A utilização de *cookies* e a (in)suficiência dos requisitos aplicáveis ao consentimento

Catarina Silva[*]

Resumo: Nos dias de hoje, a nossa pegada digital é utilizada para obter dados pessoais acerca de cada um de nós, sendo esta informação recolhida frequentemente através do armazenamento de *cookies*. Ora, sendo a perda de privacidade um tópico que se vem tornando progressivamente mais premente, importa averiguar se, do ponto de vista normativo, serão suficientes os requisitos aplicáveis ao consentimento prestado para o armazenamento de *cookies* ou se, conforme melhor veremos no presente artigo, deverão os mesmos ser concretizados e adaptados às práticas dos operadores de *websites*.

***Palavras-chave**: Diretiva 2002/58/CE; Regulamento Geral de Proteção de Dados; cookies; privacidade; consentimento.*

Abstract: Nowadays, our digital footprint is used to obtain personal data about each one of us, and this information is often collected through the storage of cookies. As the loss of privacy is a topic that has become progressively more pressing, it is important to ascertain whether, from a normative point of view, the requirements applicable to the consent given for the storage of cookies are sufficient or whether, as we will verify in this article, they should be implemented and adapted to the practices of website operators.

***Keywords:** Directive 2002/58/EC; General Data Protection Regulation; cookies; privacy; consent.*

[*] Advogada. Licenciada em Direito pela NOVA School of Law. Frequenta o II Curso de Pós-Graduação Avançada em Proteção de Dados, na Faculdade de Direito da Universidade de Lisboa.

1. Afinal, o que são *cookies*?

Numa era cada vez mais digital, tem-se tornado usual comparar, de forma metafórica, a perda de privacidade ao "Big Brother", a personificação de um governo totalitário omnipresente retratada na obra "1984" de George Orwell, ou ainda ao "O Processo", de Franz Kafka, em que o personagem Joseph K. é informado de que está preso, não chegando, contudo, a descobrir, ao longo do desenrolar da história, os motivos por detrás da sua detenção, muito embora tais fundamentos pareçam ser conhecidos de várias pessoas, exceto dele próprio.

A verdade é que ambas estas analogias (embora distintas) parecem, cada vez mais, corresponder a uma realidade e não já apenas a uma mera ficção.

Nos dias de hoje, qualquer utilizador de Internet deixa, ainda que inconscientemente, um rasto de informações e de dados à mercê dos operadores de *websites*, os quais são recolhidos, na maioria dos casos, através do armazenamento de *cookies* nos dispositivos que, cada um de nós, utiliza diariamente.

Mas afinal o que são *cookies*?

De acordo com o Comité Europeu para a Proteção de Dados, "um cookie é um pequeno ficheiro de texto que um sítio Web instala no computador ou dispositivo móvel do utilizador"[1], sendo o mesmo processado e armazenado no *browser* do utilizador.

De uma forma geral, os *cookies* podem ser classificados em função da sua duração, proveniência e finalidades:

1. A respeito da duração, é comum distinguir entre *cookies* de sessão, os quais são temporários e expiram quando o utilizador fecha o *browser*, e os *cookies* persistentes, que permanecem armazenados no *browser* do utilizador até que sejam apagados.
2. A nível da proveniência, poder-se-á distinguir entre *cookies* primários, os quais são armazenados diretamente pelo *website* que o utilizador está a visitar, e *cookies* de terceiros, os quais são armazenados por um terceiro.

---

[1] Disponível em <https://edpb.europa.eu/cookies_pt>, acedido a 18 de novembro de 2020.

3. Relativamente às finalidades, existem essencialmente quatro tipos de *cookies*:

   a. *Cookies* estritamente necessários, os quais são essenciais para que o utilizador possa navegar no *website* e utilizar determinadas funcionalidades do mesmo.
   b. *Cookies* de funcionalidade, os quais guardam as preferências do utilizador relativamente à utilização do *website*, não sendo necessário que o utilizador volte a configurar o *website* cada vez que o visita.
   c. *Cookies* de desempenho, os quais recolhem informações sobre a utilização do *website*, com vista à criação e análise de estatísticas e ao melhoramento do funcionamento do mesmo.
   d. *Cookies* de publicidade, os quais rastreiam a atividade do utilizador, de modo a direcionar a publicidade em função dos seus interesses.

A proliferação das notificações de *cookies* (ou *cookie notices*), habitualmente sob a forma de janelas *pop-up*, constituiu um resultado da Diretiva 2009/136/CE da União, a qual alterou o artigo 5.º, n.º 3 da Diretiva 2002/58/CE (Diretiva *ePrivacy*)[2].

Com efeito, o referido artigo passou a prever que o armazenamento de informação ou o acesso a informação armazenada no dispositivo de um utilizador depende da prévia obtenção de consentimento por parte do mesmo, prestado com base em "informações claras e completas [...] sobre os objectivos do processamento", excetuando-se, designadamente, as situações em que tal seja estritamente necessário. A título de exemplo, os *cookies* utilizados para adicionar artigos ao carrinho de compras numa loja *online* ou destinados a assegurar que o conteúdo de uma página carrega rápida e eficazmente são considerados estritamente necessários, pelo que a sua utilização não exige o consentimento prévio do utilizador.

---

[2] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).

A 25 de Maio de 2018, entrou em vigor o Regulamento (UE) 2016/679[3] ("RGPD"), relativo à proteção de pessoas singulares no que diz respeito ao tratamento e à livre circulação de dados pessoais.

De uma análise comparativa entre ambos os diplomas, conclui-se que o RGPD constitui *lex generalis*, na medida em que regula a proteção de dados pessoais no espaço da União Europeia (sem prejuízo do seu âmbito extraterritorial), enquanto a Diretiva *ePrivacy* se aplica especificamente ao setor das comunicações eletrónicas. Posto isto, em matéria de *cookies*, a Diretiva *ePrivacy* complementa o regime geral previsto no RGPD.

A respeito da relação entre a Diretiva *ePrivacy* e o RGPD, o Comité Europeu para a Proteção de Dados emitiu a Opinião 5/2019[4], na qual esclareceu que existem múltiplas matérias que se inserem no escopo de aplicação de ambos os diplomas legais. Assim, estando em causa o armazenamento de informação ou o acesso a informação armazenada no dispositivo de um utilizador, as provisões do RGPD, em especial os requisitos aplicáveis ao consentimento, serão subsidiariamente aplicáveis sempre que as informações armazenadas no dispositivo do utilizador constituam dados pessoais, aplicando-se, a título de regime-regra, o disposto no já mencionado artigo 5.º, n.º 3 da Diretiva *ePrivacy*. Com efeito, sendo exigida a prestação de consentimento por parte do utilizador ao abrigo do referido artigo, não é admissível que a utilização e armazenamento de *cookies* de que resulte o tratamento de dados pessoais tenha por base qualquer outro fundamento de licitude previsto no artigo 6.º do RGPD.

Atento o exposto, de modo a cumprir as disposições normativas do RGPD e da Diretiva *ePrivacy*, os operadores de *websites* devem:

a. Recolher o consentimento dos utilizadores antes de utilizar e armazenar quaisquer *cookies*, salvo nos casos legalmente previstos.

---

[3] 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.

[4] EDPB. Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, de 12 de março de 2019.

b. Fornecer informação precisa, específica e em linguagem simples sobre os dados que cada *cookie* rastreia e a sua finalidade, antes da recolha do consentimento.
c. Documentar e armazenar o consentimento recebido por parte dos utilizadores.
d. Permitir aos utilizadores o acesso ao serviço, mesmo que estes se recusem a autorizar a utilização de determinados *cookies*.
e. Adotar mecanismos que assegurem aos utilizadores ser tão fácil retirar o seu consentimento como foi dá-lo em primeiro lugar.

2. O Acórdão Planet49

No dia 1 de Outubro de 2019, foi proferido pelo Tribunal de Justiça da União Europeia ("TJUE") o Acórdão Planet49[5], em resultado de um pedido de decisão prejudicial suscitado pelo Supremo Tribunal Federal alemão no âmbito de um litígio que opunha a Federação alemã das organizações e associações de consumidores (de ora em diante, "Federação") à Planet49 GmbH (de ora em diante, "Planet49").

2.1. Enquadramento fáctico

A 24 de Setembro de 2013, a Planet49, uma empresa alemã de jogos *online*, organizou um jogo promocional no *site* www.dein-macbook.de.

Ingressando no referido *site*, e em ordem a participar no sorteio, os interessados eram obrigados a fornecer o respetivo código postal, mediante o que eram reencaminhados para uma página Web em que deviam inscrever os respetivos nomes e endereços.

Sob os campos de preenchimento do seu endereço, foram dadas aos utilizadores duas declarações descritivas juntamente com quadrículas de seleção.

---

[5] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801

A primeira quadrícula de seleção, que se encontrava desmarcada, exigia que os utilizadores dessem o seu consentimento aos patrocinadores e parceiros da Planet49 para o envio de informações promocionais via correio, telefone, email ou SMS.

Por sua vez, a segunda quadrícula de seleção, que foi pré-selecionada, exigia que os utilizadores autorizassem a utilização de *cookies* pela Planet49 por meio de uma empresa designada Remintrex que se ocuparia da recolha de dados pessoais cruciais para fins publicitários.

Sucede que os termos e condições aplicáveis ao jogo promocional supramencionado determinavam que os utilizadores só podiam participar se, pelo menos, a primeira quadrícula de seleção fosse assinalada. A este respeito, cumpre referir que os utilizadores podiam optar por não autorizar a utilização de *cookies*, desde que desmarcassem manualmente a segunda quadrícula de seleção.

2.2. Entendimento adotado pelo TJUE e principais conclusões

De acordo com o Acórdão sob análise, "[...] um consentimento dado através de uma opção pré-validada não implica um comportamento cativo por parte do utilizador de um sítio Internet"[6] e, por esse motivo, não consubstancia um consentimento suscetível de ser utilizado como fundamento de licitude do tratamento de dados pessoais.

Ora, o artigo 2.º, alínea h), da Diretiva 95/46/CE[7] do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, aplicável *ex vi* artigo 5.º, n.º 3, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002 ("Diretiva *ePrivacy*") define "consentimento da pessoa em causa" como "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento". Por conseguinte, e no

---

[6] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, para. 52.

[7] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

seguimento das conclusões do Advogado-Geral[8], o TJUE afirmou que a exigência de uma manifestação de vontade da pessoa em causa aponta, evidentemente, para um comportamento ativo, e não passivo[9]. Neste sentido, um consentimento dado através de uma opção pré-selecionada – e que o utilizador deverá desmarcar em ordem a recusar o seu consentimento – não implica, em qualquer circunstância, um comportamento cativo por parte do utilizador, pelo que não se poderá considerar que o mesmo tenha sido validamente obtido[10].

De sublinhar que a interpretação adotada nos termos acima referidos é imposta igualmente por força do RGPD, em especial à luz do Considerando 32, segundo o qual:

> "O consentimento do titular dos dados deverá ser dado mediante um acto positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato electrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, seleccionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. [...]".

A este respeito, o Tribunal esclareceu ainda que o consentimento prestado pelo utilizador, na aceção da alínea h) do artigo 2.º da Diretiva 95/46, deve ser específico, na medida em que deve incidir precisamente sobre o tratamento de dados pessoais em causa e não poderá, por conseguinte, ser deduzido de uma manifestação de vontade que tem um objeto distinto. Tal significa que – e com referência ao caso *sub judice* – o simples facto de um utilizador ativar o botão de participação num jogo

---

[8] Conclusões do Advogado-Geral Maciej Szpunar, de 21 de março de 2019, Processo C-673/17.

[9] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, para. 52.

[10] *Idem*, para. 57.

promocional não poderá ser considerado suficiente para concluir que o mesmo deu validamente o seu consentimento ao armazenamento de *cookies* ou à divulgação dos seus dados a quaisquer terceiros[11].

Ademais, o Tribunal considerou que a duração do funcionamento dos *cookies* e a possibilidade de terceiros terem ou não acesso aos mesmos se encontram abrangidas pelo leque de "informações claras e completas" que devem ser fornecidas ao utilizador por força do disposto no n.º 3 do artigo 5.º da Diretiva *ePrivacy*, constituindo, aliás, requisito de validade do consentimento prestado[12].

Ora, de acordo com as conclusões do Advogado-Geral, "as informações claras e completas devem permitir ao utilizador determinar facilmente as consequências do consentimento que possa vir a dar e garantir que esse consentimento seja dado com pleno conhecimento de causa", sendo que "essas informações devem ser compreensíveis e suficientemente pormenorizadas para permitir ao utilizador compreender o funcionamento dos cookies utilizados"[13].

Estatisticamente falando, o Relatório elaborado pelo Grupo de Trabalho do Artigo 29[14], datado de 2015, elucida-nos quanto à importância destas informações para o pleno esclarecimento do utilizador aquando da prestação do seu consentimento à utilização e armazenamento de *cookies*.

Ora, com base nos 478 *websites* analisados, apurou-se a existência de três *cookies* primários (em inglês, *first-party cookies*) com uma duração de 7985 anos, expirando a 31/12/9999 às 23:59, e de 17 *cookies* primários em 15 diferentes *websites* com uma duração superior a 100 anos. Cumpre sublinhar que a duração média de *cookies* primários utilizados pelos *sites* analisados é de 14.34 anos.

Em contraposição, os *cookies* de terceiros (em inglês, *third-party cookies*) apresentam uma duração substancialmente menor: em média, reduz-se para 1.77 anos.

---

[11] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, paras. 58 a 60.

[12] Idem, paras. 72 a 81.

[13] Conclusões do Advogado-Geral Maciej Szpunar, de 21 de março de 2019, Processo C-673/17.

[14] Grupo de Trabalho do Artigo 29. *Cookie Sweep Combined Analysis – Report*", de 3 de fevereiro de 2015.

É, pois, evidente que a duração da utilização dos *cookies* (que, em muitos casos, considerar-se-á excessiva) apresenta, em especial, extrema relevância para a prestação de um consentimento devidamente esclarecido, sendo determinante para a completa compreensão da extensão da utilização desses *cookies*.

Uma vez mais, esta interpretação é igualmente sustentada pela alínea a) do n.º 2 do artigo 13.º do RGPD, segundo a qual o responsável pelo tratamento deve facultar ao titular dos dados informação sobre, nomeadamente, o prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo, de modo a garantir um tratamento equitativo e transparente.

Além disso, e em conformidade com o disposto na alínea e) do n.º 1 do artigo 13.º do RGPD, deverá igualmente ser prestada ao titular dos dados informação relativa aos destinatários ou às categorias de destinatários dos dados, em que se integra, portanto, a possibilidade de terceiros terem ou não acesso aos *cookies*.

Mais: de acordo com o entendimento sufragado pelo TJUE[15], as obrigações legalmente impostas em matéria de *cookies* e consentimento são aplicáveis independentemente de estarem ou não em causa dados pessoais. Para o efeito, o Tribunal baseou-se no facto de o n.º 3 do artigo 5.º da Diretiva *ePrivacy* fazer referência tão-somente ao "armazenamento de informações" e à "possibilidade de acesso a informações já armazenadas", sem, todavia, qualificar essas informações como dados pessoais.

Tal decorre também das conclusões do Advogado-Geral, segundo o qual a disposição legal *supra* mencionada se destina "a proteger os utilizadores de qualquer intromissão na sua esfera privada, independentemente da questão de saber se essa intromissão envolve dados pessoais ou outros dados"[16].

Sem prejuízo do referido, no nosso entendimento, tal resultaria, desde logo, do próprio espírito da Diretiva *ePrivacy*, cujo âmbito de aplicação se distingue do do RGPD, muito embora ambos se cruzem quando esteja

---

[15] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, para. 66 a 71.

[16] Conclusões do Advogado-Geral Maciej Szpunar, de 21 de março de 2019, Processo C-673/17, para. 107.

em causa o armazenamento de informação ou o acesso a informação armazenada no dispositivo de um utilizador que constitua um dado pessoal. Posto isto, quando isoladamente considerados, verifica-se que o RGPD visa, em traços gerais, assegurar a proteção dos dados pessoais, enquanto a Diretiva *ePrivacy* procura preservar a esfera privada individual, a qual pode ou não incluir, em si mesma, dados pessoais. A este respeito, o considerando 2 da Diretiva *ePrivacy* esclarece que a mesma "visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela Carta dos Direitos Fundamentais da União Europeia. Visa, em especial, assegurar o pleno respeito pelos direitos consignados nos artigos 7.º [referente ao respeito pela vida privada e familiar] e 8.º [referente à proteção de dados pessoais] da citada carta.". O considerando 24 da Diretiva *ePrivacy* acrescenta que "o equipamento terminal dos utilizadores de redes de comunicações electrónicas 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 Protecção dos Direitos Humanos e das Liberdades Fundamentais", confirmando, assim, que a Diretiva *ePrivacy* visa salvaguardar, em primeira linha, a esfera privada de cada indivíduo face a qualquer intromissão externa, independentemente de estar ou não em causa a proteção de dados pessoais.

Em suma, e pese embora o caso sob análise anteceda a entrada em vigor do RGPD, a decisão foi tomada à luz dos padrões impostos pela referida norma, concluindo-se que:

a. As quadrículas de seleção pré-assinaladas mediante as quais a utilização de *cookies* e tecnologias semelhantes é autorizada não constituem consentimento válido ao abrigo da Diretiva *ePrivacy*.
b. Nos casos em que é exigida a obtenção de consentimento para a utilização de *cookies* nos termos da Diretiva *ePrivacy*, são aplicáveis os requisitos previstos em matéria de consentimento pelo RGPD.
c. A circunstância de os *cookies* constituírem ou não dados pessoais não é relevante, porquanto o n.º 3 do artigo 5.º da Diretiva *ePrivacy* é aplicável a qualquer informação instalada ou acedida a partir do dispositivo de um indivíduo.

d. Devem ser fornecidas aos utilizadores de um *website* informações acerca da duração da utilização dos *cookies* e da possibilidade de terceiros terem ou não acesso aos mesmos.

Na verdade, numa era pós-RGPD e pré-Regulamento *ePrivacy*, o Acórdão sob análise não parece acrescentar particulares novidades em matéria de *cookies*. Ainda assim, a presente decisão assume especial relevância na medida em que vem reforçar que a utilização de *cookies* exige um consentimento expresso, livre, informado e específico. Ademais, o Acórdão Planet49 elimina quaisquer dúvidas existentes a respeito das regras aplicáveis ao consentimento para a utilização de *cookies*, alertando para as práticas que deverão ser evitadas e encorajando os operadores de *websites* a seguir a orientação adotada pelo TJUE por forma a garantir o adequado cumprimento das regras e obrigações que lhes são impostas pelo RGPD.

Ainda assim, o Tribunal não se pronunciou acerca de outras questões relevantes a respeito deste tema, em especial relativamente à admissibilidade das chamadas *cookie walls*, que condicionam o acesso do utilizador a um *website* ou a alguns serviços ou conteúdos ao seu prévio consentimento à utilização de *cookies*, deixando, por isso, algumas dúvidas em aberto.

Não obstante, o Comité Europeu para a Proteção de Dados já se pronunciou no sentido de reconhecer que o consentimento obtido através das referidas *cookie walls* não é livre, acolhendo, assim, a posição maioritariamente adotada pelas autoridades de proteção de dados nacionais. Mas deverá mesmo ser essa a orientação a adotar? A resposta a tal questão, conforme veremos adiante, não é clara.

3. Orientação do Comité Europeu para a Proteção de Dados

A 4 de Maio de 2020, na esteira do entendimento adotado pelo TJUE no âmbito do Acórdão Planet49, o Comité Europeu para a Proteção de Dados adotou uma orientação[17] onde esclarece o que constitui um consentimento válido para o tratamento de dados pessoais ao abrigo do RGPD.

---

[17] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, de 4 de maio de 2020, disponível em <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, acedido em 14 de novembro de 2020.

Esta orientação, que atualiza as diretrizes do Grupo de Trabalho do Artigo 29º em matéria de consentimento[18], cimenta uma aplicação unificada do RGPD, sendo que, muito embora não tenha carácter vinculativo, é utilizada pelas autoridades nacionais de cada Estado-Membro na interpretação e aplicação do RGPD.

Assim, para que um consentimento seja considerado válido, nos termos previstos no RGPD, é necessário que seja:

a. Livre;
b. Específico;
c. Informado;
d. Inequívoco.

O Comité Europeu para a Proteção de Dados esclarece que "uma indicação inequívoca do consentimento do utilizador" implica uma ação clara e afirmativa por parte do utilizador. A este respeito, e num dos exemplos dados pelo Comité Europeu para a Proteção de Dados, as ações de um utilizador como o mero percorrer ou navegar de um *website* ou qualquer atividade similar constitui, em bom rigor, um consentimento implícito, não cumprindo, por conseguinte, os requisitos de validade do consentimento exigidos pelo RGPD, em especial a existência de uma ação clara e afirmativa. Posto isto, deixa de ser admissível que as notificações de *cookies* afirmem que a navegação contínua num determinado *website* vale como consentimento para a utilização de *cookies* que processam dados pessoais.

Alternativamente, as referidas notificações devem ser configuráveis e o *website* está impedido de utilizar ou armazenar quaisquer *cookies* sem a obtenção do consentimento prévio por parte do utilizador.

A este respeito, o Grupo de Trabalho do Artigo 29.º considerou que a exigência de "consentimento prévio" resulta diretamente do elemento literal do n.º 1 do artigo 6.º do RGPD "tiver dado"[19]. Neste sentido, decorre logicamente do referido artigo que se exige a existência de um fundamento

---

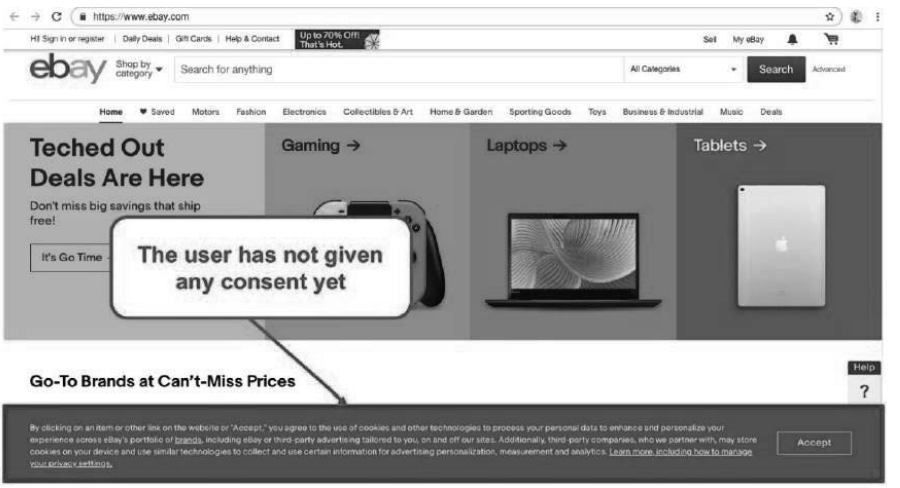
[18] Grupo de Trabalho do Artigo 29º. *Opinion 15/2011 on the definition of consent (WP 187)*, de 13 de julho de 2011.

[19] Grupo de Trabalho do Artigo 29º. *Opinion 15/2011 on the definition of consent (WP 187)*, de 13 de julho de 2011.

legal válido antes de se iniciar um qualquer tratamento de dados. De outro modo, o tratamento de dados desenvolvido desde o momento em que o referido tratamento teve início até ao momento em que o consentimento foi obtido é ilícito em virtude da inexistência de base legal.

Num estudo desenvolvido por Santos et al.[20], verificou-se que o requisito do consentimento prévio ao armazenamento de *cookies* é, muitas vezes, olvidado pelos operadores de *websites*. A título de exemplo, vejamos a Figura 1 e 2 abaixo:

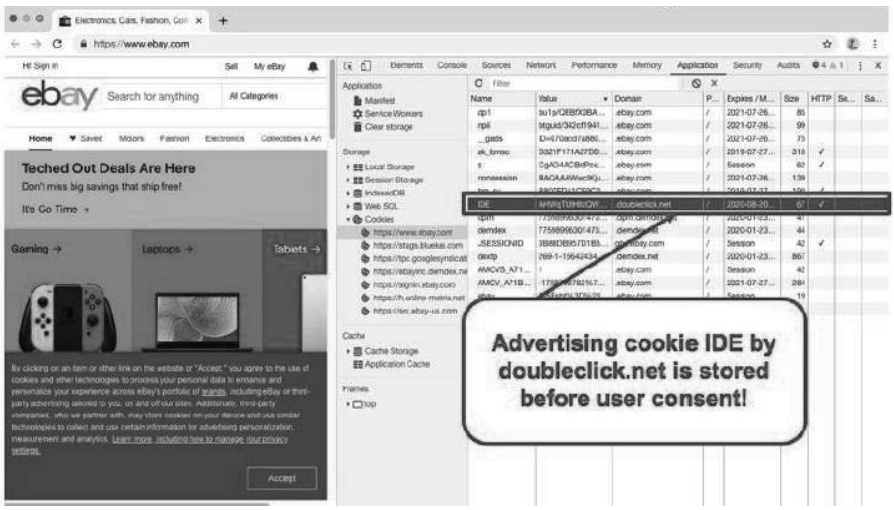
Figura 1 – Acesso ao website <www.ebay.com> em 27 de julho de 2019.
Ao aceder ao referido website, surge uma notificação relativa à utilização de *cookies*.



Fonte: Santos, Cristina; Bielova, Nataliia; Matte, Célestin. "Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners." *Technology and Regulation*, dezembro, 2020, pp. 91-135.

[20] Santos, Cristina; Bielova, Nataliia; Matte, Célestin. "Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners." *Technology and Regulation*, dezembro, 2020, pp. 91-135.

Figura 2 – Violação do requisito de obtenção de consentimento prévio ao tratamento de dados pessoais. Antes de o utilizador prestar o seu consentimento ao tratamento de dados pessoais, é instalado um *cookie* de publicidade, designado "IDE", que armazena um identificador de utilizadores no seu *browser*.



Fonte: Santos, Cristina; Bielova, Nataliia; Matte, Célestin. "Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners." *Technology and Regulation*, dezembro, 2020, pp. 91-135.

Sucede, no entanto, que, na prática, a identificação de situações de incumprimento deste requisito pelos operadores de *websites* constitui uma tarefa bastante complexa e de difícil execução.

Na mesma ordem de raciocínio, o Comité Europeu para a Proteção de Dados esclareceu que a utilização de quadrículas de seleção pré-assinaladas não cumpre com os requisitos impostos pelo RGPD, porquanto não se verifica igualmente a existência de uma "ação clara e afirmativa".

O Comité Europeu para a Proteção de Dados acrescenta ainda que as chamadas co*okie walls* não constituem uma forma legítima de obter consentimento do utilizador por parte dos operadores de *websites*.

Em termos genéricos, as *cookie walls* condicionam o acesso a um website à obtenção de consentimento do utilizador para o tratamento dos seus dados pessoais, pelo que esse mesmo consentimento, a existir, não é

livre. Isto porque as *cookie walls* forçam o consentimento do utilizador a armazenar *cookies* ou a aceder a *cookies* já armazenados em troca do acesso a determinados serviços e funcionalidades, sendo que não existe uma escolha genuína em sentido estrito.

O entendimento suprarreferido a respeito das *cookie walls* veio, portanto, harmonizar as diferentes posições adotadas pelas autoridades de proteção de dados nacionais.

Pese embora a orientação maioritária das autoridades de proteção de dados nacionais fosse já a de que as *cookie walls* não são permitidas ao abrigo do RGPD[21], esta não era, até agora, consensual.

A este respeito, a ICO, autoridade de proteção de dados do Reino Unido, defende que o consentimento que é prestado através de uma *cookie wall* é, com grande probabilidade, inválido[22]. Ainda assim, salienta a importância de conjugar o RGPD com outros direitos fundamentais, nomeadamente a liberdade de expressão e a liberdade de empresa, deixando, desta forma, margem para a possibilidade de, em determinados casos, se considerar válido o consentimento prestado através de uma *cookie wall*.

---

[21] A este respeito, *vide* a orientação da CNIL (*in* "Guidelines on cookies and other trackers", (2019) <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337), bem como da autoridade de protecção de dados *grega* (*in* "Guidelines on Cookies and Trackers" (2020)<http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=84,221,176,170,98,24,72,223>), *irlandesa* (*in* "Guidance note on the use of cookies and other tracking technologies" (2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-), *holandesa* (*in* "Cookies"(2029) <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#mag-ik-als- organisatie-een--cookiewall-gebruiken-7111> and "Many websites incorrectly request permission to place tracking cookies" (2019) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op- onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies>), *belga* (*in* "Guidance Materials and FAQs on Cookies and Other Tracking Technologies", <https://www.autoriteprotectiondonnees.be/recueillir- valablement-le-consentement-des-personnes--concernees), *alemã* (*in* "On the use of cookies and cookie banners – what must be done with consent (ECJ ruling "Planet49")?" (2019) <www.baden- wuerttemberg.datenschutz.de/zum-einsatz-von-cookies-und-cookie-bannern-was-gilt-es-bei- einwilligungen-zu-tun-eugh--urteil-planet49/>,) e *dinamarquesa* (*in* "Guide on consent" (2019) <www.datatilsynet.dk/media/6562/samtykke.pdf>).

[22] ICO, *Guidance on the rules on use of cookies and similar technologies*, Privacy and Electronic Communications Regulations, 2019.

Por sua vez, a autoridade de proteção de dados austríaca, a 30 de Novembro de 2018, emitiu uma decisão[23] na qual considerou que o consentimento obtido através de uma *cookie wall* utilizada pelo jornal austríaco *Der Standard* foi prestado livremente pelo utilizador. A este propósito, apurou que o referido jornal deu aos utilizadores a opção de: i) aceitar a utilização de *cookies*, dando-lhes acesso total ao *website*; ii) recusar a utilização de *cookies*, o que lhes permitiria um acesso limitado ao *website*; ou iii) pagar uma taxa por uma subscrição mensal sem aceitar a utilização de *cookies*. Como fundamento da sua decisão, a autoridade de proteção de dados austríaca argumentou que, no caso concreto, a *cookie wall* não era proibida, uma vez que as próprias configurações do jornal conferiam ao utilizador diferentes graus de escolha. Posto isto, concluiu que:

1. O jornal apenas procedia ao armazenamento de *cookies* depois de o utilizador prestar o seu consentimento, com base numa decisão plenamente informada;
2. Ao utilizador foi dada a opção de não prestar o seu consentimento, quer através do pagamento de uma subscrição mensal, quer saindo do website do Der Standard. Além disso, considerou ainda aquela autoridade que os preços praticados pelo jornal relativamente à subscrição mensal não eram excessivamente elevados e que, ao prestar consentimento à utilização de *cookies*, o utilizador obtém para si um resultado positivo, que se traduz num acesso ilimitado aos artigos do jornal.

Na mesma senda, a autoridade de proteção de dados espanhola reconhece que o bloqueio do acesso a um determinado *website* constitui uma prática válida se um utilizador não prestar o seu consentimento ao tratamento de dados pessoais. De acordo com esta autoridade:

> "Em certos casos, a não aceitação da utilização de cookies implica ser total ou parcialmente impedido de utilizar o serviço; os utilizadores devem ser devidamente informados desta situação. No entanto, o acesso aos serviços não

[23] Autoridade de protecção de dados austríaca, *Decision on the validity of consent*, 2018.

> pode ser negado devido à recusa de utilização de cookies nos casos em que tal recusa impeça o utilizador de exercer um direito legalmente reconhecido, sendo o website o único meio disponível para o exercício de tais direitos" (tradução livre)[24].

Pese embora a orientação emitida pelo Comité Europeu para a Proteção de Dados tenha deixado claro que as *cookie walls* não são permitidas, poder-se-á concluir que existem ainda algumas zonas cinzentas nesta matéria, designadamente, a título de exemplo, nos casos em que se verifiquem práticas idênticas à adotada pelo jornal austríaco *Der Standard* e descrita *supra*.

Na nossa opinião, ainda que as *cookie walls*, em regra, não constituam uma forma legítima de obter um consentimento verdadeiramente livre do utilizador, cremos que a sua licitude deverá ser analisada caso a caso.

Ora, a este respeito, cumpre notar que a proibição inexorável da utilização de *cookie walls* poderá ser considerada contrária à Diretiva (UE) 2019/2161[25], a qual introduz, no artigo 3.º da Diretiva 2011/83/UE[26], o número 1.º-A, de acordo com o qual: "A presente diretiva [Diretiva 2011/83/UE] aplica-se igualmente caso o profissional forneça ou se comprometa a fornecer conteúdos digitais[27] que não sejam fornecidos num suporte material ou um serviço digital ao consumidor e o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional, exceto se os dados pessoais facultados pelo consumidor forem exclusivamente tratados pelo profissional para o fornecimento de conteúdos digitais que

---

[24] Autoridade de protecção de dados espanhola, *Guide on the use of cookies*, 2019, disponível em www.aepd.es/media/guias/guia-cookies.pdf.

[25] Diretiva (UE) 2019/2161 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, que altera a Diretiva 93/13/CEE do Conselho e as Diretivas 98/6/CE, 2005/29/CE e 2011/83/UE do Parlamento Europeu e do Conselho a fim de assegurar uma melhor aplicação e a modernização das regras da União em matéria de defesa dos consumidores.

[26] Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva 93/13/CEE do Conselho e a Diretiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Diretiva 85/577/CEE do Conselho e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho.

[27] O conceito de "conteúdo digital" deve ser interpretado de acordo com o disposto no artigo 2.º, n.º 1, da Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho.

não sejam fornecidos num suporte material ou de um serviço digital, nos termos da presente diretiva, ou para que o profissional cumpra os requisitos legais a que o profissional esteja sujeito, e o profissional não proceda ao tratamento desses dados para quaisquer outros fins.".

Ao abrigo da atual redação da Diretiva 2011/83/UE, o prestador de serviços poderá, em certos casos, e desde que observados os requisitos aplicáveis ao consentimento por força do RGPD, fazer depender o acesso a um determinado conteúdo digital do fornecimento de dados pessoais por parte do consumidor.

A tendência poderá, pois, paulatinamente aproximar-se da prática já adotada pelo jornal austríaco *Der Standard*.

Em face do que antecede, cumpre perguntar: serão as exigências até agora reconhecidas suficientes para assegurar um consentimento livre, informado e esclarecido, em especial face aos mecanismos utilizados pelos operadores de *websites*?

4. Breve análise das práticas utilizadas pelos *websites*

Num estudo levado a cabo por Utz et al.[28], foram reunidas 5 087 notificações de *cookies*, de entre as quais foram aleatoriamente selecionadas 1 000 para formar uma subamostra dos diferentes mecanismos utilizados pelos vários *websites*.

Os resultados, descritos, em termos genéricos, na Tabela 1 *infra*, foram deveras surpreendentes.

---

[28] Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

Tabela 1 – Variáveis da interface gráfica das notificações de *cookies* numa subamostra de 1.000 de 5.087 notificações de *cookies* recolhidas em *websites* populares da União Europeia em agosto de 2018.

Position		**Choices (visible)**		**Choices (hidden)**		**Blocking**		**Nudging**	
top	27.0 %	no option	27.8 %	no option	26.3 %	yes	7.0 %	yes	57.4 %
bottom	57.9 %	confirmation	68.0 %	confirmation	59.9 %	no	93.0 %	no	14.8 %
top right	0.2 %	binary	3.2 %	binary	4.0 %			n/a[a]	27.8 %
bottom right	3.0 %	categories	1.0 %	slider	0.2 %				
top left	0 %	vendors	0 %	categories	8.1 %				
bottom left	3.7 %			vendors	1.1 %				
center	7.8 %			other	0.4 %				
other	0.4 %								
Link to privacy policy		**Text: Collection**		**Text: Processor**		**Text: Purposes**			
yes	92.3 %	"cookies"	94.8 %	unspecified	75.5 %	generic	45.5 %		
no	6.6 %	"data"	1.4 %	first party	0.7 %	specific	38.6 %		
other	1.1 %	both	1.6 %	third party	2.6 &	none	16.9 %		
		none	0.9 %	both	21.1 %				
		other	1.3 %	other	0.1 %				

[a] Nudging is not available for "no option" notices.

Fonte: Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

Neste sentido, os autores apuraram que as referidas notificações variavam em larga escala com base em múltiplos fatores, de entre os quais se têm por mais relevantes os seguintes:

- Posição: as notificações de *cookies* são, geralmente, exibidas em sete posições distintas: num dos quatro cantos do browser (6,9 %), no topo (27,0 %), na parte inferior (57,9 %) ou no centro (7,8%).
- Bloqueio (*cookie walls*): Algumas notificações (7,0 %) impedem os utilizadores de entrar e aceder à página enquanto não prestarem o seu consentimento.
- Opções:

    i. Nenhuma opção é dada ao utilizador (27,8%, quando visível, e 26,3%, quando não visível), limitando-se este a ser informado de que o *website* utiliza *cookies*. Por norma, nestes casos, o facto de o utilizador continuar a utilizar esse website é interpretado como um acordo tácito – cfr. Figura 3 abaixo.

ii. Apenas é apresentada a opção de clicar em "OK" ou "Concordo" (são, em bom rigor, notificações de mera confirmação) – cfr. Figura 4 abaixo.
iii. O utilizador pode optar entre aceitar ou recusar a utilização de *cookies* pelo *website* (3,2%, quando visível, e 4,0%, quando não visível) – cfr. Figura 5 abaixo.
iv. O utilizador pode permitir ou não a utilização de *cookies* relativamente a uma determinada categoria individual (1,0%, quando visível, e 8,1%, quando não visível) – cfr. Figura 6 abaixo.

Figura 3

Figura 4

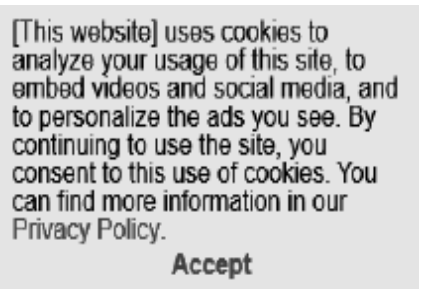
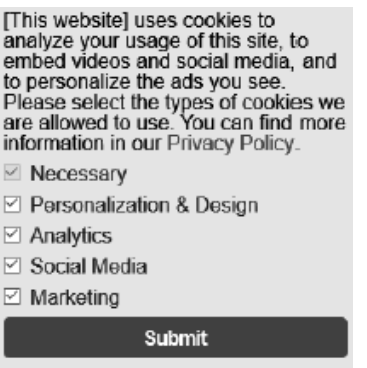


Figura 5

Figura 6



Fonte: Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

- Texto: por definição, as notificações de *cookies* devem informar o utilizador do *website* de que o mesmo utiliza *cookies* ou tecnologia semelhante, bem como fornecer outras informações relevantes (tais como as finalidades da recolha de dados, o período de duração do armazenamento dos mesmos, entre outros). Ora curiosamente, o utilizador apresenta maior probabilidade de prestar o seu consentimento quando a informação facultada refere meramente a "utilização de *cookies*" (94,8%) do que quando mencionada explicitamente a recolha dos seus dados pessoais (1,4%). Ademais, verifica-se igualmente que nos casos em que as finalidades da utilização de *cookies* são especificadas (a título de exemplo, para publicidade direcionada) existe menor propensão para o utilizador prestar o seu consentimento (38,6%), comparativamente com os casos em que essas finalidades são apresentadas de forma genérica (a título de exemplo, para melhorar a experiência do utilizador) (45,5%).
- Cores e outros elementos manipuladores: frequentemente (e pelo menos em 57,4% dos websites analisados no estudo acima mencionado), as notificações referentes à utilização de *cookies* utilizam cores e outros elementos que estimulam o consentimento – na maior parte das vezes inconsciente – do utilizador. Ora, nas conclusões do Advogado-Geral apresentadas a 21 de Março de 2019, distingue-se entre a atividade que um utilizador prossegue na Internet e o consentimento prestado à utilização de *cookies*, esclarecendo que, sendo situações autónomas e independentes, "ambas as acções devem, oticamente em especial, ser apresentadas em igualdade de condições"[29]. O mesmo se deverá aplicar, por analogia, às situações em que é dada ao utilizador a opção de aceitar ou de recusar a utilização de *cookies*, não devendo ser admitidos mecanismos que induzam o utilizador a selecionar uma determinada opção. De acordo com Gray et al.[30], as técnicas utilizadas poderão consistir

[29] Conclusões do Advogado-Geral Szpunar no caso Planet49, de 21 de março de 2019, para. 66.

[30] Gray, Colin M.; Kou, Yubo; Battles, Bryan; Hoggatt, Joseph e Toombs, Austin L. "The Dark (Patterns) Side of UX Design" (Proceedings of the CHI Conference on Human Factors in Computing Systems ACM, New York, USA, 2018).

em "Falsa Hierarquia" ou em "Manipulação Estética": a "Falsa Hierarquia" espelha uma certa relação de ordenação (visual ou interativa) hierárquica entre uma ou mais opções por referência a outras; por sua vez, a "Manipulação Estética" incita o utilizador a clicar no botão "aceitar" em vez do botão "recusar". De notar que as orientações de algumas autoridades nacionais de proteção de dados reconhecem já a existência deste tipo de mecanismo. Neste sentido, a CNIL[31] designa estes mecanismos que chamam a atenção do utilizador para um determinado ponto do *website* para a desviar de outros pontos relevantes como "Desvio de Atenção". É o caso paradigmático da utilização de um botão verde na opção "Aceitar" ou "Continuar" e na utilização de cores cinzentas ou de tamanhos mais pequenos na opção "Configurações" ou "Ver Mais", levando o utilizador a, inadvertidamente, escolher aquela primeira por lhe parecer, em termos estéticos, preferível.

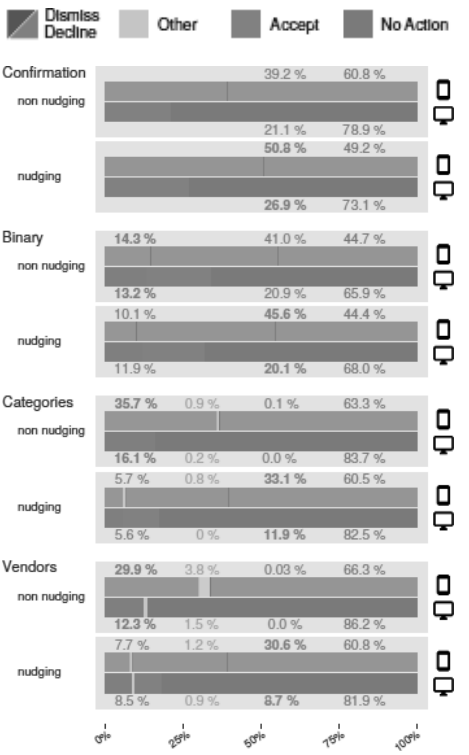
Um estudo igualmente levado a cabo por Utz et al.[32] relativamente a um *website* alemão tornou claro o forte impacto que o recurso a estes mecanismos manipuladores produz na escolha dos utilizadores. A título de exemplo, e com base no Gráfico 1 *infra*, a respeito das notificações que solicitaram apenas a confirmação da utilização de *cookies* em que se adotaram alguns dos referidos elementos de manipulação estética ("*nudging*"), verificou-se uma maior percentagem (50,8% no dispositivo móvel, 26,9% no computador) de utilizadores a clicar em "Aceitar". Em contraposição, apurou-se que, em relação a essas mesmas notificações, não havendo recurso a mecanismos de manipulação, a percentagem de utilizadores a clicar em "Aceitar" diminui, no dispositivo móvel, para 39,2% e, no computador, para 21,1%.

---

[31] CNIL. *Shaping Choices in the Digital World, From dark patterns to data protection: the influence of UX/UIdesign on user empowerment*, 2019, disponível em: <https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world>. pdf, consultado em 13 de novembro de 2020.

[32] Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

Gráfico 1 – Escolhas dos utilizadores relativamente à utilização de cookies num website alemão.



Fonte: Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

É, pois, indubitável que o destaque da cor do botão correspondente à aceitação da utilização de *cookies* e as demais técnicas utilizadas pelos operadores de *websites* suscitam algumas dúvidas quanto à prestação de um consentimento devido e totalmente esclarecido pelo utilizador.

No âmbito do artigo acima referido, e com base nos dados constantes da Tabela 1, os autores concluíram que a maioria das notificações de consentimento para a utilização e armazenamento de *cookies* são colocadas na parte inferior do ecrã (58%); não bloqueiam o acesso ao website (93%);

não oferecem outras opções para além de um botão de confirmação (68%); e tentam induzir os utilizadores a consentir na utilização de *cookies* (57%).

Ademais, verificaram que, quanto maior o número de opções oferecidas ao utilizador nas notificações de *cookies*, maior a probabilidade de que estes recusem a utilização de *cookies*.

Em suma, os autores concluem que se os operadores de *websites* cumprissem na íntegra os princípios de proteção de dados consagrados no RGPD e a exigência de um consentimento informado, prestado com base em informação explícita relativa às finalidades do tratamento de dados pessoais, menos de 0,1% dos utilizadores consentiriam na utilização de *cookies* de terceiros.

5. Regulamento *ePrivacy*: uma nova realidade?

A proposta de Regulamento *ePrivacy*[33], apresentada pela primeira vez em 2017, pretende substituir a atual Diretiva *ePrivacy*. Embora inicialmente estivesse programado que a entrada em vigor do Regulamento *ePrivacy* coincidisse com a do RGPD, cedo se percebeu que a divergência verificada entre as posições adotadas pelos Estados-Membros não permitiria dar cumprimento a essa expectativa.

Nesta senda, um relatório de progresso emitido pelo Conselho (doc. 14054/19 da Presidência finlandesa de 18 de Novembro de 2019[34]) esclareceu que o Regulamento continua a dividir os Estados-Membros, e que múltiplas alterações foram sugeridas e debatidas até agora, não tendo sido ainda encontrado um compromisso.

No dia 21 Fevereiro de 2020 foi publicada uma versão revista[35] do Regulamento *ePrivacy*, verificando-se uma alteração substancial a nível do regime aplicável à utilização de *cookies*.

---

[33] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações electrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações electrónicas).

[34] Documento do Conselho da União Europeia n.º 14054/19, de 18 de novembro de 2019, disponível em https://data.consilium.europa.eu/doc/document/ST-14068-2019-INIT/en/pdf, acedido a 14 de novembro de 2020.

[35] Documento do Conselho da União Europeia n.º 14068/19 + COR 1, de 21 de fevereiro de 2020, disponível em <https://data.consilium.europa.eu/doc/document/ST-5979-2020-INIT/en/pdf>, acedido a 14 de novembro de 2020.

Destarte, na sua versão inicial, o artigo 8.º da proposta de Regulamento *ePrivacy* estabelecia, como regime-regra, a proibição de utilização de *cookies*, exceto:

a. Se forem necessários exclusivamente para assegurar a transmissão de uma comunicação eletrónica através de uma rede de comunicações eletrónicas; ou
b. Se o utilizador final tiver dado o seu consentimento; ou
c. Se forem necessários para prestar um serviço solicitado pelo utilizador final; ou
d. Se forem necessários para a medição de audiência, desde que tal medição seja efetuada pelo prestador do serviço da sociedade de informação solicitado pelo utilizador final.

Ora, a versão revista vem introduzir as seguintes modificações:

1. A respeito dos *cookies* necessários para a medição de audiência, prevê-se que tal medição pode ser efetuada igualmente por terceiros, ou por terceiros conjuntamente, em nome de um ou mais fornecedores do serviço da sociedade da informação, desde que cumpridos os requisitos previstos no artigo 28º, ou do artigo 26.º, quando aplicável, do RGPD.
2. Foram acrescentados dois novos fundamentos que legitimam o armazenamento de *cookies*:

    a. comunicação de uma emergência;
    b. interesses legítimos prosseguidos por um prestador de serviços, excepto quando tal interesse seja anulado pelos interesses ou direitos e liberdades fundamentais do utilizador. A este respeito, considera-se que os interesses do utilizador final se sobrepõem aos interesses do prestador de serviços quando: i) o utilizador final é uma criança ou (ii) quando o prestador de serviços processa, armazena ou recolhe dados para determinar a natureza e as características do utilizador final ou para construir um perfil individual do utilizador final ou (iii) para o processamento, armazenamento ou recolha de dados subsumíveis a categorias especiais de dados pessoais, nos termos do nº 1 do artigo 9º do RGPD.

Em especial, relativamente ao consentimento, a proposta inicial do Regulamento *ePrivacy* previa já a aplicação das condições previstas no artigo 4.º, n.º 11, e no artigo 7.º do RGPD.

Contudo, e conforme fora reconhecido pelo Comité Europeu para a Proteção de Dados[36], "o conceito de consentimento, tal como utilizado na Diretiva 95/46/EC e na Diretiva *ePrivacy* até à data, tem evoluído" (tradução livre), sendo que "no que diz respeito à Diretiva *ePrivacy* em vigor, o Comité Europeu para a Proteção de Dados sublinha que as referências à Diretiva 95/46/CE, revogada, devem ser interpretadas como referências ao RGPD" (tradução livre), o que "também se aplica a referências ao consentimento na atual Diretiva 2002/58/CE (...)" (tradução livre).

Sucede que tal já resultava do próprio RGPD: o artigo 94.º prevê expressamente que as remissões para a diretiva revogada são consideradas remissões para o RGPD.

Neste sentido, ao consentimento para a utilização e armazenamento de *cookies* já eram aplicáveis, previamente à apresentação da proposta do Regulamento *ePrivacy*, os requisitos e exigências previstos no RGPD[37].

A este respeito, Degeling et al.[38] realizaram um estudo comparando a informação apresentada aos utilizadores de 6.500 websites da UE antes e depois da entrada em vigor do RGPD, tendo observado um aumento de 6% na adoção de notificações de *cookies* por parte dos *websites* analisados.

A verdade é que os requisitos concretamente aplicáveis ao consentimento e ao armazenamento de *cookies* não se encontram especificamente concretizados, não tendo ainda o TJUE tido oportunidade de explicitamente se pronunciar a respeito das muitas práticas que ainda são adotadas pelos operadores de *websites* e que suscitam dúvidas quanto à validade do consentimento prestado pelo utilizador.

---

[36] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679,* de 4 de maio de 2020, disponível em <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, acedido em 14 de novembro de 2020.

[37] Cumpre referir que, ao abrigo do disposto no n.º 11 do artigo 4.º do RGPD, consentimento é a "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento".

[38] Degeling, Martin; Utz, Christine; Lentzsch, Christopher; Hosseini, Henry; Schaub, Florian; e Holz, Thorsten, *We value your privacy ... now take some cookies: Measuring the GDPR's impact on web privacy, in* NDSS, 2019.

Conclusão

Em face do exposto, é manifesto que existe ainda um longo caminho a trilhar.

Ora, são vários os cenários em que resulta evidente que, em virtude da multiplicidade de técnicas utilizadas pelos operadores de *websites* – em muitos casos verdadeiramente manipuladoras –, o consentimento para o armazenamento de *cookies* não é totalmente livre, informado e esclarecido.

A título de exemplo, a mera remissão para uma Política de Privacidade ou para os Termos e Condições aplicáveis a determinado *website* não cumpre o requisito de fornecimento de informação, em linguagem clara e simples, compreensível a um utilizador normal.

Como vimos, também a indução do utilizador a autorizar a utilização ou armazenamento de *cookies* não consubstancia um consentimento totalmente livre e esclarecido. Em especial, é indubitável que a hierarquização e a distinção, designadamente com recurso a diferentes cores, entre as opções que correspondem à aceitação ou não da utilização de *cookies* produz um grande impacto na tomada de decisão (em muitos casos inconsciente) por parte dos utilizadores.

Ainda assim, têm sido dados passos relevantes nesta matéria, em especial com o reconhecimento de que as conhecidas *cookie walls* e as quadrículas de seleção pré-preenchidas não consubstanciam um consentimento válido à luz do RGPD, salvos os casos expressamente referidos *supra*.

Contudo, não existe uma forma legalmente prevista aplicável ao pedido de consentimento. O considerando 17 da Diretiva *ePrivacy* estabelece que o consentimento de um utilizador pode ser dado por qualquer método apropriado. Neste sentido, os operadores de *websites* são livres de utilizar ou desenvolver mecanismos de recolha de consentimento que se lhes afigurem mais apropriados, devendo, no entanto, observar um requisito: o consentimento tem de ser considerado válido ao abrigo da legislação da UE. O que, na verdade, tem sido pouco respeitado.

Indubitavelmente, muitas das práticas adotadas pelos operadores de *websites* suscitam dúvidas quanto à validade do consentimento prestado pelo utilizador à luz das regras impostas pelo RGPD.

Contudo, conforme as conclusões do estudo levado a cabo por Utz et al., *supra* citado, verificou-se que se os operadores de *websites* cumprissem

escrupulosamente os princípios e regras em matéria de proteção de dados consagrados no RGPD, menos de 0,1% dos utilizadores consentiriam a utilização de *cookies* de terceiros, o que, naturalmente, teria grande impacto na atividade destes terceiros, nomeadamente ao nível da publicidade e marketing digital e, em particular, dos mecanismos de *tracking*, *retargeting* e marketing de comportamento (*behavorial marketing*), os quais, hoje em dia, são da maior relevância para o sector de *e-commerce*.

Neste sentido, impõe-se estabelecer um equilíbrio (necessário) entre os princípios da proteção de dados pessoais e os interesses económicos das empresas, sob pena de que a excessiva proteção, quer de um, quer de outro, implique, *à la longue*, a limitação de outros direitos fundamentais. Aliás, a introdução dos interesses legítimos do prestador de serviços como fundamento para o armazenamento de *cookies* na nova versão do Regulamento *ePrivacy*, publicada no dia 21 de fevereiro de 2020, parece já caminhar nessa direção.