunho de conexão é estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado.

Apesar destas exceções previstas, quer na Diretiva 2002/58/CE, quer na 2009/136/CE, não encontramos nenhum considerando que no-las esclareça.

O Grupo do Artigo 29.º publicou, em junho de 2012, o importante Parecer 4/2012, sobre a isenção de consentimento para a utilização de testemunhos de conexão [613], que passamos a analisar, atendendo às diferentes utilizações dos testemunhos de conexão que vimos no Título 2.4. do Capítulo I.

Importa, antes do mais, realçar que as situações isentas da obrigação de obtenção de consentimento não põe em causa o direito de informação da pessoa em causa e correspondente obrigação de informar da entidade responsável.

O Grupo do Artigo 2.º adota uma abordagem aos conceitos de "testemunhos de origem" e "testemunhos de terceiros" diferente da que avançamos no Capítulo I deste Trabalho[614].

Embora, na prática, ambas as abordagens comummente se sobreponham, interessa agora percebermos a diferença entre elas.

Tivemos já a oportunidade de analisar[615] os testemunhos de origem e de terceiros, na perspetiva dos programas de navegação. Explicamos que

[613] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit..
[614] Título 2.3.2. do Capítulo I.
[615] Título 2.3.2. do Capítulo I.

são testemunhos de origem aqueles que são enviados pelo domínio (ou subdomínio) diretamente visitado pelo utilizador ou assinante, visível na barra de endereços do navegador. Por sua vez, seriam "testemunhos de terceiros" aqueles que são enviados por um domínio (ou subdomínio) diferente daquele que é visitado pelo utilizador e que aparece na barra de endereços do navegador.

Já no contexto da proteção de dados a nível europeu, a Diretiva 95/46/CE define o terceiro como "a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não a pessoa em causa, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão habilitadas a tratar dos dados". Assim, o Grupo do Artigo 29.º considera testemunhos de origem aqueles que são instalados pelo responsável pelo tratamento (ou um dos seus subcontratantes) que opere o *site web* visitado, que aparece na barra de endereços do programa de navegação, e testemunhos de terceiros os instalados por um responsável pelo tratamento diferente daquele que explora o *site web* visitado pelo utilizador.[616]

Atendendo às características técnicas, podemos considerar uma orientação genérica no sentido de que é mais provável que um testemunho de origem de sessão esteja isento da obrigação de obtenção de consentimento do que um testemunho de terceiros permanente.[617]

No entanto, para determinar no caso concreto se os testemunhos estão ou não isentos da obrigação de obter consentimento, é a finalidade do testemunho que se deve ter em conta. Mais do que as informações neles contidas ou do que as características técnicas, importa considerar as finalidades para que são utilizados.

Assim, atendendo à possibilidade da utilização de testemunhos polivalentes, para que se possa concluir pela isenção é necessário que todas as suas finalidades, sem exceção, estejam individualmente isentas.[618]

[616] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 5.
[617] Cf. GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 6.
[618] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 6 e 13.

9.1. Testemunhos que tenham como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas

Estão isentos da obrigação de obter o consentimento informado do utilizador ou assinante os testemunhos de conexão que têm como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas. É esta a primeira exceção prevista no artigo 5ª n.º 3 da Diretiva da Privacidade Eletrónica e a que o Grupo do Artigo 29.º se refere como "CRITÉRIO A"[619].

A versão original do artigo 5.º, n.º 3, era menos restrita e permitia a utilização de testemunhos de conexão com a "finalidade exclusiva de efetuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas".

O critério "única finalidade" é determinante na interpretação destas situações. De modo a aferir o preenchimento deste critério, é necessário verificar que sem o recurso ao testemunho de conexão a comunicação não seria possível.

Excluídas da isenção ficam todas aquelas situações em que o testemunho seja utilizado para "facilitar, acelerar ou regular a transmissão"[620].

O Grupo do Artigo 29.º esclarece que a expressão "transmissão de uma comunicação através de uma rede de comunicações eletrónicas" e, em especial, o termo "através de", se referem "a qualquer tipo de intercâmbio de dados que utiliza uma rede de comunicações eletrónicas (como definida na

[619] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 3.
[620] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 3.

Diretiva 2002/21/CE), incluindo eventualmente os dados de «nível de aplicação»"[621] [622].

Para nos ajudar a perceber o âmbito material desta exceção, o Grupo do Artigo 29.º descreve três situações em os testemunhos de conexão são considerados estritamente necessários para efetuar a comunicação através de uma rede de comunicações eletrónicas:

1) A capacidade para encaminhar as informações através da rede, nomeadamente identificando as extremidades da cadeia de comunicação;

2) A capacidade para trocar os dados na ordem prevista, nomeadamente através da numeração de pacotes de dados; e

3) A capacidade para detetar erros de transmissão ou perdas de dados.[623]

Assim, são testemunhos isentos da obrigação de obter consentimento com base neste critério, conforme esclarece o Grupo do Artigo 29.º, os testemunhos de sessão utilizados para equilibrar a carga[624], na medida em que tenham como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas.

9.2. Testemunhos estritamente necessários para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador

A segunda exceção prevista no artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica refere-se à isenção de consentimento informado de que gozam os testemunhos de conexão estritamente necessários para

[621] O Grupo do Artigo 29.º refere-se ao "nível de aplicação" sem esclarecer qual é o modelo de internet que tem por referência.
No Título 1.1.1. do Capítulo I adotamos o modelo de internet de cinco camadas e vimos que o protocolo *http*, onde encontramos o mecanismo dos testemunhos de conexão, pertence à camada de aplicação.
[622] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 3.
[623] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 3.
[624] Cf. GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.
Sobre os "testemunhos de sessão para equilibrar a carga" ver Título 2.4. do Capítulo I.

fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.

No mesmo sentido, o considerando 66 da Diretiva 2009/136/CE dispõe que "as exceções à obrigação de prestar informações e de permitir o direito de recusar deverão limitar-se às situações em que o armazenamento técnico ou o acesso é estritamente necessário para o objetivo legítimo de permitir a utilização de um serviço específico explicitamente solicitado pelo assinante ou utilizador".

Este "CRITÉRIO B"[625] exige que, cumulativamente, se verifique uma ação positiva do utilizador ou assinante – solicitação expressa de um serviço da sociedade da informação – e que sem o testemunho de conexão seja impossível prestar o serviço em causa. O Grupo do Artigo 29.º refere-se à necessidade de "um vínculo claro entre a necessidade estrita de um testemunho e a prestação de um serviço expressamente solicitado pelo utilizado".[626]

O critério da "estrita necessidade" deve ser aferido do ponto de vista do utilizador, e não do prestador de serviços. [627] [628]

De modo a aferir o alcance da expressão "serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador", o Grupo do Artigo 29.º propõe que, neste particular contexto "serviços da sociedade de informação deve ser entendido como um conjunto de várias funcionalidades, enquanto o alcance exato de tal serviço pode variar, portanto, de acordo com as funcionalidades solicitadas pelo utilizador (ou assinante)" [629]. É em relação a cada funcionalidade, como parte do serviço da sociedade da informação, que se devem verificar os pressupostos desta isenção: a funcionalidade tem de depender estritamente do testemunho

[625] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 3 e ss.
[626] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 4.
[627] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 13.
[628] O Information Commissioner's Office (ICO) considera, ainda, que o critério da "estrita necessidade" pode ser aferido em relação ao cumprimento de qualquer outra legislação a que se sujeite o prestador de serviços. UK INFORMATION COMISSIONER'S OFFICE (ICO), *Guidance on the* ... , cit., p. 7.
[629] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 4.

de conexão para ser disponibilizada e tem de ser expressamente solicitada pelo utilizador ou assinante.

Assim, os testemunhos de sessão de autenticação[630] encontram-se isentos da obrigação de obter consentimento, na medida em que a funcionalidade de autenticação é uma parte essencial do serviço da sociedade de informação expressamente solicitado pelo utilizador. [631]

O mesmo não acontece em relação aos testemunhos de autenticação permanentes. O Grupo do Artigo 29.º avança com uma solução para obtenção do consentimento que se operaria pela utilização de "uma caixa de comprovação (*checkbox*) [632] e uma simples nota informativa como, por exemplo, «recordar os meus dados (utiliza testemunhos)», junto do formulário de pedido" e que seria um meio adequado para obter o consentimento, tornando desnecessário aplicar uma isenção neste caso.[633]

Parece-nos infeliz a explicação avançada pelo Grupo do Artigo 29.º. Embora concordando que a isenção deva ser reconhecia apenas aos testemunhos de autenticação de sessão, consideramos que a diferença essencial reside no facto de a manutenção das informações entre sessões extravasar a funcionalidade estritamente necessária à prestação do serviço. A utilização de um testemunho permanente de autenticação não é estritamente necessário à prestação do serviço solicitado.

Os testemunhos de personalização da interface do utilizador [634], enquanto mecanismo necessário a uma funcionalidade expressamente

[630] Sobre os testemunhos de autenticação, ver Título 2.4. do Capítulo I.
[631] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 7 e 8.
[632] Uma caixa de comprovação ou *checkbox* é um elemento visual da interface do utilizador que lhe permite manifestar a sua opção perante uma escolha binária, selecionando, não selecionando (ou desseleccionando) um quadrado através de um visto ou uma cruz.
O consentimento prestado através da seleção de uma *checkbox* é considerado explícito, em conformidade com a opinião emitida pelo Grupo do Artigo 29.º para a Proteção de Dados no sentido de que "num ambiente on-line, o consentimento explícito pode ser dado através de assinaturas eletrónicas ou digitais. Contudo, pode também ser dado clicando num botão, dependendo do contexto, enviando mensagens de correio electrónico de confirmação, clicando em ícones, etc.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 29.
[633] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 7 e 8.
[634] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 9.
Sobre os "testemunhos de personalização da interface do utilizador" ver Título 2.4. do Capitulo I.

solicitada (o utilizador clica num botão de validação manifestando expressamente a intenção de que as informações lhe sejam apresentadas numa determinada língua durante a sessão de navegação), também estão isentos da obrigação de obter consentimento, a título deste CRITÉRIO B, de acordo com o Grupo do Artigo 29.º. [635]

Também neste caso, a isenção comtempla apenas os testemunhos de sessão. O Grupo do Artigo 29.º conclui que "acrescentar informações suplementares num local de destaque (por exemplo, «utiliza testemunhos» ao lado da bandeira) seriam dados suficientes para o consentimento válido tendo em vista recordar a preferência do utilizador durante um período mais longo, eliminando assim a necessidade de aplicar uma isenção neste caso" [636].

Mais uma vez consideramos a explicação avançada pelo Grupo do Artigo 29.º desadequada. Desde logo, pelos motivos que destacamos a propósito dos testemunhos de autenticação permanentes, os testemunhos de personalização da interface do utilizador permanentes na medida em que mantêm informações entre sessões extravasam a funcionalidade (e.g. de escolha da língua) estritamente necessária à prestação do serviço solicitado. Depois, porque não se verificando a isenção, as informações não seriam "suplementares" mas resultariam da própria regra vertida no artigo 5º n.º 3.

Os testemunhos de sessão alimentados pelo utilizador [637] também estão isentos da obrigação de obter consentimento, na medida em que pressupõe a prestação de um serviço solicitado pelo utilizador ou assinante. [638] É o caso típico dos "carrinhos de compras", em que ao utilizador ou assinante é atribuído um número aleatoriamente gerado que vai permitir agregar os produtos selecionados ao longo de várias páginas, até à compra final, ou dos testemunhos utilizados para manter o registo de dados

[635] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 9. Sobre os "testemunhos de personalização da interface do utilizador" ver Título 2.4. do Capitulo I.
[636] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 9. Sobre os "testemunhos de personalização da interface do utilizador", ver Título 2.4. do Capitulo I.
[637] Sobre os testemunhos alimentados pelo utilizador, ver Título 2.4 do Capítulo I.
[638] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 7.

fornecidos através do preenchimento de um formulário ao longo de várias páginas.

O Grupo do Artigo 29.º chama a atenção para o facto de estes testemunhos alimentados pelo utilizador deverem ser, em princípio, testemunhos de sessão e de origem, normalmente associados a um número aleatório e temporário (identificador de sessão), para que a sua utilização esteja isenta da obrigação de obtenção de consentimento.[639]

Os testemunhos alimentados pelo utilizador e os testemunhos de personalização do interface do utilizador, assim como todos os testemunhos isentos, pressupõem uma duração limitada às finalidades para que são utilizados. Porém, a propósito destas duas utilizações, o Grupo do Artigo 29.º refere-nos o critério relativo às "expectativas razoáveis do utilizador ou assinante médio".

O Grupo do Artigo 29.º esclarece este conceito de "as expectativas razoáveis do utilizador ou assinante médio" recorrendo-se do exemplo do "carrinho de compras". Admitindo que o utilizador ou assinante pode encerrar acidentalmente a sessão e ter uma expectativa razoável de recuperar o conteúdo do "carrinho de compras" regressando ao *site* em causa nos minutos seguintes, admite que o atributo "data de expiração" esteja definido para que o testemunho tenha uma longevidade superior à duração da sessão, nos casos particulares dos testemunhos alimentados pelo utilizador e os testemunhos de personalização do interface do utilizador.[640]

Tendo em conta que o testemunho de conexão pode ser legitimamente persistente por solicitação expressa do utilizador ou assinante que pretende que o serviço memorize certas informações entre sessões, é-nos difícil aceitar o critério respeitante às "expectativas razoáveis do utilizador ou assinante médio".

Atendendo aos interesses conflituantes – privacidade do utilizador ou assinante e expectativas razoáveis de obter a prestação de um serviço ou

[639] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 7.
[640] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 5, 7, 9 e 12.

aceder a uma funcionalidade específica – defendemos que, por defeito, não se deve admitir que o testemunho dure além da sessão para que foi gerado, salvo expressa solicitação do utilizador ou assinante.[641]

No que respeita aos testemunhos de segurança centrados no utilizador[642], o Grupo do Artigo 29.º esclarece que estão isentos, na medida em que tenham como exclusiva finalidade reforçar a segurança de um serviço expressamente solicitado pelo utilizador. Esta utilização compreende uma exceção ao indicador geral de que os testemunhos isentos devam estar definidos para terminar no final da sessão, já que a sua finalidade pressupõe que se mantenham por um período de tempo mais alargado.[643]

Na medida em que se limitem a informações estritamente necessárias à reprodução de conteúdos que façam parte de um serviço expressamente solicitado pelo utilizador, os testemunhos *flash*[644] estão isentos da obrigação de obtenção de consentimento, de acordo com este segundo critério em análise.[645]

Os testemunhos relativos a módulos de extensão (*plug-in*) para partilha de conteúdos sociais[646] de sessão estão isentos da obrigação de obter consentimento quando utilizados enquanto mecanismo estritamente necessário à funcionalidade expressamente solicitada por um utilizador "ligado" através do seu navegador a uma conta especial da rede social. [647]

Esta é a única exceção prevista para testemunhos de terceiros.[648]

---

[641] Por outro lado, vimos a propósito do funcionamento dos testemunhos de conexão os atributos relativos à longevidade dos mesmos (Título 2.2. do Capítulo I.). Por defeito, estes expiram assim que a sessão termina, independentemente do motivo que a fez cessar, e que apenas podem ser definidos atributos que indiquem ou a data em que deve expirar (*Expires Attribute*) ou o tempo restante até expirar (*Max-age Attribute)*. Assim, a menos que se definisse previamente uma duração máxima para a sessão e, em função desta, uma duração máxima para o testemunho que excederia em alguns minutos a primeira, não nos parece fácil implementar a solução desejada pelo Grupo do Artigo 29.º sem o recuso a um testemunho permanente (por mais curta que fosse a sua duração).
[642] Sobre os testemunhos de segurança centrados no utilizador, ver Título 2.4. do Capítulo I.
[643] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.
[644] Sobre os testemunhos *flash*, ver Título 2.4 do Capítulo I.
[645] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 8.
[646] Sobre os testemunhos relativos a módulos de extensão (*plug-in*) para partilha de conteúdos sociais, ver Título 2.4 do Capítulo I.
[647] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p.p. 9 e 10.
[648] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 9 e 10.

9.3. Utilizações não isentas da obrigação de obter consentimento

O Grupo do Artigo 29.º distingue três utilizações dos testemunhos de conexão não isentas da obrigação de obter consentimento[649].

Desde logo, o Grupo destaca os "testemunhos de extensão de redes sociais para seguimento". Trata-se de testemunhos relativos a módulos de extensão (*plug-in*) para partilha de conteúdos sociais que servem a finalidades de monitorização da atividade do utilizador em linha (*tracking cookies*)[650].

Facilmente se percebe que, atendendo à sua finalidade, estes testemunhos de conexão não preenchem os pressupostos de nenhuma das exceções previstas no artigo 5.º, n.º 3, e, por isso, a sua utilização legítima dependa da obtenção de consentimento prévio, concedido com base em informações claras e completas, em conformidade com a Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento.[651]

Não estão, igualmente, isentos da obrigação prevista na regra plasmada no artigo 5.º, n.º 3 da Diretiva da Privacidade Eletrónica, os testemunhos de conexão utilizados na publicidade comportamental[652]. O Grupo do Artigo 29.º esclarece que a exigência de consentimento "aplica-se naturalmente a todos os testemunhos de terceiros conexos utilizados na publicidade, incluindo os testemunhos para efeitos da limitação de frequência, historial financeiro e afiliação de publicidade, deteção da fraude do clique, investigação e análise de mercados, melhoria de produto e

[649] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 10 e ss.
[650] Ver Título 2.4 do Capítulo I.
[651] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 10 e 11.
[652] A propósito da utilização de testemunhos de conexão no contexto da publicidade comportamental, ver titulo 2.4. do Capítulo I.

depuração, pois nenhuma destas finalidades pode ser considerada relacionada com um serviço ou funcionalidade de um serviço da sociedade da informação expressamente solicitado pelo utilizador"[653].

Finalmente, em relação à utilização de testemunhos de conexão para finalidades de "analítica de origem"[654], o Grupo do Artigo 29.º entende que apesar de não estar isenta da obrigação de obter consentimento, nos termos do n.º 3 do artigo 5.º, não representa um risco para a privacidade quando se limite a "fins próprios de estatísticas agregadas e quando são utilizados por sítios Web que já fornecem informações claras sobre estes testemunhos, conformes com a sua política de proteção da vida privada, bem como garantias adequadas de proteção da privacidade", sendo que "tais garantias deveriam incluir mecanismos de fácil utilização para excluir qualquer recolha de dados e tornar os dados completamente anónimos, a fim de serem aplicáveis a outros dados identificáveis recolhidos, tais como os endereços I.P." [655]. Nesse sentido, recomenda a inserção de um terceiro critério de isenção, aquando de uma futura revisão do n.º 3 do artigo 5.º, para os testemunhos que tenham por finalidade estrita obter estatísticas agregadas e anónimas de origem.[656]

10. A prestação de informações e a obtenção do consentimento em linha

A utilização de testemunhos de conexão pressupõe, como temos vindo a analisar, por regra, que num primeiro momento sejam prestadas ao utilizador ou assinante informações claras e completas, com base nas quais se exige, e num segundo momento que este preste o seu consentimento. São estes dois passos, a observar antes da instalação de um testemunho,

[653] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 11.
[654] Título 2.4 do Capítulo I.
[655] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., pp. 11 e 12.
[656] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., 11 e 12.

que legitimam a sua utilização. Será assim sempre que, atendendo às suas finalidades, os testemunhos não preencham os requisitos de nenhuma das exceções previstas à obrigação de obtenção de consentimento.

O considerando 66 da Diretiva 2009/136/CE refere que "as formas de prestação de dar informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão simples quanto possível". [657]

Obedecendo à ordem das etapas descritas para a legitima utilização de um testemunho de conexão, comecemos por atender à problemática subjacente à forma de prestação de informações "claras e completas" em linha.

No entanto, esta questão não releva apenas para os testemunhos de conexão cuja utilização deva preencher os requisitos vertidos na rega do artigo 5.º, n.º 3, sendo igualmente importante para as utilizações situações isentas de obtenção de consentimento prévio, quando em causa esteja o tratamento de dados pessoais. O direito da pessoa em causa de ser informada sobre o tratamento, nos termos da Diretiva 95/45/CE mantém-se e, por isso, apesar de ser distinto o momento em que estas informações devem ser prestadas (antes da instalação do testemunho ou desde a instalação do testemunho), a verdade é que o responsável pelo tratamento não está escusado de as prestar.

[657] No mesmo sentido, o considerando 25, da Diretiva 2002/58/CE dispunha que "as modalidades para prestar as informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível".
Já tivemos oportunidade de ver, as versões inglesa e francesa da do considerando 66, da Diretiva 2009/136/CE não se referem ao métodos para obter consentimento mas apenas para prestar informações e proporcionar o direito de recusar.
Importa ter essas versões em atenção, também, de modo a perceber o sentido dos requisitos de convivialidade e simplicidade vertidos nas versões portuguesas. Apesar da alteração terminológica, estes devem ser percebidos no mesmo sentido.
Nas versões inglesas é adotado o termo "user friendly" enquanto requisito para os métodos de prestação de informações, em ambas as Diretivas: "The methods for giving information, (...) should be made as user-friendly as possible" (considerando 25, da Diretiva 2002/58/CE) e "The methods of providing information (...) should be as user-friendly as possible" (considerando 66, da Diretiva 2009/136/CE). A mesma estabilidade se verifica nas versões francesas onde termo "conviviales" se repete: "Les méthodes retenues pour communiquer des informations, offrir un droit de refus ou solliciter le consentement devraient être les plus conviviales possibles" (considerando 25, da Diretiva 2002/58/CE) e "Les méthodes retenues pour fournir des informations et offrir le droit de refus devraient être les plus conviviales possibles." (considerando 66, da Diretiva 2009/136/CE).

Por estar em causa um tratamento de dados considerado invisível é da maior relevância não só a prestação de informações completas à pessoa em causa mas a garantia de que essas informações chegam, realmente, ao conhecimento do seu destinatário, de modo a cumprirem os seus objetivos. A informação é essencial à livre prestação do consentimento, sendo condição essencial à sua validade.

O Grupo do Artigo 29.º a respeito da qualidade da informação refere que esta se deve sempre ter em consideração ser prestada em texto simples, sem uso de gíria, compreensível, evidente, de modo a ser suscetível de ser entendida por um utilizador médio.

No que respeita à acessibilidade e visibilidade da informação, o Grupo entende que esta deve ser prestada diretamente às pessoas, não sendo suficiente " que a informação esteja «disponível» num qualquer local". A informação deve, ainda, "ser claramente visível (tipo e tamanho das letras), proeminente e completa". [658]

A apresentação de um mínimo de informações diretamente no monitor, de forma interativa, facilmente visível acessível e compreensível[659] é a forma mais eficaz de prestar informações, de acordo com o Grupo do Artigo 29.º[660].

Entendemos que esse mínimo de informação deve focar as que resultam do artigo 10.º da Diretiva 95/46/CE[661], ainda que de forma não exaustiva[662], bem como informações relativas ao modo como pode expressar

[658] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 22.
[659] Para que possa ser considerada compreensível, é importante ter em atenção não só o idioma em que a informação é prestada mas, também, a linguagem que deve ser acessível ao utilizador comum.
[660] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 20.
[661] Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 20, nota de rodapé 40, que remete para a *Recomendação 2/2001 sobre determinados requisitos mínimos para a recolha de dados pessoais em linha na União* Europeia, segundo a qual Grupo entende que, quando através de um *site* se proceda ao tratamento de dados pessoais, devem ser exibidas diretamente no ecrã, antes da recolha, informações respeitantes à identidade do responsável pelo tratamento dos dados; às finalidade(s); ao carácter obrigatório ou facultativo da informação solicitada; aos destinatários ou categorias de destinatários dos dados recolhidos; à existência do direito de acesso e rectificação; à existência do direito a opor-se a qualquer comunicação dos dados a terceiros, para fins que não sejam a prestação do serviço solicitado, e indicações sobre o modo de o fazer; e informação relativa ao nível de segurança durante todas as fases de tratamento, incluindo a transmissão. GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Recomendação 2/2001 sobre determinados requisitos ...* , cit., pp. 7 e 8.
[662] Por exemplo, a informação mínima deve contemplar a eventual comunicação (transmissão) dos dados, podendo a identidade dos destinatários constar de uma página com informações mais completas para que aquela tenha uma hiperligação.

o seu consentimento em relação a todos, alguns ou a nenhum dos testemunhos, à forma de alterar as suas preferências no futuro e à eventual utilização de testemunhos de terceiros[663].

O Grupo entende que as informações prestadas com recurso aos termos de utilização e às declarações de privacidade[664] dos *sites* estão, na verdade, "escondidas" e, por conseguinte, não apresentam como os melhores métodos com vista a cumprir com o requisito em causa.

Atendendo a que, do ponto de vista técnico, podem existir muitas formas de prestar informações, a criatividade é encorajada. [665]

No caso dos testemunhos de terceiros, como vimos [666] , a responsabilidade pelo cumprimento da obrigação de prestar informações é partilhada entre o titular do *site* terceiro e o titular do *site* diretamente visitado.

A mera referência no *site* diretamente visitado à instalação de testemunhos de terceiros não é considerada suficiente. No caso da publicidade comportamental em linha, a colocação de ícones com ligações para informações adicionais junto dos anúncios publicados por terceiros na página do *site web* visitado pelo utilizador é um método que tem a aprovação do Grupo do Artigo 29.º.[667]

A coordenação entre o *site* diretamente visitado e o site terceiro deve atender à finalidade visada pela imposição da obrigação de prestar informações. O que releva é a capacidade das informações chegarem eficazmente, de modo claro e completo, ao utilizador para que este, com base nelas, possa tomar uma decisão válida.[668]

---

[663] Neste sentido, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on* … , cit. p. 3.

[664] Um estudo publicado em 2008, concluiu que os utilizadores da Internet dos Estados Unidos da Améria precisariam de aproximadamente 201 horas por ano para ler, uma vez, as políticas de privacidade dos *sites* que visitam. MCDONALD, Aleecia M. e CRANOR, Lorrie Faith, *The Cost of Reading Privacy Policies,* em "A Journal of Law and Policy for the Information Society", Privacy Year in Review issue, 2008, disponível em http://www.is-journal.org/, última consulta em 30 de agosto de 2013.

[665] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., pp. 20 e 21.

[666] Título 5. e Título 7.1. deste Capítulo III.

[667] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., pp. 20 e 21.

[668] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., p. 22.

A duplicação de informações enquanto tentativa de cumprir formalmente o requisito em análise não é, pois, a melhor estratégia e, nem sequer, aconselhável. Em termos práticos, o Grupo do Artigo 29.º sugere que o *site* diretamente visitado disponibilize um espaço no seu para os *sites* terceiros apresentarem as informações necessárias, já que é com aquele que o utilizador diretamente interage.[669]

Atendendo à possibilidade prática decorrente do considerando 25 da Diretiva 2002/58/CE que permite que o consentimento para instalar um testemunho abranja os acessos posteriores ao mesmo, importa que as entidades responsáveis encontrem formas de informar periodicamente as pessoas de que estão a ser monitorizadas, dando-lhes a possibilidade de revalidar ou revogar o consentimento prestado. O Grupo do Artigo 29.º considera essencial a prestação periódica de informações no caso concreto da publicidade comportamental, por entender ser "muito provável que, decorrido algum tempo, estas já não estejam cientes de que estão a ser monitorizadas e não se lembrem de que prestaram o seu consentimento"[670]. Entendemos que a necessidade da implementação desta prática se estende a todas as situações que envolvam testemunhos persistentes, independentemente de serem de origem ou de terceiros, pelo mesmo motivo.

No que respeita à obtenção do consentimento, o considerando 17 da Diretiva 2002/58/CE dispõe que "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 *site* na internet."[671]

[669] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 22.
[670] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 21.
[671] "The website operator is free to use different means for achieving consent as long as this consent can be deemed as valid under EU legislation.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on ...* , cit., p. 2.

A primeira alteração proposta pelo Parlamento Europeu[672] ao artigo 5.º, n.º 3 previa que a configuração do programa de navegação constituísse consentimento prévio, mas não vingou na versão final da Diretiva 2009/136/CE.

O considerando 66 da Diretiva dos Cidadãos acolheu esta intenção do Parlamento e dispõe a respeito da utilização dos testemunhos de conexão que "sempre que tecnicamente possível e eficaz, e em conformidade com as disposições aplicáveis da Diretiva 95/46/CE, o consentimento do utilizador relativamente ao tratamento de dados pode ser manifestado através do uso dos parâmetros adequados do programa de navegação ou de outra aplicação".

Para ser considerado válido o consentimento prestado através das definições do navegador, é necessário que estas permitam a eficaz manifestação de vontade prévia, informada, livre, específica e inequívoca, pela qual a pessoa em causa aceite que dados pessoais que lhe dizem respeito sejam objeto de tratamento, nos termos dos artigos 2.º, alínea h), e 7.º, alínea a),da Diretiva 95/46/CE.

No caso particular do consentimento para a utilização de testemunhos de conexão, o consentimento exigido tem, ainda, de cumprir com os requisitos do artigo 5.º, n.º 3, da Diretiva da Privacidade Eletrónica, e ser prévio ao tratamento – conforme confirmou o Grupo do Artigo 29.º.º[673] – e prestado com base em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento. [674]

---

[672] PARLAMENTO EUROPEU, I Resolução legislativa do Parlamento Europeu, de 24 de Setembro de 2008 , sobre uma proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n. °2006/2004 relativo à cooperação no domínio da defesa do consumidor (COM(2007)0698 — C6-0420/2007 — 2007/0248(COD)) - P6_TC1-COD(2007)0248 Posição do Parlamento Europeu aprovada em primeira leitura em 24 de setembro de 2008.

[673] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., op. citada, p. 14.

[674] O Grupo do Artigo 29.º, aquando das alterações à Diretiva 2002/58/CE pela Diretiva dos Cidadãos, manifestou o seu desacordo perante a admissibilidade da prestação de consentimento através das definições do navegador:
"Além do problema formal de inserir na diretiva linguagem específica e tecnológica, o Grupo de Trabalho preocupa-se com a erosão da definição de consentimento e com a consequente falta de transparência. A maior parte dos programas de navegação utilizam configurações pré-definidas que não permitem que os utilizadores sejam informados sobre eventuais tentativas de armazenamento ou de acesso ao seu equipamento terminal. Por isso, a

Conforme constatou o Grupo, a maioria dos navegadores atualmente disponíveis não cumpre com estes requisitos. [675]

Todos os navegadores permitem, por defeito, a instalação de testemunhos de conexão de origem e, a maioria permite, também por defeito, a instalação de testemunhos de terceiros.

Como vimos, é mais provável que os testemunhos de origem preencham algumas das exceções previstas ao requisito de consentimento prévio, no entanto muitos deles visam finalidades não isentas.

Apesar de a discussão em torno do consentimento através de definições do navegador tender a cingir-se às permissões concedidas à instalação de testemunhos de terceiros, por ser em relação a estes que

configuração pré-definida do programa de navegação deve respeitar a privacidade, não podendo ser um meio de obter o consentimento livre, específico e informado dos utilizadores, previsto na alínea h) do artigo 2.º, da Diretiva da proteção de dados. No que se refere aos testemunhos de conexão, o Grupo de Trabalho considera que os controladores destes testemunhos devem informar os utilizadores na sua declaração de privacidade e não podem contar com a configuração (pré-definida) do programa de navegação.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 1/2009 sobre as propostas ... , cit.* p. 10.

[675] O Grupo do Artigo 29.º referia que "dos quatro principais programas de navegação no mercado, apenas um está pré-configurado para bloquear testemunhos de terceiros a partir do momento em que é instalado. Os outros três estão pré-configurados para aceitar todos os testemunhos." GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., pp. 15 e 16.

Em causa estavam os navegadores Internet Explorer, Mozilla Firefox, Google Chrome e Safari. Em 2009, aquando da elaboração do parecer em causa, o cenário não era muito diferente do que se mantém ainda hoje. Apenas o navegador Safari bloqueava, por defeito, a utilização de testemunhos de terceiros, o que vinha a fazer desde 2003. ("Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from websites you visit.", em *Safari Features - Learn about the 250+ innovative features available in Safari*, Safari, disponível em http://www.apple.com/safari/features.html#security, ultima consulta em 20 de Julho de 2013). Desde 2007 que a versão do navegador Safari para iOS, o sistema operativo móvel da Apple, também bloqueia os testemunhos de terceiros, em conformidade com o princípio da privacidade desde a conceção.

Em 22 de fevereiro de 2013, a Mozilla lançou um "patch" para o Firefox, desenvolvido por Jonathan Mayer, um estudante da Universidade de Stanford de Direito e Ciências da Computação, que altera a predefinição relativa aos testemunhos de terceiros, bloqueando-os. Trata-se de uma nova abordagem que teve em conta a abordagem do Safari, a rápida expansão do recurso a este mecanismo por parte das empresas e a necessidade e maior controlo por parte dos utilizadores, estiveram na base desta decisão da Mozilla. (FOWLER, Alex, *Firefox getting smarter about third-party cookies*, Mozilla Privacy Blog Covering the latest developments in privacy & data safety, 25 de fevereiro de 2013, disponível em http://blog.mozilla.org/privacy/2013/02/25/firefox-getting-smarter-about-third-party-cookies/). A nova definição seria implementada na versão final do Firefox 22, lançada a 25 de junho de 2013. Esta intenção da Mozilla de bloquear testemunhos de terceiros foi, porém, largamente criticada pela indústria publicitária. Os argumentos principais prenderam-se com o facto de tal opção ser uma ameaça aos negócios de pequenas empresas e reduzir das o leque de utilizações possíveis deste mecanismo, nomeadamente destacando que estes podem servir para a proteção dos utilizadores e para análises diferentes das destinadas à publicidade. A Mozilla veio dizer que precisa de mais informação e de proceder a este "patch" (atualização de *software*) antes de o poder incluir por defeito nas versões finais. (RIBEIRO, John, *Mozilla postpones default blocking of third-party cookies in Firefox*, em "COMPUTER WORLD", 17 de maio de 2013, disponível em http://www.computerworld.com/s/article/9239325/Mozilla_postpones_default_blocking_of_third_party_cookies_in_Firefox, última consulta em 20 de julho de 2013)

"«I think, at the end of the day, privacy has never been a priority for the developers of Web browsers,» states Dr. Lorrie Faith Cranor. She's an associate professor of computer science at Carnegie Mellon University, but more importantly for this discussion, she's a contributing architect and former W3C working group chair for the Platform for Privacy Preferences (P3P). It may or may not be at the center of the latest privacy controversy surrounding Google's alleged thwarting of Web browser privacy policies, depending on whether you see things from Microsoft's perspective. Privacy may indeed be a priority for certain people within browser companies, Dr. Cranor continues. « But there is a disconnect between what's important to the browser development team, versus what's important to the privacy officer and the lawyers and other people within their companies.» FULTON, Scott M., *Expert: Microsoft's P3P "Ineffective," Google's Privacy Bypass Unhelpful*, ReadWrite, 24 de fevereiro de 2012, disponível em http://readwrite.com/2012/02/23/expert-microsofts-p3p-ineffect, última consulta em 30 de agosto de 2013.

encontramos abordagens práticas distintas, entendemos que o debate deve ser alargado também aos testemunhos de origem, aplicando-se-lhes o mesmo raciocínio, já que é possível definir o navegador para aceitar ou bloquear todos os testemunhos.

O facto de um utilizador instalar e/ou utilizar um navegador que, por defeito, aceite testemunhos não resulta numa clara e inequívoca manifestação da sua vontade. É irrelevante que o navegador informe o utilizador da possibilidade de alterar estas definições.

Como bem entendeu o Grupo do Artigo 29.º, a responsabilidade pela utilização de testemunhos de conexão "não pode ser limitada à responsabilidade de o utilizador adotar ou não determinadas precauções na configuração do seu navegador"[676].

Assim, rejeita-se a possibilidade do consentimento prestado através das definições de origem do navegador. A instalação e/ou utilização de um navegador, não pode ser interpretada como uma manifestação de vontade válida e eficaz.

Na medida em que a maioria dos navegadores aceita, por defeito, todo o tipo de testemunhos, o ato voluntário do utilizador alterar as definições não é prévio em relação aos testemunhos entretanto instalados.

O Grupo do Artigo 29.º chama, ainda, a atenção para fragilidade do consentimento prestado por esta via, dada a possibilidade dos *sites* contornarem as definições do navegador, nomeadamente recorrendo-se de testemunhos *flash*[677]. [678]

[676] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 1/2008 sobre questões de proteção ...* , cit., p. 22.

[677] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 16.

A propósito dos testemunhos *flash*, Título 2.4. do Capítulo I.

[678] Em Fevereiro de 2012, o investigador Jonathan Mayer da Universidade de Stanford, descobriu que a Google conjuntamente com a Vibrant Media, a Media Innovation Group e a PointRoll, contornavam as definições de privacidade do navegador Safari – que por defeito bloqueia testemunhos de conexão de terceiros – através da exploração de uma exceção que o navegador reservava para *sites* com que o utilizador diretamente interagisse, por exemplo, através do preenchimento de um formulário. Estas empresas instaram testemunhos de conexão que, à partida, estariam bloqueados, através de inserção de código que indicava ao navegador que o utilizador lhe estava a enviar um formulário – que na realidade nunca era apresentado ao utilizador –, simulando assim uma interação direta.

O caso foi publicado pelo Wall Street Journal, em 17 de fevereiro de 2012. ANGWIN, Júlia e VALENTINO-DEVRIES, Jennifer, *Google's iPhone Tracking - Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall Street Journal, 17 de fevereiro de 2012, disponível em

Mas de todos os requisitos relativos ao consentimento, aquele mais difícil de observar pela via das definições do navegador é o da especificidade. Como tivemos oportunidade de ver, o consentimento é específico em relação às finalidades do tratamento e deve circunscrever-se a um contexto limitado.

As configurações do programa de navegação permitem a aceitação ou o bloqueio de testemunhos em bloco e para o futuro, sem considerações acerca das finalidades específicas de cada testemunho nem das circunstâncias atuais relativas ao momento do processamento, mas apenas atendendo a características respeitantes à sua proveniência (de sites terceiros, ou de alguns sites específicos).

Além das dificuldades em preencher os requisitos relativos ao momento da prestação do consentimento e da especificidade do mesmo, também o requisito relativo às informações exigidas para a prestação do consentimento com vista à legítima utilização de testemunhos de conexão não é facilmente preenchido por esta via. E esta dificuldade relaciona-se intimamente com o suprarreferido requisito da especificidade. A aceitação ou bloqueio em bloco não terá por base informações claras e completas, nomeadamente sobre os objetivos do processamento, nos termos da Diretiva 95/46/CE; o utilizador não será informado sobre a identidade do responsável pelo tratamento nem sobre as finalidades do mesmo. Ou seja, apesar de na aceitação ou bloqueio em bloco o utilizador poder manifestar a sua intenção previamente ao tratamento, não decidirá com base em informações que permitam qualificar o seu consentimento como específico.

---

http://online.wsj.com/news/articles/SB10001424052970204880404577225380456599176#articleTabs=interactive, última consulta em 20 de agosto de 2013.
Em agosto de 2012, a Google foi condenada a pagar uma coima de 22,5 milhões de dólares nos Estados Unidos da América, pela Federal Trade Commission, por ter ultrapassado ilegalmente os mecanismos de proteção da privacidade dos utilizadores do navegador Safari.
Entretanto, em janeiro de 2013, um grupo de utilizadores do navegador Safari do Reino Unido processou a Google pela instalação ilegal de testemunhos. Em agosto de 2013, a empresa alegou que não tem de responder perante os tribunais britânicos e que as leis de privacidade deste país não se lhe aplicam. RIBEIRO, John, *Google says it is not answerable in the* UK *in Safari cookies privacy suit The company says plaintiffs should sue in California*, em "COMPUTER WORLD", 19 de agosto de 2013, disponível em http://www.computerworld.com.au/article/524099/google_says_it_answerable_uk_safari_cookies_privacy_suit/, última consulta em 20 de outubro de 2013.
Trata-se de um caso a acompanhar, cujo desfecho poderá ser muito interessante para avaliar a eficácia das leis de proteção de dados pessoais da União Europeia e, em particular, as questões relativas à sua aplicação territorial.

O Grupo do Artigo 29.º considera que apenas em condições muito restritas o consentimento prestado através da configuração do programa de navegação será válido. "Os programas de navegação ou outras aplicações que estão pré-configurados para rejeitar testemunhos de terceiros[679] e que exigem que a pessoa em causa pratique um ato voluntário para aceitar tanto a instalação como a transmissão contínua de informações contidas nos testemunhos por sítios Web específicos, podem prestar um consentimento válido e eficaz", sendo que para cumprir os requisitos da Diretiva 95/46/CE, os navegadores deveriam fornecer, em nome da entidade responsável, "as informações relevantes sobre as finalidades dos testemunhos e o seu posterior tratamento", já que "não é suficiente emitir avisos genéricos" sem referir expressamente a entidade responsável que instala o testemunho.[680]

Concordamos com a posição assumida pelo Grupo do Artigo 29.º. O consentimento prestado através de definições do navegador só pode ser válido quando os navegadores estejam configurados para rejeitar testemunhos, por defeito, e a pessoa em causa pratique um ato voluntário para aceitar tanto a sua instalação como o seu acesso futuro, com base em informações específicas, nomeadamente sobre as finalidades e entidade responsável pelo mesmo, cumprindo com os requisitos da Diretiva 95/46/CE.

No que respeita aos testemunhos de origem, destacamos desde logo uma dificuldade acrescida à validade do consentimento prestado através das configurações do navegador.

Vimos que logo o primeiro dos apertados requisitos para a validade do consentimento prestado por esta via passa pelo navegador estar configurado para rejeitar testemunhos. Ora, tendo em conta que o bloqueio de testemunhos de origem comporta consideráveis prejuízos à fluente navegação na *web*, tal configuração tenderia a ser alterada pelos utilizadores,

[679] Os navegadores que, por defeito, bloqueiem testemunhos de terceiros estão, ademais, em conformidade com a iniciativa *Do Not Track*, promovida pela Comissão Europeia, o W3C e a US Federal Trade Comission, que já tivemos oportunidade de referir no Título 2.5. do Capítulo I.

[680] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., pp. 16 e 17.

o que comprometeria a validade do consentimento prestado[681]. Os motivos subjacentes a esta alteração não decorreriam de uma opção livre, mas de uma tentativa de ultrapassar entraves técnicos. Assim, somos do entendimento de que tal ação não poderia ser considerada uma manifestação de vontade livre, e não conformaria os requisitos do artigo 5.º, n. 3 da Diretiva da Privacidade Eletrónica, pelo que os testemunhos de origem estariam excluídos da obtenção de válido consentimento por esta via.

O Grupo do Artigo 29.º sugere, ainda, a implementação de um "assistente de privacidade" com o objetivo de auxiliar o utilizador a configurar as definições de privacidade do navegador aquando da sua instalação ou atualização e de proporcionar ao utilizador uma maneira simples de aceitar ou recusar a instalação de testemunhos de conexão durante a utilização[682].

A Autoridade Europeia para a Proteção de Dados já tinha chamado a atenção para a necessidade prática de um "assistente de privacidade", enquanto medida complementar com vista à concretização do princípio da privacidade desde a conceção. Assim, atendendo a que "os programas de navegação na Internet permitem, normalmente, um certo nível de controlo sobre alguns tipos de cookies", que "por defeito, os programas de navegação estão definidos para aceitar todos os cookies, independentemente da finalidade destes últimos" e que "o utilizador só deixará de receber cookies se alterar as definições da sua aplicação de navegação para eles serem recusados", a Autoridade sugeriu que os programas de navegação devem bloquear, por defeito, testemunhos de terceiros e devem "exigir que os

[681] Já que "se [o consentimento] for utilizado incorretamente, o controlo da pessoa em causa torna-se ilusório e o consentimento constitui uma base inadequada para o tratamento dos dados"., GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 2.

[682] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 17.
Apesar da versão portuguesa do documento referir que "os programas de navegação deveriam lançar automaticamente um assistente de privacidade aquando da sua instalação ou atualização e prever um modo fácil de escolher a opção desejada durante a utilização", parece-nos que a intenção do Grupo do Artigo 29.º não terá sido a promoção de mecanismos capazes de prever intenções com base em padrões de comportamento passados mas sim proporcionar ao utilizador uma maneira simples de manifestar durante a utilização, como decorre das versões francesa ("les navigateurs devraient imposer aux utilisateurs de recourir à un "assistant de protection de la confidentialité" lorsqu'ils installent leur navigateur pour la première fois ou le mettent à jour, et prévoir une procédure simple leur permettant de choisir en cours d'utilisation") e inglesa ("the browsers should require users to go through a privacy wizard when they first install or update the browser and provide for an easy way of exercising choice during use").

utilizadores passassem por um assistente de privacidade quando instalam ou atualizam o programa de navegação".[683]

Como reforço ao consentimento prestado através das definições do navegador, o Grupo do Artigo 29.º destaca a implementação de mecanismos de auto-exclusão no contexto da publicidade comportamental, que permitem ao utilizador recusar que lhe seja direcionada publicidade.[684]

O Grupo quis destacar este exemplo positivo, levado a cabo por fornecedores de publicidade, que permitem aos utilizadores indicar, no seu *site*, que pretendem ver-se excluídos do tratamento processado para fins de publicidade comportamental[685]. No entanto, este tipo de mecanismo permitia o eficaz exercício do direito de oposição previsto na versão original do artigo 5.º, n.º 3, como regra para a utilização de testemunhos. Dado o atual regime, estes mecanismos não podem ser vistos como um meio de prestar consentimento válido, mas como um mero reforço das garantias do direito de controlo da pessoa em causa.

Para cumprir com os atuais requisitos, o Grupo sugere a alteração deste sistema de "auto exclusão" por um outro de "aceitação prévia". Assim, o *site* (terceiro) deve exibir uma mensagem em qualquer tipo de área de informação (incluindo a área do *site* visitado em que é apresentado o conteúdo do *site* terceiro) e oferecer ao utilizador as opções de aceitar a instalação e futuros acessos ao testemunho, recusar a instalação de qualquer testemunho ou aceitar um testemunho permanente que indique a recusa de certos testemunhos.

Esta terceira alternativa pode causar estranheza. O Grupo do Artigo 29.º emitiu esta sugestão no contexto da publicidade comportamental. Em causa estão, testemunhos permanentes de terceiros. No caso de o utilizador

---

[683] AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS, Parecer da Autoridade Europeia para a Proteção de Dados sobre a promoção da confiança na sociedade da informação através do reforço da proteção dos dados e da privacidade (2010/C 280/01), 18 de março de 2010.
A Autoridade Europeia para a Proteção de Dados foi criada em 2001 e tem por missão garantir que todas as instituições e órgãos da UE respeitam o direito à privacidade dos cidadãos quando processam os seus dados pessoais (sobre a Autoridade Europeia para a Proteção de Dados ver http://europa.eu/about-eu/institutions-bodies/edps/index_pt.htm).

[684] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental* ... , cit., p. 17.

[685] A propósito da utilização de testemunhos de conexão no contexto da publicidade comportamental, ver titulo 2.4. do Capítulo I.

optar por recusar a instalação de qualquer testemunho, sempre que se voltar a "cruzar" com um conteúdo com origem no mesmo *site* terceiro, uma vez que este não tem como reconhecer o utilizador e saber que aquele já manifestou a sua opção acerca da instalação dos seus testemunhos, confrontá-lo-á novamente com a necessidade desta escolha. Assim, o Grupo sugere que o utilizador possa, ao mesmo tempo, recusar testemunhos para fins de publicidade comportamental e, simultaneamente, aceitar um testemunho que permita recordar esta sua recusa. Este tipo de testemunho de recusa é compatível com o disposto no artigo 5.º, n.º 3, na medida em que a sua instalação é precedida do consentimento do utilizador.[686]

A Comissão Europeia tem participado nos trabalhos do W3C com vista à implementação da solução "*Do Not Track*".[687]

Apesar de soluções como esta serem bem-vindas enquanto mecanismos capazes de reforçar a privacidade dos utilizadores da *web*, na prática esta solução representa um meio do utilizador exercer o seu direito a recusar o tratamento[688] e não de prestar consentimento[689].[690]

Assim, "os mecanismos de aceitação prévia, que exigem que a pessoa em causa pratique um ato voluntário para manifestar o seu consentimento antes que o testemunho lhe seja enviado, são mais consentâneos com o artigo 5.º, n.º 3".[691]

No que respeita à possibilidade decorrente do considerando 25 da Diretiva 2002/58/CE de o consentimento prestado para a instalação de um testemunho legitimar os acessos posteriores ao mesmo, o Grupo do Artigo 29.º entendeu que após o utilizador ter consentido em receber determinado

[686] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 16/2011 sobre a recomendação ...* , cit., p. 12.
[687] A que já tivemos oportunidade de nos referir no Título 2.5. do Capítulo I.
[688] *Opt-out*.
[689] *Opt-in*.
[690] Neste sentido, KOSTA, Eleni, *Consent in European...* , op. cit., p. 316.
[691] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 18.

testemunho, a presença do testemunho no equipamento terminal do utilizador pode ser utilizada como um indicador desse consentimento.[692]

O Grupo propõe, no entanto, que o consentimento seja limitado temporalmente, sugerindo o prazo de um ano, findo o qual a entidade responsável deve obter novo consentimento, e destaca a necessidade de serem fornecidas informações claras sobre a possibilidade e a forma de revogar o consentimento prestado.[693]

Defendemos, no entanto, que não é só o consentimento que deve ser renovado mas o próprio testemunho.

Pode acontecer que o utilizador ou assinante nunca mais visite o *site* em questão, ou não o faça num largo período de tempo, pelo que entendemos que é o próprio testemunho de conexão, ainda que legitimamente instalado após a válida obtenção do consentimento da pessoa em causa, que não deve ter uma longevidade superior a um ano.

Um método considerado eficaz para a prestação de informações e para obtenção do consentimento em linha é o recurso a janelas instantâneas[694]. [695]

Além deste, o Grupo do Artigo 29.º destaca outras formas conviviais de obter o consentimento e esclarece, ainda, que para que se cumpram os requisitos do artigo 5º, n.º 3, não é necessário que o *site* forneça informações e obtenha o consentimento do utilizador separadamente para cada testemunho ou para cada finalidade de cada testemunho[696]. O que releva é que a informação seja fornecida de modo claro e completo e o consentimento seja válido por observância dos seus requisitos essenciais.

---

[692] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 16/2011 sobre a recomendação ...* , cit., p. 12.
[693] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p. 19.
[694] Uma janela instantânea ou *pop up window* é uma "janela que surge, sem a intervenção do utilizador e muito rapidamente, com propostas informativas (publicidade) ou relativas à situação de utilização (por exemplo, uma mensagem de erro ou de aviso)", de acordo com a definição que encontramos no Glossário *online* da Agência para a Sociedade do Conhecimento, IP, disponível em http://www.umic.pt/index.php?option=com_content&task=view&id=2965&Itemid=476, últma consulta em 30 de agosto de 2013.
As janela instantânea podem, ainda, ter a característica de bloquear a interação do utilizador com as restantes janelas, reclamando a sua ação.
[695] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 16/2011 sobre a recomendação ...* , cit., p. 10.
[696] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2012 sobre a isenção ...* , cit., p. 6.

As faixas de informação estáticas, colocadas na parte superior de um *site*, solicitando o consentimento do utilizador para a instalação de alguns testemunhos, com uma hiperligação para a respetiva declaração de privacidade que contenha informações mais detalhadas sobre as diferentes entidades responsáveis e sobre os objetivos do tratamento, são outro mecanismo de obtenção de consentimento em ambiente *web*.

A entidade responsável – o *site web* que instala e lê o testemunho – pode, ainda, optar pelo recurso a um ecrã inicial que forneça ao utilizador as informações legalmente exigidas e solicite o seu consentimento.

Além dos métodos que visam a obtenção de consentimento expresso, o Grupo do Artigo 29.º veio reconhecer que há formas válidas de obtenção de consentimento tácito no contexto da instalação de testemunhos de conexão[697]. O que realmente revela é que o utilizador manifeste a sua vontade através de um comportamento ativo, com base em informações claras e completas e consciente de que através dele está a consentir na utilização de testemunho(s) de conexão[698].

O ICO apesar de reconhecer que o consentimento expresso confere um grau de segurança maior e se revelar mais apropriado em determinadas circunstâncias já tinha admitido, como vimos[699], a validade do consentimento tácito no contexto da utilização de testemunhos de conexão. Em termos práticos sugeriu que este podia ser aferido, por exemplo, quando ao utilizador fossem apresentadas informações sobre a utilização de testemunhos e ele optasse por selecionar o botão que lhe permita continuar a navegação.[700]

[697] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on* ... , cit., p. 4.
[698] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on* ... , cit., pp. 4 e 5.
[699] Título 7.5. deste Capítulo III.
[700] UK INFORMATION COMISSIONER'S OFFICE (ICO), *Guidance on the* ... , cit., p. 9.

É, agora, claro que o Grupo do Artigo 29.º reconhece a validade do consentimento prestado através de qualquer comportamento ativo [701] do utilizador, aquando da prestação de informações, a partir do qual o titular do *site* possa concluir pelo consentimento inequívoco, específico e informado[702].

O atual regime não considera abordagens distintas ao modo de fornecer informações e obter o consentimento de acordo com a relação entre o utilizador e o *site web*, nomeadamente diferenciando os casos em que se trate de um utilizador registado ou de um visitante ocasional. Porém, na prática, os titulares dos *sites* têm formas privilegiadas de fornecer informações e obter o consentimento dos seus utilizadores registados. Os testemunhos instalados depois do utilizador se registar podem ser consentidos por este, ativamente, durante o próprio processo de registo.[703]

Aparentemente complicado, na prática o cumprimento com o n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica pode ser esquematizado da seguinte forma:

O artigo 6.º da Diretiva 95/46/CE, relativo à qualidade dos dados, apesar de só se aplicar quando as informações em causa configurem dados pessoais, deve orientar sempre o tratamento de informações através de testemunhos de conexão – sendo obrigatório, no entanto, quando as informações sejam dados pessoais.

[701] "For the purpose of this paper active behaviour means an action the user may take, typically one that is based on a traceable user-client request towards the website, such as clicking on a link, image or other content on the entry webpage, etc. The form of these types of user requests are such that the website operator can be confident that the user has actively requested to engage with the website and (assuming the user is fully informed) does therefore indeed consent to cookies and that the action is an active indicator of such consent. In any case it must be clearly presented to the user, which action will signify consent to cookies. It must be made sure, that the choice expressed with active behaviour is actually based on clear information that cookies will be set due to this action. (....) Absence of any behaviour cannot be regarded as valid consent." GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on ...* , cit., pp. 4 e 5.

[702] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on ...* , cit., p. 4.

[703] No sentido de que devem ser promovidas abordagens diferentes consoante a relação estabelecida entre o utilizador e o *site web*, KOSTA, Eleni, *Consent in European...* , op. cit., p. 322.

Assim, a entidade responsável deve optar por utilizar testemunhos de conexão que respeitem os princípios da finalidade, proporcionalidade e adequação[704].

A entidade responsável deve, então, elaborar uma lista dos testemunhos de conexão que utiliza, das informações que cada um recolhe, das finalidades que visam e da sua transferência ou não a terceiros.

De seguida, deve escrutinar quais os testemunhos que se encontram isentos da obrigação de obter consentimento, a coberto de alguma das exceções previstas na segunda parte do artigo 5.º, n.º 3 da Diretiva da Privacidade Eletrónica.

Finalmente, deve adotar um dos métodos sugeridos, nomeadamente janelas instantâneas ou faixas de informação estáticas, onde apresente um mínimo de informações[705], com hiperligação para uma página que contenha informações mais detalhadas, e completar esses métodos com mecanismos que permitam ao utilizador prestar o seu consentimento através de uma ação positiva ou um comportamento ativo[706] [707].

Uma vez obtido o consentimento para a instalação dos testemunhos, os acessos posteriores aos mesmos não dependem de novo consentimento.

Não nos parece, por outro lado, aconselhável que as entidades responsáveis se escusem de obter o consentimento da pessoa em causa confiando que o cumprimento dessa obrigação se verifique com recurso às definições do navegador, dada a incapacidade das soluções atualmente existentes no mercado garantirem o cumprimento dos requisitos respeitantes ao consentimento em relação a todos os testemunhos[708].

---

[704] Sobre os princípios relativos à qualidade dos dados, ver Título 2.2.1. do Capítulo II e CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., pp. 229 e ss..

[705] As informações que resultam do artigo 10.º, da Diretiva 95/46/CE, apresentadas de modo não exaustivo, bem como informações relativas ao modo como pode expressar o seu consentimento em relação a todos, alguns ou a nenhum dos testemunhos, à forma de alterar as suas preferências no futuro e à eventual utilização de testemunhos de terceiros.

[706] Como, por exemplo, através de uma caixa de confirmação (ou *checkbox*), através da qual o utilizador pode ativamente manifestar a sua opção perante uma escolha binária, selecionando, não selecionando (ou desseleccionando) um quadrado através de um visto ou uma cruz.

[707] A Proposta de RGPD prevê, no seu artigo 7.º, n.º 1, que "Incumbe ao responsável pelo tratamento o ónus de provar o consentimento do titular dos dados ao tratamento dos seus dados pessoais para finalidades específicas".

[708] No entanto, o consentimento prestado através das configurações do navegador pode, em determinas circunstâncias e em relação a determinados testemunhos, ser informado, livre, específico e prévio, pelo que, consequentemente, válido.

11. As consequências jurídicas do incumprimento

A Diretiva dos Cidadãos aditou à Diretiva da Privacidade Eletrónica um artigo relativo à "aplicação e execução"[709].

É da responsabilidade dos Estados-membros estabelecer as regras relativas às sanções aplicáveis às infrações de disposições nacionais aprovadas por força da presente diretiva, nomeadamente as de natureza penal, bem como tomar todas as medidas necessárias para garantir a sua aplicação. As sanções devem ser eficazes, proporcionadas e dissuasivas e podem ser aplicadas para abranger a duração de qualquer infração, mesmo que tenha posteriormente cessado.[710]

As autoridades nacionais devem dispor de poderes para ordenar a cessação das infrações às disposições nacionais aprovadas por força da presente diretiva[711], bem como de poderes e recursos de investigação.[712] [713]

Quando esteja em causa o tratamento de dados pessoais aplicam-se, ainda, as mediadas sancionatórias aprovadas pelos Estados-membros para assegurar a plena aplicação das disposições da Diretiva da Proteção de Dados.

"Where the website operator can be confident that the user has been fully informed and actively configured their browser or other application then, in the right circumstances, such a configuration, would signify an active behaviour and therefore be respected by the website operator.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Working Document 02/2013 providing guidance on ...* , cit., p. 4.

[709] Artigo 15.º-A, da Diretiva da Privacidade Eletrónica.

[710] Artigo 15.º-A, n.º 1, da Diretiva da Privacidade Eletrónica.

[711] Artigo 15.º-A, n.º 2, da Diretiva da Privacidade Eletrónica.

[712] Artigo 15.º-A, n.º 3, da Diretiva da Privacidade Eletrónica.

[713] No direito nacional português, o regime sancionatório foi introduzido no Capitulo III da Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto.
O Artigo 13.º-D da Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto define as competências da CNPD e do ICP-ANACOM.
O não cumprimento da obrigação de obtenção de consentimento prévio do utilizador ou assinante para a utilização de testemunhos de conexão é um contraordenação punível com a coima mínima de 1500€ e máxima de 25 000€, quando praticada por pessoas singulares, e com coima mínima de 5000€ e máxima de 5 000 000€, quando praticada por pessoas coletivas, nos termos do artigo 14.º, n.º 1, alínea e) da Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto.

Além das sanções administrativas e penais previstas nas legislações nacionais, as entidades responsáveis podem, igualmente, ter de indemnizar as pessoas em causa nos termos gerais de direito. [714]

12. Os Testemunhos de Conexão no futuro da regulação comunitária da privacidade

A Proposta de Regulamento Geral de Proteção de Dados contempla uma referência expressa aos testemunhos de conexão, no seu considerando 24:

> ***(24) Ao utilizarem os serviços em linha, as pessoas singulares podem ser associadas a identificadores em linha, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (Protocolo Internet) ou testemunhos de conexão (cookie). Estes identificadores podem deixar vestígios que, em combinação com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizadas para a definição de perfis[715] e a identificação das pessoas. Daí decorre que números de identificação, dados de localização, identificadores em linha ou outros elementos específicos não devem ser necessariamente considerados como dados pessoais em todas as circunstâncias.***

O último período do considerando citado suscitou críticas do Grupo do Artigo 29.º para a Proteção de Dados, que entendeu que "na fase atual, esta última frase, pode conduzir a uma interpretação demasiado restritiva da noção de dados pessoais no que se refere, por exemplo, aos endereços IP ou os testemunhos de conexão («cookies»)", recordando que os dados

[714] Entre nós, sobre o incumprimento das disposições sobre proteção de dados ver CASTRO, Catarina Sarmento e, *Direito da Informática ...* , op. cit., p. 303 a 321, e GUERRA, Amadeu, *A Lei de ...*, cit., pp. 166 a 169.
[715] *Profiling*.

pessoais “são os dados que se referem a uma pessoa identificável”, sendo que se referem “a uma pessoa se dizem respeito à identidade, características ou ao comportamento de uma pessoa ou se essas informações forem utilizadas para determinar ou influenciar a forma como essa pessoa é tratada ou avaliada” [716] .

O Grupo do Artigo 29.º já se tinha pronunciado no sentido de que “se um testemunho contiver um identificador único do utilizador, esse identificador constitui claramente um dado pessoal” [717].

O Grupo entende que, através da utilização de testemunhos de conexão, o responsável pelo tratamento terá ao seu dispor “«meios suscetíveis de serem razoavelmente utilizados» [718] para identificar as pessoas”[719] .[720]

A consagração dos princípios da privacidade desde a conceção e por defeito prevista na Proposta de RGPD[721] revela-se, também, importante no contexto da utilização de testemunhos de conexão.

A discussão em torno da introdução de definições de privacidade por defeito e, possivelmente, da introdução de um assistente de privacidade poderão vir a ser abordadas com outra incidência, atendendo a que a

[716] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 08/2012, que presta um contributo suplementar o debate sobre a reforma em matéria de proteção de dados* (WP 199), de 5 de outubro de 2012, p. 7, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_pt.pdf, última consulta em 30 de agosto de 2013.
[717] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 1/2008 sobre questões de proteção ...* , cit., p. 9.
[718] “(...) para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa” Nos termos do considerando 26, da Diretiva 95/46/CE.
Sobre a noção de “meios para identificar” ver GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007 sobre o conceito de …* , cit., pp. 15 e ss..
[719] ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 01/2012 sobre as propostas ...* , cit., p. 7.
[720] O Grupo do Artigo 29.º para a Proteção de Dados sugeriu a alteração do considerando 24 da Proposta de RGPD, propondo a seguinte redação: “Ao utilizarem os serviços em linha, as pessoas singulares podem ser associadas a identificadores em linha, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (Protocolo Internet) ou testemunhos de conexão (cookies). Estes identificadores podem deixar vestígios que, em combinação com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizadas para a definição de perfis e a identificação ou distinção das pessoas. Daí decorre que números de identificação, dados de localização, identificadores em linha ou outros elementos específicos devem, em regra, ser considerados [suprimir 'não devem ser necessariamente considerados como'] dados pessoais [suprimir 'em todas as circunstâncias'].” GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 01/2012 sobre as propostas ...* , cit., p. 7.
[721] Artigo 23.º da Proposta de RGPG

Proposta obriga o responsável pelo tratamento a aplicar mecanismos que garantam, por defeito, que apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento e, especialmente, que não são recolhidos ou conservados para além do mínimo necessário para essas finalidades, tanto em termos da quantidade de dados, como da duração da sua conservação. [722]

A Proposta de Regulamento Geral de Proteção de Dados prevê, ainda, a clarificação do conceito de consentimento no âmbito da proteção de dados pessoais, no sentido de que este deve sempre ser explícito[723] [724]. Se este requisito do consentimento, até aqui especial para o tratamento de categorias especiais de dados[725], passar a geral conforme consta do texto da proposta da Comissão, contribuirá para dirimir as divergências de interpretação existentes.

Os titulares dos *sites* devem, nesse sentido, promover a implementação de métodos que permitam aos utilizadores ou assinantes manifestar expressamente o seu consentimento[726]. Devem fazê-lo, ainda, atendendo à previsão do artigo 7.º, n.º 1, que faz recair sobre si o ónus de provar o consentimento da pessoa em causa.

O Grupo do Artigo 29.º, atendendo ao facto de "a noção de consentimento tem uma aceção genérica numa vasta gama de situações", nomeadamente na utilização de testemunhos de conexão[727], sublinhou que "as condições estabelecidas no artigo 4.º, ponto 8, e no artigo 7.º são

[722] Artigo 23.º, n.º 2, da Proposta de RGPG
[723] Artigo 4.º, n.º 8, da Proposta de RGPG.
[724] "O grupo de trabalho teve conhecimento de que foram levantadas dúvidas quanto à viabilidade do termo «explícita» relativamente ao consentimento, no contexto do artigo 4.º, ponto 8. O grupo de trabalho entende que a inclusão do termo «explícita» constitui uma clarificação importante do texto, necessária para permitir verdadeiramente que os titulares de dados exerçam os seus direitos, especialmente na Internet, onde se verificam demasiadas utilizações incorretas da autorização. Seria altamente indesejável que essa clarificação importante fosse suprimida do texto.", GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 08/2012, que presta um ...* , cit., p. 8.
[725] Artigo 8.º, n.º 2, alínea a), da Diretiva 95/46/CE.
[726] E.g. caixas de confirmação.
No sentido de que as caixas de confirmação são meios válidos para prestar consentimento expresso *on-line*, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição ...* , cit., p. 29.
[727] Em relação à utilização de testemunhos de conexão, o Grupo do Artigo 29.º destaca a flexibilidade reconhecida através do Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão. GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 08/2012, que presta um ...* , cit., p. 8.

adequadas para garantir uma utilização apropriada do consentimento em todas essas as situações"[728].

A consagração expressa do princípio da transparência, também se revela positivo no contexto da utilização de testemunhos de conexão na medida em que obriga os responsáveis pelo tratamento a adotar políticas de privacidade "transparentes, de fácil acesso e compreensão"[729].

Consideramos, porém, que reconhecimento expresso do direito do titular dos dados a não ser objeto de uma medida com base na definição de perfis, consagrado no artigo 20.º da Proposta de RGPD[730], é a principal novidade relacionada com a proteção das pessoas em relação à utilização de testemunhos de conexão.

Vimos[731] como os testemunhos de conexão podem ser utilizados para monitorizar a atividade dos utilizadores em linha e definir perfis com base no seu comportamento. O Grupo do Artigo 29.º dedicou especial atenção à utilização de testemunhos de conexão no contexto da publicidade comportamental[732].

[728] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 08/2012, que presta um ...* , cit., p. 8.

[729] Artigo 11.º da Proposta de RGPD, que se inspira na Resolução de Madrid sobre as normas internacionais em matéria de proteção de dados pessoais e da vida privada, cf. Exposição de Motivos, p. 9.

[730] Que "assenta, com as devidas alterações e garantias adicionais no artigo 15.º, n.º 1, da Diretiva 95/46/CE, relativo a decisões individuais automatizadas, e tem em consideração a recomendação do Conselho da Europa sobre a definição de perfis [CONSELHO DA EUROPA, *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*, Adotada pelo Comité de Ministros em 23 de novembro de 2010, disponível em https://wcd.coe.int/ViewDoc.jsp?id=1710949.]", COMISSÃO EUROPEIA, Proposta de Regulamento Geral de Proteção de Dados, Exposição de Motivos, p. 10.

[731] Título 2.4. do Capítulo I.

[732] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., e GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 16/2011 sobre a recomendação ...* , cit..

"A publicidade em linha é uma das principais fontes de rendimento de um vasto leque de serviços em linha e um fator importante para o crescimento e expansão da economia da Internet. Porém, na prática, a publicidade comportamental suscita questões importantes em matéria de proteção de dados e privacidade. Graças às tecnologias de base da Internet, os fornecedores de redes de publicidade podem monitorizar as pessoas em causa ao longo do tempo através de diversos sítios Web. As informações recolhidas sobre o comportamento de navegação destas pessoas são analisadas, tendo em vista a criação de perfis exaustivos sobre os seus interesses. Estes perfis podem ser utilizados para apresentar publicidade personalizada às pessoas em causa. Face à crescente utilização da publicidade comportamental baseada em testemunhos persistentes (*tracking cookies* ou *persistent cookies*) e dispositivos análogos e tendo em conta o seu elevado grau de intrusão na privacidade das pessoas, o Grupo do Artigo 29.º decidiu dedicar o presente parecer à análise da publicidade comportamental em linha em diversos sítios *Web*(...)" GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2010 sobre publicidade comportamental ...* , cit., p 4.

O n.º 1 do artigo 20.º estabelece a proibição geral de sujeitar uma qualquer pessoa singular "a uma medida que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, ou a analisar ou prever, em especial, a sua capacidade profissional, situação financeira, localização, saúde, preferências pessoais, fiabilidade ou comportamento"[733].

O considerando 21 refere-se "controlo do comportamento" e dispõe que "a fim de determinar se uma atividade de tratamento pode ser considerada de «controlo do comportamento» de titulares de dados, deve ser apurado se essas pessoas são seguidas na Internet através de técnicas de tratamento de dados que consistem em aplicar um «perfil» a uma pessoa singular, especialmente para adotar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e atitudes"[734].

O supracitado considerando 24 refere-se expressamente à definição de perfis e à identificação de pessoas com recurso a testemunhos de conexão.

O considerando 51 acrescenta que "cada titular de dados deve ter o direito de conhecer e ser informado, em especial, das finalidades a que se destinam os dados tratados, da duração da sua conservação, da identidade dos destinatários, da lógica subjacente ao tratamento dos dados e das suas consequências eventuais, pelo menos quando tiver por base a definição de perfis"[735].

[733] Artigo 20.º da Proposta de RGPD.
[734] Considerando 21 da Proposta de RGPD.
[735] No entanto, "este direito não deve prejudicar os direitos e as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o suporte lógico. Todavia, estas considerações não devem resultar na recusa total de prestação de informações ao titular dos dados", considerando 51 da Proposta de DGPD.

As medidas baseadas na definição de perfis através de tratamento automatizado, são permitidas em três situações excecionais [736], se "acompanhadas das garantias adequadas, incluindo uma informação específica do titular dos dados e o direito de obter a intervenção humana, e que tal medida não diga respeito a uma criança" [737]: quando aplicadas no âmbito da celebração ou da execução de um contrato [738], quando expressamente autorizadas por lei [739], ou mediante o consentimento da pessoa em causa[740].

O Grupo do Artigo 29.º para a Proteção de Dados chama a atenção para a expressão "que a afete de modo significativo", do artigo 20.º, n.º 1, que considera imprecisa[741], e destaca que "é conveniente especificar que esta abrange igualmente a aplicação, por exemplo, de ferramentas de análise Web que realizam um seguimento dos utilizadores para avaliar o seu comportamento, a criação de perfis de movimentos por aplicações móveis, ou a criação de perfis pessoais por redes sociais" [742].

O Grupo entende que deve ser adotada "uma abordagem que defina claramente as finalidades para as quais podem ser criados e utilizados perfis, nomeadamente obrigações específicas que incumbem aos responsáveis pelo tratamento de dados de informar os titulares dos dados, em especial sobre o seu direito de oposição à criação e utilização de perfis" [743].[744]

[736] Artigo 20.º, n.º 2 da Proposta de RGPD.
[737] Considerando 58 da Proposta de RGPD e Artigo 20.º, n.º 5, da Proposta de RGPG.
[738] Artigo 20.º, n.º 2, alínea a), da Proposta de RGPG.
[739] Artigo 20.º, n.º 2, alínea b), da Proposta de RGPG.
[740] Artigo 20.º, n.º 2, alínea c), da Proposta de RGPG.
[741] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 01/2012 sobre as propostas ...* , cit., p. 15.
GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 01/2012 sobre as propostas ...* , cit., p. 15.
[743] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 01/2012 sobre as propostas ...* , cit., p. 15.
[744] Desde a Proposta inicial da Comissão, de 25 de janeiro de 2005, e até ao momento em que escrevemos este título não tinham sido alcançados acordos significativos sobre alterações entretanto propostas àquele texto, pelo que optamos por nos limitar à Proposta da Comissão: Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), de 25 de janeiro de 2005, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf.
No entanto, a Comissão Parlamentar das Liberdades Cívicas, Justiça e Assuntos Internos votou a reforma legislativa no dia 21 de outubro de 2013. Alterações entretanto debatidas foram aprovadas. Com esta votação iniciaram-se as negociações entre os eurodeputados e os governos nacionais da União Europeia.

Conclusões

Este trabalho permitiu-nos perceber os testemunhos de conexão enquanto tecnologia antes de nos debruçarmos sobre a análise da sua regulamentação específica no quadro legislativo europeu da proteção de dados.

Assim, pudemos olhar com objetividade para este mecanismo e para todo o regime jurídico que disciplina a sua utilização.

Percebemos que estamos perante uma tecnologia que surgiu da necessidade de resolver uma limitação técnica e que, hoje, é utilizada para várias finalidades.

Percebemos como evoluíram o direito à privacidade e o direito à proteção de dados. Vimos que o desenvolvimento tecnológico teve um contributo inquestionável nesse percurso.

Vimos que a União Europeia aprovou, em 1995, regras específicas sobre o tratamento de dados pessoais.

Na medida em que fossem utilizados para o tratamento (e é assim quando recolhem ou permitem a associação de informações) de dados pessoais (que, como vimos, são todos aqueles que direta ou indiretamente permitam identificar uma pessoa, através da associação de conceitos ou conteúdos), os responsáveis pelo tratamento que recorressem a testemunhos de conexão tinham de respeitar as regras decorrentes da Diretiva de Proteção de Dados. Tinham de respeitar, além do mais, os princípios relativos à qualidade dos dados e basear o tratamento num dos fundamentos legitimantes.

No entanto, vimos que a utilização desta tecnologia se manteve sempre subtil, invisível aos olhos do utilizador médio, já que em momento algum reclamava a sua intervenção.

Na prática, as regras de proteção de dados pessoais não eram suficientes para proteger as pessoas contra a invasão da sua esfera privada que este mecanismo representava.

A Diretiva 2002/58/CE vem contemplar uma regra especial para a utilização de testemunhos de conexão. Esta Diretiva impunha que, para ser lícita, a utilização de testemunhos de conexão dependia de que fossem dadas ao utilizador ou assinante informações claras e completas e lhe fosse garantido o direito de recusar o tratamento. Apesar de estabelecer garantias para o armazenamento e acesso a informações no terminal do utilizador, a norma em causa representava um retrocesso em relação às garantias gerais quando em causa estivesse o tratamento de dados pessoais.

Esta norma foi alterada pela Diretiva dos Cidadãos, que veio estabelecer o consentimento do assinante ou utilizador como fundamento específico para o armazenamento ou acesso a informações já armazenadas no seu equipamento terminal; consentimento esse que deve ser prestado com base em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento.

Os princípios relativos à legitimidade previstos na Diretiva da Proteção de Dados são afastados e o consentimento assume-se como única base para a utilização de testemunhos de conexão. A norma mantém o seu largo âmbito de aplicação e impõe que o consentimento seja prestado sempre que esta tecnologia seja usada e não apenas quando se destine ao tratamento de dados pessoais, uma vez que qualquer utilização de testemunhos de conexão implica o armazenamento ou o aceso a informações previamente armazenadas no equipamento terminal do utilizador.

Neste estudo analisamos as questões mais relevantes que se levantam em relação à eficaz implementação prática do n.º 3 do artigo 5.º da Diretiva da Privacidade Eletrónica.

A intenção do Parlamento Europeu com a introdução do requisito respeitante ao consentimento para o armazenamento e acesso a informações

previamente armazenadas no equipamento terminal do utilizador foi promover a transparência da utilização dos testemunhos de conexão e dispositivos similares e garantir o direito à autodeterminação informativa.

Além das questões tecnológicas levantadas a propósito dos meios adequados para cumprir com estas regras, a fragmentada interpretação do próprio conceito de consentimento, ou mais precisamente, das formas de cumprir com os seus requisitos, têm-se revelado um desafio, desde o momento em que se pretendeu implementar este fundamento para legitimar o armazenamento e acesso a informações previamente armazenadas no terminal do utilizador. Registam-se diferenças, nomeadamente, a propósito do momento em que o consentimento deve ser obtido e do modo como este deve ser manifestado.

O consentimento assumiu-se como fundamento para a utilização destas tecnologias com o intuito de lhes dar visibilidade. No entanto, o recurso a este fundamento, enquanto princípio relativo à legitimidade que é, pode revelar-se um exagero. Passa-se da consciencialização do problema, associado ao desconhecimento dos utilizadores a respeito destes mecanismos, para a assunção de que o seu consentimento será suficiente para, sem mais, legitimar a sua utilização.

O consentimento deve ser utilizado de modo a conferir à pessoa em causa controlo sobre o tratamento dos seus dados. Se utilizado incorretamente, o consentimento não pode constituir um fundamento legitimante do tratamento, já que o controlo dado à pessoa em causa se torna meramente ilusório.

Além disso, a proteção das pessoas passa pela imposição de obrigações concretas à entidade responsável. Quando em causa não esteja o tratamento de dados pessoais, vimos que a entidade responsável não se encontra obrigada a mais do que à obtenção do consentimento e à prestação de informações.

A falta de clarificação relativa às situações isentas da obrigação de obtenção de consentimento é outro desafio que se coloca à implementação destas regras.

É de louvar a iniciativa do Grupo de Trabalho do Artigo 29.º a este propósito, apesar de discordamos de algumas opiniões no que respeita à conformação de utilizações isentas da obtenção de consentimento.

Constatamos que, afinal, são menos as finalidades não isentas do que as excluídas da obrigação de obtenção de consentimento.

Vimos que para determinar no caso concreto se os testemunhos estão ou não isentos da obrigação de obter consentimento, é a finalidade do testemunho que se deve ter em conta. Mais do que as informações neles contidas ou do que as características técnicas, importa considerar as finalidades para que são utilizados.

As características técnicas dos testemunhos de conexão, que estabeleçam parâmetros desnecessários ou excessivos à prossecução da finalidade concreta, podem, ainda, justificar a sua não isenção. Esta questão poderia ser mais facilmente precavida pela aplicabilidade direta dos princípios relativos à qualidade dos dados à utilização de testemunhos de conexão.

De todo o modo, sempre que o testemunho em causa seja considerado dado pessoal, o consentimento ainda que prestado não exonera o responsável pelo tratamento da observância estrita dos princípios relativos à qualidade dos dados, pelo que os princípios da finalidade, adequação e proporcionalidade sempre tornariam ilícita a utilização de um testemunho que não os respeitasse.

Louva-se a iniciativa do legislador europeu no sentido de contribuir para a transparência de uma tecnologia tendencialmente invisível aos utilizadores.

A atual abordagem legislativa que regula indiferenciadamente os testemunhos de conexão não nos parece a melhor. Da mesma forma que, no atual regime, as finalidades servem à estipulação dos regimes excecionais,

defendemos que é através da consideração destas que deve ser estruturado todo o regime especial aplicável aos testemunhos de conexão.

Assim, a utilização desta tecnologia deve ser disciplinada e sujeita a regras estritas em relação às finalidades visadas, em cada utilização concreta.

Parece-nos, pois, feliz a previsão relativa à utilização dos testemunhos de conexão com finalidade de definir perfis com base no comportamento, na Proposta de Regulamento Geral de Proteção de Dados.

No entanto, uma aplicação de todas as normas relativas à proteção de dados a qualquer utilização dos testemunhos de conexão, descontextualizada de qualquer finalidade, no Regulamento Geral de Proteção de Dados, parece-nos desproporcional.

Bibliografia

ANDRADE, Francisco, *Da contratação eletrónica – Em particular da contratação inter-sistémica inteligente*, Universidade do Minho, 2008

AUTORES VÁRIOS, Lei *do Comércio Electrónico Anotada*, Ministério da Justiça, Coimbra Editora, 2005

ANGWIN, Júlia e VALENTINO-DEVRIES, Jennifer, *Google's iPhone Tracking - Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, em "Wall Street Journal", 17 de fevereiro de 2012, disponível em http://online.wsj.com/news/articles/SB10001424052970204880404577225380456599176#articleTabs=interactive

BARTH, A., *HTTP State Management Mechanism*, RFC 6265, The Internet Engineering Task Force (IETF), abril de 2011, disponível em http://tools.ietf.org/html/rfc6265

BOTTMANN, Denise e BRUCHARD, Dorothée de, *História da Vida Privada*, Da Primeira Guerra a nossos dias, Editora Schwarcz, Lda., São Paulo, 2009, (Uma tradução para português da obra PROST, Antoine e VINCENT, Gérard, *Histoire de la vie privée*, sob a direção de Philippe Ariès e Georges Duby, Editions du Seuil, volume 5)

BRAIN, Marchall, *How Internet Cookies Work*, HowStuffWorks, disponível em http://www.howstuffworks.com/cookie.htm

CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, Relatório 2000, Parte II – Orientações da CNPD, 2000, disponível em http://www.cnpd.pt/bin/relatorios/anos/relat00.htm

CORRY, Bil Corry e STEINGRUEBL, Andy, *Where is the Comprehensive Online Privacy Framework?*, Position Paper for W3C Workshop on Web Tracking and User Privacy, Princeton, NJ, abril de 2011

CRANOR, Lorrie, HOGBEN, Giles, LANGHEINRICH, Marc, MARCHIORI, Massimo, PRESLER-MARSHALL, Martin, REAGLE, Joseph e SCHUNTER, Maltthias, *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*, W3C Working Group Note 13, novembro, 2006, disponível em http://www.w3.org/TR/P3P11/

CRANOR, Lorrie, LANGHEINRICH, Marc, MARCHIORI, Massimo, PRESLER-MARSHALL, Martin e REAGLE, Joseph, *The Platform for*

Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation, 16 April 2002 http://www.w3.org/TR/P3P/

FIELDING, R. [et al], *Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616, The Internet Engineering Task Force (IETF), junho, 1999, disponível em http://www.ietf.org/rfc/rfc2616.txt

FOWLER, Alex, *Firefox getting smarter about third-party cookies*, Mozilla Privacy Blog Covering the latest developments in privacy & data safety, 25 de fevereiro de 2013, disponível em http://blog.mozilla.org/privacy/2013/02/25/firefox-getting-smarter-about-third-party-cookies/

FULTON, Scott M., *Expert: Microsoft's P3P "Ineffective," Google's Privacy Bypass Unhelpful*, ReadWrite, 24 de fevereiro de 2012, em http://readwrite.com/2012/02/23/expert-microsofts-p3p-ineffect

GLENN, Ricard A., *The right to privacy: rights and liberties under the law*, ABC-Clio, Inc. Santa Bárbara, Califórnia, 2003

GUERRA, Amadeu, *A Lei da Proteção de Dados Pessoais*, em "Direito da Sociedade da Informação", Volume II, Coimbra Editora, fevereiro de 2001

GUTWIRTH, Serge, DE HERT, Paul, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitucionalization in Action*, em "Reinventing Data Protection?", Springer, 2009

HEMPHILL, Thomas A., *DoubleClick and Consumer Online Privacy: An E-Commerce Lesson Learned*, em *Business and Society Review,* Volume 105, Issue 3, pp 361 a 372, 2000.

HERT, Paul De, GUTWIRTH, Serge, MOSCIBRODA, Anna, WRIGHT, e GONZALEZ-FUSTER, Gloria, *Legal Safeguards for Privacy and Data Protection in Ambient Intelligence*, From the SelectedWorks of Serge Gutwirth, outubro 2008, disponível em http://works.bepress.com/serge_gutwirth/4/

HUSTINX, Peter, *EU Data Protection Law - Current State and Future Perspectives*, em "Ethical Dimensions of Data Protection and Privacy" Centre for Ethics, University of Tartu / Data Protection Inspectorate Tallinn, Estónia, 9 de janeiro de 2013, disponível em https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2013/13-01-09_Speech_Tallinn_EN.pdf

JACOBS, Francis, *SEMINARS ON QUALITY OF LEGISLATION How to interpret legislation which is equally authentic in twenty languages - Summary report*, Comissão Europeia, Lecture by Advocate General,

Bruxelas, 20 de outubro de 2003, disponível em http://ec.europa.eu/dgs/legal_service/seminars/agjacobs_summary.pdf

JAYE, Dan, *HTTP State Management Proposal foi Certified Cookies*, 30 de março de 1997, disponível em http://lists.w3.org/Archives/Public/ietf-http-wg-old/1997JanApr/0742.html

KOSTA, Eleni, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, Países Baixos, 2013

KOSTA, Eleni, DUMORTIER, Jos, GRAUX, Hans, TIRTEA, Rodica and IKONOMOU, Demosthenes, *Study on data collection and storage in the EU*, ENISA – European Network and Information Security Agency, 23 de fevereiro de 2012, disponível em http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection

KOSTA, Eleni, *Handling cookies within the european union: making the cookies crumble?*, em "VIII Congreso Internet, Derecho y Política 2012 Retos y oportunidades del entretenimiento en línea", Barcelona, 2012

KRISTOL, D. e MONTULLI, L., *HTTP State Management Mechanism*, RFC 2109, The Internet Engineering Task Force (IETF), fevereiro de 1997, disponível em http://www.ietf.org/rfc/rfc2109.txt

KRISTOL, D. e MONTULLI, L., *HTTP State Management Mechanism*, RFC 2965, The Internet Engineering Task Force (IETF), outubro de 2000, disponível em http://www.ietf.org/rfc/rfc2965.txt

KRISTOL, David M., *HTTP Cookies: Standards, privacy, and politics*, em "ACM Transactions on Internet Technology", Vol. 1, Issue 2, novembro de 2001, disponível em http://dl.acm.org/citation.cfm?id=502153&dl=ACM&coll=DL&CFID=286587961&CFTOKEN=78841520

KRISTOL, David M., *Proposed HTTP State-Info Mechanism*, HTTP Working Group, The Internet Engineering Task Force (IETF), 5 de agosto de 1995, 3. STATE AND SESSIONS, disponível em http://tools.ietf.org/html/draft-kristol-http-state-info-00

KUROSE, James F. e ROSS, Keith W., *Computer networking a top-down approach,* Pearson Education, Inc., 6ª Edição, 2012

MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*, 2ª Edição Refundida e Atualizada, Almedina, Coimbra, 2006

MAZZEO, Luzia Maria (coordenadora) *Evolução da Internet no Brasil e no Mundo*, Ministério da Ciência e Tecnologia Secretaria de Política de Informática e Automação, Brasil, abril, 2002

MCDONALD, Aleecia M. e CRANOR, Lorrie Faith, *The Cost of Reading Privacy Policies,* em "A Journal of Law and Policy for the Information Society", Privacy Year in Review issue, 2008, disponível em http://www.is-journal.org/

MENEZES LEITÃO, Luís Manuel Teles de, *Os Testemunhos de Conexão (Cookies)*, Homenagem da Faculdade de Direito de Lisboa ao Professor Doutor Inocêncio Galvão Telles, 90 Anos, Almedina, 2007

MONTULLI, Lou e GIANNANDREA, John, *Persistent Client State - HTTP Cookies*, Netscape Communications Corporation, 1994.

MOORE, K. E FREED, N., *Use of HTTP State Management, RFC 2964*, The Internet Engineering Task Force (IETF), de outubro de 2000, disponível em https://tools.ietf.org/html/rfc2964

MOREIRA, Teresa Alexandra Coelho, *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo eletrônico do empregador*, Almedina, 2010

RAGGETT, Dave, HORS, Arnaud Le e JACOBS, Ian Jacobs, *HTML 4.01 Specification*, W3C Recommendation, 24 December 1999, disponível em http://www.w3.org/TR/html401/

RIBEIRO, John, *Google says it is not answerable in the* UK *in Safari cookies privacy suit The company says plaintiffs should sue in California*, em "COMPUTER WORLD", 19 de agosto de 2013, disponível em http://www.computerworld.com.au/article/524099/google_says_it_answerable_uk_safari_cookies_privacy_suit/

RIBEIRO, John, *Mozilla postpones default blocking of third-party cookies in Firefox*, em "COMPUTER WORLD", 17 de maio de 2013, disponível em http://www.computerworld.com/s/article/9239325/Mozilla_postpones_default_blocking_of_third_party_cookies_in_Firefox

SCHWARZ, John *Giving the Web a Memory Cost Its Users Privacy*, in "The New York Times", 4 de setembro de 2001, disponível em http://www.nytimes.com/2001/09/04/technology/04COOK.html

SHAH, Rajiv C. E KESAN, Jay P., *Deconstructing Code,* Illinois Public Law and Legal Theory Research Papers Series, Research Paper No. 04-22, 29 de setembro, 2004.

SILVEIRA, Luís Novais Lingnau da, *O Direito à Proteção de Dados Pessoais (Tentativa de caracterização)*, em "Sociedade da Informação - O Percurso Português" - Parte I, APDSI, 2007, disponível http://www.apdsi.pt/index.php/news/545/82/Livro-Sociedade-da-Informacao---O-Percurso-Portugues-Parte-I

STALLINGS, William, *Data and Computer Communications*, 8ª edição, Pearson Education, Inc., 2007

TENE, Omer Tene e WOLF Christopher Wolf, White Paper - *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation*, The Future of Privacy Forum, Washington, DC, 2013, disponível em http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf

UK INFORMATION COMISSIONER'S OFFICE (ICO), Guidance on the rules on use of cookies and similar technologies, VV.3, maio de 2012, disponível em http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookiespp

VASCONCELOS, Pedro Pais de, *Proteção de Dados Pessoais e Direito à Privacidade*, em "Direito da Sociedade da Informação", Volume I, Coimbra Editora, outubro 1999

WARREN, Samuel e BRANDEIS, Louis, *The right to privacy*, em "Harvard Law Review", Vol. IV, n.º 5, 15 de dezembro de 1890, disponível em http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

WHALEN, David, *The Unofficial Cookie Faq*, Cookie Central, em http://www.cookiecentral.com/faq/

ZALEWSKI, Michael, *HTTP cookies, or how not to design protocols*, em "lcamtuf's blog", 28 de outubro de 2010, disponível em *http://lcamtuf.blogspot.pt/2010/10/http-cookies-or-how-not-to-design.html*

ZINS, Chaim, *Conceptual Approaches for Defining Data, Information, and Knowledge*, Journal of the American Society for Information science and Technology, 15 de fevereiro, 2007, disponível em http://www.success.co.il/is/zins_definitions_dik.pdf

Commission decisions on the adequacy of the protection of personal data in third countries, Comissão Europeia, disponível em http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

Commission proposes a comprehensive reform of the data protection rules, Comissão Europeia, em http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Cookie Laws Across Europe, em Cookipédia, disponível em http://cookiepedia.co.uk/cookie-laws-across-europe

Em que medida irá a reforma da proteção de dados reforçar os direitos dos cidadãos?, Comissão Europeia, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_pt.pdf.

Em que medida irá a reforma da UE adaptar as regras de proteção de dados aos novos progressos tecnológicos?, Comissão Europeia, em http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_pt.pdf

Glossário online, Agência para a sociedade do conhecimento, IP, disponível em http://www.umic.pt/index.php?option=com_content&task=view&id=2965&Itemid=476

How the EU has implemented the new law on cookies, updated, 8 de outubro de 2012, DLA PIPER, disponível em http://www.dlapiper.com/files/Publication/c12bf543-f878-420b-b05d-90a25022df07/Presentation/PublicationAttachment/8384fccd-731f-4c7b-ac70-95ca52e0fb68/EU_cookies_update_October_2012.pdf

HTML 4.01 Specification, W3C Recommendation, 24 December 1999, disponível em http://www.w3.org/TR/html401/

HTTP State Management Mechanism (httpstate), disponível em http://datatracker.ietf.org/wg/httpstate/charter/

Platform for Privacy Preferences (P3P) Project - Enabling smarter Privacy Tools for the Web, The World Wide Web Consortium, disponível em http://www.w3.org/P3P/

Porque precisamos de uma reforma da proteção de dados na UE?, Comissão Europeia, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_pt.pdf

Safari Features - Learn about the 250+ innovative features available in Safari, disponível, em http://www.apple.com/safari/features.html#security

Sir Tim Berners-Lee - Web Inventor and Founding Director of the World Wide Web Foundation, World Wide Web Foundation, disponível em http://www.webfoundation.org/about/sir-tim-berners-lee/

Statement Concerning CERN W3 Software Release into Public Domain, European Organization Nuclear Research, disponível em http://tenyears-www.web.cern.ch/tenyears-www/Declaration/Page1.html e em http://tenyears-www.web.cern.ch/tenyears-www/Declaration/Page2.html

The Free On-line Dictionary of Computing, disponível em http://foldoc.org/magic+cookie

We are the web, em "Google take action", disponível em https://www.google.com/intl/en/takeaction/we-are-the-web/

UNIÃO EUROPEIA

Comissão Europeia

COMISSÃO DAS COMUNIDADES EUROPEIAS, *Recomendação da Comissão relativa a uma convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal*, (81/679/CEE), Jornal Oficial nº L 246 de 29/08/1981 p. 0031 – 0031, Edição especial portuguesa: Capítulo 16 Fascículo 1 p. 0077, de 29 de Julho de 1981, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31981H0679:PT:HTML

COMISSÃO EUROPEIA, *Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões, de 10 de novembro de 1999 - Para um novo quadro das infraestruturas das comunicações eletrónicas e serviços conexos* - Análise das comunicações - 1999 [COM(1999) 539 final, 10 de novembro de 1999 - Não publicado no Jornal Oficial], disponível em http://europa.eu/legislation_summaries/internal_market/single_market_services/l24216_pt.htm

COMISSÃO DAS COMUNIDADES EUROPEIAS, *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas*, COM(2000) 385 final – 2000/0189(COD), Bruxelas, 12 de julho de 2000, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0385:FIN:PT:PDF

COMISSÃO DAS COMUNIDADES EUROPEIAS, *Proposta de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor*, {SEC(2007) 1472} {SEC(2007) 1473}, COM(2007) 698 final 2007/0248 (COD), Bruxelas, 13 de novembro de 2007, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0698:FIN:pt:PDF

COMISSÃO DAS COMUNIDADES EUROPEIAS, *Proposta alterada de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor*, COM(2008)723 final 2007/0248 (COD), Bruxelas, 6 de novembro de 2008, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0723:FIN:pt:PDF

COMISSÃO DAS COMUNIDADES EUROPEIAS, *Parecer da Comissão nos termos do artigo 251.º, n.º 2, terceiro parágrafo, alínea c), do Tratado CE, sobre as alterações do Parlamento Europeu à posição comum do Conselho respeitante à proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor QUE ALTERA A PROPOSTA DA COMISSÃO nos termos do n° 2 do artigo 250° do Tratado CE*, COM(2009) 421 final 2007/0248 (COD), Bruxelas, 29 de julho de 2009, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0421:FIN:PT:PDF

COMMUNICATIONS COMMITTEE (EUROPEAN COMMISSION Information Society and Media Directorate-General Electronic Communications Policy Implementation of Regulatory Framework), *Working Document Implementation of the revised Framework – Article 5(3) of the ePrivacy Directive*, COCOM10-34, Bruxelas, 20 de outubro de 2010, disponível

em http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-35-guidance-implementation-telecoms-rules-privacy

COMISSÃO EUROPEIA, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Proteção da privacidade num mundo interligado Um quadro europeu de proteção de dados para o século XXI*, /* COM/2012/09 final */, de 25 de janeiro de 2012, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:PT:HTML

COMISSÃO EUROPEIA, *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados*, COM/2012/010 final - 2012/0010 (COD), de 25 de janeiro de 2012, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:PT:HTML

COMISSÃO EUROPEIA, *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados)*, COM(2012) 11 final 2012/0011 (COD), de 25 de janeiro de 2012, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf

COMISSÃO EUROPEIA, *MEMO/13/923*, de 22 de outubro de 2013, disponível em http://europa.eu/rapid/press-release_MEMO-13-923_en.htm

Conselho da União Europeia

CONSELHO DA UNIÃO EUROPEIA, *Adenda ao Projeto de Ata, 2970.ª* reunião do Conselho da União Europeia (Assuntos Gerias e Relações Externas), realizada no Luxemburgo, em 26 de outubro de 2009, (OR. fr) 14985/09 ADD 1 PV/CONS 55, Bruxelas, 17 de novembro de 2009

CONSELHO DA UNIÃO EUROPEIA, *Adenda à nota Ponto "I/A" Proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, a Diretiva 2002/19/CE relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos e a Diretiva 2002/20/CE relativa à autorização de redes e*

serviços de comunicações eletrónicas (AL + D) (terceira leitura), Declarações 15864/09 ADD 1 REV 1 Bruxelas, de 18 de novembro de 2009

Parlamento Europeu

PARLAMENTO EUROPEU, *Processo de co-decisão: primeira leitura, Proposta de diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrônicas* (COM(2000) 385 – C5-0439/2000 – 2000/0189(COD)), de 12 de Julho de 2000

PARLAMENTO EUROPEU, *I Resolução legislativa do Parlamento Europeu sobre uma proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n. °2006/2004 relativo à cooperação no domínio da defesa do consumidor* (COM(2007)0698 — C6-0420/2007 — 2007/0248(COD)) - P6_TC1-COD(2007)0248, *de 24 de Setembro de 2008*

PARLAMENTO EUROPEU, *Resolução legislativa do Parlamento Europeu, referente à posição comum aprovada pelo Conselho tendo em vista a aprovação de uma diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor* (16497/1/2008 – C6-0068/2009 – 2007/0248(COD)), *de 6 de Maio de 2009*

PARLAMENTO EUROPEU, Comissão das Liberdades Cívicas, Justiça e Assuntos Internos, *AMENDMENTS (4) 1189 - 1492 on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Proposal for a regulation* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Draft report Jan Philipp Albrecht (PE501.927v04-00), 8 de março de 2013

Tribunal de Justiça da União Europeia

Acórdão do Tribunal de Justiça, *Erich Stauder e Cidadede Ulm — Sozialamt*, Processo 29/69, de 12 de Novembro de 1969

Acórdão do Tribunal de Justiça, *Roland Rutili*, residente em Gennevilliers, e Ministro do Interior, Processo 36/75, de 28 de outubro de 1975

Acórdão do Tribunal de Justiça, Regina (A Rainha) e Pierre Bouchereau, Processo 30/77, de 27 de outubro de 1977

Acórdão do Tribunal de Justiça, *Bond van Adverteerders e outros contra Estado neerlandês*, Processo 352/85, de 26 de abril de 1988

Acórdão do Tribunal de Justiça, *Estado Belga Contra Rene Humbel e Marie-Therese Edel*, Processo 263/86, de 27 de setembro de 1988

Acórdão do Tribunal de Justiça, *Bodil Lindqvist*, Processo C-101/01, de 6 de novembro de 2003

Acórdão do Tribunal de Justiça, *Scarlet Extended SA contra Société belge des auteurs*, compositeurs et éditeurs SCRL (SABAM), Processo C-70/10, de 24 de novembro de 2011

Grupo do Artigo 29.º para a Proteção de Dados

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Recomendação 1/99 sobre o tratamento invisível e automatizado de dados pessoais na Internet realizado por software e hardware* (WP17), de 23 de Fevereiro de 1999, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Recomendação 2/2001 sobre determinados requisitos mínimos para a recolha de dados pessoais em linha na União Europeia* (WP 43), de 17 de maio de 2001, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp43_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Documento de trabalho sobre a determinação da aplicação internacional da legislação da UE em matéria de proteção de dados ao tratamento de dados pessoais na Internet efectuado por sites não-europeus* (WP 56), de 30 de Maio de 2002, disponível em

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp156_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 8/2006 sobre a revisão do quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, com destaque para a Diretiva relativa à privacidade e às comunicações eletrónicas* (WP 126), de 26 de Setembro de 2006, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp126_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (RSE)* (WP 131), de 15 de fevereiro de 2007, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 4/2007 sobre o conceito de dados pessoais* (WP 136), de 20 de junho de 2007., disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 1/2008 sobre questões de proteção de dados ligadas aos motores de pesquisa* (WP 148), de 4 de Abril de 2008, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_pt.pdf#h2-6

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 2/2008 sobre a revisão da Diretiva 2002/58/CE relativa à privacidade no sector das comunicações eletrónicas (Diretiva Privacidade Eletrónica)* (WP 150), de 15 de maio de 2008, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *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 sector das comunicações eletrónicas (diretiva da privacidade eletrónica)* (WP 159), de 10 de fevereiro de 2009, disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 2/2010 sobre publicidade comportamental em linha* (WP 171), de 22 de Junho de 2010, disponível em

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 15/2011 sobre a definição de consentimento* (WP 194), de 13 de julho de 2011, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 16/2011 sobre a recomendação da EASA/IAB relativa às melhores práticas em matéria de publicidade comportamental em linha* (WP 188), de 8 de dezembro de 2011, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_pl.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 01/2012 sobre as propostas de reforma em matéria de proteção de dados* (WP 191), de 23 de março de 2012, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão* (WP 194), de 7 de junho de 2012, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_pt.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications* (WP 197), de 12 de julho de 2012, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp197_en.pdf

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Parecer 08/2012, que presta um contributo suplementar o debate sobre a reforma em matéria de proteção de dados* (WP 199), de 5 de outubro de 2012, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_pt.pdf,

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DOS DADOS, *Working Document 02/2013 providing guidance on obtaining consent for cookies* (WP 208) disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

SITES RELEVANTES

Autoridade Europeia para a Proteção de Dados, *site* oficial, disponível em https://secure.edps.europa.eu/EDPSWEB/edps/lang/pt/EDPS

Comissão Nacional de Proteção de Dados, *site* oficial, disponível em http://www.cnpd.pt/

Conselho da Europa, *site* oficial, disponível em http://hub.coe.int/

Electronic Frontier Foundation, *site* official, disponível em https://www.eff.org/

Grupo do Artigo 29.º para a Proteção de Dados, *site* oficial, disponível em http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

Internet Engineering Task Force, *site* oficial, disponível em http://www.ietf.org/about/

Organização para a Cooperação e Desenvolvimento Económico, *site* oficial, disponível em http://www.oecd.org

Parlamento Europeu, *site* oficial, disponível em http://www.europarl.europa.eu/

The World Wide Web Consortium, *site* official, disponível em http://www.w3.org/

Tribunal de Justiça da União Europeia, *site* oficial, disponível em http://curia.europa.eu

UK Information Commissioner's Office, *site* oficial, disponível em http://www.ico.org.uk/

União europeia, *site* oficial, disponível em http://europa.eu/index_pt.htm