Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2022, n. 2

EDITORIALE SCIENTIFICA
ES

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2022, n. 2

Éditorial

Saggi e Articoli

Commenti e Note

IL PANOPTICON DIGITALE. I *COOKIES* TRA DIRITTO E PRATICA NELL'UNIONE EUROPEA

Flavia Zorzi Giustiniani*

"before cookies, the Web was essentially private. After cookies, the Web becomes a space capable of extraordinary monitoring."[1]

SOMMARIO: 1. Osservazioni preliminari. – 2. La disciplina dei *cookies* nel diritto dell'unione europea. – 3. *Cookies* e trasferimento dei dati personali al di fuori dell'Unione europea. – 4. Il nuovo regolamento *eprivacy*. – 5. Considerazioni conclusive.

1. Osservazioni preliminari

Al giorno d'oggi la tecnologia di tracciamento più utilizzata per raccogliere, elaborare e condividere i dati personali degli utenti finali su internet è indubbiamente costituita dai *cookies*. La gran parte delle società operanti nel mondo digitale analizza oramai i comportamenti dei propri utenti soprattutto grazie a tali strumenti.

I *cookies* consistono in microfile digitali che consentono di associare un dispositivo, come pure un indirizzo IP, alle scelte comportamentali di un determinato utente. Una siffatta associazione perdura fintantoché l'utente non elimina dalla cronologia i siti visitati e le opzioni di scelta relative alla registrazione di *cookies*. Le informazioni codificate nei *cookies* possono includere dati personali (un nome utente, un identificativo univoco, un indirizzo e-mail o un indirizzo IP) oppure dati non personali (quali ad esempio informazioni sul tipo di dispositivo utilizzato).

I *cookies* rientrano tra i cd. "identificatori attivi", i quali, attraverso strumenti azionabili autonomamente, permettono all'utente di rifiutare il proprio consenso al tracciamento come pure di procedere direttamente alla rimozione dei *cookies* archiviati

Articolo sottoposto a doppio referaggio anonimo.

* Associato di Diritto dell'Unione europea, Università Link Campus Roma. Indirizzo e-mail: f.zorzigiustiniani@unilink.it.

[1] Cfr. J. SCHWARTZ, *Giving the Web a Memory Cost Its Users Privacy*, in *New York Times*, 4 settembre 2001, disponibile al link http://www.nytimes.com/2001/09/04/technology/04Cook.html.

sul proprio dispositivo[2]. Gli identificatori "passivi", di converso, come ad esempio il *fingerprinting*, non implicando la memorizzazione di informazioni e/o l'accesso a queste sul dispositivo dell'utente, ma soltanto la lettura della sua configurazione, rimangono nella piena e sola disponibilità del titolare.

I *cookies* si suddividono in *cookies* proprietari o di prime parti, allorché sono installati, cancellati e modificati direttamente dal sito visitato, e *cookies* di terze parti, che sono invece creati da altri siti proprietari dei contenuti visualizzati nella pagina web del sito che si sta visitando. Sulla base delle funzioni svolte, i *cookies* sono poi distinti in tecnici, analitici e di profilazione. I *cookies* tecnici sono usati al fine di migliorare l'esperienza di navigazione in un sito *web* e consentire il pieno utilizzo di tutte le funzionalità del sito stesso (ad esempio per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazione di informazioni specifiche sugli utenti). I *cookies* analitici servono invece ai servizi *web* per raccogliere informazioni relative all'accesso degli utenti, quali il numero di visitatori su un sito web, la durata della loro permanenza sul sito e quali parti del sito visitano (cd. "*web audience measurement*").

Infine, i *cookies* di profilazione sono quelli utilizzati per monitorare e profilare gli utenti durante la navigazione, studiare i loro movimenti e abitudini di consultazione del web o di consumo, principalmente allo scopo di misurare l'efficacia del messaggio pubblicitario, nonché di conformare tipologia e modalità dei servizi resi ai comportamenti degli utenti oggetto di osservazione.

L'utilizzo dei *cookies* si deve generalmente a motivi commerciali, in particolare al fine di procedere alla profilazione degli internauti. L'attuale mondo digitale, dove l'*AdTech* (la tecnologia pubblicitaria) la fa da padrone, deve la sua origine in larga parte proprio allo sviluppo dei *cookies* nell'ormai lontano 1993[3] e al conseguente passaggio dalla pubblicità contestuale, che si basa sul contenuto del sito in cui compare l'annuncio, alla pubblicità comportamentale, basata invece sulla raccolta di dati, tramite *cookies*, dell'attività di navigazione di un computer-utente e del suo comportamento *online*, al fine di fornirgli annunci su misura basati sui suoi interessi.

Con l'eccezione dei *cookies* meramente tecnici, le altre tipologie di *cookies* sono suscettibili di avere un impatto significativo sulla riservatezza degli internauti. L'utilizzo di *cookies* potrebbe infatti rendere identificabili i singoli utenti anche mediante la raccolta di dati apparentemente anonimi come gli indirizzi IP.

Nel presente contributo ci si soffermerà anzitutto sull'attuale quadro giuridico che regola l'utilizzo dei *cookies* nell'Unione europea. Specifico approfondimento sarà di seguito dedicato alle problematiche concernenti il trasferimento dei dati personali

[2] Sulla differenza tra identificatori attivi e passivi v. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida cookie e altri strumenti di tracciamento*, 10 giugno 2021, p. 5.

[3] La tecnologia *cookie* fu sviluppata nel 1993 dall'ingegnere Lou Montulli per il consorzio Netscape. Sulle origini e lo sviluppo dei *cookies* si veda R.C. SHAH, J.P. KESAN, *Deconstructing Code*, in *Yale Journal of Law and Technology*, 2004, p. 278; L. EDWARDS, *Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling*, in L. EDWARDS (ed.), *Law, Policy and the Internet*, London, 2018, pp. 119, 126-7. "The cookies technology was the most innovative feature and one that would forever alter the web". (R.C. SHAH, J.P. KESAN, *Deconstructing Code*, cit., p. 298).

dall'Unione europea a Paesi terzi, e più in particolare agli Stati Uniti, giacché tali trasferimenti sono subordinati *inter alia* al rispetto delle norme europee relative all'uso dei *cookies*. Si valuterà poi il possibile impatto delle modifiche all'attuale disciplina dei *cookies* ora in discussione nel progetto di regolamento *ePrivacy*. Nel concludere si mostrerà, alla luce della prassi più recente, che il divario tuttora esistente tra normativa vigente e suo rispetto *effettivo* pare venir meno.

2. La disciplina dei *cookies* nel diritto dell'Unione europea

In materia di *cookies* l'ordinamento dell'Unione europea si conferma essere, almeno su di un piano formale, il più avanzato al mondo, ponendo una disciplina assai stringente e protettiva per gli utenti-internauti. Ad oggi lo strumento principale che regola l'utilizzo dei *cookies* è ancora la direttiva 2002/58/CE, relativa alla vita privata e alle comunicazioni elettroniche (cd. direttiva *ePrivacy*)[4], come emendata dalla direttiva 2009/136/CE[5]. Obiettivo generale della direttiva *ePrivacy* è quello di garantire la riservatezza delle comunicazioni di ordine elettronico. La relativa disciplina del trattamento di informazioni personali è imperniata sul principio del consenso informato, che l'utente deve prestare preliminarmente all'utilizzo da parte del gestore di un sito internet di *cookies* che consentano la memorizzazione e/o l'accesso a dati sul suo computer[6] (art. 5.3). L'unica eccezione alla regola del consenso concerne i *cookies* di carattere tecnico, ovvero quei *cookies* utilizzati "al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente"[7]. A seguito delle modifiche introdotte nel 2009, che si inseriscono nel più ampio quadro della riforma europea delle reti e dei servizi di comunicazione elettronica, in tema di *cookies* si è così effettuato il passaggio da un modello di *opt-out*, secondo il quale era sufficiente permettere all'utente di rifiutare l'installazione dei *cookies*, a un modello di *opt-in*, che richiede invece obbligatoriamente il consenso dell'utente per qualsiasi uso non strettamente connesso con il servizio reso.

Il principio del consenso quale presupposto del trattamento dei dati personali è stato poi disciplinato *ex novo*, in modo più dettagliato e rigoroso rispetto alla normativa

[4] Non a caso tale direttiva è definita anche «*cookie law*».

[5] Cfr. direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

[6] Cfr. art. 5.3 della direttiva *ePrivacy*.

[7] "Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato *sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento* in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento" (*ibid.*, corsivo nostro).

precedente, dal Regolamento generale per la protezione dei dati personali 2016/679 (cd. GDPR). Il consenso è ivi definito quale una manifestazione di volontà libera, specifica, informata[8] e inequivocabile dell'interessato[9]. Tale consenso al trattamento deve essere prestato per una o più finalità specifiche *ex* art. 6. Dovrebbe inoltre essere espresso "mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano"[10]. Il consenso così espresso è revocabile in qualsiasi momento[11]. Qualora poi "il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste"[12]. Tale disciplina si applica, per espressa previsione[13], anche con riguardo all'impiego dei *cookies*.

Di rilievo particolare per l'utilizzo dei *cookies* è poi il requisito di modalità trasparenti e sintetiche[14] per i *cookie banners*, ovvero gli avvisi che devono essere mostrati agli utenti al momento del primo accesso di un utente ad un sito internet al fine di informarlo della presenza di eventuali *cookies*, dei suoi diritti a riguardo e di chiederne il consenso all'installazione.

A dispetto della specificazione dei requisiti inerenti all'utilizzo dei *cookies* introdotti dal GDPR, la grande maggioranza dei titolari di trattamento online hanno continuato ad impiegare caselle di spunta preselezionate che, per impostazione predefinita, inducono gli utenti ad accettare sui propri dispositivi *cookies* di prime o di terze parti. Questa prassi è stata censurata dalla Corte di Giustizia, la quale nel caso *Planet49* ha affermato senza mezzi termini che l'unica forma di consenso valido per il trattamento dei dati dell'utente sia il consenso espresso, ovvero quello prestato in modo attivo e specifico[15]. La preselezione delle caselle per esprimere il consenso all'uso dei *cookies* è pertanto vietata. Gli utenti devono inoltre essere informati in merito alla durata dei *cookies* e alla eventualità che soggetti terzi accedano ai loro dati, giacché entrambi i profili costituiscono specifiche modalità di trattamento dei dati personali. L'insopprimibilità di un consenso attivo da parte dell'interessato è stata poi ribadita dai giudici di Lussemburgo nella causa *Orange România SA*[16].

---

[8] L'informativa che deve precedere il consenso è disciplinata dall'art. 13 del GDPR.
[9] Cfr. art. 4 del GDPR.
[10] *Sic* il considerando 32 del GDPR.
[11] Cfr. art. 7 del GDPR.
[12] Cfr. il considerando 32 del GDPR.
[13] *Ibid.*
[14] Cfr. art. 5.1 lett. a e art. 12 GDPR su informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato.
[15] Cfr. Corte di giustizia, sentenza del 1° ottobre 2019, *Bundesverband der Verbrauchenzentrale und Verbraucherverbände –Verbraucherzentrale Bundesverband eV c. Planet49*, causa C-673/17. In dottrina si vedano tra gli altri: K. WIEDEMANN, *The ECJ's Decision in ''Planet49'' (Case C-673/17): A Cookie Monster or Much Ado About Nothing?*, in *IIC - International Review of Intellectual Property and Competition Law,* n. 51, 2020, pp. 543-553; R. CABAZZI, *Utilizzo dei cookie e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di giustizia nel caso Planet49*, in *medialaws.eu*, 15 luglio 2020.
[16] Cfr. Corte di giustizia, sentenza dell'11 novembre 2020, *Orange România SA contro Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP),* causa C-61/19. In

3. *Cookies* e trasferimento dei dati personali al di fuori dell'Unione europea

Le problematiche connesse al rispetto della normativa europea sui *cookies* sono ancora maggiori allorché i dati personali sono trasferiti al di fuori dell'Unione europea. Se infatti il trasferimento dei dati personali oltre frontiera è essenziale per lo sviluppo degli scambi internazionali[17] e tali flussi costituiscono la componente del commercio in maggior crescita nella UE (come pure negli USA), la circostanza che la normativa europea in materia ponga gli standard più elevati al mondo determina il rischio di un approccio puramente formalistico alla *compliance* da parte dell'Unione stessa[18].

La Commissione europea, peraltro, già nel 1998 aveva ricompreso, fra le categorie di trasferimenti che rappresentano una minaccia particolare per la vita privata e meritano quindi particolare attenzione, quelli "che comportano la raccolta di dati per mezzo di nuove tecnologie secondo modalità particolarmente occulte o clandestine (per es. i cosiddetti "cookies" di Internet)"[19].

Il trasferimento di dati personali verso Paesi terzi rispetto allo Spazio Economico Europeo (SEE) o organizzazioni internazionali è regolato dal capo V del GDPR (artt. 44-50)[20], nel quale si richiede l'adozione di meccanismi *ad hoc* atti a garantire che dopo il trasferimento sia stabilito un livello di protezione adeguato. Nel suddetto contesto normativo, specifico e imponente rilievo ha assunto la questione del trasferimento di dati verso entità giuridiche stabilite negli Stati Uniti, e ciò sia per la mole dei flussi che per il livello di tutela, nettamente inferiore a quello garantito nella UE, di cui gode la riservatezza nell'ordinamento statunitense[21]. Com'è noto, il tema è stato oggetto di due successivi accordi tra USA e UE, il *Safe Harbor* e il *Privacy Shield*, le cui relative decisioni di adeguatezza della Commissione sono state dichiarate invalide dalla Corte di giustizia europea nella cosiddetta saga *Schrems*[22]. Nella seconda pronuncia (cd. *Schrems*

---

questo caso la Corte ha ritenuto che la semplice mancata spunta di una casella precompilata non costituisce un'attività idonea a rappresentare un consenso legittimamente prestato ai sensi della normativa europea.

[17] Come già si riconosceva nella direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (cfr. considerando preambolare 56).

[18] Come già osservato, tra gli altri, da C. CELLERINO, *Trasferimenti internazionali di dati personali e clausole contrattuali tipo dopo Schrems II*, in *Il diritto dell'Unione europea*, 2021, n. 2, p. 361.

[19] Cfr. Commissione europea, Gruppo di lavoro "Tutela delle persone fisiche con riguardo al trattamento dei dati personali" DG XV D/5025/98 WP 12.

[20] V. anche il considerando 101 del GDPR.

[21] Invero, l'unica normativa in materia di protezione dei dati personali online di tenore in qualche misura analogo al GDPR è rinvenibile nello Stato della California, dove dal 1° gennaio 2020 è in vigore il *California Consumer Privacy Act*. Sulla diversa concezione della riservatezza e del trattamento dei dati personali nei due continenti si veda J.Q. WHITMAN, *The two Western cultures of privacy: dignity versus liberty,* in *Yale Law Journal*, 2004, p. 1151 ss.

[22] Preme sottolineare che, da un punto di vista giuridico, né il *Safe Harbour* né il *Privacy Shield* sono qualificabili come accordi internazionali, e invero in nessuno dei due casi si è fatto ricorso all'apposita e complessa procedura prevista dal TFUE per la conclusione degli accordi internazionali tra l'Unione e i Paesi terzi agli artt. 218, 219 e 207 del TFUE. "Essi rimangono, dunque, in entrambi i casi atti secondari dell'Unione vincolanti per gli Stati membri (o persone fisiche e giuridiche degli Stati membri), con una (ovvia) scarsa incidenza all'esterno, verso i Paesi terzi" (cfr. F. BORGIA, *Profili critici in materia di*

II)[23], in particolare, la Corte ha dichiarato la decisione di esecuzione (UE) 2016/1250 (cd. decisione *Privacy Shield*[24]) incompatibile con il GDPR, letto alla luce degli articoli 7, 8 e 52 della Carta dei Diritti Fondamentali, per mancato rispetto del principio di proporzionalità. I giudici di Lussemburgo hanno infatti rilevato che siffatta decisione della Commissione, come la precedente (2000/520, che consentiva il trasferimento dei dati tra UE e USA sulla base dei *Safe Harbour Principles*[25]), sancisse il primato delle esigenze di sicurezza nazionale rispetto ai principi stabiliti dal *Privacy Shield* e posti a tutela dei diritti fondamentali delle persone i cui dati personali erano trasferiti, senza prevedere alcun limite né garanzie di tutela per gli interessati.

Venuta così meno la base giuridica costituita dalla decisione di adeguatezza della Commissione, gli esportatori di dati personali hanno dovuto ricorrere in via principale ed

trasferimento dei dati personali verso i Paesi extra-europei, in *Diritto Mercato Tecnologia*, Numero speciale 2017, p. 140).

[23] Corte di giustizia, Grande Sezione, sentenza del 16 luglio 2020, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems*, causa C-311/18. Sul caso *Schrems II* cfr., *inter alia*: G. CAGGIANO, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza Schrems II della Corte di giustizia*, in *Studi sull'integrazione europea*, 2020, p. 563 ss.; F. CALOPRISCO, *La Corte di giustizia nega per la seconda volta la legittimità del trasferimento dei dati personali dall'Unione europea agli Stati Uniti senza una protezione "sostanzialmente equivalente" (Schrems II)*, in *Eurojus*, 1/2021, disponibile al link http://rivista.eurojus.it/wp-content/uploads/pdf/Articolo-Caloprisco-per-pubblicazione-def.pdf; A. CHANDER, *Is Data Localization a Solution for Schrems II?*, in *Journal of International Economic Law*, 2020, n. 23, p. 771ss.; T. CHRISTAKIS, *After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, in *Europeanlawblog.eu*, 21 luglio 2020; J.X. DHONT, *Schrems II. The EU adequacy regime in existential crisis?*, in *Maastricht Journal of European and Comparative Law*, 2019, n. 5, p. 597 ss.; E. FLETT, J. WILSON, J. CLOVER, *Schrems Strikes Again: EU-US Privacy Shield Suffers Same Fate as Its Predecessor*, in *Computer and Telecommunication Law Review*, 2020, n. 6, p. 161 ss.; C. GENTILE, *La saga Schrems e la tutela dei diritti fondamentali*, in *Federalismi.it*, 13.01.2021, pp. 35-56; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 2020, p. 733 ss.; I. OLDANI, *The future of data transfer rules in the aftermath of Schrems II*, in *SIDIBlog*, 23 ottobre 2020; C. PERARO, *Protezione extraterritoriale dei diritti: il trasferimento dei dati personali dall'unione Europea verso Paesi terzi*, in *Ordine internazionale e diritti umani*, 2021, p. 666 ss., disponibile al link https://aisberg.unibg.it/retrieve/handle/10446/187922/433697/7_Peraro_OIDU%202021%20n.%203_Protezione%20extraterritoriale.pdf; F. ROSSI DAL POZZO, *L'Accordo Privacy Shield non è un vero scudo per la privacy: scenari passati e futuri in merito a trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti*, in *Rivista di diritto internazionale*, 2020, p. 1112 ss.; D. SIMON, *Coup de tonnerre dans le monde du numérique*, in *Europe*, 2020, n. 8-9, p. 5 ss.; X. TRACOL, *"Schrems II": The return of the Privacy Shield*, in *Computer Law & Security Review*, 2020, n. 39, p. 1 ss.; W.G. VOSS, *Cross-Border Data Flows, the GDPR, and Data Governance*, in *Washington International Law Journal*, 2020, n. 3, p. 485 ss. Si veda anche COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner c.Facebook Ireland Ltde Maximillian Schrems, 23 luglio 2020, reperibili al link https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_it.

[24] Cfr. Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy [notificata con il numero C(2016) 4176], in GUUE, L 207 del 1° agosto 2016, p. 1ss.

[25] Cfr. Decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti [notificata con il numero C(2000) 2441], in GUCE, L 215 del 25 agosto 2000, p. 7 ss.

esclusiva agli altri strumenti giuridici previsti dal GDPR agli articoli 46 e seguenti. Si tratta anzitutto delle deroghe *ex* art. 49, la cui applicabilità è tuttavia meramente residuale[26] e soggetta a molteplici condizioni[27]. Un'alternativa percorribile, ai sensi del GDPR, è poi offerta dalle Clausole Contrattuali Tipo e dalle Norme Vincolanti di Impresa. Nondimeno, entrambe le tipologie di norme, come puntualizzato dal Comitato Europeo di Protezione dei Dati, possono costituire una valida base giuridica soltanto sulla base dell'esito di una valutazione condotta caso per caso dall'esportatore "tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili". In assenza di una valida decisione di adeguatezza non è tuttavia chiaro come per la Corte uno strumento privatistico, quali indubbiamente sono le misure supplementari, non vincolando lo Stato di destinazione possa garantire una protezione adeguata ai sensi del GDPR[28]. Così argomentando, peraltro, la Corte di giustizia ha posto in capo a privati, nella specie gli operatori del mercato digitale dei dati, rilevanti e onerose responsabilità. Per quanto qui ci occupa, uno degli effetti dirompenti della pronuncia è stato poi quello di condurre, su iniziativa dell'organizzazione non governativa *None of Your Business* ("NOYB") dell'attivista austriaco Max Schrems, alcune autorità di controllo nazionali dei dati ad affermare la contrarietà al GDPR del trasferimento dei dati personali effettuato mediante il *cookie Google Analytics*[29].

La prima a pronunciarsi al riguardo è stata l'autorità di protezione dei dati austriaca (*Datenschutzbehörde* o DSB), che in una decisione pubblicata il 13 gennaio 2022[30] ha asserito che *Google Analytics* trasmette dati personali, riferibili a interessati identificati o "identificabili" ai sensi dell'art. 4.1 del GDPR, quali *inter alia* gli identificatori univoci, gli indirizzi IP e i parametri del *browser*. Il Garante austriaco ha inoltre concluso che né le clausole contrattuali standard né le misure supplementari previste offrivano un livello di protezione sufficiente in questo caso perché i dati archiviati da *Google*, malgrado l'utilizzo di tecnologie di crittografia, sono soggetti a sorveglianza da parte delle agenzie di *intelligence* statunitensi. In base alla sezione 702 del *Foreign Intelligence Surveillance Act*, infatti, *Google* è tenuto a concedere l'accesso o rilasciare i dati importati che sono in suo possesso, custodia o controllo e tale obbligo può applicarsi espressamente anche alla chiave crittografica senza la quale tali dati non possono essere letti. Lo strumento *Google Analytics* (almeno nella versione del 14 agosto 2020) non è pertanto conforme a quanto richiesto dal Capo V del GDPR poiché non garantisce un livello adeguato di protezione dei dati trasmessi ex art. 44 dello stesso Regolamento. Il 10 febbraio scorso una decisione analoga è stata resa dall'omologa autorità francese, la *Commission nationale de*

[26] Come ribadito dal Comitato europeo di protezione dei dati nelle relative Linee Guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, 25 maggio 2018.
[27] Cfr. art. 49.1 GDPR.
[28] Cfr. R.A. COSTELLO, *Schrems II: Everything Is Illuminated?*, in *European Papers*, Vol. 5, 2020 n. 2, p. 1054.
[29] Come la più ampia categoria dei *cookies* analitici, *Google Analytics* consente di osservare, in tempo reale, i movimenti degli utenti su un dato sito web. Dal punto di vista tecnico, *Google Analytics* opera attraverso *tags JavaScript* che vengono eseguiti nel codice sorgente del sito e che impostano sui *browser cookies* per raccogliere ed elaborare dati personali, talvolta anche sensibili.
[30] Cfr. https://noyb.eu/sites/default/files/2022-01/E-DSB%20%20Google%20Analytics_EN_bk.pdf.

l'informatique et des libertés (CNIL). Anche secondo la CNIL le misure supplementari adottate da Google "ne suffisent pas à exclure la possibilité d'accès des services de renseignements américains à ces données"[31]. La CNIL ha pertanto dichiarato l'illegalità di *Google Analytics* per violazione del GDPR.

In senso conforme si era espresso, il 5 gennaio, il Garante europeo per la protezione dei dati, che aveva censurato il Parlamento europeo per aver permesso a *Google Analytics* e alla piattaforma di pagamento *Stripe*, tramite un portale web dedicato ai test Covid dei parlamentari stessi, il trasferimento dei dati dei suoi dipendenti agli Stati Uniti, in contrasto con quanto richiesto dal regolamento 2018/1725[32] (che costituisce l'equivalente del GDPR per le istituzioni europee).

In risposta alle censure mossegli, Google ha annunciato nel marzo scorso il lancio di *Google Analytics 4*. Rispetto alle versioni precedenti, il nuovo sistema non farà uso della registrazione e della memorizzazione delle informazioni sull'indirizzo IP degli utenti europei come meccanismo per il monitoraggio e l'analisi, limitando così i possibili trasferimenti di dati connessi ad un uso siffatto[33].

Ancora più significativo, per l'impatto sistemico che dovrebbe generare in tema di trasferimento dei dati personali dall'Unione europea agli USA, è il cosiddetto *Trans-Atlantic Data Privacy Framework* ('TADPF'), un accordo "di principio" raggiunto tra i due Paesi e annunciato il 25 marzo, il cui scopo è quello di regolare la cooperazione tra USA e UE nelle operazioni sui dati personali che prevedono il trasferimento degli stessi tra le due parti. Giunto dopo più di un anno di trattative l'accordo, nelle parole della Presidente della Commissione Ursula Von Der Leyen, consentirà "predictable and trustworthy data flows" tra l'Unione e gli Stati Uniti sulla base di un nuovo bilanciamento tra sicurezza e diritti alla privacy e alla protezione dei dati personali[34].

Il *Trans-Atlantic Data Privacy Framework* prevede che i dati potranno fluire liberamente e in sicurezza tra le aziende partecipanti dell'Unione europea e degli Stati Uniti, sulla base di nuove regole che limiteranno l'accesso ai dati da parte dell'*intelligence* statunitense ai soli casi in cui l'accesso si riveli necessario e proporzionato al fine di proteggere la sicurezza nazionale[35]. Le agenzie di *intelligence* saranno chiamate ad adottare procedure per garantire un controllo efficace della privacy e il rispetto delle

[31] Cfr. CNIL, Mise en demeure anonymisée – Google analytics, 10 febbraio 2022, disponibile al link https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf.
[32] Cfr. Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (Testo rilevante ai fini del SEE).
[33] Cfr. https://blog.google/products/marketingplatform/analytics/prepare-for-future-with-google-analytics-4/.
[34] Cfr. Commissione europea, Statement by President von der Leyen with US President Biden, Bruxelles, 25 marzo 2022, p. 1.
[35] I principi cardine dell'accordo di principio sono stati resi pubblici sia dalla Commissione europea (si veda https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087) sia, in modo invero più dettagliato, dalla Casa Bianca (https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/).

norme sulle libertà civili. Le aziende americane che trattano dati personali provenienti dalla UE dovranno invece autocertificare la propria adesione ai principi del *Privacy Shield* attraverso il Dipartimento del Commercio statunitense[36]. È poi prevista la creazione, da parte statunitense, di un meccanismo di ricorso multi-livello che includa un tribunale di revisione della protezione dei dati indipendente al quale potranno rivolgersi i residenti della UE.

Il TADPF non è ancora operativo e per divenire tale il suo contenuto dovrà essere riprodotto e precisato in atti giuridici. Da parte statunitense ciò avverrà allorché gli impegni assunti prenderanno la forma di un atto interno, ovvero più specificamente, come annunciato dalla Casa Bianca, di un decreto esecutivo (*executive order*). Successivamente, e in base al contenuto di tale atto statunitense, la Commissione europea adotterà poi una nuova decisione di adeguatezza che diventerà la base giuridica per il trasferimento dei dati verso gli USA. Solo al termine di tale processo, che probabilmente richiederà diversi mesi, sarà possibile valutare appieno la portata delle modifiche introdotte al *Privacy Shield*. Si deve tuttavia rimarcare che, al fine di colmare le patenti inadeguatezze del quadro normativo statunitense in materia di tutela della vita privata, recentemente evidenziate dalla sentenza della Corte Suprema nel caso *FBI v. Fazaga*[37], che ha confermato lo *state secrets privilege*, l'*executive order* non appare uno strumento idoneo. Per evitare l'ennesima declaratoria di invalidità da parte della Corte di Lussemburgo sarebbe invero necessario che il Congresso procedesse per via legislativa ad una più ampia ed organica riforma del settore[38].

4. Il nuovo regolamento *ePrivacy*

La disciplina dei *cookies* è oggetto del nuovo progetto di regolamento *ePrivacy*, che ha lo scopo di disciplinare il trattamento dei dati di comunicazione elettronica che si verifica durante la fornitura e l'utilizzo di servizi di *e-communication* in modo uniforme in tutti gli Stati membri dell'Unione e, una volta approvato, sostituirà l'oramai risalente direttiva *ePrivacy*. A differenza dell'attuale direttiva, che non si applica ai servizi di comunicazione elettronica offerti da fornitori che operano su internet, la proposta di

[36] Va sottolineato che la Corte di giustizia non ha invalidato il *Privacy Shield* bensí la relativa decisione di adeguatezza della Commissione. Ne consegue che, nella misura in cui non saranno modificati dalla normativa di attuazione del nuovo *Privacy Framework*, i principi affermati nel *Privacy Shield* rimangono validi.

[37] Cfr. Corte Suprema degli Stati Uniti d'America, *Federal Bureau of Investigation et al. v. Fazaga et al. Certiorari to the United States Court of Appeals for the Ninth Circuit*, 4 marzo 2022.

[38] In materia di *privacy* e protezione dei dati personali negli Stati Uniti non vi è una normativa unica e onnicomprensiva a livello federale che sia comparabile al GDPR, bensí varie leggi federali di settore (quali ad esempio il Financial Services Modernisation Act del 1999, l'Health Insurance Portability and Accountability Act del 1996 e il Children's Online Privacy Protection Act del 1998) e alcune leggi statali (cfr. D. MANFREDA, *GDPR and Data Transfer: Focusing on Data Flow Between the EU and USA Before and After the Schrems II Decision*, European Union Law Working Papers No. 62, 2022, p. 15, che rileva: "USA is unique among the world's leading countries in that it lacks an umbrella privacy legislation and a governmental authority, who would be responsible for protecting privacy of personal information").

regolamento è applicabile a tutte le tipologie di titolari di trattamento, estendendo così il campo di applicazione ai servizi equivalenti dal punto di vista funzionale, compresi i cosiddetti servizi "Over-the-Top" (OTT)[39].

La prima bozza del Regolamento era stata proposta dalla Commissione nel gennaio 2017[40], ed invero tale atto sarebbe dovuto entrare in vigore in concomitanza con il GDPR nel maggio 2018. I negoziati si sono tuttavia rivelati più difficili del previsto e le *Big Tech* hanno portato avanti sin dall'inizio un'intensa attività di *lobby* al fine di indebolire le parti del testo più innovative in quanto orientate ad una maggiore tutela dell'utente finale[41]. Ciò spiega perché si sia giunti ad un accordo all'interno del Consiglio, con conseguente differimento dell'avvio dei triloghi interistituzionali, soltanto nel febbraio 2021[42].

Tra le novità di rilievo, nel testo del nuovo strumento in discussione, si segnala l'applicabilità non solo ai *cookies* ma anche ad altri identificatori assimilabili. Gli utilizzatori potranno pertanto limitare l'intero complesso di siffatti identificatori mediante le impostazioni del programma di navigazione (*browser*).

Le disposizioni relative ai *cookies* hanno rappresentato sinora uno dei punti di maggior attrito. Una lunga discussione si è avuta, in particolare, sull'individuazione delle condizioni di liceità al trattamento dei dati tramite *cookies* oltre al consenso. Il ricorso ai *cookies* è invero proibito salvo che ricorra una delle eccezioni specificamente elencate all'art. 8. Tra le tipologie di *cookies* che non richiedono il consenso dell'utente finale figurano quelli (di prima parte) che sono tecnicamente necessari al solo scopo di produrre statistiche aggregate, di fornire un servizio specificamente richiesto dall'utente finale o ancora di fornire un servizio di comunicazione elettronica. È previsto, infine, che agli utenti che hanno prestato il proprio consenso al trattamento dei dati debba essere ricordata la possibilità di ritirare il consenso a intervalli periodici non maggiori di dodici mesi finché dura il trattamento.

La bozza concordata in seno al Consiglio sembrerebbe poi legittimare l'uso dei cosiddetti *cookie walls*. Con detta espressione ci si riferisce tipicamente a quei meccanismi vincolanti (cd. "*take it or leave it*") tramite i quali l'utente viene obbligato, senza alternativa, ad esprimere il proprio consenso alla ricezione di *cookies* ovvero altri

[39] Per servizi OTT si intendono contenuti e applicazioni di tipo "*rich media*", ovvero forme di comunicazione online che utilizzano elementi multimediali interattivi.
[40] Cfr. Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), Bruxelles, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).
[41] In un promemoria preparato da Google in vista di un incontro con Facebook, Apple e Microsoft si riportava che "[Google has] been successful in slowing down and delaying the [ePrivacy Regulation] process and have been working behind the scenes hand in hand with the other companies]" (cfr. https://videoweek.com/2022/03/29/can-eprivacy-come-back-from-the-dead/).
[42] Cfr. Consiglio dell'Unione europea, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)-Mandate for negotiations with EP, Brussels, 10 February 2021 (OR. en) 6087/21.

strumenti di tracciamento, pena l'impossibilità di accedere al sito[43]. Sulla base della considerazione che il consenso che deve essere ottenuto nel quadro del regolamento *ePrivacy* ha lo stesso significato di quello disciplinato dal GDPR, e pertanto deve tra l'altro essere liberamente espresso, il Comitato europeo per la protezione dei dati aveva considerato i *cookie walls* incompatibili con la normativa europea[44]. Nella formulazione con la quale sono stati recepiti nel testo dal Consiglio, tuttavia, i *cookie walls* – ammesso che sia corretto qualificare in tal modo la relativa opzione di cui possono avvalersi i fornitori[45] – appaiono conformi ai requisiti posti dal GDPR in tema di consenso. Tali strumenti sono infatti consentiti a condizione che l'utente abbia una facoltà di scelta effettiva, ovvero che possa scegliere tra diversi servizi sulla base di informazioni chiare, precise e di facile utilizzo circa le finalità dei *cookies* o di tecnologie similari. I servizi alternativi includono, ad esempio, una versione a pagamento senza *cookies* dello stesso fornitore o un servizio comparabile senza *cookies* di un altro fornitore.

Il consenso ai *cookies* può essere accordato anche tramite le impostazioni del programma di navigazione (ad es. utilizzando una *whitelist* configurabile per uno o più fornitori[46]). Tuttavia, il consenso dichiarato direttamente dall'utente finale prevale sempre su quello espresso tramite le impostazioni del *browser*. Al riguardo si segnala un passo indietro rispetto a quanto proposto originariamente dalla Commissione. Nella prima bozza del Regolamento *ePrivacy* si prevedeva infatti, conformemente al principio della *privacy by design*[47], che le impostazioni predefinite del *browser* fossero generalmente posizionate sul massimo livello di riservatezza con il risultato di escludere automaticamente i *cookies* di terze parti[48].

Strettamente legato ai *cookies* è poi il trattamento dei metadati relativi alle comunicazioni elettroniche. I metadati, ovvero i "dati sui dati", sono quei dati, quali ad esempio informazioni sul luogo, sull'ora e sul destinatario della comunicazione, che possono essere derivati dall'uso di altri dati che ne rappresentano il contenuto

[43] Si veda la definizione fornita dalle Linee guida cookie e altri strumenti di tracciamento del Garante italiano per la protezione dei dati personali, pubblicate il 10 giugno 2021 (v. p. 8).
[44] Secondo l'opinione espressa dal Comitato europeo il 25 maggio 2018 (cfr. Dichiarazione del Comitato europeo per la protezione dei dati sulla revisione del regolamento *ePrivacy* e sul suo impatto sulla tutela delle persone fisiche in relazione alla privacy e alla riservatezza delle loro comunicazioni, p. 3), "la necessità di ottenere un consenso espresso liberamente impedirà ai fornitori di servizi di imporre ai loro utenti cookie wall". Un'opinione di massima contraria ai *cookie walls* è stata espressa anche dal Garante italiano, che li ha ritenuti in contrasto con il requisito della "libertà" del consenso ex art. 4.11 GDPR facendo salva tuttavia "l'ipotesi da verificare caso per caso nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di cookie o altri strumenti di tracciamento" (cfr. Linee guida cookie cit., p. 9).
[45] Cfr. cons. preambolare 20(aaaa) del testo come approvato dal Consiglio nel febbraio 2021.
[46] Cfr. cons. preambolare 20(a) del testo come approvato dal Consiglio nel febbraio 2021.
[47] Tale principio è accolto dal GDPR all'art. 25.2, laddove si dispone che "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità …".
[48] 20(a). Si tratta com'è noto della categoria di *cookies* che, raccogliendo informazioni sulla navigazione connesse agli utenti su siti web distinti, comportano maggiori rischi per la riservatezza.

principale[49]. Tra le ipotesi predefinite e tassative che consentono il trattamento dei dati delle comunicazioni elettroniche in assenza del consenso, quelle che allo stato attuale riguardano i metadati appaiono troppo indeterminate e generiche[50]. A fronte di tale indeterminatezza vi è dunque il rischio concreto di un abbassamento del livello di protezione dei dati attualmente garantito dalla direttiva *ePrivacy*[51].

5. Considerazioni conclusive

Nel dicembre scorso la CNIL francese ha sanzionato, con due provvedimenti gemelli, sia Google (comprensivo del sito YouTube) che Facebook per condotte similari, consistenti in violazioni della normativa europea sui *cookies*[52]. La multa comminata ai due colossi digitali ammonta rispettivamente a 150 milioni di euro per quanto concerne Google (90 milioni per Google Llc e 60 milioni per Google Ireland Limited) e 60 milioni di euro per Facebook.

La CNIL ha riscontrato che i *cookie banners* presenti sui siti di Google, Facebook e YouTube, prevedendo un solo click per accettare e ben cinque per rifiutare, sono congegnati in modo tale da indurre gli internauti ad accettare i marcatori senza una chiara cognizione delle implicazioni connesse a tale scelta. Ne consegue, secondo il garante d'oltralpe, che le suddette società e i relativi *banners*, pur permettendo di scegliere tra l'accettazione e il rifiuto dei *cookies*, nondimeno utilizzano delle modalità "par lesquelles

[49] Cfr. C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Bologna, 2015, p. 28 ss.

[50] L'art. 6b prevede attualmente il trattamento dei metadati allorché: (a) it is necessary for the purposes of network management or network optimisation, or to meet technical quality of service requirements pursuant to Directive (EU) 2018/1972 or Regulation (EU) 2015/212020; or (b) it is necessary for the performance of an electronic communications service contract to which the end-user is party, or if necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or (c) the end-user concerned has given consent to the processing of communications metadata for one or more specified purposes; or (d) it is necessary in order to protect the vital interest of a natural person; or (e) in relation to metadata that constitute location data, it is necessary for scientific or historical research purposes or statistical purposes […] (pp. 54-55).

[51] Al riguardo lo stesso Comitato europeo per la protezione dei dati aveva espresso preoccupazione: "l'approccio della proposta di regolamento […] prevede ampi divieti, eccezioni limitate e il ricorso al consenso. Di conseguenza, il regolamento ePrivacy non dovrebbe prevedere la possibilità di trattare i contenuti e i metadati delle comunicazioni elettroniche sulla base di presupposti giuridici meno stringenti, quali ad esempio i cosiddetti "legittimi interessi", che vanno al di là di quanto necessario per la fornitura di un servizio di comunicazione elettronica. Il regolamento ePrivacy non dovrebbe altresì consentire di trattare imetadati delle comunicazioni elettroniche per l'esecuzione di un contratto, il che significa che non dovrebbero essere previste eccezioni basate sul fine generico dell'esecuzione di un contratto, in quanto il regolamento stabilisce quale trattamento specifico è legittimo a tal fine, ad esempio quello a fini di fatturazione" (EUROPEAN DATA PROTECTION BOARD, Dichiarazione del Comitato europeo per la protezione dei dati sulla revisione del regolamento ePrivacy e sul suo impatto sulla tutela delle persone fisiche in relazione alla privacy e alla riservatezza delle loro comunicazioni, 25 maggio 2018, p. 2).

[52] Cfr. CNIL, Délibération de la formation restreinte n° SAN-2021-023 du 31 décembre 2021 concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED, pubblicato il 6 gennaio 2022, disponibile al link https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840062; ID., Délibération de la formation restreinte n°SAN-2021-024 du 31décembre 2021 concernant la société FACEBOOK IRELAND LIMITED, pubblicato il 6 gennaio 2022, disponibile al link https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532.

ce refus peut être exprimé […] [qui] biaise l'expression du choix en faveur du consentement de façon à altérer la liberté de choix"[53].

Le condotte censurate sono qualificabili come "*dark patterns*" (modelli oscuri), ovvero interfacce orientate a indirizzare gli utenti, sfruttando i loro pregiudizi cognitivi, verso la soluzione più favorevole al titolare di un servizio online[54]. I molteplici studi effettuati sul tema riportano conclusioni analoghe su due punti principali: 1) solo una piccola minoranza degli internauti di fronte a *cookie banners* con *dark patterns* arriva al secondo livello per negare il proprio consenso; 2) la situazione è rimasta pressoché immutata nel tempo, a seguito dell'entrata in vigore del GDPR[55].

Il primo punto, ben riassunto dall'espressione *consent fatigue*, è il risultato, da un lato, dell'esigenza, considerata insopprimibile dalla maggioranza degli internauti, di poter procedere ad una navigazione rapida e senza intralci, e dall'altro, delle false percezioni – indotte in larga dai *dark patterns* che ancora caratterizzano molti *cookie banners* – circa le conseguenze di un mancato consenso ai *cookies.* Il nuovo regolamento *ePrivacy* auspicabilmente dovrebbe ridurre la quantità di notifiche a cui gli utenti sono esposti, anzitutto eliminando la necessità del consenso per i *cookies* necessari o innocui[56]. La previsione di *whitelists*, non obbligatorie, dovrebbe egualmente ridurre la *consent fatigue*.

---

[53] *Ibid.*, par. 135.

[54] Sui *dark patterns* si veda *inter alia*: H. BRIGNULL, *What are Dark Patterns?*, 2018, disponibile al link https://darkpatterns.org; C. M. GRAY, Y. KOU, B. BATTLES, J. HOGGATT, A.L. TOOMBS, *The Dark (Patterns) Side of UX Design (Proceedings of the CHI Conference on Human Factors in Computing Systems ACM, New York, USA, 2018)*; CNIL"s 6th Innovation and Foresight Report "Shaping Choices in the Digital World, "From dark patterns to data protection: the influence of UX/UI design on user empowerment", 2019, disponibile al link https://linc.cnil.fr/fr/ip-report-shaping-choices-digital-world; M. NOUWENS, I. LICCARDI, M. VEALE, D. KARGER, L. KAGAL, *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, in Proceedings of CHI '20 CHI Conference on Human Factors in Computing Systems, April 25-30, 2020, Honolulu, HI, USA, disponibile al link https://arxiv.org/abs/2001.02479; T.H. SOE, O.E. NORDBERG, F. GURIBYE, M. SLAVKOVIK, *Circumvention by design - dark patterns in cookie consents foronline news outlets*, giugno 2020, disponibile al link https://arxiv.org/abs/2006.13985v1. V. anche EDPB, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, Version 1.0*, 14 marzo 2022.

[55] Si vedano tra gli altri gli studi di: C. UTZ, M. DEGELING, S. FAHL, F. SCHAUB, A. ARBOR, T. HOLZ, *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, 019 ACM SIGSAC Conference on Computer and Communications Security (CCS'19), November 11–15, 2019, London, United Kingdom.ACM, New York, NY, USA, https://doi.org/10.1145/3319535.3354212; C. SANTOS, N. BIELOVA, C. MATTE, *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, Tilburg University, 2020, pp. 91-135; D. BOLLINGER, K. KUBICEK, C. COTRINI, D. BASIN, *Automating Cookie Consent and GDPR Violation Detection*, ETH Zurich, 2021, disponibile al link https://karelkubicek.github.io/assets/pdf/Automating_Cookie_Consent_and_GDPR_Violation_Detection.pdf; F. LANCIERI, Narrowing Data Protection's Enforcement Gap, in Maine Law Review, Vol. 74 n. 1, gennaio 2022.

[56] Come avvertiva la Commissione nel presentare la proposta di regolamento, «[l]a norma sul consenso è sovrabbondante, poiché riguarda anche le pratiche non lesive della vita privata» (cfr. Cfr. Commissione europea, Proposta di Regolamento cit., p. 6). In senso conforme, anche gli autori dello studio Dark and bright patterns in cookie consent requests (P. GRAßL, H. SCHRAFFENBERGER, FR. ZUIDERVEEN BORGESIUS, M. BUIJZEN, in *Journal of Digital Social Research*, Vol. 3, n. 1, 2021, p. 28) ritengono che "the upcoming ePrivacy Regulation of the EU should limit the number of cookie consent requests peopleare confronted with".

Quanto al secondo punto, ovvero l'assenza di reali modifiche nel comportamento di molti titolari a dispetto delle sostanziali modifiche introdotte nel tempo al *cookie law* europeo per garantire una maggiore tutela agli utenti finali, l'inadempimento e/o l'aggiramento degli obblighi posti dal diritto UE sono stati ricondotti principalmente ad un problema di insufficiente *enforcement*[57]. Tale problema accomuna invero molteplici normative nazionali in tema di protezione dei dati ed è stato generalmente ricondotto alla mancata previsione da parte dei legislatori di come "the particularly pervasive information asymmetries and market power found in many data markets undermine the role of markets, torts, and regulatory enforcement as mechanisms to ensure legal compliance"[58]. A livello europeo, tuttavia, *le recenti e molteplici iniziative, sia sul piano regolamentare (si pensi alle Linee Guida sui cookies, adottate da ultimo dal Garante italiano per la privacy*[59]*) che decisionale, sembrano aver finalmente imposto un cambio di passo. L'iniziativa spetta ora alle aziende, grandi e piccole, che dovranno adeguarsi, pena la comminazione di multe salate.*

ABSTRACT: L'articolo intende fornire un'analisi critica dell'evoluzione dell'uso dei *cookies* nel diritto e nella pratica dell'Unione Europea. Particolare attenzione è attribuita anche al trasferimento di dati personali al di fuori dell'UE, in particolare negli Stati Uniti, e alle persistenti criticità che tale trasferimento comporta, con il rischio dell'ennesimo rigetto da parte della Corte di Giustizia Europea. Il contributo affronta poi le modifiche normative attualmente in discussione nel contesto del nuovo regolamento *ePrivacy* e conclude, alla luce della pratica recente, che l'*enforcement gap* rilevato da più parti sta già per essere colmato.

KEYWORDS: cookies – trasferimento di dati – Regolamento Generale sulla protezione dei dati personali – consenso – regolamento ePrivacy.

[57] "Many websites do not give users a choice over which cookies are collected, despite the GDPR and ePrivacy Directive requirements. Multiple prior studies report on this, and we contribute to this analysis by showing that even from the websites providing choices, the vast majority, namely 94.7%, contain at least one potential violation. This situation cannot be resolved through new regulations alone, such as the planned ePrivacy Regulation, as it is mostly enforcement that is significantly lacking behind" (D. BOLLINGER, K. KUBICEK, C. COTRINI, D. BASIN, *Automating Cookie Consent* cit., p. 13). "All in all, the extent to which the GDPR bans dark patterns must become clear in case law and enforcement actions by Data Protection Authorities" (P. GRAßL, H. SCHRAFFENBERGER, FR. ZUIDERVEEN BORGESIUS, M. BUIJZEN, *Dark and bright patterns* cit., p. 26).

[58] Cfr. F. LANCIERI, *Narrowing Data Protection's* cit., p. 64.

[59] Tali Linee Guida sono state adottate al fine di fornire un quadro aggiornato alle novità normative introdotte dal GDPR e permettere, anche sulla base delle attività di monitoraggio compiute dal Garante italiano (come pure dai suoi omologhi in altri Stati membri) e dei numerosi reclami, segnalazioni e richieste di pareri, una corretta implementazione delle norme europee sui *cookies.* Il loro rilievo non è da sottovalutare, specie se si considera che il nuovo regolamento *ePrivacy* è ancora in fase negoziale e che vi si prevede un periodo transitorio della durata di due anni.

THE DIGITAL PANOPTICON. COOKIES BETWEEN LAW AND PRACTICE IN THE EUROPEAN UNION

ABSTRACT: The article aims to provide a critical analysis of the development of the use of cookies in EU law and practice. A specific focus is also given to the transfer of personal data outside the EU, particularly to the United States, and the persistent critical issues that such transfer implies, with the risk of yet another rejection by the European Court of Justice. The paper then discusses the regulatory changes currently under discussion in the context of the new ePrivacy regulation and positively contends, in the light of recent practice, that the identified enforcement gap is already about to be filled.

KEYWORDS: Cookies – Data transfer – General Data Protection Regulation – Consent – ePrivacy Regulation.