Do consentimento para a utilização de testemunhos de conexão (*cookies*)

Emília Golim Fontaínhas
Senior Adviser EY – Amsterdam
Mestre em Direito e Informática

Francisco Andrade
Professor da Escola de Direito
da Universidade do Minho

José Bacelar Almeida
Professor do Departamento de Informática
da Escola de Engenharia da Universidade do Minho

Resumo: O n.º 3 do art. 5.º da Diretiva da Privacidade Eletrónica (Diretiva 2002/58/CE) 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 de conexão (*cookies*), entendidos na acepção da definição dada pela norma RFC 6265 da Internet Engineering Task Force (IETF).

Na sua versão original, a Diretiva da Privacidade Eletrónica 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 (direito de autoexclusão ou direito de *opt-out*). Em 2009, a Diretiva dos Cidadãos (Diretiva 2009/136/CE) veio dar uma nova redação ao n.º 3 do art. 5.º da Diretiva da Privacidade Eletrónica e passou a fazer depender a utilização de *cookies* da prévia obtenção do consentimento da pessoa em causa (direito de *opt-in*).

O novo requisito de consentimento veio abalar as práticas correntes no que respeita à utilização de *cookie*s e está na base de um aceso debate sustentado pelas dúvidas acerca da sua interpretação e condições de implementação prática.

Procuramos, com este trabalho, contribuir para o esclarecimento dos conceitos de *cookies* e de consentimento enquanto fundamento legitimante para a sua utilização.

Palavras-chave: Testemunhos de conexão / *Cookies* / *Web cookies* / Consentimento/ *opt-in* / Privacidade eletrónica

Introdução

A utilização da internet está plenamente enraizada na sociedade, sendo hoje um meio preferencial para acesso à informação (*e. g.*, acesso a jornais e outros meios de comunicação); de comunicação (*e. g.*, *email*, redes sociais); acesso a serviços e plataformas de comércio eletrónico (*e. g.*, *home-banking*); e até de interação com organismos públicos e do Estado (*e. g.*, portal do cidadão). Mas essa utilização universal da internet é suportada por aplicações informáticas e protocolos de comunicação de dados tecnologicamente elaborados, que em última análise são passíveis de ser utilizados de forma a comprometer a privacidade dos utilizadores. Torna-se assim necessário enquadrar legalmente certos aspetos da sua utilização que possam colocar em risco a privacidade dos utilizadores.

Neste artigo abordam-se os aspetos de privacidade na navegação *web*, e mais especificamente no que concerne à utilização de "testemunhos de conexão" (doravante também referidos por *cookies*), surgidos da necessidade de ultrapassar o problema da falta de estado das ligações HTTP (Protocolo de Transferência de Hipertexto). Trata-se de um mecanismo tecnológico desenvolvido para ultrapassar limitações do protocolo de comunicação usado na navegação *web*, mas que rapidamente encontrou numerosas aplicações que permitem coletar informação dos utilizadores e, assim, colocar potencialmente em risco a sua privacidade.

O HTTP é o protocolo de comunicação de dados em que se baseia a *Web*. É este protocolo que permite que, utilizando um navegador *web*, possamos solicitar páginas *web* aos servidores *web* e que estes no-las possam transferir. O HTTP tem, porém, uma característica a que importa atender: trata-se de um protocolo sem estado, o que significa que foi desenvolvido com a premissa que o servidor não necessita manter qualquer informação sobre anteriores pedidos dos clientes que a ele se co-

nectem[1], *i. e.*, o servidor não consegue relacionar um pedido atual com pedidos passados ou futuros, tratando cada pedido de modo totalmente independente. Sem estado, os *sites web* não são capazes, por exemplo, de registar e agregar produtos eficazmente numa lista de compras ("cestos de compras") e processá-los numa única encomenda final. John Schwarz, no seu célebre artigo publicado no New York Times[2], faz a seguinte analogia: fazer compras na *web* era, então, como visitar uma loja em que o balconista tinha amnesia[3][4].

Os testemunhos de conexão, também designados por *cookies*, surgem da necessidade de ultrapassar o problema da falta de estado das ligações HTTP. Lou Montulli trabalhava ao serviço da Netscape quando, em 1994, desenvolveu a ideia dos *cookies*, adaptando uma tecnologia conhecida por *magic cookie*[5], usada nas plataformas Unix, às necessidades de comunicação entre o computador de um utilizador e um *site web* por si visitado, de modo a suprir o problema da falta de estado das ligações HTTP[6]. A primeira utilização dos *cookies* 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 mesmo ano, com o seu colega John Giannandrea, aquela que foi a especificação original dos *cookies*: "*Persistent Client State HTTP Coo-*

---

[1] Adotamos a terminologia utilizada por R. Fielding [*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 8/5/2016].

[2] John Giving Schwarz, "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 8/5/2016].

[3] "it was like visiting a store where the shopkeeper had amnesia." John Giving Schwarz, "The *Web* a Memory Cost Its Users Privacy", *cit.*

[4] 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.*" – Rajiv Shah, C. E Kesan, Jay P., "Deconstructing Code", in *Illinois Public Law and Legal Theory Research Papers Series, Research Paper* No. 04-22, september 29, 2004, p. 298.

[5] "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 8/5/2016].

[6] Até então, os mecanismos de cestos de compras implicavam o armazenamento de informação, por exemplo, no URL.

kies"[7]. Conforme explicava a especificação, na sequência da recepção 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 cliente, armazenado e reenviado àquele, por este, que Montulli chamou *cookie*[8].[9]

Os *cookies* consistem em 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 e com permissão para tal, são armazenadas como um arquivo de texto por este no terminal do utilizador e, aquando de um novo pedido ao *site*, são reenviadas inalteradas, no cabeçalho *cookie* do pedido HTTP. O servidor dá, desta forma, ordem ao navegador para armazenar o *cookie* e reenviá-lo aquando de uma nova solicitação. O navegador, cooperante e com permissão para tal, armazena o *cookie* juntamente com os seus atributos, como um ficheiro de texto numa pasta ou subpasta no terminal do utilizador e, se este não tiver expirado ou sido apagado, reenvia-o na nova solicitação.

O servidor pode enviar múltiplos cabeçalhos set-*cookie* numa mesma resposta. Cada um destes cabeçalhos, por sua vez, conforme explica a especificação[10], compreende obrigatoriamente o atributo nome=valor, seguido de nenhum ou vários atributos que regulam o tratamento dado ao *cookie* por parte do navegador. São eles:

---

[7] Lou Montulli e John Giannandrea, *Persistent Client State – HTTP Cookies*, Netscape Communications Corporation, 1994.

[8] "The state object is called a cookie, for no compelling reason.", Lou Montulli e John Giannandrea, *Persistent Client State – HTTP Cookies*, *cit.*

[9] À especificação original seguiram-se outras três: D. Kristol e L. Montulli, *HTTP State Management Mechanism*, RFC 2109, The Internet Engineering Task Force (IETF), Fevereiro de 1997; D. Kristol e L. Montulli, *HTTP State Management Mechanism*, RFC 2965, The Internet Engineering Task Force (IETF), Outubro de 2000; e A. Barth, *HTTP State Management Mechanism*, RFC 6265, The Internet Engineering Task Force (IETF), Abril de 2011.

[10] Cf. A. Barth, *HTTP State Management Mechanism*, RFC 6265, The Internet Engineering Task Force (IETF), Abril de 2011, disponível em *http://tools.ietf.org/html/rfc6265* [última consulta em 8/5/2016], pp. 10 e segs.

Os atributos "data de expiração" e "idade-máxima", que indicam a longevidade do *cookie* – uma vez expirada a validade de um *cookie*, ele deverá ser eliminado pelo navegador perdendo-se assim os dados nele contidos. Quando nenhum destes dois atributos estiver definido, o navegador deve apagar automaticamente o *cookie* quando a sessão para que foi gerado expirar. De qualquer o modo o utilizador pode, sempre e a qualquer momento, apagar o *cookie* por iniciativa própria.

O atributo "domínio" determina a aplicabilidade dos *cookies* e é particularmente importante nos casos – tão comuns – em que o *site* conta com vários servidores para suportar a sua atividade na rede. Quando esse atributo está definido, o *site* consegue que o *cookie* seja acessível por todos os servidores desse domínio. A título de exemplo, se o valor do atributo "domínio" for "example.com"[11], o navegador vai reenviar o *cookie* em pedidos dirigidos a servidores como "store.example.com" ou "www.corp.example.com". Em oposição, quando esse atributo não está definido, o navegador apenas envia o *cookie* ao servidor que o originou. Ademais, os navegadores estão configurados para bloquear *cookies* que tenham definido o atributo "domínio" com um domínio público de topo (como .com ou .pt, por exemplo). O atributo "caminho" cumpre uma função semelhante, já que define os caminhos (URLs) para os quais o *cookie* é válido. Só as páginas compreendidas nos caminhos definidos podem ler o *cookie*. Por omissão, é considerado somente o URL que enviou o *cookie*.

O atributo "segurança" indica que o *cookie* só deve ser enviado através de uma ligação segura – através de uma ligação HTTPS – que vai garantir que o *cookie* seja transmitido cifrado e não em claro. De forma análoga, o atributo "HttpOnly" dá indicação ao navegador de que o *cookie* apenas pode ser usado em pedidos HTTP, impedindo que seja dado acesso ao *cookie* às chamadas Interfaces de Programação de Aplicativos[12].

A menos que o navegador esteja configurado para ignorar o cabeçalho set-*cookie*[13], uma vez recebida uma resposta com esse cabeçalho, o navegador armazena o respetivo *cookie* no terminal do utilizador. Cada navegador tem a sua área de ar-

---

[11] Utilizamos aqui, sem alterações, o exemplo dado no RFC 6265, A. BARTH, *HTTP State Management Mechanism*, RFC 6265, *cit.*, p. 11.

[12] 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.

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

mazenamento de *cookies*. A especificação[14] recomenda que os navegadores forneçam as capacidades de, pelo menos, 4096 bytes por *cookie*, 50 *cookies* por domínio e 3000 *cookies* no total. Em novos pedidos ao mesmo servidor (ou servidores do domínio especificado) o navegador adiciona ao pedido um cabeçalho *cookie*, onde envia o par nome-valor contendo a informação previamente recebida, permitindo assim a esse *site* associar o presente pedido ao anterior.

Classificações

Interessa distinguir diferentes padrões de utilização dos *cookies*, que em última análise irão determinar o grau de risco potencial que estes colocam aos aspetos de privacidade dos utilizadores.

A primeira grande distinção é entre *cookies* de sessão e *cookies* permanentes. Os *cookies* de sessão são ficheiros temporários, armazenados na memória do computador enquanto o utilizador navega no *site* que o(s) criou, sendo apagados assim que o utilizador desliga o navegador. Se o *cookie* não tiver definido o atributo "data de expiração", por defeito é suprimido assim que o utilizador encerra o navegador. Os *cookies* 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 evita que a cada página, a cada pedido ao servidor, o utilizador seja considerado sempre um novo e distinto visitante. Note-se que se o *cookie* não tiver definido o atributo "data de expiração", por norma é suprimido logo que o utilizador encerra o navegador, tratando-se assim de um *cookie* de sessão. Se pelo contrário, o *cookie* tiver definida uma data de expiração – maior do que a que dura uma sessão – 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 o *cookie* seja, então, suprimido: nesse caso é designado por *cookie* permanente.

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

---

[14] A. Barth, *HTTP State Management Mechanism*, RFC 6265, *cit.*, p. 27.

Uma segunda distinção relevante é entre *cookies* de origem e *cookies* de terceiros. Os *cookies* de origem são aqueles que são enviados pelos *sites* diretamente visitados pelo utilizador. O domínio (ou subdomínio) definido no *cookie* corresponde àquele visível na barra de endereços do navegador. Já os *cookies* de terceiros são, na perspetiva dos programas de navegação[15], 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 *cookies* de terceiros vai permitir que um *site* que exiba conteúdos num outro envie *cookies* 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 *cookies* com origem num *site* que não visitou diretamente. Note-se que, em rigor, o *site* que envia *cookies* é sempre acedido pelo navegador. No entanto o utilizador, no caso dos *cookies* de terceiros, não promove esse acesso – este só acontece porque estão incorporados conteúdos de *sites* terceiros em páginas deliberadamente visitadas.

Do mesmo modo que pode receber *cookies* 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.

Os *cookies* e a privacidade *online*

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[16]. Os *cookies* estavam desenhados para ser transmitidos e armazenados discretamente, sem que a intervenção do utilizador fosse necessária ou reclamada em

---

[15] O Grupo do Artigo 29.º distingue o conceito de "testemunho de terceiros" no contexto da proteção de dados a nível europeu e na perspetiva 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 8/5/2016].

[16] "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." – JOHN GIVING SCHWARZ, "The *Web* a Memory Cost Its Users Privacy", *cit.*

qualquer momento. Mas dessa forma vieram permitir que uma monitorização muito pormenorizada dos utilizadores na *web* fosse realizada de forma furtiva. Se é verdade que o utilizador tem controlo sobre os *sites* que deliberadamente visita – no limite tem a opção de os visitar ou não –, deixa de ser assim nas chamadas "transações não verificáveis", onde o acesso aos *sites* é promovido de forma indireta pelo conteúdo das páginas visitadas. O exemplo paradigmático é o dos fornecedores de serviços de publicidade *online*.

A publicidade representa uma das principais fontes de rendimento *online*, contribuindo para o crescimento e expansão da economia da Internet[17]. A possibilidade de extrair informação sobre o histórico de navegação dos utilizadores permite a criação de perfis que possibilita o envio de publicidade extremamente incisiva. De facto, as empresas de publicidade puseram em prática uma técnica que a comunidade científica já tinha teorizado, como relata SCHWARTZ[18]: através da exibição de anúncios em diferentes *sites*, estas empresas conseguem reutilizar os mesmos *cookies* em diferentes *sites* da rede, o que lhes permitia reconhecer o mesmo visitante ou, mais precisamente, o mesmo navegador, em todos eles. Este recurso aos designados *cookies* de terceiros permite realizar a monitorização da atividade levada a cabo não dentro do mesmo site web mas através de diferentes *sites web*[19]. Esta técnica permite por isso a criação de perfis muito mais detalhados e abrangentes da atividade dos utilizadores na rede.

Deve salientar-se que os *cookies* não são um mecanismo imprescindível ou exclusivo para a monitorização ou da criação de perfis *online*. Porém, permitem fazê-lo com maior facilidade e mais pormenor[20]. A existência dos *cookies*, e a capacidade de monitorização da atividade dos utilizadores em linha que este mecanismo per-

---

[17] 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, disponível em *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pt.pdf* [última consulta em 8/5/2016], pp. 4 e 5.

[18] JOHN GIVING SCHWARZ, "The *Web* a Memory Cost Its Users Privacy", *cit.*

[19] "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 compliance with law enforcement requests" – BIL CORRY e ANDY STEINGRUEBL, "Where is the Comprehensive Online Privacy Framework?", in *Position Paper for W3C Workshop on Web Tracking and User Privacy*, Princeton, NJ, abril de 2011.

[20] "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." – A. BARTH, *HTTP State Management Mechanism*, RFC 6265, *cit.*, p. 28.

mite, só foi exposta à consciência pública em 1996, como realçam RAJIV C. SHAH e JAY P. KESAN[21]. Em 12 de Fevereiro de 1996, o *Financial Times* publicou aquele que é apontado como o primeiro artigo a expor pública e mediaticamente os *cookies*, da autoria de Tim Jackson, sob o título "This Bug in Your PC is a Smart Cookie"[22]. 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"[23]. A privacidade dos utilizadores na *web* é, assim, incontornavelmente, uma questão associada à utilização do mecanismo dos *cookies*.

O consentimento como fundamento legitimante da utilização de *cookies*

O art. 5.º, n.º 1, da Diretiva da Privacidade Eletrónica[24] protege a confidencialidade das comunicações em geral e o n.º 3 do mesmo artigo regula a proteção da confidencialidade no caso concreto do armazenamento e acesso a informação armazenada no terminal do utilizador ou assinante[25]. Esta norma aplica-se, portanto, à utilização de *cookies*, bem como a outras tecnologias semelhantes.

O considerando 25 da Diretiva 2002/58/CE refere-se expressamente aos *cookies*, que reporta como um instrumento que pode ser "legítimo e útil, nomeadamente na análise da eficácia da concepção e publicidade do sítio *web*, e para verificar a identidade dos utilizadores que procedem a transacções em linha"[26].

---

[21] RAJIV C. SHAH e JAY P. KESAN, *Deconstructing Code*, *cit.*, pp. 300 e segs.

[22] "Este *bug* no seu Computador é um Testemunho de Conexão", em tradução livre.

[23] "Os Testemunhos de Conexão podem estar a espiá-lo", em tradução livre.

[24] Salvo indicação em contrário, neste Capítulo 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. A Diretiva 2002/58/CE foi transposta para a ordem jurídica nacional pela Lei n.º 41/2004, de 18/8, e a Diretiva 2009/136/CE pela Lei n.º 46/2012, de 29/8.

[25] Na versão portuguesa, da Diretiva 2009/136/CE lê-se "terceiros podem desejar armazenar informações sobre o equipamento de um utilizador (...)" (considerando 66). Entendemos tratar-se de um lapso. Na versão em inglês da mesma lê-se "Third parties may wish to store information on the equipment of a user (...)".

[26] O Regulamento Geral de Proteção de Dados – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, no seu art. 95.º refere de modo expresso a sua relação com a Diretiva 2002/58/CE, dizendo que "[o] presente regulamento não impõe obrigações suplementares a pessoas singulares ou coletivas no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações na União em matérias que estejam sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na Diretiva 2002/58/CE.".

Na versão de 2002 da Diretiva da Privacidade Eletrónica, o n.º 3 do art. 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 (direito de autoexclusão ou direito de *opt-out*).

Assim, era legítimo à entidade responsável proceder ao tratamento de informações através da utilização de *cookies*, 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[27], a utilização de *cookies* passou a depender da prévia obtenção do consentimento da pessoa em causa.

Conforme decorre do considerando 10 da Diretiva da Privacidade Eletrónica, "é aplicável a Directiva 95/46/CE[28], especialmente no que se refere a todas as questões relacionadas com a protecção dos direitos e liberdades fundamentais não abrangidos especificamente pelas disposições da presente directiva, 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 art. 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, exceto em relação às disposições expressamente previstas na Diretiva da Privacidade Eletrónica, que correspondem essencialmente ao art. 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 se-

---

Entretanto, o art. 94.º do Regulamento expressamente revoga a Directiva 95/46/CE com efeitos a partir de 25 de Maio de 2018.

[27] Directiva 2004/38/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros.

[28] 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 26/10, que revogou a Lei n.º 10/91, de 29/4.

gurança do tratamento e as transferências internacionais de dados, serão plenamente aplicáveis"[29]. Assim, sempre que as informações abrangidas por um *cookie* sejam dados pessoais, além das regras estabelecidas no art. 5.º, n.º 3, da Diretiva da Privacidade Eletrónica, são aplicáveis as disposições da Diretiva 95/46/CE.

Objetivo do art. 5.º, n.º 3, da Diretiva da Privacidade Eletrónica

A Diretiva da Privacidade Eletrónica visa a proteção do direito à privacidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas[30].

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 de Lisboa, a Carta dos Direitos Fundamentais da União Europeia (CDFUE) tornou-se vinculativa. Nela, a União consagrou autonomamente o direito ao respeito pela vida privada e familiar[31] e o direito à proteção de dados pessoais[32].

O art. 5.º, n.º 3, é um complemento ao art. 5.º, n.º 1, da Diretiva da Privacidade Eletrónica.

Assim como o conteúdo das comunicações e os respetivos dados de tráfego são passíveis de conter informações do âmbito da esfera privada dos 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[33].

---

[29] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 11.

[30] Art. 1.º da Diretiva da Privacidade Eletrónica.

[31] Art. 7.º da CDFUE.

[32] Art. 8.º da CDFUE.

[33] 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.

O principal objetivo do art. 5.º, n.º 3, é, portanto, a proteção do equipamento terminal do utilizador e de quaisquer informações aí armazenadas, enquanto parte da esfera privada dos utilizadores, no que respeita ao tratamento de dados pessoais.

Os 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 art. 5.º da Diretiva da Privacidade Eletrónica. São estes, portanto, os fundamentos relativos à legitimidade da utilização de *cookies*.

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[34].

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"[35].

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 art. 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.

Sintetizando, o consentimento enquanto fundamento de legitimidade específico para a utilização de *cookies* 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 *cookies* pode envolver o tratamento de dados pessoais sensíveis. Neste caso, o consentimento deve ainda ser explícito[36].

---

[34] Art. 2.º, alínea *f)*, da Diretiva da Privacidade Eletrónica.

[35] Art. 2.º, alínea *h)*, da Diretiva 95/46/CE.

[36] Art. 8.º, n.º 2, alínea *a)*, da Diretiva 95/46/CE.

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[37] previsto no art. 14.º da Diretiva 95/46/CE. Enquanto aquele 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[38].

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[39][40].

Atendendo ao facto de que o mesmo *cookie* pode servir a diversas finalidades – "cookies polivalentes"[41] – o consentimento prestado tem, ainda, de preencher todos os requisitos em relação a cada uma delas, para que a sua utilização seja legítima.

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"[42].[43]

---

[37] Entre nós, sobre o direito de oposição previsto no art. 14.º da Diretiva 95/46/CE e transposto através do art. 12.º da Lei n.º 67/98, de 26/10, ver Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005, pp. 254 a 261, e Garcia Marques e Lourenço Martins, *Direito da Informática*, 2.ª ed., refundida e atualizada, Coimbra, Almedina, 2006, p. 359.

[38] Neste sentido, Eleni Kosta, *Consent in European Data Protection Law*, Países Baixos, Martinus Nijhoff Publishers, 2013, 251.

[39] Neste sentido, Eleni Kosta, *Consent in European Data Protection Law*, *cit.*, p. 251.

[40] Entre nós, o consentimento prestado pode sempre ser revogável nos termos do art. 81.º, n.º 2, do Código Civil. "A revogação do consentimento deve dar lugar à imediata destruição dos dados e é lícita, embora possa fazer incorrer o titular na obrigação de indemnizar os danos causados pela revogação" – cf. Pedro Pais de Vasconcelos, "Proteção de Dados Pessoais e Direito à Privacidade", em *Direito da Sociedade da Informação*, vol. I, Coimbra Editora, outubro 1999, p. 252.

[41] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 6.

[42] 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 8/5/2016].

[43] Entre nós, sobre os tratamentos visíveis e invisíveis de dados pessoais, com especial referência aos

A utilização de *cookies* representa um exemplo típico de tratamento invisível de dados(44).

Este mecanismo veio sendo largamente utilizado sem que fosse dado ao utilizador conhecimento de que estavam a ser armazenadas e/ou 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(45).

---

testemunhos de conexão, ver Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, *cit.*, pp. 156 a 160, e Garcia Marques e Lourenço Martins, *Direito da Informática*, *cit.*, pp. 432 a 441.

(44) "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 invisível e automatizado de dados pessoais na Internet realizado por software e hardware* (WP17), *cit.*, p. 4.

(45) «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 rules on use of cookies and similar technologies*, VV.3, maio de 2012, disponível em *https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf* [última consulta em 8/5/2016], p. 3.

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.

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 que se tenciona armazenar no *cookie*, com que objetivo e, também, qual o seu prazo de validade"[46].

O art. 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 de dar ao utilizador ou assinante o direito de recusar o tratamento, o responsável estava obrigado a fornecer-lhe 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 legítima utilização de *cookies*, nos termos do n.º 3 do art. 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 do consentimento do utilizador ou assinante, depois de lhe terem sido fornecidas aquelas informações.

Para ser tido como informado, o consentimento deve basear-se "numa apreciação e compreensão dos factos e implicações de uma ação"[47].

---

[46] 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), *cit.*, p. 3.

[47] 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 15/2/2007, p. 9, disponível em *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_pt.pdf* [última consulta em 30/8/2013].

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.

O art. 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 art. 5.º, n.º 3, da Diretiva da Privacidade Eletrónica seria, portanto, escusada não fosse o seu amplo âmbito de aplicação[48] – esta norma não se limita ao tratamento de dados pessoais, mas aplica-se ao armazenamento ou acesso de quaisquer informações no equipamento terminal do utilizador ou assinante.

Desta forma, a obrigação do responsável pelo tratamento, ou do seu representante, de fornecer à pessoa em causa, junto da qual recolha dados que lhe digam respeito, pelo menos as informações especificadas no art. 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 *cookies* de terceiros, 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 art. 5.º da Diretiva da Privacidade Eletrónica, por ser este quem o envia e lê.

Porém, o Grupo do Artigo 29.º é da opinião[49] que os titulares dos *sites* que alojam conteúdos de terceiros são corresponsáveis pelos *cookies* por eles instalados, na medida da sua colaboração. Trata-se aqui de uma normal aplicação do regime de responsabilidade dos prestadores de serviços da sociedade da informação[50].

Entre nós, o art. 2.º da Lei n.º 67/98, de 26/10, reconhece o princípio geral da transparência. Sobre este princípio ver Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, *cit.*, p. 229.

[48] Neste sentido, Eleni Kosta, *Consent in European Data Protection Law*, *cit.*, p. 309, e "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. 406.

[49] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, pp. 12 e 13.

[50] O que está em consonância com o espírito da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000 (Diretiva sobre Comércio Electrónico), que no seu considerando 46 refere o seguinte: "A fim de beneficiar de uma delimitação de responsabilidade, o prestador de um ser-

No que respeita à obrigação de prestar as 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 de as informações chegarem de modo eficaz, claro e completo ao utilizador para que este, com base nelas, possa tomar uma decisão válida[51].

Independentemente da medida em que partilhe as obrigações decorrentes do n.º 3 do art. 5.º com o titular do *site* terceiro, o titular do *site* diretamente visitado tem obrigações para com o utilizador que decorrem da Diretiva 95/45/CE. A verdade é que este é responsável pelo redirecionamento do utilizador para o site *web* terceiro, nomeadamente através da transferência do seu endereço IP[52][53].

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 *cookie* 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 *cookies*[54].[55]

As informações prestadas serão, então, completas se compreenderem as finalidades do *cookie*; 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 *cookie*[56]; a

---

viço da sociedade da informação, que consista na armazenagem de informação, a partir do momento em que tenha conhecimento efectivo da ilicitude, ou tenha sido alertado para esta, deve proceder com diligência no sentido de remover as informações ou impossibilitar o acesso a estas". O teor deste considerando encontra-se plasmado no art. 14.º da referida Directiva, que foi entretanto transposta para a ordem jurídica portuguesa pelo DL n.º 7/2004, de 7/1, que, no seu art. 16.º, foi no mesmo sentido.

[51] Neste sentido, Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 22.

[52] 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 em linha*, *cit.*, p. 21.

[53] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 21.

[54] Sem prejuízo de outras informações devidas pelo reencaminhamento de outros dados pessoais dos seus utilizadores a terceiros.

[55] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, pp. 20 e 21.

[56] 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 8/5/2016].

necessidade de aceitar a instalação e/ou o acesso e as possíveis consequências no caso de não aceitar; a existência do direito ao acesso aos dados e do direito de os retificar[57]; e, se for caso disso, a possibilidade de instalação de *cookies* de terceiros, respetivas finalidades e identidade da entidade terceira[58].

O Grupo do Artigo 29.º destaca que é, ainda, essencial que ao utilizador ou assinante seja dada informação relativa ao modo como pode expressar o seu consentimento em relação a todos, alguns ou nenhum dos *cookies*, e à forma de alterar as suas preferências no futuro[59].

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"[60].

O Grupo do Artigo 29.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.[61] A respeito da qualidade da informação o Grupo refere[62] que esta 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[63] mas, também, a linguagem que deve ser acessível ao utilizador comum. A forma de prestar a informação devida depende sempre do contexto. No que respeita à acessibilidade e visibilidade da informação,

---

[57] Art. 10.º, alínea *c)*, 3.º travessão, da Diretiva 95/46/CE.

[58] 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 8/5/2016].

[59] Grupo do Artigo 29.º para a Proteção de Dados, *Working Document 02/2013 providing guidance on obtaining consent for cookies* (WP 208), *cit.*, pp. 3 e 4.

[60] Considerando 25 da Diretiva 2002/58/CE.

[61] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187),* de 13 de julho de 2011, disponível em *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_pl.pdf* [última consulta em 8/5/2016], p. 22.

[62] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 22.

[63] Também aqui podemos constatar a aplicação dos princípios que nortearam a Diretiva 2000/31/CE no que respeita aos deveres de informação dos prestadores de serviços da Sociedade da Informação (art. 10.º), princípios esses que foram transpostos para o direito português através do DL n.º 7/2004 (cfr. os deveres de informação constantes do art. 10.º deste Decreto-Lei).

esta deve ser prestada diretamente às pessoas, "deve ser claramente visível (tipo e tamanho das letras), proeminente e completa."[64].

O consentimento prévio

A redação do considerando 66 da Diretiva 2009/136/CE, respeitante ao armazenamento e acesso a informações previamente armazenadas no terminal do utilizador ou assinante refere-se à prestação de informações e ao direito de recusar o tratamento, na senda da versão de 2002 do art. 5.º, n.º 3[65].

Foi com base neste considerando que a Áustria, a Bélgica, a Estónia, a Finlândia, a Alemanha, a Irlanda, a Letónia, 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 art. 5.º deve, na prática, ser exercido como direito de recusar o armazenamento ou o posterior acesso[66].

O art. 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 *cookies* e a tecnologias similares, cuja utilização pode ser legítima em numerosas circunstâncias. O texto alterado do art. 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 art. 5.º, n.º 3, alterado, não se destina a modificar o requisito em vigor segundo o qual tal consentimento deve ser exercido como direito de recusar a

---

[64] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 22.

[65] 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 modalidades para prestar informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível."), as versões inglesa e francesa daquele considerando 66 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".

[66] Cf. Eleni Kosta, *Consent in European Data Protection Law*, *cit.*, pp. 404 e 405.

utilização de *cookies* 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[67].

O texto final do novo art. 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.

O Grupo do 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 art. 5.º «tem de ser obtido antes do *cookie* ser instalado e/ou as informações armazenadas no equipamento terminal do utilizador serem recolhidas, o que habitualmente se designa por "consentimento prévio"»[68][69].

O consentimento livre

"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."[70]

---

[67] 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.

[68] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 14, e *Working Document 02/2013 providing guidance on obtaining consent for cookies* (WP 208), *cit.*, p. 4.

[69] 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." – *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 34.

[70] Neste sentido, Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 14.

O consentimento livre garante o exercício do direito de autodeterminação informativa[71], que é uma liberdade fundamental[72].

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"[73].

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.

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 "[t]al é particularmente importante nos casos em que outros 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 *cookie* (ou dispositivo análogo), caso seja utilizado para um fim legítimo.

Ora, a liberdade de aceitar ou não o *cookie* 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[74].

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 *cookie*

---

[71] Sobre o direito à autodeterminação informativa ver CATARINA SARMENTO E CASTRO, *Direito da Informática, Privacidade e Dados Pessoais*, *cit.*, pp. 22 a 29.

[72] ELENI KOSTA, *Consent in European Data Protection Law*, *cit.*, p. 171.

[73] Neste sentido, Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, pp. 14 e 15.

[74] Neste sentido, ELENI KOSTA, *Consent in European Data Protection Law*, *cit.*, p. 312.

nos seus computadores e para a necessidade de clarificação ou revisão do mesmo[75], o que não veio a acontecer.

Assim, quando o *cookie* seja utilizado para um fim legítimo é permitida uma limitação à liberdade do consentimento, nos termos *supra* referidos[76].

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 podendo ser genérico. Trata-se de um requisito em estreita conexão com a obrigação da entidade responsável de prestar informações[77].

O consentimento deve ser prestado em relação aos diferentes aspetos do tratamento, nomeadamente quanto às informações recolhidas e às finalidades do tratamento[78].

O Grupo do Artigo 29.º entende que devem ser consideradas as "expectativas razoáveis das partes"[79][80]. 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[81].

---

[75] 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 26/9/2006, p. 3, disponível em *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp126_pt.pdf* [última consulta em 8/5/2016].

[76] Conforme decorre do considerando 25 da Diretiva 2002/58/CE.

[77] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 19.

[78] A propósito do princípio da finalidade, ver Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, *cit.*, pp. 229 a 237.

[79] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 19.

[80] "As it ["reasonable expectation of privacy"] makes privacy protection dependent on contextual factors, it could simply 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." Paul de Hert, Serge Gutwirth, Anna Moscibroda, David Wright e Gloria Gonzalez-Fuster, *Legal Safeguards for Privacy and Data Protection in Ambient Intelligence*, From the SelectedWorks of Serge Gutwirth, outubro 2008, p. 5.

[81] A este propósito o Grupo do Artigo 29.º refere o acórdão do Tribunal de Justiça, *Deutsche Telekom AG*, proc. C-543/09, de 5 de Maio de 2011, que a propósito do art. 12.º, n.º 2, da Diretiva da Privacidade

Em relação ao caso concreto da utilização de *cookies*, 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". Socorrendo-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 *cookie* abrange os acessos posteriores ao mesmo, que têm lugar sempre que o utilizador visita um *site web* que instalou o *cookie* ou, no caso dos *cookies* de terceiros, outro *site* parceiro da mesma rede de publicidade a que pertence aquele que instalou o *cookie*[82].

Assim, o consentimento não tem de ser prestado previamente a cada acesso às informações contidas num *cookie* cuja instalação foi consentida com base em informações claras e completas. Porém, 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[83].

O consentimento inequívoco

O consentimento é inequívoco quando se baseia em declarações ou atos que manifestem aceitação.

Este requisito adicional do art. 7.º, alínea *a)*, da Diretiva 95/46/CE reforça o sentido do requisito que se prende com a manifestação de vontade do art. 2.º, alínea *h)*, do mesmo diploma. A verdade é que o conceito de "manifestação" é muito

---

Eletrónica entendeu que, "tendo um assinante sido informado da possibilidade da transmissão de dados de carácter 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" – cf. *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, pp. 19 e 20.

[82] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 19.

[83] 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 de consentimento (WP 187), cit.*, p. 19.

amplo, já que 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[84].

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[85].

Quando esteja em causa o tratamento de dados pessoais sensíveis através de *cookies*, o consentimento exigido pelo art. 5.º, n.º 3, da Diretiva da Privacidade Eletrónica não é suficiente e, nos termos do art. 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[86].

O consentimento explícito depende da resposta ativa do utilizador à questão que lhe apresenta a alternativa de aceitar ou não a instalação de *cookie*(s) de conexão.

Mas o requisito do consentimento explícito não está expressamente previsto para o tratamento de informações que não sejam dados pessoais sensíveis, através de *cookies*.

Por entender que no contexto da Internet "o consentimento tácito nem sempre conduz a um consentimento inequívoco"[87], o Grupo do Artigo 29.º defende que as

---

[84] Neste sentido, Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 23.

[85] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 15/2011 sobre a definição de consentimento (WP 187), cit.*, p. 28.

[86] Tem-se colocado a questão de saber se o consentimento expresso tem de ser por escrito, entendimento que tem sido sustentado pela Comissão Nacional de Proteção de Dados mas que suscita dúvidas. Subscrevemos a posição de Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005, segundo a qual, relativamente à prestação do consentimento "em termos de demonstração da sua existência, ... a sua redução a escrito deverá considerar-se vantajosa". Posição que, agora, aparece como manifestamente em consonância com o espírito do art. 7.º, n.º 1, do novo Regulamento Geral de Proteção de Dados Pessoais que estabelece que "[q]uando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais".

[87] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 18.

pessoas em causa devem manifestar a sua vontade, prestando o seu consentimento de modo explícito[88].

As diferentes autoridades nacionais competentes assumiram posições divergentes sobre a necessidade de o consentimento ser expresso no contexto da utilização de *cookies*[89].

Numa clara tentativa de dirimir estas diferenças, omitindo as classificações de consentimento explícito ou tácito, o Grupo do Artigo 29.º defendeu, mais recentemente, que os utilizadores podem manifestar o seu consentimento para instalação de *cookies* através de uma "ação positiva ou outro comportamento ativo, desde que completamente informados do que essa ação representa"[90]. 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 *cookies*.

As excepções 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 excepções.

Nos termos do n.º 3 do art. 5.º da Diretiva da Privacidade Eletrónica estão isentas da obtenção de consentimento as situações em que o *cookie* tem como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, e aquelas em que a utilização do *cookie* é estritamente ne-

---

[88] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 18

[89] Na Bélgica, na Dinamarca, em Espanha, na 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 …*, e *Cookie Laws Across Europe*, Cookipedia, disponível em *http://cookiepedia.co.uk/cookie-laws-across-europe*, última consulta em 8/5/2016.

[90] "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 obtaining consent for cookies* (WP 208), *cit.*, p. 4.

cessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado.

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 *cookies*[91], que passamos a analisar, atendendo às diferentes utilizações dos *cookies*.

Importa, antes do mais, realçar que as situações isentas da obrigação de obtenção de consentimento não põem em causa o direito de informação da pessoa em causa e correspondente obrigação de informar da entidade responsável.

Para determinar no caso concreto se os *cookies* estão ou não isentos da obrigação de obter consentimento é a finalidade do *cookie* que se deve ter em conta. Mais do que as informações neles contidas ou as características técnicas, importa considerar as finalidades para que são utilizados.

Estão isentos da obrigação de obter o consentimento informado do utilizador ou assinante os *cookies* que têm como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas[92]. A versão original do art. 5.º, n.º 3, era menos restrita e permitia a utilização de *cookies* 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 *cookie* a comunicação não seria possível.

Excluídas da isenção ficam todas aquelas situações em que o *cookie* seja utilizado para "facilitar, acelerar ou regular a transmissão".

A segunda excepção prevista no art. 5.º, n.º 3, da Diretiva da Privacidade Eletrónica refere-se à isenção de consentimento informado de que gozam os *cookies* estritamente necessários para 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 "[a]s excepções 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 ne-

---

[91] 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), *cit.*

[92] 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), *cit.*, p. 3.

cessário para o objectivo legítimo de permitir a utilização de um serviço específico explicitamente solicitado pelo assinante ou utilizador". Este critério[93] 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 *cookie* 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 *cookie* e a prestação de um serviço expressamente solicitado pelo utilizador"[94].

O critério da "estrita necessidade" deve ser aferido do ponto de vista do utilizador, e não do prestador de serviços[95][96]. 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, "serviço 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)"[97]. 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 *cookie* para ser disponibilizada e tem de ser expressamente solicitada pelo utilizador ou assinante[98].

A obtenção do consentimento em linha

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 in-

---

[93] 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), *cit.*, pp. 3 e segs.

[94] 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), *cit.*, p. 4.

[95] 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), *cit.*, p. 13.

[96] 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 rules on use of cookies and similar technologies, *cit.*, p. 7.

[97] 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), *cit.*, p. 4.

[98] 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), *cit.*, pp. 7 e 8.

dicação comunicada de livre vontade, específica e informada sobre os seus desejos, incluindo por via informática, ao visitar um sítio na internet."[99].

A primeira alteração proposta pelo Parlamento Europeu[100] ao art. 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 *cookies* que "[s]empre 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 arts. 2.º, alínea *h)*, e 7.º, alínea *a)*, da Diretiva 95/46/CE.

Na medida em o navegador aceite, por defeito, todo o tipo de *cookies*, o ato voluntário de o utilizador alterar as definições não é prévio em relação aos *cookies* entretanto instalados.

As configurações do programa de navegação que permitem a aceitação ou o bloqueio de *cookie*s em bloco e para o futuro, sem considerações acerca das finalidades específicas de cada *cookie* 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), não terá, à partida, por base informações claras e completas, nomeadamente sobre os objetivos do processamento, nos termos da Diretiva 95/46/CE. Assim, apesar de na aceitação ou blo-

---

[99] "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 obtaining consent for cookies* (WP 208), *cit.*, p. 2.

[100] 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 setor das comunicações eletrónicas, e o Regulamento (CE) n.º 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.

queio 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.

Concordamos com a posição assumida pelo Grupo do Artigo 29.º[101]: o consentimento prestado através de definições do navegador só pode ser válido quando os navegadores estejam configurados para rejeitar um *cookie*, 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 à possibilidade decorrente do considerando 25 da Diretiva 2002/58/CE de o consentimento prestado para a instalação de um *cookie* legitimar os acessos posteriores ao mesmo, o Grupo do Artigo 29.º entendeu que após o utilizador ter consentido em receber determinado *cookie*, a presença do *cookie* no equipamento terminal do utilizador pode ser utilizada como um indicador desse consentimento[102]. O Grupo propõe, porém, 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[103]. Defendemos que não é só o consentimento que deve ser renovado, mas o próprio *cookie* que deve ter uma longevidade limitada, pois pode acontecer que o utilizador ou assinante nunca mais visite o *site* em questão, ou não o faça num largo período de tempo.

Um método considerado eficaz para a prestação de informações e para obtenção do consentimento em linha é o recurso a janelas instantâneas[104]. Além deste método, 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 art. 5.º, n.º 3,

---

[101] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, pp. 16 e 17.

[102] 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*, p. 12.

[103] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 2/2010 sobre publicidade comportamental em linha*, *cit.*, p. 19.

[104] 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*, *cit.*, p. 10.

não é necessário que o *site* forneça informações e obtenha o consentimento do utilizador separadamente para cada *cookie* ou para cada finalidade de cada *cookie*[105]. 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.

As faixas de informação estáticas, colocadas na parte superior de um *site*, solicitando o consentimento do utilizador para a instalação de alguns *cookies*, 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 *cookie* – pode, ainda, optar pelo recurso a um ecrã inicial que forneça ao utilizador as informações legalmente exigidas e solicite o seu consentimento.

O Grupo do Artigo 29.º reconhece a validade do consentimento prestado através de qualquer comportamento ativo[106] do utilizador, aquando da prestação de informações, a partir do qual o titular do *site* possa concluir pelo consentimento inequívoco, específico e informado[107].

O requisito do consentimento para a utilização de *cookies* no futuro da regulação europeia da proteção de dados

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 pro-

---

[105] 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), *cit.*, p. 6.

[106] "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 obtaining consent for cookies* (WP 208), *cit.*, pp. 4 e 5.

[107] Grupo do Artigo 29.º para a Proteção de Dados, *Working Document 02/2013 providing guidance on obtaining consent for cookies* (WP 208), *cit.*, p. 4.

teção de dados em vigor, com vista a reforçar a proteção da privacidade em linha e impulsionar a economia digital europeia[108]. Após mais de quatro anos de negociações, o novo Regulamento Geral sobre a Proteção de Dados[109], que revoga a Diretiva 95/46/CE, foi finalmente aprovado e será aplicável a partir de 25 de maio de 2018.

As novas regras, porém, não promovem uma rutura com o regime atual, mas respeitam uma linha de continuidade. Os princípios consagrados na Diretiva 95/46/CE são tão válidos hoje como eram em 1995[110].

O novo Regulamento contempla uma referência expressa aos *cookies*, no seu considerando 30, enquanto identificadores que podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.

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"[111].

No que em particular respeita aos requisitos relativos ao consentimento, o art. 7.º do novo Regulamento vem clarificar as condições aplicáveis ao consentimento, esclarecendo nomeadamente que o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento, que o titular dos dados tem de ser previamente informado do seu direito de retirar o consentimento a todo o tempo e que este deve ser tão fácil de retirar quanto de dar. O art. 8.º, por sua vez, dispõe a respeito da oferta direta de serviços da sociedade da informação a crianças, estabelecendo que o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais.

Há, porém, uma particularidade na versão portuguesa do Regulamento que merece a nossa especial atenção. O consentimento do titular dos dados é definido

---

[108] 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 10/5/2016].

[109] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[110] 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.

[111] Grupo do Artigo 29.º para a Proteção de Dados, *Parecer 1/2008 sobre questões de protecção dos dados ligadas aos motores de pesquisa*, p. 9.

como uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento[112]. A verdade é que o Parlamento Europeu e o Conselho da União Europeia não concordaram que o consentimento deva, em todos os casos, ser explícito, conforme havia proposto a Comissão Europeia[113]. Diferentemente da versão em português do Regulamento – e de acordo com as conclusões das negociações entre as instituições europeias envolvidas no processo legislativo –, nas versões inglesa e francesa do Regulamento não se lê que o consentimento tenha de ser sempre explícito mas antes uma manifestação de vontade, livre, específica, informada/esclarecida e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo claro, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento[114]. Lamentamos este tipo de inconsistências que contribuem para fragmentar a interpretação e implementação destas normas em oposição ao objetivo de uniformização do regime.

Como parte da sua estratégia para um mercado único digital na Europa, a Comissão Europeia pretende rever a Diretiva da Privacidade Eletrónica, de modo a: assegurar a sua coerência com o novo Regulamento Geral sobre a Proteção de Dados; atualizar o seu âmbito de aplicação, estendendo-o aos provedores de serviços de comunicação através da internet (*over-the-top providers*); melhorar a segurança e confidencialidade das comunicações; e resolver os problemas de implementação inconsistente e fragmentada[115].

---

[112] Art. 4.º (11) do Regulamento Geral sobre a Proteção de Dados.

[113] Consolidated text (outcome of the trilogue of 15/12/2015) Consolidated text (outcome of the trilogue of 15/12/2015), disponível em *http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884* [última consulta em 10/5/2016].

[114] Na versão em inglês do Regulamento Geral sobre a Proteção de Dados: «'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her»; na versão em francês: «"consentement" de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement».

[115] Comissão Europeia, *Public Consultation on the Evaluation and Review of the ePrivacy Directive*, disponível em *https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive* [última consulta em 10/5/2016].

A consulta pública decorre no momento em que produzimos este trabalho. As questões postas pela Comissão, no que mais particularmente respeita aos *cookies*, prendem-se com a disponibilidade dos próprios utilizadores para que lhes seja pedido consentimento para a utilização de diferentes tipos de *cookies*, com a efetiva liberdade de escolha dos utilizadores e com o impacto que a prática de obter consentimento tem na experiência de navegação[116]. Antecipamos, pois, que estes desafios venham a ser relevantes numa eventual alteração à Diretiva da Privacidade Eletrónica.

Conclusão

Este trabalho permitiu-nos perceber os *cookies* enquanto tecnologia antes de nos debruçarmos sobre a análise da sua regulamentação específica no quadro legislativo europeu da proteção de dados.

Percebemos que estamos perante uma tecnologia que permitiu superar uma limitação tecnológica e que, hoje, é utilizada para várias finalidades. Trata-se de uma tecnologia que permite a monitorização da atividade dos utilizadores *online* e que, por muito tempo, se manteve subtil, invisível aos olhos do utilizador médio. Na prática, as regras gerais para a 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 veio contemplar uma regra especial para a utilização de *cookies*. Esta Diretiva impunha que, para ser lícita, a utilização de *cookies* dependia de serem dadas ao utilizador ou assinante informações claras e completas e de lhes ser garantido o direito de recusar o tratamento. Apesar de estabelecer garantias para o armazenamento e acesso a informações no terminal do utilizador, esta norma não foi suficiente para promover a transparência da utilização deste mecanismo.

A Diretiva dos Cidadãos, que alterou a Diretiva 2002/58/CE, 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.

---

[116] Comissão Europeia, *Questionnaire for the Public Consultation on the Evaluation and Review of the E-Privacy Directive*, disponível em *https://ec.europa.eu/eusurvey/runner/EPRIVACYReview2016*.

A norma impõe que o consentimento seja prestado sempre que esta tecnologia seja usada e não apenas quando se destine ao tratamento de dados pessoais – a menos que se verifique alguma das excepções previstas. Sempre que as informações abrangidas por um *cookie* sejam dados pessoais, além das regras estabelecidas no art. 5.º, n.º 3, da Diretiva da Privacidade Eletrónica, são aplicáveis as disposições da Diretiva 95/46/CE – com excepção do art. 7.º, a que se sobrepõe aquela regra especial.

Com este estudo prestamos a nossa contribuição para o esclarecimento dos requisitos relativos ao consentimento para a utilização de *cookies*.

Vimos que para determinar no caso concreto se os *cookies* estão ou não isentos da obrigação de obter consentimento é a sua finalidade que se deve ter em conta. Mais do que as informações neles contidas ou as características técnicas, importa considerar as finalidades para que são utilizados. As características técnicas dos *cookies*, que estabeleçam parâmetros desnecessários ou excessivos à prossecução da finalidade concreta, podem, ainda, justificar a sua não isenção da obrigação de obtenção de consentimento prévio.

De todo o modo, sempre que o *cookie* em causa compreenda dados pessoais, 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 *cookie* que não os respeitasse.

A revisão da Diretiva da Privacidade Eletrónica, em curso, permitirá rever o regime jurídico aplicável aos *cookies* na União Europeia, beneficiando das novas regras gerais para a proteção de dados. Resta saber se as novidades passarão pela consagração de mais excepções à regra da obrigatoriedade de obtenção de consentimento ou se se irá mais além, talvez, abandonando a atual abordagem legislativa que regula quase indiferenciadamente a utilização deste tipo de tecnologias e estruturando o regime especial em torno de finalidades abusivas.