mediaLAWS

Rivista di diritto dei media
2/2022 settembre

DIRETTORE RESPONSABILE
EDITOR-IN-CHIEF
Oreste Pollicino (Università Bocconi)

DIRETTORI
EDITORS
Giulio Enea Vigevani (Università di Milano - Bicocca)
Carlo Melzi d'Eril (Avvocato in Milano)
Marina Castellaneta (Università di Bari)
Marco Bassini (Università della Tuscia)

VICEDIRETTORI
VICE-EDITORS
Marco Cuniberti (Università di Milano)
Giovanni Maria Riccio (Università di Salerno)
Marco Orofino (Università di Milano)
Ernesto Apa (Avvocato in Roma)

REDAZIONE
EDITORIAL BOARD
Marco Bassini (*coordinatore*) (Università Bocconi)
Maria Chiara Meneghetti (*vice coordinatore*) (Università Bocconi)
Flavia Bavetta (*vice coordinatore*) (Università Bocconi)
Ludovico Bossi, Niccolò Iurilli, Elena Mandarà

SEDE
CONTACTS

ACCMS Studio Legale
Via Podgora 13 – 20122 Milano

Università Bocconi - Dipartimento di Studi Giuridici
Via Roentgen 1 - 20136 Milano

e-mail: submissions@medialaws.eu

COMITATO SCIENTIFICO- STEERING COMMITTEE

Shulamit Almog *(University of Haifa),* Fabio Basile *(Università di Milano),* Mirzia Bianca *(La Sapienza – Università di Roma),* Elda Brogi *(European University Institute),* Giuseppe Busia *(Autorità Nazionale Anticorruzione),* Licia Califano *(Università di Urbino, già Garante per la protezione dei dati personali),* Angelo Marcello Cardani *(Università Bocconi, già Autorità per le garazie nelle comunicazioni),* Marta Cartabia *(Università Bocconi, Presidente emerito della Corte costituzionale),* Massimo Ceresa-Gastaldo *(Università Bocconi),* Pasquale Costanzo *(Università di Genova),* Marilisa D'Amico *(Università di Milano),* Filippo Donati *(Consiglio Superiore della Magistratura),* Mario Esposito *(Università del Salento),* Giusella Finocchiaro *(Università di Bologna)*, Tommaso Edoardo Frosini *(Università Suor Orsola Benincasa),* Maurizio Fumo *(Suprema Corte di Cassazione),* Alberto Maria Gambino *(Università Europea – Roma),* Michale Geist *(University of Ottawa),* Glauco Giostra *(La Sapienza – Università di Roma),* Enrico Grosso *(Università di Torino),* Uta Kohl *(University of Southampton),* Krystyna Kowalik-Bańczyk *(Tribunale dell'Unione europea),* Simone Lonati *(Università Bocconi),* Fiona Macmillan *(University of London),* Vittorio Manes *(Università di Bologna),* Michela Manetti *(Università di Siena),* Christopher Mardsen *(University of Sussex),* Manuel D. Masseno *(Instituto Politécnico de Beja),* Roberto Mastroianni *(Tribunale UE),* Luigi Montuori *(Garante per la protezione dei dati personali),* Antonio Nicita *(LUMSA, già Autorità per le garanzie nelle comunicazioni),* Monica Palmirani *(Università di Bologna)*, Miquel Pequera *(Universitat Oberta de Catalunya),* Vincenzo Pezzella *(Suprema Corte di Cassazione),* Laura Pineschi *(Università di Parma),* Giovanni Pitruzzella *(Corte di giustizia UE),* Francesco Pizzetti *(Università di Torino),* Andrea Pugiotto *(Università di Ferrara),* Margherita Ramajoli *(Università di Milano),* Gianpaolo Maria Ruotolo *(Università di Foggia),* Sergio Seminara *(Università di Pavia),* Salvatore Sica *(Consiglio di Presidenza della Giustizia Amministrativa),* Pietro Sirena *(Università Bocconi),* Francesco Viganò *(Corte costituzionale),* Luciano Violante *(Fondazione Leonardo - Civiltà delle Macchine)*, Lorenza Violini *(Università di Milano),* Roberto Zaccaria *(Università di Firenze),* Nicolò Zanon *(Corte costituzionale),* Vincenzo Zeno-Zencovich *(Università di Roma Tre)*

COMITATO DEGLI ESPERTI PER LA VALUTAZIONE - ADVISORY BOARD

Maria Romana Allegri, Giulio Allevato, Benedetta Barbisan, Marco Bellezza, Daniela Bifulco, Elena Bindi, Carlo Blengino, Monica Bonini, Manfredi Bontempelli, Fernando Bruno, Daniele Butturini, Irene Calboli, Simone Calzolaio, Quirino Camerlengo, Gianluca Campus, Nicola Canzian, Marina Caporale, Andrea Cardone, Corrado Caruso, Stefano Catalano, Adolfo Ceretti, Francesco Clementi, Roberto Cornelli, Giovanna Corrias Lucente, Filippo Danovi, Monica Delsignore, Giovanni De Gregorio, Giovanna De Minico, Gabriele Della Morte, Marius Dragomir, Fernanda Faini, Fabio Ferrari, Roberto Flor, Federico Furlan, Giovanni Battista Gallus, Marco Gambaro, Gianluca Gardini, Ottavio Grandinetti, Antonino Gullo, Erik Longo, Valerio Lubello, Federico Lubian, Nicola Lupo, Paola Marsocci, Claudio Martinelli, Alberto Mattiacci, Alessandro Melchionda, Massimiliano Mezzanotte, Francesco Paolo Micozzi, Donatella Morana, Piergiuseppe Otranto, Omar Makimov Pallotta, Anna Papa, Paolo Passaglia, Irene Pellizzone, Sabrina Peron, Bilyana Petkova, Davide Petrini, Marina Pietrangelo, Federico Gustavo Pizzetti, Augusto Preta, Giorgio Resta, Francesca Rosa, Andrej Savin, Salvatore Scuto, Monica Alessia Senor, Stefania Stefanelli, Giulia Tiberi, Bruno Tonoletti, Emilio Tosi, Lara Trucco, Luca Vanoni, Gianluca Varraso, Silvia Vimercati, Thomas Wischmeyer, Paolo Zicchittu

ANNO 2022 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

MediaLaws - Rivista di diritto dei media è una rivista quadrimestrale telematica, ad accesso libero, che si propone di pubblicare saggi, note e commenti attinenti al diritto dell'informazione italiano, comparato ed europeo.

La rivista nasce per iniziativa di Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril e Marco Bassini e raccoglie le riflessioni di studiosi, italiani e stranieri, di diritto dei media.

I contributi sono scritti e ceduti a titolo gratuito e senza oneri per gli autori. Essi sono attribuiti dagli autori con licenza Creative Commons "Attribuzione – Non commerciale 3.0" Italia (CC BY-NC 3.0 IT). Sono fatte salve, per gli aspetti non espressamente regolati da tale licenza, le garanzie previste dalla disciplina in tema di protezione del diritto d'autore e di altri diritti connessi al suo esercizio (l. 633/1941).

Il lettore può utilizzare i contenuti della rivista con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons "Attribuzione – Non commerciale 3.0 Italia" (CC BY-NC 3.0 IT), in particolare menzionando la fonte e, laddove necessario a seconda dell'uso, conservando il logo e il formato grafico originale.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

La qualità e il rigore scientifici dei saggi della Rivista sono garantiti da una procedura di *double-blind peer review* affidata a un comitato di esperti per la valutazione individuato secondo criteri di competenza e rotazione e aggiornato ogni anno.

MediaLaws - Rivista di diritto dei media
Regolamento per la pubblicazione dei contributi

1. "MediaLaws – Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione.

2. Gli organi della rivista sono il Comitato di direzione, il Comitato scientifico e il Comitato degli esperti per la valutazione. L'elenco dei componenti del Comitato di direzione e del Comitato scientifico della rivista è pubblicato sul sito della stessa (rivista.medialaws.eu). Il Comitato degli esperti per la valutazione è sottoposto ad aggiornamento una volta l'anno.

3. La rivista si compone delle seguenti sezioni: "Saggi", "Note a sentenza" (suddivisa in "Sezione Europa", "Sezione Italia" e "Sezione comparata"), "Cronache e commenti" e "Recensioni e riletture". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse.

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico.

5. La sezione "Note a sentenza" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere.

6. La sezione "Cronache e commenti" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata.

7. La sezione "Recensioni e riletture" ospita commenti di opere rispettivamente di recente o più risalente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica submissions@medialaws.eu, corredata dei dati, della qualifica e dei recapiti dell'autore, nonché della dichiarazione che il contributo sia esclusiva opera dell'autore e, nel caso in cui lo scritto sia già destinato a pubblicazione, l'indicazione della sede editoriale.

9. La direzione effettua un esame preliminare del contributo, verificando l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

10. In caso di esito positivo, la direzione procede ad assegnare il contributo alla sezione opportuna.

11. I saggi sono inviati alla valutazione, secondo il metodo del doppio cieco, di revisori scelti dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore. La direzione garantisce l'anonimato della valutazione.

12. La direzione comunica all'autore l'esito della valutazione.
Se entrambe sono positive, il contributo è pubblicato.
Se sono positive ma suggeriscono modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. La direzione si riserva la facoltà di sottoporre il contributo così come modificato a nuova valutazione, anche interna agli organi della rivista. Se solo una valutazione è positiva, con o senza modifiche, la direzione si riserva la facoltà di trasmettere il contributo a un terzo valutatore. Se entrambe le valutazioni sono negative, il contributo non viene pubblicato.

13. Per pubblicare il contributo, l'Autore deve inviare una versione definitiva corretta secondo le regole editoriali della rivista pubblicate sul sito della stessa, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri editoriali costituisce motivo di rigetto della proposta.

14. Le valutazioni vengono archiviate dalla direzione della rivista per almeno tre anni.

15. A discrezione della direzione, i saggi di autori di particolare autorevolezza o richiesti dalla direzione possono essere pubblicati senza essere sottoposti alla procedura di referaggio a doppio cieco ovvero essere sottoposti a mero referaggio anonimo, previa segnalazione in nota.

Indice
Index

Saggi

Note a sentenza

Cronache

Recensioni

Indice
Index

Essays

Case notes

Comments

Book reviews

Sono stati sottoposti a referaggio a doppio cieco i contributi di: Maria Romana Allegri, Andrea Buratti, Ylenia Maria Citino, Caterina Di Costanzo, Federica Giovanella, Angela Mendola, Daniela Messina, Cristina Evanghelia Papadimitriu, Alberto Randazzo.
Su determinazione della direzione, sono inoltre stati sottoposti a referaggio anonimo i contributi di: Filippo Donati, Simone Lonati e Vincenzo Zeno Zencovich.

Cronache

Google Analytics e GDPR. Possibili soluzioni di un equilibrio instabile

Valerio Lubello

Sommario

1. Introduzione

Gli Stati Uniti da tempo non considerati più un porto sicuro per la tutela dei dati personali[1] e recentemente l'Autorità garante per la protezione dei dati personali italiana[2], l'Autorità austriaca[3] e l'autorità francese[4] hanno adottato tre distinti provvedimenti che inibiscono di fatto l'utilizzo di Google Analytics proprio in ragione dei rischi connessi al trasferimento di dati personali oltreoceano.

Tali provvedimenti, frutto della sempre più evidente collaborazione tra le Autorità, sono dunque strettamente correlati allo scenario venutosi a delineare a seguito della sentenza della Corte di giustizia c.d. *Schrems II* che, come noto, nel luglio 2020 ha sancito l'invalidità dell'accordo (c.d. Privacy Shield) tra Commissione europea e Stati Uniti, in base al quale i dati personali potevano liberamente transitare tra le due spon-

[1] CGUE, C-362/14, *Schrems I* (2015), relativa al c.d. Safe Harbour nonché la sentenza c.d. CGUE, C-311/18 (2020), *Schrems II*. Per quanto riguarda la sterminata dottrina si veda *ex plurimis* O. Pollicino, *Diabolical Persistence: Thoughts on the Schrems II Decision*, VerfBlog, nonché O. Pollicino - M. Bassini, *Bridge is Down, Data Truck Can't Get Through... A Critical View of the Schrems Judgment in the Context of European Constitutionalism*, in G. Ziccardi Capaldo (ed.), *The Global Community Yearbook of International Law and Jurisprudence* 2016, 2017, 245 ss. Per le implicazioni connesse alla c.d. sovranità digitale già emerse con tutta evidenza nella prima delle decisioni Schrems, cfr. *ex multis*, V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Diritto dell'informazione e dell'informatica,* 2016, 683 ss.; A. Simoncini, *Sovranità e potere nell'era digitale*, in O. Pollicino - T.E. Frosini - E. Apa – M. Bassini (a cura di), *Diritti e libertà in internet,* Firenze, 2017, 19 ss. Per una lettura attenta dell'intera saga di C. Gentile, *La saga Schremse la tutela dei diritti fondamentali,* in *Federalismi.it*, 1, 2021.

[2] Provvedimento n. 9782890 del 9 giugno 2022 pubblicato il 23 giugno 2022.

[3] DSB, *Information der Datenschutzbehörde zum vollständigen Auslaufen der Standardvertragsklauseln*.

[4] CNIL, *Google Analytics et transferts de données: comment mettre son outil de mesure d'audience en conformité avec le RGPD?* .

de dell'Oceano Atlantico[5].
L'assenza prolungata di tale accordo – o meglio di una decisione di adeguatezza ai sensi dell'art. 45, par. 1, GDPR, *amplius infra* – ha generato non poca incertezza nelle dinamiche globali e finanche geopolitiche legate ai flussi di dati personali.
I provvedimenti in commento – come peraltro dimostrato dall'intenso dibattito del periodo[6] – proiettano dunque tale incertezza su Google Analytics, lo strumento più utilizzato al mondo per il tracciamento delle performance di ciascun sito nonché per la profilazione degli utenti a fini pubblicitari. Una vera e propria architrave tecnologica su cui si poggiano business di portata non commensurabile.
È appena il caso di segnalare come l'Autorità italiana abbia richiesto ai soggetti titolare del trattamento — vale a dire coloro i quali utilizzano Analytics nelle proprie pagine web – di trovare una soluzione compatibile con le prescrizioni del GDPR nell'arco di 90 giorni, entro 21 settembre 2022.
Scopo delle presenti note è dunque quello di ripercorrere il *reasoning* dei provvedimenti, analizzando le possibili soluzioni di breve e medio periodo che possano se non legittimare quantomeno lenire gli effetti di Google Analytics rispetto al GDPR.

2. Il capitolo V del GDPR e il trasferimento di dati verso Paesi terzi

Il Capo V del Regolamento – rubricato per l'appunto "Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali" – è interamente dedicato alle tutele e alle garanzie richieste per i trasferimenti in questione.
Il Principio generale – *ex* art. 44 GDPR – dispone che tali trasferimenti sono possibili nella misura in cui «il livello di protezione delle persone fisiche garantito […] dal regolamento non sia pregiudicato».
Chiaro sul punto il legislatore eurounitario: «la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni

[5] CGUE, *Schrems II*, cit.

[6] Come recentemente sottolineato: «È un tema enorme: l'accordo è stato annunciato da Biden a Bruxelles a fine marzo per promuovere l'innovazione e aiutare le aziende a competere e definito dalla presidente della Commissione europea Ursula von der Leyen, importante per salvaguardare privacy e libertà civili. Sul tavolo ci sono una base giuridica durevole per i flussi di dati e la promessa degli Stati Uniti di aver assunto impegni senza precedenti, come la possibilità per i cittadini europei di chiedere risarcimenti a una corte indipendente o nuove regole per la raccolta di informazioni tramite le attività di Signal intelligence. Peccato che al momento la trattativa risulterebbe arenata. Siamo a un binario morto e non c'è ancora niente di concreto. Questo crea un problema molto serio, anche e non solo in Italia». Con specifico riferimento a Google Analytics: «Vale per Google Analytics e soluzioni analoghe: abbiamo dato un termine di 90 giorni (che scadono a fine settembre, ndr), poi partiranno le verifiche istruttorie e forse i blocchi del trattamento. Siamo in una condizione di illiceità, si spera che in questo tempo possano intervenire meccanismi di regolazione». Così G. Cerrina Feroni, Vicepresidente Garante Privacy, intervista di Martina Pennisi, *Corriere della Sera*, 25 luglio 2022, Si veda inoltre l'*Intervista a Guido Scorza, Componente del Garante per la protezione dei dati personali,* in *Giornalettismo,* 24 giugno 2022.
Con riferimento ad una analisi comparata dei commenti si vedano E. Picciotto - M. Martini, *Schrems II e le decisioni delle autorità di protezione dei dati – Una sfida o la fine per i servizi di Google & Co?,* in *Fondazione Leonardo – Civiltà delle Macchine*, 19 aprile 2022.

internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali»[7]. Il corredo di tutele e di garanzie previste dal GDPR deve allora trovare applicazione anche quando i dati fuoriescono dall'Unione europea.

2.1 Il venir meno della decisione di adeguatezza

Secondo quanto disposto dall'art. 45, par. 1, del GDPR un trasferimento di dati verso Paesi extra UE può anzitutto considerarsi legittimo quando passa attraverso una c.d. decisione di adeguatezza adottata dalla Commissione europea: «il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche»[8].

In assenza di una siffatta decisione, un trasferimento di dati personali verso gli Stati Uniti comporta una certa criticità di fondo, stante l'accesso indiscriminato da parte delle agenzie governative statunitensi a tali dati: «ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti [...]. Più in particolare, [...] siffatte ingerenze possono derivare dall'accesso, da parte delle autorità pubbliche statunitensi, ai dati personali, trasferiti dall'Unione verso gli Stati Uniti, e dall'utilizzo di tali dati nell'ambito dei programmi di sorveglianza PRISM e UPSTREAM»[9].

2.2. Le misure contrattuali

Qualora — come nel contesto attuale — manchi una decisione di adeguatezza «il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo solo se ha previsto «garanzie adeguate» e a condizione che gli

[7] Considerando 6 del GDPR.

[8] Con riferimento al concetto di adeguatezza è bene richiamare quanto stabilito dal considerando 104 del Regolamento «Il paese terzo dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono trattati in uno o più settori specifici. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale». Vale altresì ricordare che *ex* art. 288, par. 4, TFUE, una decisione della Commissione – e ciò è vero anche per le decisioni di adeguatezza di cui si discute – ha carattere vincolante, in tutti i suoi elementi, per tutti gli Stati membri destinatari (*Schrems II,* cit., § 117)

[9] CGUE, *Schrems II*, cit., §§ 155 ss. e, per analogia, i richiami ivi contenuti alla decisione CGUE, *Schrems I*, cit., § 87. Per un'analisi della tematica ancorché non strettamente correlata alle vicende di Google Analytics, v. *ex plurimis* E. Teriolli, *Privacy e protezione dei dati personali Ue vs. Usa. Evoluzioni del diritto comparato e il trasferimento dei dati dopo la sentenza* "Schrems II", in *Diritto dell'informazione e dell'informatica,* 1, 2021, 49 ss.

interessati dispongano di «diritti azionabili e mezzi di ricorso effettivi», potendo tali garanzie adeguate essere fornite, segnatamente, mediante clausole tipo di protezione dei dati adottate dalla Commissione»[10].
Quest'ultime, ancorché non obbligatorie, rappresentano certamente lo standard di riferimento per il trasferimento di dati personali verso paesi terzi (cfr. art. 46, par. 2, lett. c) e sono volte a garantire che il trasferimento avvenga nel rispetto dei principi e delle garanzie del GDPR[11]. Da tale parametro il soggetto esportatore e il soggetto importatore possono discostarsi nell'ambito della loro autonomia contrattuale ma al solo fine di innalzare le garanzie e i diritti riconosciuti ai soggetti interessati.
A fianco alle soluzioni di natura contrattuale – e soprattutto nel caso in cui le stesse non dovessero risultare sufficienti — se ne aggiungono altre di natura tecnica ed organizzativa volte a promuovere un fascio di garanzie almeno pari a quello previsto dal GDPR nei confronti dei soggetti interessati.

2.3 Le ulteriori misure tecniche e organizzative

Le misure tecniche e organizzative non sono definite *ex ante* ma rimesse al principio di c.d. *accountability,* vale a dire alla corretta valutazione del titolare o del responsabile che trasmettono i dati. In tal senso – come specificato dall'EDPB (European Data Protection Board da ora in poi "EPDB") – "qualsiasi" misura può ritenersi efficace nella misura in cui è capace di colmare le eventuali carenze individuate nello scenario giuridico complessivo del Paese terzo[12].
Tali misure assumono un ruolo suppletivo[13] e possono tra loro diversamente combinarsi[14]. Così, ad esempio, rientrano in tali misure: la crittografia dei dati in un momento antecedente la trasmissione verso il paese terzo, senza che ovviamente a tale invio segua anche la condivisione con il paese di destinazione delle chiavi crittografiche; la completa pseudonimizzazione dei dati inoltrati[15]; la possibilità di fare soltanto transita-

[10] Cfr. CGUE*, Schrems II*, cit., § 91.

[11] Standard Contractual Clauses (SCC).

[12] Raccomandazione 1/2020, p. 70, nonché *Schrems II*, cit., § 134 a mente del quale: «spetta al "titolare del trattamento o al responsabile del trattamento verificare, caso per caso, e, eventualmente, in collaborazione con il destinatario del trasferimento, se il diritto del paese terzo di destinazione garantisca una protezione adeguata, alla luce del diritto dell'Unione, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati, fornendo, se necessario, garanzie supplementari rispetto a quelle offerte da tali clausole».

[13] Considerando 108 del GDPR nonché lo stesso art. 46, par. 1, GDPR, nonché *Schrems II*, cit., § 202.

[14] Sul punto è utile richiamare quanto disposto dal considerando 109 del GDPR «la possibilità che il titolare del trattamento [...] utilizzi clausole tipo di protezione dei dati adottate dalla Commissione [...] non dovrebbe precludere ai titolari del trattamento [...] di aggiungere altre clausole o garanzie supplementari». Aggiungendo altresì che gli stessi titolari «dovrebbero essere incoraggiati a fornire garanzie supplementari (...) che integrino le clausole tipo di protezione».

[15] Sul concetto di pseudonimizzazione si rimanda alla definizione fornita dallo stesso art. 4, par. 1, n. 5 del GDPR: «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o

re i dati nel paese terzo, purché crittografati, per poi far approdare gli stessi in un paese "coperto" da una decisione di adeguatezza; oppure il frazionamento dei pacchetti in modo che nel paese destinatario arrivi solo una parte, di fatto non decifrabile, di dati.

2.4 Il potere di controllo delle Autorità con rispetto ai singoli trasferimenti di dati personali

Vale altresì rimarcare come il GDPR attribuisca dei poteri *ad hoc* alle Autorità per poter sondare la legittimità di ciascun trasferimento nonché la congruità delle misure adottate[16]. Come ricordato dalla sentenza Schrems II, all'Autorità del singolo Stato membro spetta «sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 del GDPR e dalla Carta, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo»[17].

3. La natura dei dati trasferiti attraverso Google Analytics: l'indirizzo IP come fenomeno quantistico

Nell'ambito di tale attività di controllo le Autorità hanno pertanto mosso alcune considerazioni circa la natura del c.d. indirizzo IP concludendo che lo stesso e gli altri dati trattati da Google Analytics, possano insieme essere considerarsi dati personali ai sensi dell'art. 4, par. 1, n. 1, del GDPR.

L'indirizzo IP è un codice numerico di 12 cifre che viene attribuito a ciascuna connessione. Può essere fisso o dinamico e contenere in ogni caso alcune informazioni circa l'utenza, *rectius* la rete, ad esso correlata. Preso singolarmente non è dunque un dato personale in quanto manca dell'essenziale requisito dell'associabilità ad una persona fisica di cui alla nota definizione di dato personale[18].

identificabile».

[16] Per analogia, per quanto riguarda l'art. 28 della direttiva 95/46/CE, si vede CGUE, *Schrems I*, cit., § 47, nonché con riferimento al GDPR, *Schrems II*, cit., § 121.

[17] CGUE, *Schrems II,* cit., § 57, altresì art. 58, par. 2, lett. f) e j), GDPR.

[18] Secondo consolidata giurisprudenza della Corte di giustizia, infatti, «un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di detto fornitore, un dato personale, ai sensi dell'articolo 4, punto 1, del regolamento 2016/679, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare l'interessato grazie alle informazioni aggiuntive di detta persona di cui il fornitore di accesso a Internet dispone» (CGUE, C-597/19, § 102 che richiama la precedente sentenza CGUE, C-582/14, § 49).

Orbene se questo è vero per un soggetto che osserva il solo indirizzo IP, non è altrettanto vero per quei soggetti che insieme all'indirizzo IP possono osservare altri dati e, attraverso un'analisi incrociata, associare all'indirizzo IP una determinata identità, ancorché con una latente cifra di approssimazione[19].

Tali soggetti sono, ad esempio, il provider di rete che conosce l'intestatario di un determinato indirizzo IP o gruppo di indirizzi IP oppure coloro i quali possono osservare l'attività di un indirizzo IP associato ad una determinata utenza, ad esempio perché l'utente si è "loggato" in un determinato servizio.

Sicché, al pari dei fenomeni quantistici, l'indirizzo IP cambia la sua natura e la sua essenza a seconda del punto di vista dal quale lo si osserva.

Secondo le Autorità, la configurazione relativa all'oscuramento dell'indirizzo IP, configurazione che peraltro è ora parametro immodificabile del nuovo GA4 (*amplius infra*), non è sufficiente a rispettare i parametri delineati dalla Corte di giustizia e ciò nella misura in cui gli stessi indirizzi IP – ancorché oscurati per gli utilizzatori di Analytics – continuerebbero ad essere trasferiti verso gli Stati Uniti.

I numerosi metadati gestiti da Google permettono infatti di associare comunque l'indirizzo IP ad una determinata utenza, rendendo così i dati raccolti attraverso Google Analytics dati personali: «l'indirizzo IP costituisce un dato personale nella misura in cui consenta di identificare un dispositivo di comunicazione elettronica, rendendo pertanto indirettamente identificabile l'interessato in qualità di utente …. Tutto ciò soprattutto ove, come nel caso di specie, l'IP sia associato ad altre informazioni relative al browser utilizzato, alla data all'ora della navigazione (cfr. considerando 30 del Regolamento)»[20].

A riguardo, come ben descritto dall'Autorità austriaca, sono molti i dati che Google può conoscere e incrociare grazie all'utilizzo di Analytics: l'identificatore univoco ottenuto grazie all'analisi del *device* e del browser utilizzati da ciascun utente (grazie all'utilizzo di Google Analytics Account Identify)[21]; la cronologia dell'utente con l'indicazione di data e ora per ciascun sito visitato; informazioni circa il sistema operativo utilizzato dall'utente; la risoluzione dello schermo e la lingua preferita delle impostazioni. Si tratta in sintesi della c.d. "Digital footprint" richiamata anche dal Garante italiano nel suo provvedimento, attraverso la quale i dati possono essere facilmente associati ad un utente specifico, rendendo dati personali anche quei dati che presi singolarmente, come il caso dell'indirizzo IP, non sono tali.

3.1 La crittografia come tecnica non sufficiente per il rispetto delle adeguate garanzie

Seguendo ancora il *reasoning* delle diverse Autorità, vale la pena sottolineare come secondo l'Autorità francese l'utilizzo della crittografia non è una misura tecnica tale da poter fornire adeguate garanzie nell'ambito di un trasferimento di dati verso un paese terzo. L'utilizzo del protocollo https, che garantisce un flusso di dati crittografato, non

[19] CGUE, C-434/16, § 31, nonché CGUE, C-582/14, § 43.

[20] Così l'Autorità italiana sul punto nel suo provvedimento relativo a Google Analytics in commento. Cfr. altresì Gruppo di lavoro Articolo 29, WP 136 - Parere n. 4/2007 sul concetto di dati personali, del 20 giugno 2007, pag. 16.

[21] Google Analytics poggia il suo utilizzo come noto sull'installazione di alcuni cookies tra i quali rientrano "_ga", "cid" "_gid" volti proprio ad associare un ID univoco a ciascun utente a prescindere dunque dallo stesso indirizzo IP.

può infatti considerarsi uno strumento adeguato stante il fatto che il terminale dell'interessato continuerebbe, e non può che essere altrimenti, a *pingare* verso i poderosi server di Google situati in US.
A conclusioni analoghe è altresì approdata l'Autorità italiana secondo la quale — in ossequio alle Raccomandazioni dell'EDPB *supra* richiamate — l'utilizzo della crittografia nella fase di trasmissione (c.d cifratura in transit) e di conservazione dei dati (at rest) non è infatti sufficiente ad evitare un accesso indiscriminato ai dati da parte delle Autorità statunitensi. Considerando, peraltro, che la stessa Google è tenuta a condividere con le Autorità anche le chiavi crittografiche per poter conoscere del contenuto di ciascun dato: «fintanto che la chiave di cifratura rimanga nella disponibilità dell'importatore, le misure adottate non possono ritenersi adeguate»[22].

4. Le possibili soluzioni per rendere Google Analytics compatibile con il GDPR

Volendo fornire un primo quadro di soluzioni che possano rendere in qualche maniera Google Analytics compatibile con le prescrizioni del GDPR nonché con gli approdi giurisprudenziali e amministrativi sopra richiamati, vale la pena passare in rassegna alcune linee guida adottate da diverse Autorità degli Stati membri.
In tal senso, l'Autorità francese ha fornito un breve memo per coloro i quali vogliono continuare ad utilizzare Google Analytics[23]. In sintesi, per la CNIL soltanto l'interruzione del flusso di dati tra il titolare del trattamento e i *server* di Google potrebbe rendere Analytics conforme al GDPR.
La possibile soluzione individuata dall'Autorità francese è infatti quella di creare un c.d. *proxy server* su cui indirizzare tutti i flussi di dati raccolti tramite Analytics, assicurando al contempo che lo stesso *server proxy* non trasferisca a sua volta i dati in paesi che non garantiscono garanzie almeno equivalenti a quelle della stessa Unione europea.
In tale processo, sarebbe altresì necessario pseudonimizzazione i dati prima ancora che gli stessi dati siano inviati verso il *proxy server* in modo che gli stessi non possano essere in nessun modo riferibili ad una determinata persona fisica[24].
La CNIL declina poi quelle che potrebbero essere le caratteristiche del server *proxy* su cui dirottare i dati di tracciamento raccolti tramite Analytics.
Con riferimento alla possibile geolocalizzazione, le impostazioni di tracciamento devono essere tali da permettere un elevato grado di approssimazione capace di impedire l'associabilità del dato georeferenziato ad una determinata persona fisica.
Il c.d. *hashing* dei dati deve inoltre variare nel tempo in modo che lo stesso soggetto interessato non riceva il medesimo codice hash a distanza di tempo. Al contempo deve essere garantita l'assenza di qualsiasi *finger printing* o dei c.d. *user agents,* capaci di rendere identificabile il dato raccolto nell'attività di trattamento grazie alle specifiche

[22] Cfr. Raccomandazione 1/2020, § 81, e 95.

[23] CNIL, *Google Analytics et transferts de données: comment mettre son outil de mesure d'audience en conformité avec le RGPD?*, 2022

[24] A riguardo l'EDPB stabilisce con la sua comunicazione 1/2020.

impostazioni definite dall'utente stesso nel proprio *device*.
Il *proxy server* deve essere configurato in modo che si possa escludere qualsiasi trasferimento di dati oltre i confini dell'Unione europea e dallo spazio economico europeo.
Fermo in ogni caso il principio di *accountability* e ciò in quanto spetterà comunque al titolare valutare la congruità delle misure adottate anche alla luce delle costanti evoluzioni tecnologiche in materia.
Per ammissione della stessa CNIL si tratta di un'"*exit strategy*" costosa e complessa e per ciò stesso non sempre in grado di soddisfare le esigenze dei fruitori di Analytics.
A fronte di tale consapevolezza il Garante francese invita dunque a sondare delle possibili alternative che non trasferiscono dati personali verso paesi terzi[25].

4.1 Alcuni opportuni parametri di Google Analytics (Universal)

Per quanto concerne le impostazioni ad oggi presenti in Google Analytics nella versione c.d. Universal, è possibile modulare le stesse per ridurre l'impatto nei confronti dei singoli utenti.
A riguardo, sono certamente utili le linee guida dell'Autorità Garante dei Paesi Bassi adottate nel 2018[26].
Nel dettaglio, la prima delle indicazioni sembra ormai essere superata dalla nuova *release* di Google Analytics. Si tratta infatti della possibilità di oscurare parte dell'indirizzo IP, funzionalità ormai integrata nella nuova versione di Analytics.
Altra impostazione riguarda invece la possibilità di disabilitare la condivisione dei dati raccolti tramite Analytics con la stessa Google. Tale condivisione di dati permette infatti a Google di soddisfare alcune sue finalità come, ad esempio, previo consenso specifico di ciascun utente, lo sviluppo di prodotti e/o l'inoltro di pubblicità c.d. targettizzata.
Risulta altresì opportuno disattivare le analisi delle condotte tenute da ciascun utente attraverso i diversi dispositivi allo stesso riconducibili.
Fermi, in ogni caso, gli obblighi di informativa nei confronti dei soggetti interessati.

4.2 Le nuove funzionalità di Google Analytics 4

Come ormai noto, Universal Analytics smetterà di raccogliere dati a partire dal 30 giugno 2023. Da quel momento in poi l'infrastruttura di riferimento sarà la sola Google Analytics 4, caratterizzata da alcune funzionalità che sembrerebbero *prima facie* recepire le indicazioni provenienti dalle Autorità degli Stati membri[27].

[25] CNIL, *Cookies: solutions pour les outils de mesure d'audience*, 2021.

[26] Autoriteit Persoonsgegevens, *Handleiding privacyvriendelijk instellen van Google Analytics*, 2022. Le stesse sono state recentemente modificate con il non trascurabile avviso che recentemente modificate, peraltro, con il non trascurabile avviso che a breve non sarà più possibile utilizzare Google Analytics.

[27] Si veda il sito support.google.com.

Come accennato, l'anonimizzazione dell'indirizzo IP diventa ora lo standard di riferimento. Google Analytics 4 sembrerebbe infatti non analizzare né archiviare gli indirizzi IP degli utenti[28]. L'indirizzo IP verrebbe così utilizzato da Google soltanto per individuare il *server* più vicino ed efficiente per un determinato utente. Una volta però che i dati raggiungono il *server* così individuato l'indirizzo IP non verrebbe in alcun modo comunicato né tanto meno salvato.
Tale configurazione sembrerebbe altresì permettere la raccolta dei dati in *server* collocati all'interno dell'Unione europea facendo apparentemente venir meno le problematiche relative al trasferimento dei dati verso Paesi terzi come gli Stati Uniti. Non è chiaro però se permane comunque attivo un qualche flusso di dati verso gli Stati Uniti. Con il protrarsi, eventualmente, delle problematiche descritte.

4.3 Il c.d. *Server Side Tagging* come facilitatore del proxy server.

Una delle novità che sembrano poter in qualche modo assecondare le richieste di territorialità provenienti dalle Autorità europee è senza dubbio il servizio c.d. di *Server Side Tagging*. Seguendo tale impostazione, i dati possono infatti essere raccolti in un *server* individuato dal singolo proprietario del sito e non già nei *server* di Google. Tale funzione permette così l'inoltro dei dati verso un ecosistema proprietario diverso dalla piattaforma di Google. Un sistema *proxy,* dunque, che sembrerebbe rispettare le linee guida proposte dal Garante francese[29]. I dati raccolti in ogni caso non dovranno poi essere soggetti a flussi ulteriori tali da vanificare l'esistenza stessa del *proxy* server.
Rimane però da comprendere appieno il concreto utilizzo che la stessa Google fa dei dati nel momento antecedente l'invio al c.d. *proxy server*. Sono infatti gli strumenti di Google che raccolgono i dati e li inoltrano al *server* proprietario e non è perciò possibile escludere a priori un flusso di dati verso i server di Google situati negli Stati Uniti.

4.4 Le pericolose connessioni di Google Signals

Google Signals è una funzione di Analytics che permette la raccolta di informazioni ancora più dettagliate nei confronti di ogni singolo utente, con il fine di poter veicolare allo stesso dei messaggi pubblicitari personalizzati. In Google Analytics 4 è ora possibile disabilitare tale raccolta di dati che riguardano, tra l'altro, la posizione geografica dell'utente nonché alcune caratteristiche tecniche dei dispositivi utilizzati.

[28] Privacy policy di Google Analytics 4, in *support.google.com*.

[29] *An introduction to server-side Tagging*, in *developers.google.com*.

4.5 Il consenso ora necessario per l'installazione di Google Analytics e il parziale superamento delle Linee Guida sui cookie del giugno 2021

Altro aspetto da prendere in considerazione è la diversa modulazione dei consensi necessari per permettere a Google Analytics di raccogliere dati.
Nelle linee guida adottate dal Garante italiano in materia di cookies nel luglio 2021, l'Autorità ha infatti sostenuto che «Affinché i cookie analytics siano equiparati ai tecnici è [..] indispensabile precludere la possibilità che si pervenga, mediante il loro utilizzo, alla diretta individuazione dell'interessato (cd. single out), il che equivale impedire l'impiego di cookie analytics che, per le loro caratteristiche, possano risultare identificatori diretti ed univoci. La struttura del cookie analytics dovrà allora prevedere la possibilità che lo stesso cookie sia riferibile non soltanto ad uno, bensì a più dispositivi, in modo da creare una ragionevole incertezza sull'identità informatica del soggetto che lo riceve. Di regola questo effetto si ottiene mascherando opportune porzioni dell'indirizzo IP all'interno del cookie»[30].
Il Garante ha altresì sottolineato, anticipando in parte le problematiche in commento, che «Resta inteso pertanto che i soggetti terzi, che forniscono al publisher il servizio di web measurement, non dovranno comunque combinare i dati, anche così minimizzati, con altre elaborazioni (file dei clienti o statistiche di visite ad altri siti, ad esempio) nè trasmetterli a loro volta ad ulteriori terzi, pena l'inaccettabile incremento dei rischi di identificazione dell'utente; tranne il caso in cui la produzione di statistiche da loro effettuata con i dati minimizzati interessi più domini, siti web o app riconducibili al medesimo publisher o gruppo imprenditoriale».
Tale passaggio sembrerebbe ora essere superato data l'ormai accertata riconducibilità dei dati raccolti tramite Google Analytics ad una determinata utenza a prescindere dall'oscuramento o meno del solo indirizzo IP.
Sembrerebbe dunque che i cookie analytics non possano più essere equiparati a quelli necessari e pertanto dovranno ora ottenere per la loro installazione un esplicito consenso da parte del soggetto interessato. Le cookie policy andranno inoltre aggiornate, dando la possibilità agli utenti di impostare le singole preferenze anche per tale tipologia di cookie. Da classificare ora, nel caso in cui si utilizzi Google Analytics, tra i cookie di profilazione.

4.6 Il diritto di cancellazione dei dati personali

Tra le funzionalità che più sembrano soddisfare i principi del GDPR e in particolare il catalogo dei diritti del soggetto interessato vi è senza dubbio la possibilità di rimuovere i dati del singolo utente in modo da poter accogliere eventuali istanze di cancellazione dei dati. Attraverso il c.d. ID dispositivo è infatti ora astrattamente possibile eliminare i dati provenienti da una determinata utenza. Il che se da un lato è

[30] Il riferimento è alle *Linee guida cookie e altri strumenti di tracciamento* del 10 giugno 2021, doc. web n. 9677876.

certamente da considerarsi un passo in avanti nell'esercizio del diritto di cancellazione dei dati personali da parte degli utenti, dall'altro sembrerebbe ribadire indirettamente quanto sostenuto dalle singole Autorità. Vale a dire che attraverso la c.d. *digital fingerprint* è sostanzialmente sempre possibile associare un flusso di dati di navigazione ad una determinata utenza.

5. Conclusioni

In attesa di conclusioni sul piano politico, vale a dire di una decisione di adeguatezza ai sensi dell'art. 45 del GDPR, diversi sono le alternative possibili per gli strumenti di tracciamento.

Le Autorità europee suggeriscono più o meno direttamente un passaggio a soluzioni alternative a Google Analytics che possano garantire trattamento dei dati all'interno dei confini dell'Unione europea.

L' attuale compatibilità di Google Analytics con il GDPR è infatti del tutto incerta anche per la nuova versione c.d. Google Analytics 4. La recente *release* – per quanto presenti delle funzionalità più garantiste della privacy dei soggetti interessati – non è come visto esente da rischi.

Ad ogni buon conto, per i titolari di trattamento che vorranno comunque mantenere il servizio di Google, il passaggio da Universal Analytics a Google Analytics 4 pare un passaggio obbligato. Ancorché alcuni "settaggi" – orientati ad una maggiore garanzia nei confronti dei diritti degli utenti – si rendono oltremodo necessari.

Da capire quali e quanti dati, nonostante tutte le precauzioni del caso, possano essere comunque oggetto di un trasferimento verso gli Stati Uniti, con le conseguenti criticità del caso.

Elenco autori

Maria Romana Allegri
professoressa associata di istituzioni di diritto pubblico, Sapienza - Università di Roma
Andrea Buratti
professore ordinario di diritto pubblico comparato, Università degli Studi di Roma "Tor Vergata"
Liliana Ciliberti
esperta di copyright e di regolamentazione dei media e delle comunicazioni elettroniche
Ylenia Maria Citino
assegnista di ricerca di istituzioni di diritto pubblico, LUISS Guido Carli
Caterina Di Costanzo
assegnista di ricerca di diritto costituzionale, Università degli Studi di Firenze
Filippo Donati
professore ordinario di diritto costituzionale, Università degli Studi di Firenze
Andrea Fedi
avvocato in Roma
Filippo Luigi Giambrone
ricercatore di diritto tributario, Università degli Studi del Sannio
Federica Giovanella
professoressa associata di diritto privato comparato, Università degli Studi di Udine
Carloalberto Giusti
professore ordinario di diritto privato comparato, Link University
Ottavio Grandinetti
avvocato in Roma
Simone Lonati
professore associato di diritto processuale penale, Università Bocconi
Valerio Lubello
avvocato in Milano
Angela Mendola
docente a contratto di diritto privato, Università degli studi di Salerno
Daniela Messina
docente a contratto di diritto dell'informazione e dell'informatica, Università degli Studi di Napoli "Parthenope"
Matteo Monti
assegnista di ricerca di diritto pubblico comparato, LUISS Guido Carli
Cristina Evanghelia Papadimitriu
ricercatrice di diritto dell'economia, Università degli Studi di Messina
Maria Pia Peluso
dottoranda di ricerca, Università degli Studi di Roma "Tor Vergata"
Ludovica Paseri
assegnista di ricerca di diritto amministrativo, Università degli Studi di Torino
Cesare Pinelli
professore ordinario di istituzioni di diritto pubblico, Sapienza - Università di Roma
Alberto Randazzo
professore associato di istituzioni di diritto pubblico, Università degli Studi di Messina
Marco Ventoruzzo
professore ordinario di diritto commerciale, Università Bocconi
Vincenzo Zeno Zencovich
professore ordinario di diritto privato comparato, Università degli Studi Roma Tre

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

mediaLAWS

ANNO 2022 - CODICE ISSN 2532-9146