Schrems II e le decisioni delle autorità di protezione dei dati – Una sfida o la fine per i servizi di *Google* & Co?

Un'analisi delle recenti decisioni dell'autorità di protezione dei dati austriaca e dell'autorità di protezione dei dati francese sul trasferimento transatlantico dei dati personali.

di *Edoardo Picciotto* & *Matteo Martini* *

Sommario: 1. Il conflitto tra il RGPD e *Google Analytics*. – 2. Queste decisioni rappresentano la fine per *Google* e l'intero settore digitale? – 3. Un primo piano delle decisioni delle APD. – 4. Possibili soluzioni, sfide e ostacoli. – 4.1. Clausole Contrattuali Standard. – 4.2. Anonimizzazione e pseudonimizzazione dei dati personali. – 4.3. Il consenso. – 4.4. Trattamento dei dati europei in Europa. – 4.5. *Privacy Shield II* – 5. Conclusioni.

Abstract: L'obiettivo di questo paper è analizzare le implicazioni delle recenti decisioni emanate dalle autorità di protezione dei dati austriaca e francese. Entrambe hanno dichiarato che l'utilizzo del servizio noto come *Google Analytics* rappresenti una violazione dell'art. 44 del Regolamento Generale sulla Protezione dei Dati (RGPD). Il nostro obiettivo è di fornire una visione d'insieme delle possibili soluzioni che potrebbero essere utilizzate per reagire a queste decisioni.

1. Il conflitto tra il RGPD e *Google Analytics*

Circa un anno e mezzo dopo la pubblicazione della decisione *Schrems II*, le autorità di protezione dei dati (APD) sono al centro dell'attenzione mediatica. L`APD austriaca (*Datenschutzbehörde*) è stata la prima a dichiarare la violazione dell'art. 44 RGPD da parte di *Google Analytics*, così come interpretato dalla Corte di Giustizia dell´Unione Europea (CGEU).[1] La decisione dell´APD francese (*CNIL*), presa all´inizio dell´anno, di seguire

* Edoardo Picciotto si è laureato in giurisprudenza presso l'Università Commerciale Luigi Bocconi, Milano. Matteo Martini si è laureato in giurisprudenza presso la Rheinische Friedrich-Wilhelms-Universität Bonn. Attualmente entrambi partecipano al master di secondo livello LL.M. in Law of Internet Technologies presso l'Università Commerciale Luigi Bocconi.

l´interpretazione della *Datenschutzbehörde* austriaca ha rinforzato quest´attenzione mediatica.[2] Tuttavia, probabilmente questo non rappresenterà l´ultimo capitolo di questa saga dal momento che anche altre autorità europee potrebbero decidere che *Google Analytics* violi l´art. 44 RGPD. Da un lato la *CNIL* ha espressamente dichiarato di aver cooperato con altre APD europee nella valutazione del caso *Google Analytics*,[3] dall'altro la presidentessa dell'APD austriaca ricopre anche la posizione di presidente del Comitato europeo per la protezione dei dati. Perciò, sembra probabile che nel futuro altre APD europee possano decidere in maniera simile.

Di conseguenza, molti osservatori hanno proclamato la fine dell'Internet per come lo conosciamo, considerando che la NGO *None Of Your Business* (NOYB), co-fondata da Schrems, ha sottoscritto appelli simili in 30 stati membri del SEE.[4]

Tuttavia, potrebbe essere utile fare un passo indietro e analizzare queste recenti decisioni più attentamente, prima di dedurre le loro implicazioni future.

2. Queste decisioni rappresentano la fine per *Google* e l'intero settore digitale?

Da un punto di vista giuridico, l'effetto legale di entrambe le decisioni risulta fortemente limitato. In primo luogo, si tratta di decisioni di natura esclusivamente amministrativa, considerato che non esiste ancora in merito una sentenza emessa da una corte. In secondo luogo, l'effetto giuridico è circoscritto esclusivamente ai fatti come stabiliti dalle APD. Infine, l'APD austriaca ha dichiarato espressamente che non tanto *Google*, quanto i gestori del sito web che incorporano *Google Analytics* sui propri siti, violino il RGPD.[5]

Nonostante questo, le implicazioni pratiche, economiche e politiche delle decisioni saranno immense, come ammesso anche da *Google*.[6]

---

[1] Autorità di protezione dei dati austriaca, *Teilbescheid* D155.027 GA, Google LLC, 22.12.2021.
[2] CNIL, *Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply*, 10.02.2022.
[3] *Ibid.*
[4] Vd. il sommario di tutti gli appelli pubblicati sul sito web di NOYB, 31.03.2022.
[5] Autorità di protezione dei dati austriaca, *Teilbescheid* D155.027 GA, Google LLC, 22.12.2021, pp. 37-38.
[6] Vd. la dichiarazione pubblicata dal presidente delle *Global Affairs & Chief Legal Officer* di *Google* Mr. Kent Walker, 19.01.2022.

Le APD hanno deciso non solo che l'uso di *Google Analytics* determinerà l'emanazione delle sanzioni stabilite dal RGPD, ma le loro decisioni implicano che il trasferimento transatlantico dei dati personali in generale sia problematico. Eppure, l'attività economica delle aziende big tech si basa principalmente su tali trasferimenti di dati dall'Europa alle loro sedi logistiche, per lo più situate negli Stati Uniti. Ne conseguono implicazioni di vasta portata, illustrate tra l´altro dalla relazione annuale di *Meta*, in cui viene riportata una dichiarazione inerente alla possibile rimozione di *Instagram* e *Facebook* dal mercato europeo a causa della pressione esercitata dal RGPD.[7] Nonostante *Facebook* abbia già emesso una controdichiarazione smentendo la sua eventuale uscita dal mercato europeo,[8] è chiaro come il RGPD e le sue regole sui trasferimenti dei dati personali siano ora un tema di massima priorità per i colossi del settore tecnologico.

3. Un primo piano delle decisioni delle APD

Così, per comprendere se l'applicazione della sentenza *Schrems II* da parte delle diverse APD europee possa davvero causare una trasformazione dell'intero settore tecnologico, è necessario esaminare le decisioni delle APD più nel dettaglio.

A tal fine, bisogna studiare i precedenti sviluppi avvenuti negli anni recenti in tema di protezione dei dati.

In particolare, la cosiddetta *Schrems* saga, originata nel 2013 in seguito alle rivelazioni da parte di Edward Snowden, ha senza dubbio influenzato in maniera cruciale il dibattito odierno sul diritto alla *privacy* in Europa.[9]

In queste decisioni, comunemente note come *Schrems I*[10] e *II*[11], la CGUE ha ritenuto che il livello di protezione offerto dalle autorità americane ai cittadini europei non potesse considerarsi adeguato, se comparato con quello europeo. In *Schrems II*, per esempio, la Corte

[7] Meta, *annual report pursuant to the securities exchange act of 1934 for the fiscal year 2021*, 02.02.2022, p. 9.
[8] Vd. Redazione Tramillas, *Facebook threaten to pull out of the EU*, in *marca.com*, 07.02.2022.
[9] Vd. Ewen Macaskill/Gabriel Dance/Feidling Cage/Greg Chen, *NSA Files: Decoded*, in *theguardian.com*, 01.11.2013.
[10] CGUE, Caso C-362/14, Schrems v Data Protection Commissioner, 06.10.2015, ECLI:EU:C:2015:650.
[11] CGUE, Caso C-311/18, Data Protection Commissioner v Facebook Ireland Ltd/Schrems, 16.07.2020, ECLI:EU:C:2020:559.

ha evidenziato come la sezione 702 del Foreign Intelligence Surveillance Act (FISA) non consentisse di garantire il livello di protezione dei dati richiesto dall'art. 44 del RGPD.[12]

Di conseguenza, la Corte ha invalidato in entrambe le decisioni gli accordi che, all'epoca, consentivano il trasferimento transatlantico dei dati personali: il cosiddetto *Safe Harbour* in *Schrems I* e il *Privacy Shield* in *Schrems II*.[13]

Queste sentenze hanno creato incertezza rispetto ai requisiti giuridici per i trasferimenti transatlantici dei dati personali. Le recenti decisioni delle APD provano a ridurre tali incertezze rispondendo a due principali domande. In primo luogo, i dati raccolti da *Google Analytics* e poi trasferiti a *Google LLC* sono effettivamente dati personali? In altre parole, gli art. 44 e ss. del RGPD sono applicabili nel caso in esame? In secondo luogo, il trasferimento negli Stati Uniti ha violato i suddetti articoli? Entrambe le domande hanno ricevuto risposta affermativa. Poiché la decisione della *CNIL* segue la linea argomentativa esposta dalla *Datenschutzbehörde* austriaca nella sua precedente decisione, la nostra analisi si concentrerà principalmente su quest'ultima.

Per capire se i dati raccolti e successivamente trasferiti negli Stati Uniti costituiscano dati personali, la ADP austriaca ha analizzato la tipologia di dati raccolti da *Google Analytics*.[14]

L'ADP ha concluso che i più importanti dati raccolti ricomprendevano, tra gli altri, un numero di identificazione unico impostato tramite *cookies*, in grado di distinguere i diversi utenti, senza però rilevare direttamente la loro identità. Inoltre, *Google Analytics* ha raccolto indirizzo IP degli utenti e altri dati tecnici, permettendo così il *fingerprinting* dei dispositivi.

Successivamente, l'APD austriaca ha verificato se tali dati costituissero dati personali ai sensi dell´art. 4 (1) RGPD. La risposta sarebbe affermativa nel caso in cui i dati rendessero "identificabile" con qualsiasi mezzo una persona fisica, indipendentemente dal fatto che un'identificazione sia stata effettivamente eseguita o meno.[15] Tuttavia, il considerando 26 RGPD suggerisce che questo test sia limitato ai mezzi che possono essere utilizzati "ragionevolmente" per identificare una persona. In altre parole, dovrebbe essere

[12] CGUE, Caso C-311/18, Data Protection Commissioner v Facebook Ireland Ltd/Schrems, 16.07.2020, ECLI:EU:C:2020:559, p. 43.
[13] Gentile Chiara, *La saga Schrems e la tutela dei diritti fondamentali,* in *Federalismi.it*, 13.01.2021, pp. 35-56 (35ss).
[14] Autorità di protezione dei dati austriaca, *Teilbescheid* D155.027 GA, Google LLC, 22.12.2021, p. 24.
[15] Art. 4 (1) Regolamento Generale per la Protezione dei Dati.

ragionevole supporre che un determinato agente sarebbe in grado di identificare l'interessato (*data subject*) dall'insieme dei dati raccolti, ad esempio, tramite "l'individuazione" dell'interessato.[16]

Nel caso in esame l'APD austriaca ha individuato due determinati agenti in grado di "identificare" un individuo grazie ai dati raccolti da *Google Analytics*: *Google LLC* e le agenzie di sorveglianza statunitensi.

Da un lato, *Google LLC* sarebbe stata in grado di determinare l'accesso da parte di un distinto utente con un account *Google*, purché tale utente fosse collegato al suo account *Google* mentre effettuava l'accesso al sito.[17] Dall'altro lato, le agenzie di sorveglianza statunitensi avrebbero avuto i mezzi per identificare un individuo combinando i dati raccolti e trasferiti da *Google Analytics* con i dati già in loro possesso.[18] Quest'ultimo scenario è stato considerato "ragionevolmente" probabile considerando quanto determinato dalla Corte in *Schrems II* e i rapporti di trasparenza di *Google*, che proverebbero come le agenzie statunitensi facciano effettivamente frequentemente richiesta di dati a *Google*.[19] In sintesi, secondo l'APD austriaca il trasferimento dei dati riguarderebbe dati personali e perciò sarebbe soggetto alle limitazioni delineate negli artt. 44ss RGPD.

Successivamente, l'APD austriaca ha dichiarato che il trasferimento dei dati personali europei verso gli Stati Uniti viola questi articoli. Le Clausole Contrattuali Standard (CCS), basate sulla decisione della Commissione dell'Unione Europea del 05.02.2010,[20] non garantirebbero un livello di protezione appropriato a quello richiesto dall´art. 46 RGPD.[21] Inoltre, le misure supplementari introdotte da *Google* non sarebbero sufficienti ad affrontare i rischi per la *privacy* che emergono dalla FISA.[22]

Conseguentemente, secondo la decisione dell'APD non sarebbe più possibile per *Google* utilizzare *Google Analytics* così come ha fatto sino ad ora. La *CNIL* ha persino raccomandato

[16] Autorità di protezione dei dati austriaca, *Teilbescheid* D155.027 GA, Google LLC, 22.12.2021, p. 25.
[17] *Ivi*, p. 28.
[18] *Ivi*, p. 29.
[19] Vd. Google, *Google Transparency Report*, 31.03.2022.
[20] Commissione Europea, commission decision 2010/87/EU, 05.02.2010.
[21] Autorità di protezione dei dati austriaca, *Teilbescheid* D155.027 GA, Google LLC, 22.12.2021, p. 32.
[22] *Ivi*, pp. 35-36.

la cessazione dell'utilizzo di *Google Analytics* qualora le sue funzioni non venissero modificate.[23]

4. Possibili soluzioni, sfide e ostacoli

Dunque, nel capitolo seguente, verranno esaminate le opzioni a disposizione delle aziende tech che volessero conformarsi alle decisioni delle APD e gli ostacoli che incontrerebbero a cause dell'implementazione di tali opzioni.

4.1. Clausole Contrattuali Standard

In giugno 2021, la Commissione Europea ha emanato una versione modernizzata delle clausole contrattuali standard che, se implementata, renderebbe valido il trasferimento dei dati al di fuori dell'Unione Europea.[24] Questo strumento, di conseguenza, potrebbe rappresentare una valida soluzione al problema in esame.

Tuttavia, la natura contrattuale delle CCS le rende vincolanti solo per gli attori privati coinvolti nel trasferimento dei dati. Al contrario, le autorità pubbliche situate in paesi terzi non sarebbero toccate in nessun modo.

Di conseguenza, la CGUE ha dichiarato che il *data controller* deve effettuare una valutazione caso per caso per verificare che il paese destinatario fornisca un adeguato livello di protezione dei dati personali.[25]

Nel caso in questione, è stato comprovato che il sistema giuridico statunitense, principalmente per via della sezione 702 della FISA, non garantisce garanzie a sufficienza per la sicurezza dei dati personali europei. Secondo la CGUE, infatti, il sistema americano consente alle autorità pubbliche una possibilità di accesso sproporzionata alle comunicazioni

[23] CNIL, *Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply*, 10.02.2022.
[24] Vd. Commissione Europea, *Standard Contractual Clauses (SCC)*, 04.06.2021.
[25] Gentile Chiara, *La saga Schrems e la tutela dei diritti fondamentali,* in *Federalismi.it*, 13.01.2021, pp. 35-56 (44).

elettroniche e non prevede rimedi legali o mezzi di opposizione significativi per gli individui coinvolti.[26]

In conclusione, nonostante la versione aggiornata delle CCS rappresenti una soluzione economicamente vantaggiosa, esse possono essere applicate solo nei casi in cui il trasferimento venga effettuato verso paesi terzi che non prevedano un accesso sproporzionato da parte delle autorità pubbliche ai dati personali degli stranieri. Sfortunatamente, per quanto riguarda gli Stati Uniti, il problema permarrà fintanto che resterà in vigore la regolamentazione americana sulla sorveglianza.

4.2. Anonimizzazione e pseudonimizzazione dei dati personali

Un'altra possibile soluzione al problema connesso al trasferimento di dati personali a paesi terzi potrebbe essere l'anonimizzazione di tali dati. Infatti, il preambolo 26 del RGPD dispone che i principi della protezione dei dati non dovrebbero applicarsi a informazioni anonimizzate, escludendo così l'applicazione del RGDP ai dati resi anonimi.

Diversamente, la mera pseudonimizzazione dei dati li renderebbe comunque soggetti al RGPD e ai suoi standard sul trasferimento dei dati fuori dall'Unione.

Al fine di meglio comprendere questa differenza, è necessario effettuare una distinzione preliminare tra anonimizzazione e pseudonimizzazione.

L'anonimizzazione, da un lato, è stata definita come un processo attraverso il quale i dati personali sono alterati in modo tale per cui un individuo non può più essere identificato, direttamente o indirettamente, sia dal *data controller* operante in autonomia, sia in collaborazione con altre parti.[27]

Questa definizione implica che i dati personali, una volta alterati, non possano più essere attribuiti all'individuo a cui appartengono, rendendone così impossibile la reidentificazione. Secondo alcuni studiosi però, l'anonimizzazione è difficilmente realizzabile.[28] Si ritiene,

[26] CGUE, Caso C-311/18, Data Protection Commissioner v Facebook Ireland Ltd/Schrems, 16.07.2020, ECLI:EU:C:2020:559, p. 43.
[27] ISO, *Health Informatics – Pseudonymisation*, ISO 25237:2017, 2017, p. 7.
[28] Ira S. Rubinstein/Woodrow Hartzog, *Anonymisation and Risk,* New York University School of Law, 2015.

infatti, che il costante incremento del potere computazionale delle machine e la disponibilità di colossali quantità di dati facilmente accessibili a chiunque rendano possibile la reidentificazione degli individui anche con informazioni estremamente scarse.[29]

Si può dunque affermare che, con i mezzi tecnologici attualmente disponibili, sia quasi impossibile garantire una vera e propria anonimizzazione.

Inoltre, anche qualora l'anonimizzazione diventasse possibile attraverso tecnologie innovative, rimarrebbero comunque delle problematiche di natura economica. Nell'economia dei dati, infatti, il valore risiede nella possibilità di profilare gli utenti per poi indirizzare loro pubblicità personalizzata. Questo è specialmente vero per grandi compagnie come *Google* e *Meta*. Tuttavia, una totale anonimizzazione renderebbe praticamente impossibile ricavare informazioni significative dai dataset, privandoli così del loro valore. Di conseguenza, l'anonimizzazione non sembra essere una soluzione praticabile.

Dall'altro lato, la pseudonimizzazione, secondo l'art. 4 (5) del RGPD consiste in una procedura che renda i dati personali non più riconducibili a specifici individui a meno non siano fornite informazioni aggiuntive. Nella maggior parte dei casi è necessaria una chiave che consente la reidentificazione dei soggetti.

Tale pseudonimizzazione può essere effettuata attraverso molteplici tecniche di encriptazione in grado di soddisfare il livello di protezione richiesto dal RGPD.[30]

Tuttavia, è necessario tenere a mente che questo sistema non sia infallibile, dal momento che esisterà sempre una chiave in grado di reidentificare i dati.

Nel caso in esame, l'APD austriaco ha ritenuto che gli identificatori raccolti da *Google Analytics* come dati di navigazione o indirizzi IP rendessero possibile la reidentificazione degli individui con mezzi ragionevoli.[31]

Di conseguenza, la Corte ha concluso che il processo di pseudonimizzazione implementato da *Google Analytics* non sia in linea con quanto richiesto dal RGPD.

---

[29] Vd. Arvind Narayanan/Vitaly Shmatikov, *Robust De-anonymisation of Large Sparse Dataset,* The University of Texas at Austin, dove è stato dimostrato che anche con poche informazioni, come delle liste anonime di valutazioni dei film, la reidentificazione dei soggetti resta possibile.

[30] Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 2014.

[31] Autorità di protezione dei dati austriaca, *Teilbescheid* D155.027 GA, Google LLC, 22.12.2021, p. 29.

Tuttavia, anche qualora i dati venissero pseudonimizzati in una maniera in linea con I requisiti del RGDP, permarrebbe l'insormontabile ostacolo rappresentato dalla sezione 702 della FISA.

Difatti, negli U.S.A. gli importatori di dati sono sottoposti all'obbligo di garantire l'accesso o di riconsegnare dati personali di cui sono in possesso, custodia o controllo. Tale obbligo è esteso anche alle chiavi criptografiche necessarie per rendere i dati intellegibili.[32]

Di conseguenza, nonostante la pseudonomizzazione, se correttamente implementata dalle aziende private, potrebbe rappresentare una soluzione percorribile, essa rischia in questo caso di essere resa invalida ancora una volta dall'ordinamento americano.

4.3. Il consenso

Come terza opzione per garantire un trasferimento transatlantico dei dati legittimo le aziende tecnologiche potrebbero affidarsi al consenso espresso esplicitamente dall'interessato, come stabilito dall´art. 49 (1) (a) RGPD. Tuttavia, questa soluzione comporterebbe molti ostacoli. A parte l'incerta natura legale dell´art. 49 RGPD, potrebbe infatti risultare impegnativo soddisfare i requisiti previsti da tale articolo.

Attualmente si discute della sussidiarietà dell´art. 49 RGPD rispetto agli art. 45 e 46 RGPD.[33] Inoltre, ci si chiede se tale articolo possa essere applicato soltanto in casi eccezionali o se le aziende tecnologiche possano affidarsi ad esso come regola generale.[34] L´EDPB, basandosi sul considerando 111 RGPD, interpreta l´art. 49 (1) (a) RGPD come applicabile solo in casi eccezionali.[35] L´APD austriaca non si è pronunciata su tale questione, poiché nel caso di *Google Analytics* la persona interessata non aveva fornito nessun consenso al trasferimento dei suoi dati.

---

[32] European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0*, 2021, p. 29.

[33] Sascha Kremer/Julia Christmann-Thoma/Kristof Kamm/Michael Matejek/Nadine Schneider, *Datentransfer nach Art. 49 DSGVO: Was geht, wenn sonst nichts geht?,* Computer und Recht (CR), 2021, pp. 784-796 (785).

[34] *Ivi*, pp. 785-787.

[35] European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25.05.2018.

Di conseguenza, le aziende che scelgono di affidarsi solamente al consenso dell'interessato rischiano di creare un'incertezza giuridica, che potrebbe anche essere amplificata nel caso in cui l'interessato ritirasse il suo consenso dopo l'esercizio del trasferimento.

Oltre a ciò, queste aziende si troverebbero ad affrontare il problema della richiesta da parte della legge di un consenso informato ed esplicito. Pertanto, in pratica, il consenso al trasferimento dei dati dovrebbe essere richiesto separatamente da quello legato all'accettazione dei *cookies*. Inoltre, per essere definita informativa, la notificazione del trasferimento dei dati dovrebbe richiedere un linguaggio che dichiari che negli Stati Uniti i dati personali potrebbero essere accessibili in circostanze che in Europa sarebbero considerate illegali.[36] Una formulazione (inevitabilmente) così forte potrebbe essere poco attraente dal punto di vista economico, poiché potrebbe avere un effetto deterrente sugli utenti di strumenti come *Google Analytics*.

In conclusione, né gli argomenti economici, né quelli giuridici incoraggiano questa soluzione.

4.4. Trattamento dei dati europei in Europa

Contrariamente alle soluzioni appena presentate, un sistema che rinunciasse al trasferimento dei dati verso gli Stati Uniti eviterebbe tutti gli ostacoli discussi fin qui. Si tratterebbe di una soluzione perfettamente in linea con il RGPD. Aziende big tech come *Google* potrebbero, ad esempio, espandere le loro *server capacity* in Europa, per trattare lì tutti i dati ivi raccolti. La sostituzione di *Google LLC* con *Google Ireland Ltd.* come partner contrattuale per gli utenti europei potrebbe essere interpretata come un primo passo in questa direzione.

Ma in seconda analisi, la sezione 10.1 dei Termini di trattamento dei dati di *Google*[37] afferma che *Google* si riserva il diritto di scegliere di trattare i dati in qualunque paese essa operi. Inoltre, non sembra probabile che aziende tecnologiche, in particolare start-ups, siano dispose a

[36] Sascha Kremer/Julia Christmann-Thoma/Kristof Kamm/Michael Matejek/Nadine Schneider, *Datentransfer nach Art. 49 DSGVO: Was geht, wenn sonst nichts geht?,* Computer und Recht (CR), 2021, pp. 784-796 (791).
[37] Vd. Google, *Google Business Data Responsibility*, 31.03.2022.

sostenere i costi legati all'implementazione di due sistemi separati per il trattamento dei dati, cancellando contemporaneamente tutte le esternalità positive derivanti dalla combinazione dei dati europei e americani. Perciò, nonostante questa soluzione sia perfettamente in linea con il RGPD, essa risulta di difficile realizzazione.

4.5. *Privacy Shield II*

Le soluzioni proposte fino a questo punto alternativamente non sono ammissibili dal punto di vista giuridico, mancano di certezza giuridica, oppure sono soggette a contraccolpi economici. Quindi, un *Privacy Shield II* potrebbe alla fine essere la soluzione migliore per risolvere le implicazioni pratiche derivanti da *Schrems II*?

Le dichiarazioni del *Chief Legal Officer* di *Google* danno l'impressione che il settore aziendale preferirebbe tale soluzione, poiché combinerebbe la certezza giuridica con la possibilità di beneficiare dell'infrastruttura commerciale già stabilita.[38]

Allo stesso tempo, anche i legislatori sembrano preferire questa soluzione. Le trattative su un nuovo "migliorato" ("*enhanced*") *Privacy Shield*, già iniziate nell'agosto del 2020,[39] si sono "intensificate" ("*intensified*") a marzo 2021.[40]Inoltre, un summit è previsto per maggio di quest'anno,[41] e le recenti decisioni delle APD europee alimentano le speranze che la discussione possa diventare più dinamica. Anche il Parlamento Europeo ha dato l'impressione di essere più interessato allo stato delle negoziazioni.[42] Contemporaneamente, dall'altra parte dell'Atlantico, gli Stati Uniti hanno indicato la loro volontà a fare concessioni, come riscontrabile nelle parole del segretario al commercio degli Stati Uniti, Gina Raimondo,

[38] Vd. la dichiarazione pubblicata dal presidente delle *Global Affairs & Chief Legal Officer* di *Google* Mr. Kent Walker, 19.01.2022.

[39] Commissione Europea, *Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross*, 10.08.2020.

[40] Commissione Europea, Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by Didier Reynders and U.S. Secretary of Commerce Gina Raimondo, 25.03.2021.

[41] Tobias Kaiser/Benedikt Fuest, *Meta threatens EU boycott; The US group fears for its advertising business because of strict EU data protection laws and warns: Facebook and Instagram could soon be shut down in the EU*, Die Welt, No. 27, 08.02.2022, p. 9 (9).

[42] Vd. Assita Kanko, *Question for a written answer to the Commission E-000629/2022*, 10.02.2022.

che ha sottolineato che un nuovo *Privacy Shield* risponderebbe alle preoccupazioni dell´UE.[43] Oltre a ciò, Joe Biden e Ursula von der Leyen hanno recentemente annunciato in una dichiarazione politica che un "accordo di principio" sia stato raggiunto.[44] Tuttavia, non è ancora stato pubblicato un documento legale che potrebbe essere analizzato.

Fatte queste premesse, gli ostacoli per il reale raggiungimento di un accordo sembrano ancora difficili a superare. Nonostante l´amministrazione Biden abbia segnalato l'intenzione di adottare nuovi *executive* e *administrative orders*, questi potrebbero non essere sufficienti per superare i problemi principali sollevati da *Schrems II*.[45] In questa decisione la CGEU ha sottolineato che in primo luogo, la sezione 702 FISA non soddisfa il requisito di proporzionalità, in quanto l´autorità delle agenzie di sorveglianza.[46] In secondo luogo, la legge statunitense non fornisce alcun rimedio giuridico agli interessati europei.[47] Se il nuovo accordo tra i Stati Uniti e l´Europa non affrontasse espressamente queste questioni, rischierebbe di essere nuovamente invalidato dalla CGEU.

Ricapitolando, un *Privacy Shield II* rappresenterebbe una soluzione che potrebbe beneficiare l'economia del trattamento dei dati, fornendo allo stesso tempo una protezione di alto livello dei dati personali europei. Tuttavia, anche il nuovo "accordo di principio" non rende ancora prevedibile quando un tale accordo sarà finalmente raggiunto.

5. Conclusioni

Avendo esaminato le più rilevanti soluzioni attualmente disponibili, riteniamo che, almeno per ora, un sistema che rinunci a trasferire i dati negli Stati Uniti sarebbe decisamente il più sicuro dal punto di vista del rispetto dei principi del RGDP. Tuttavia, tale soluzione sarebbe economicamente una sfida per le economie basate sul trattamento dei dati americani ed

[43] Vd. Foo Yun Chee, *EU aims to tighten curbs on data transfers to non-EU governments – EU document*, in *reuters.com*, 03.02.2022.
[44] Vincent Manancourt, *EU, US strike preliminary deal to unlock transatlantic data flows*, 28.03.2022.
[45] Congressional Research Service, *U.S.-EU Privacy Shield and Transatlantic Data Flows*, 22.09.2022, p. 17.
[46] CGUE, Caso C-311/18, Data Protection Commissioner v Facebook Ireland Ltd/Schrems, 16.07.2020, ECLI:EU:C:2020:559, preamboli 178-180.
[47] CGUE, Caso C-311/18, Data Protection Commissioner v Facebook Ireland Ltd/Schrems, 16.07.2020, ECLI:EU:C:2020:559, preamboli 181.

europei. Di conseguenza, riteniamo che un *Privacy Shield II* sarebbe la soluzione più vantaggiosa nel lungo periodo. Ciononostante, sarà opportuno tenere in conto il rispetto dei principi del RGDP e la giurisprudenza della CGUE nel corso delle trattative.