Provvedimento del 21 luglio 2022 [9808698]

[doc. web n. 9808698]

Provvedimento del 21 luglio 2022

Registro dei provvedimenti
n. 254 del 21 luglio 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito, "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTO il reclamo del 18 agosto 2020 presentato ai sensi dell'art. 77 del Regolamento dal Sig. XX nei confronti di Fastweb S.p.A.;

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. Il reclamo nei confronti della società e l'attività istruttoria.

Con reclamo presentato in data 18 agosto 2020, il Sig. XX ha lamentato che Fastweb S.p.A. (di seguito anche "la Società"), avrebbe trasferito a Google LLC, con sede negli Stati Uniti, i dati personali che lo riguardano trattati per il tramite del sito internet www.fastweb.it; ciò in assenza delle garanzie previste dal Capo V del Regolamento.

Nell'ambito dell'attività istruttoria avviata dal Garante, l'Ufficio, con note del 16 novembre 2020 e del 20 luglio 2021, ha chiesto alla Società di fornire informazioni e chiarimenti sui fatti oggetto di reclamo.

Con le comunicazioni del 13 gennaio 2021 e del 18 ottobre 2021, nel dare riscontro alle richieste dell'Ufficio, Fastweb S.p.A. ha dichiarato quanto segue:

il trattamento dei dati personali degli utenti del sito web www.fastweb.it è posto in

essere dalla Società per il tramite di Google Analytics 360, strumento che, mediante cookies trasmessi al browser dell'utente, raccoglie informazioni su come gli utenti del sito interagiscono con le singole pagine e con i servizi proposti. Google Analytics 360 "ha lo scopo di analizzare statisticamente ed in maniera aggregata -non, quindi, per singolo utente-, cosa accade durante la navigazione sul sito, anche al fine di migliorarne l'efficacia promozionale. (..) Le analisi sui succitati aspetti vengono (..) fornite, poi, a Fastweb sotto forma di un output statistico aggregato sulla piattaforma di visualizzazione di Google Analytics 360, che non consente di risalire al singolo utente e [al]le specifiche informazioni sottostanti" (v. nota del 13 gennaio 2021, pag. 2);

i dati oggetto di trattamento consistono nell'identificativo del cookie scaricato sul browser dell'utente, nell'indirizzo IP e nel tipo di device utilizzato (v. nota del 13 gennaio 2021, pag. 17). Oltre alle variabili di default inviate ai server di Google, la Società trasmette ulteriori informazioni di tipo personalizzato (custom), in ragione delle esigenze di reportistica, "in aggiunta, appunto, a quelle standard eseguite da Google Analytics 360" (v. nota del 18 ottobre 2021, pag. 7). Con particolare riferimento all'indirizzo IP, a partire dal 23 dicembre 2020, esso è stato "forzatamente anonimizzato da Fastweb", seguendo la procedura resa disponibile da Google a tal fine. La funzione, denominata IP-Anonymization, "corrisponde alla soppressione dell'ultimo byte dell'indirizzo IPV4 - e/o degli ultimi 80 bit dell'indirizzo IPv6 - dell'utente". La predetta operazione è posta in essere "da parte di Google stessa nel momento intermedio tra la ricezione del dato e la memorizzazione del dato pseudonimizzato sui sistemi di storage di Google". Inoltre, "l'indirizzo IP del client viene trasmesso sempre e integralmente a Google non oscurato direttamente dal browser dell'utente. L'informazione in questione –a quanto dato sapere– è poi server side oggetto di pseudonimizzazione «non appena è tecnicamente possibile» nel caso il gestore abbia impostato tale funzionalità" (v. nota del 13 gennaio 2021, pag. 11 e nota del 18 ottobre 2021, pagg. 19 e 20);

- per quanto riguarda la suddetta procedura, Fastweb S.p.A. ha altresì affermato che "non dispone (..) dell'informazione esatta se tale attività sia posta in essere da Google Ireland Limited o da Google LLC né se ciò avvenga anteriormente o meno al trasferimento dei dati verso paesi al di fuori dell'UE poiché questo dettaglio non è reso noto da Google" (v. nota del 18 ottobre 2021, pag. 20);

- in merito alla possibilità che i dati pseudonimizzati possano essere associati ad informazioni aggiuntive che consentano l'attribuzione degli stessi ad una persona fisica identificata o identificabile, la Società ha rappresentato che "non è possibile escludere che i dati pseudonimizzati possano essere associati ad ulteriori dati in possesso di Google LLC in modo da procedere alla successiva identificazione degli interessati" (v. nota del 18 ottobre 2021, pag. 23);

in relazione al trattamento sopra complessivamente delineato, la Società, il 16 agosto 2020, per il tramite del reseller iProspect S.r.l., ha sottoscritto con Google Ireland Limited i "Google Analytics Terms of Service" e sulla base dei "Google Ads Data Processing Terms" (v. art. 7 delle predette condizioni contrattuali) "ha provveduto [in qualità di titolare del trattamento] a nominare Google Ireland Limited quale responsabile (…), la quale a sua volta ha nominato quale suo sub-responsabile Google LLC" (nota del 13 gennaio 2021, pag. 31 e nota del 18 ottobre 2021, pagg. 2-4);

il trasferimento dei dati è disciplinato dall'art. 10 dei "Google Ads Data Processing Terms" ed è, pertanto, posto in essere in ragione dell'adozione, da parte di Fastweb S.p.A. in qualità di esportatore, di "Model contract clauses" individuate ai sensi dell'art. 46 del Regolamento (v. Google Ads Data Processing Terms, art. 2.1); in base a

quest'ultime, la Società acconsente che Google Ireland Limited, in veste di responsabile del trattamento, possa ricorrere alle società affiliate di Google, quali sub-responsabili, tra cui Google LLC stabilito negli Stati Uniti (v. nota del 13 gennaio 2021, pag. 20 e nota del 18 ottobre 2021, pagg. 4 e 24);

le predette clausole sono state integrate dalle misure supplementari adottate da Google (come riportate dalla Società nella nota del 13 gennaio 2021, pagg. 22-30). In merito Fastweb S.p.A. ha rappresentato che le stesse risultano adeguate poiché "sostanzialmente in linea con quanto previsto dalle linee guida" contenute nella Raccomandazione n. 1/2020 relativa alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE adottata, dal Comitato europeo per la protezione dei dati (di seguito "EDPB"), il 18 giugno 2021 (cfr. nota del 18 ottobre 2021, pagg. 21 e 22). La Società è pertanto giunta "alla conclusione che non sia necessario [implementare] ulteriori garanzie ai sensi del Capo V alla luce delle informazioni fornite da Google in merito alla gestione dei dati personali e alla valutazione del livello di adeguatezza di tali trasferimenti, tenuto conto delle circostanze del trasferimento e delle misure tecniche ed organizzative adottate da Google" (v. nota di riscontro del 13 gennaio 2021, pag. 30);

nello specifico, con riferimento alla misura tecnica definita "Encryption", la Società ha inoltre precisato che "le chiavi di cifratura, sia per la parte at rest che in transit, sono sotto il controllo di Google. In particolare le chiavi di cifratura at rest, attesa la gestione dello storage da parte di Google LLC, sono sotto il controllo della entity statunitense" (v. nota di riscontro del 18 ottobre 2021, pag. 23);

in ordine alle informazioni che la Società ha reso al Sig. XX, ai sensi dell'art. 13 del Regolamento, esse sono contenute nella "cookie policy mostrata al momento di apertura della sito www.fastweb.it (..), che rinvia in termini di eterointegrazione all'informativa di Google per quanto riguarda il servizio analytics"; mentre per quanto concerne gli aggiornamenti da riportare nell'informativa a seguito della pronuncia della Corte di Giustizia dell'Unione Europea, del 16 luglio 2020, n. C-311/18, le "modifiche sono state apportate direttamente da Google a valle delle proprie valutazioni" (v. nota del 13 gennaio 2021, pag. 14 e nota del 18 ottobre 2021, pag. 25 e All. 8).

In merito a quanto rappresentato dalla Società, sono state inoltre acquisite ulteriori osservazioni da parte del reclamante, trasmesse con nota del 21 febbraio 2021.

Il 22 dicembre 2021 l'Ufficio ha notificato, ai sensi dell'art. 166, comma 5, del Codice, le presunte violazioni del Regolamento riscontrate con riferimento dell'art. 5, par. 1, lett. a), e par. 2, del Regolamento e dell'art. 13 del Regolamento, nonché degli artt. 44 e 46, del Regolamento.

Il 21 febbraio 2022 Fastweb S.p.A. ha inviato i propri scritti difensivi nei quali ha rappresentato che:

a) in ordine alla natura dei dati, le informazioni oggetto di trasferimento "anche a seguito delle misure adottate dal titolare non [sono] qualificabili quali dati personali ex art 4 c. 1 GDPR"; ciò in quanto "l'indirizzo IP presumibilmente utilizzato in una connessione eseguita da un utente residenziale, normalmente, non consente l'identificazione di una singola sessione di navigazione riferibile ad un solo utente, ma piuttosto di una moltitudine di utenti" (v. nota del 21 febbraio 2022, pagg. 3-4);

b) in merito alla funzione di IP-Anonymization, a seguito della sua attivazione "l'indirizzo IP nella sua completezza non viene memorizzato in nessun momento in modo permanente giacché il troncamento avviene integralmente nella memoria volatile dei server di Google, in

maniera quasi istantanea dopo che la connessione è stata avviata dall'utente". Invero, "il tempo intercorrente tra la ricezione dell'indirizzo IP e il suo troncamento è quantificabile nella misura di millesimi di secondo. In sostanza, la pseudonimizzazione dell'IP avviene entro un massimo di 500 microsecondi il ~50% delle volte ed entro 1 millisecondo il 99% delle volte, in funzione dal carico puntuale del server che provvede all'operazione." (v. nota del 21 febbraio 2022, pag. 5);

c) relativamente agli elementi in base ai quali Fastweb S.p.A. ha effettuato la propria valutazione in ordine all'adeguatezza dello strumento prescelto ai fini del trasferimento e all'adozione delle misure supplementari da adottare nel caso di specie, la Società ha tenuto conto del fatto che "i dati trasferiti sono di natura molto limitata in termini di qualità e quantità" rendendo pertanto "molto difficile la (..) identificazione concreta [dell'utente]"; ciò considerato altresì che a seguito dell'attivazione, nel caso in esame, della IP-Anonymization "la possibilità per chiunque di identificare il ricorrente sulla base dell'indirizzo IP troncato è ancora più ridotta, se non nulla" (v. nota del 21 febbraio 2022, pag. 13). Ha inoltre evidenziato che "i dati come IP address -peraltro pseudonimizzati- e unique identifier del device" non possano essere considerati "utili e di interesse per la sorveglianza da parte dell'intelligence USA" in quanto l'"obiettivo di sorveglianza preposto dalla Sezione 702 (..) è limitato alle sole informazioni di intelligence straniera" (v. nota del 21 febbraio 2022, pag. 14). A sostegno di ciò, la Società ha da ultimo riportato quanto dichiarato da Google in un recente blog post dello scorso 19 gennaio 2022 (consultabile al seguente indirizzo: https://blog.google/around-the-globe/google-europe/its-time-for-a-new-eu-us-data-transfer-framework/), rispetto alla circostanza che "nei 15 anni di operatività del servizio non è mai stata avanzata una richiesta di accesso ai dati di Analytics da parte dell'intelligence statunitense" (nota del 21 febbraio 2022, pag. 8);

d) con riferimento alle misure supplementari, quelle implementate nel caso in esame, devono considerarsi adeguate in quanto "rientrano tra quelle esplicitamente raccomandate come misure supplementari nell'allegato 2 della Raccomandazione n. 1/2020" (v. nota del 21 febbraio 2021, pagg. 13-14);

e) per quanto concerne il livello di autonomia di Fastweb S.p.A. in merito alle scelte relative ai trasferimenti di dati verso Paesi terzi, la Società ha ribadito che in ragione della posizione di monopolio rivestita da Google nel mercato, sussiste di fatto "l'impossibilita per la Società di chiedere e ottenere approfondimenti o verifiche tecniche puntuali" in ordine allo strumento di Google Analytics, nonché di "apportare modifiche o correttivi di sorta al prodotto, al di là della cautela già adottata di attivare la funzione di mascheramento dell'indirizzo IP" (v. nota del 21 febbraio 2022, pagg. 8-9);

f) in ordine all'inadeguatezza dell'informativa ex art. 13 del Regolamento, la stessa è stata aggiornata dalla Società secondo le indicazioni fornite dall'Autorità nella notifica di violazione trasmessa ai sensi dell'art. 166, comma 5 del Codice (v. nota del 21 febbraio 2022, pag. 10).

In data 28 marzo 2022, nel corso dell'audizione richiesta dalla Società, quest'ultima, nel richiamare integralmente le memorie sopra citate, ha altresì rappresentato che:

- in ordine alle misure supplementari di natura tecnica adottate nel caso di specie, Google Analytics, in quanto strumento di web analytics, "non può prescindere dall'individuazione del device, del browser e del sito visitato, rendendo quindi impossibile l'adozione della cifratura at rest con chiavi di cifratura gestite dal titolare (misura suggerita dall'EDPB nella Raccomandazione n. 1/2020), salvo grandemente ridurre se non direttamente annullare le funzionalità di analisi della piattaforma stessa" (v. verbale del 28 marzo 2022, pag. 3);

- la Società "ha valutato concretamente la possibilità di avvalersi di strumenti alternativi a

Google Analytics, identificandone dei possibili sostituti", evidenziando al contempo che "le soluzioni identificate non sono comunque in grado di garantire a Fastweb S.p.A. le medesime prestazioni e condizioni di servizio" (v. verbale del 28 marzo 2022, pag. 3).

2. Osservazioni sulla normativa in materia di protezione dei dati personali e violazioni accertate.

In primis si rappresenta che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante".

Tanto doverosamente premesso, all'esito dell'attività istruttoria e dell'esame della documentazione acquisita nel corso della stessa è stato accertato che i trasferimenti effettuati da Fastweb S.p.A. verso Google LLC (con sede negli Stati Uniti), per il tramite dello strumento di Google Analytics (di seguito anche "GA"), sono stati posti in essere in violazione degli artt. 44 e 46 del Regolamento; si rileva, altresì, che sono emerse le violazioni dell'art. 5, par. 1, lett. a) e par. 2, dell'art. 13, par. 1, lett. f), e dell'art. 24, del Regolamento, come di seguito esplicitato.

2.1 I trasferimenti di dati personali verso gli Stati Uniti effettuati per il tramite di Google Analytics.

Google Analytics è uno strumento di web analytics fornito da Google ai gestori di siti internet che consente a questi ultimi di analizzare dettagliate statistiche sugli utenti nell'ottica di ottimizzare i servizi resi e di monitorare le proprie campagne di marketing.

Nell'ambito del perseguimento di finalità statistiche, ovvero volte ad ottenere informazioni aggregate sull'attività degli utenti all'interno del proprio sito web, Fastweb S.p.A. utilizza GA nella sua versione a pagamento (denominata Google Analytics 360). La stessa agisce in qualità di titolare del trattamento e designa Google Ireland Limited responsabile, ai sensi dell'art. 28 del Regolamento, sulla base dei "Google Analytics Terms of Service" e dei "Google Ads Data Processing Terms". Quest'ultima, ai sensi dei predetti termini di servizio, può avvalersi di altri soggetti, in qualità di sub-responsabili del trattamento, fra cui Google LLC con sede negli Stati Uniti.

Per quanto concerne il trattamento effettuato tramite GA, è stato rilevato che Fastweb S.p.A. raccoglie, mediante cookies trasmessi al browser degli utenti, informazioni in ordine alle modalità di interazione di questi ultimi con il sito web, nonché con le singole pagine e con i servizi proposti.

Più nel dettaglio, i dati raccolti consistono in: identificatori online unici che consentono sia l'identificazione del browser o del dispositivo dell'utente che visita il sito web, sia del gestore stesso del sito (attraverso l'ID account Google); indirizzo, nome del sito web e dati di navigazione; informazioni relative alle variabili c.d. custom; indirizzo IP del dispositivo utilizzato dall'utente; informazioni relative al browser, al sistema operativo, alla risoluzione dello schermo, alla lingua selezionata, nonché a data e ora della visita al sito web.

Al riguardo, merita evidenziare contrariamente a quanto rappresentato dalla Società sul punto (v. supra par. 1, punto a) che 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 (v. Gruppo ex art. 29, WP 136 - Parere n. 4/2007 sul concetto di dati personali, del 20 giugno 2007, pag. 16). Tutto ciò soprattutto ove, come nel caso di specie, l'IP sia associato ad altre informazioni relative al browser utilizzato, alla data e all'ora della navigazione (cfr. considerando 30 del Regolamento).

A questo si aggiunga che, qualora il visitatore del sito web faccia accesso al proprio account

Google –circostanza, peraltro verificatasi nell'ipotesi in esame, che può essere numericamente molto rilevante– e abbia selezionato alcune opzioni in tale account (ad esempio quella volta alla ricezione di pubblicità personalizzata), i dati sopra indicati possono essere associati ad altre informazioni presenti nel relativo account, quali l'indirizzo email (che costituisce l'user ID dello stesso), il numero di telefono ed eventuali ulteriori dati personali tra cui il genere, la data di nascita o l'immagine del profilo dell'utente.

Resta comunque fermo che, indipendentemente dall'accesso all'account Google, l'indirizzo IP può ad ogni modo consentire soprattutto, come sopra già esplicitato, ove associato ad altre informazioni relative al browser utilizzato e alla data e all'ora della navigazione di identificare un dispositivo di comunicazione elettronica e, quindi, indirettamente l'utente.

Nell'ambito del servizio GA, Google ha inoltre messo a disposizione dei gestori dei siti web l'opzione denominata "IP-Anonymization" che comporta l'invio a Google Analytics dell'indirizzo IP dell'utente previo oscuramento dell'ottetto meno significativo (in base a tale operazione, ad esempio, gli indirizzi da 122.48.54.0 a 122.48.54.255 sarebbero sostituiti da 122.48.54.0). Nel caso di specie, la Società ha dichiarato che la suddetta opzione è stata attivata dal 23 dicembre 2020 (v. nota del 13 gennaio 2021, pag. 11 e nota del 18 ottobre 2021, pag. 19).

Sul punto, è emerso in primis che di regola tale operazione è effettuata sui server di Google LLC, ma che, rispetto ai dati raccolti nell'Unione europea, la stessa è posta in essere nei sistemi ivi ubicati, salvo casi eccezionali. Con riferimento a queste ultime ipotesi non sono stati tuttavia rinvenuti sufficienti elementi riguardo a tali casistiche, nonché al grado di probabilità che il trattamento dell'IP avvenga negli Stati Uniti. Più in generale, pertanto, non appare possibile individuare con certezza ove abbia effettivamente luogo l'operazione di troncamento dell'ottetto meno significativo (ovvero se nei sistemi di Google siti nell'Unione europea o in quelli statunitensi). Non può dunque escludersi a priori che l'indirizzo IP, nella sua interezza, sia trasmesso ai sistemi di Google LLC prima dell'operazione di troncamento, con il rischio che lo stesso possa essere oggetto di accesso da parte di Autorità pubbliche.

In secondo luogo, con riferimento all'efficacia della misura di "IP-Anonymization", merita ad ogni modo evidenziare che la stessa consiste di fatto in una pseudonimizzazione del dato relativo all'indirizzo di rete dell'utente, poiché, a differenza di quanto sostenuto dalla Società al riguardo (v. supra par. 1, punto b), il troncamento dell'ultimo ottetto non impedisce a Google LLC di re-identificare l'utente medesimo, tenuto conto delle informazioni complessivamente detenute dalla stessa relative agli utenti del web. Sussiste, poi, in capo alla medesima Google LLC la possibilità qualora l'interessato abbia effettuato l'accesso al proprio profilo Google di associare, come già evidenziato, l'indirizzo IP ad altre informazioni aggiuntive già in suo possesso (quali le informazioni contenute nell'account utente). Pertanto, si ritiene, che Google nonostante l'attivazione dell'"IP-Anonymization" sia in grado di identificare comunque un utente in modo diretto (qualora quest'ultimo abbia fatto accesso al proprio account), ovvero tramite l'indirizzo IP, ricevuto prima dell'operazione di "IP-Anonymization", o, ancora, tramite re-identificazione effettuata sulla base dell'indirizzo IP privo dell'ultimo ottetto in combinazione con le altre informazioni in suo possesso.

Considerato quindi che, per tutte le ragioni sopra espresse, l'utilizzo di GA, da parte dei gestori dei siti web quale Fastweb S.p. comporta il trasferimento dei dati personali dei visitatori dei suddetti siti a Google LLC con sede negli Stati Uniti; trattandosi di trasferimenti effettuati verso un paese terzo che non garantisce un livello di protezione adeguato ai sensi della normativa di protezione dei dati (ossia gli Stati Uniti), gli stessi devono essere posti in essere in conformità al Capo V del Regolamento.

2.2 L'illiceità dei trasferimenti a seguito della pronuncia C-311/18, del 16 luglio 2020, c.d. Schrems II.

Si rammenta che la Corte di Giustizia dell'Unione Europea, con la pronuncia C-311/18, del 16 luglio 2020 (c.d. Schrems II), nel dichiarare l'invalidità della decisione della Commissione UE n. 2016/1250 del 12 luglio 2016, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (c.d. Privacy Shield), ha constatato che il diritto interno degli Stati Uniti (in particolare l'Executive Order 12333 e l'art. 702 del Foreign Intelligence Surveillance Act - di seguito "FISA 702") comporta deroghe alla normativa in materia di protezione di dati che eccedono le restrizioni ritenute necessarie in una società democratica. Tutto ciò con particolare riferimento alle disposizioni che consentono alle Autorità pubbliche, nel quadro di determinati programmi di sicurezza nazionale, di accedere senza adeguate limitazioni ai dati personali oggetto di trasferimento, nonché alla mancata previsione di diritti, in capo ai soggetti interessati, azionabili in sede giudiziaria.

La Corte, con la medesima pronuncia, ha inoltre ribadito la validità della decisione n. 2010/87/CE della Commissione del 5 febbraio 2010 concernente le clausole contrattuali tipo per il trasferimento di dati personali a responsabili stabiliti in paesi terzi – clausole adottate da Fastweb S.p.A. nel caso di specie.

Al contempo ha puntualizzato che, in base al principio di accountability, i titolari del trattamento, in qualità di esportatori, sono comunque tenuti a verificare, caso per caso e, ove necessario, in collaborazione con l'importatore nel paese terzo, se la legge o la prassi di quest'ultimo incidano sull'efficacia delle garanzie adeguate contenute nelle predette clausole; ciò al fine di determinare se le garanzie previste dalle clausole contrattuali tipo possano essere rispettate nella pratica (art. 5, par. 2, e art. 24; cfr. anche Raccomandazione n. 1/2020 relativa alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, del 18 giugno 2021, paragrafi 1-5).

In termini generali, occorre dunque valutare, in concreto, ossia sulla base delle circostanze del trasferimento, se lo strumento prescelto dall'esportatore, tra quelli individuati dall'art. 46 del Regolamento, sia efficace nel caso specifico.

Tale esame, come rilevato dal Comitato europeo per la protezione dei dati - di seguito "EDPB" (v. Raccomandazione n. 1/2020, cit., pag. 4), deve "concentrarsi innanzitutto sulla legislazione del paese terzo [e sulle prassi applicabili] rilevant[i] per il trasferimento [nonché] sullo strumento di trasferimento [individuato] ai sensi dell'articolo 46 del RGPD" al fine di verificare che la predetta legislazione e le suddette prassi non impediscano, di fatto, il rispetto, da parte dell'importatore, degli obblighi previsti dallo strumento utilizzato.

Più nel dettaglio, la valutazione di cui sopra "comporta l'esigenza di determinare se il trasferimento in questione rientri o meno nell'ambito di applicazione della [sovra citata normativa]". Essa deve "essere basata su fattori oggettivi, indipendentemente dalla probabilità di accesso ai dati personali" (v. Parere congiunto 2/2021 dell'EDPB e del GEPD sulla decisione di esecuzione della Commissione europea relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi, adottato il 14 gennaio 2021, par. 86).

Rilevano a tal fine le caratteristiche dello specifico trasferimento posto in essere quali: le finalità, la natura dei soggetti coinvolti, il settore in cui avviene il trasferimento, le categorie dei dati personali trasferiti, la circostanza che i dati siano conservati nel paese terzo o vi si acceda da remoto, il formato dei dati da trasferire e gli eventuali trasferimenti successivi (v. Raccomandazione n. 1/2020, cit., par. 33).

La valutazione richiesta all'esportatore, dunque, deve concentrarsi sulla legislazione e sulle prassi applicabili, nel paese terzo, ai dati specificamente trasferiti e comportare la verifica della "possibilità o meno, per le autorità pubbliche del paese terzo (…) di tentare di accedere ai dati" nonché della "capacità o meno, per le autorità pubbliche del paese terzo (…) di accedere ai dati

attraverso l'importatore stesso o attraverso i fornitori di telecomunicazioni o i canali di comunicazione" (v. Raccomandazione n. 1/2020, cit., par. 31).

In merito alla predetta possibilità di accesso, da parte delle Autorità statunitensi, peraltro, occorre considerare che essa trova conferma nel "Transparency report on United States national security requests for user information" messo a disposizione da Google sul proprio sito (reperibile al seguente link https://transparencyreport.google.com/user-data/us-national-security?hl=en); report ove sono riportati i dati numerici inerenti alle richieste di accesso ricevute da Google, ai sensi del FISA 702, su istanza delle Autorità statunitensi.

Tanto doverosamente premesso, con riferimento a quanto sostenuto dalla Società rispetto a tali profili nelle proprie memorie difensive, merita evidenziare che:

- in ordine alla valutazione di idoneità delle misure supplementari adottate nel caso di specie (v. supra, par. 1, punto c), la Società ha basato la propria valutazione sulla limitata capacità di identificazione degli utenti in ragione della natura e della quantità dei dati raccolti; circostanza che, come sopra evidenziato (v. par. 2.1), non risulta configurabile rispetto ai trattamenti dei dati posti in essere tramite GA. La stessa ha inoltre considerato che la possibilità di accesso da parte dell'Autorità statunitensi rappresenta "un evento probabilistico di realizzazione del tutto incerta e statisticamente trascurabile" (v. nota del 21 febbraio 2022, pag. 8). Sul punto, di contro, si ribadisce che la Corte, nella succitata pronuncia, non ha fatto riferimento ad "alcun fattore soggettivo, come ad esempio, la probabilità di accesso" ai dati personali trasferiti (v. Parere congiunto 2/2021 dell'EDPB e del GEPD, cit., par. 87);

- relativamente alle limitazioni addotte dalla Società rispetto alla tipologia di dati che possono essere oggetto di accesso ai sensi del FISA 702 (v. supra, par. 1, punto c), anche l'indirizzo IP è ricompreso tra le informazioni d'interesse per le Autorità statunitensi unitamente ad altri metadata; circostanza che emerge peraltro dal "Transparency report on United States national security requests for user information" messo a disposizione da Google sul proprio sito web (v. in particolare, la descrizione contenuta nella sezione denominata "non-content requests under FISA", che riporta espressamente il riferimento anche a "non-content metadata", quali gli indirizzi IP).

2.3. Inidoneità delle misure supplementari adottate dal titolare del trattamento.

Qualora a seguito della valutazione di cui sopra si rilevi che la legislazione e le prassi del paese terzo impediscano all'importatore di rispettare gli obblighi previsti dallo strumento di trasferimento prescelto, come constatato nel caso di specie, gli esportatori devono adottare misure supplementari che garantiscano un livello di protezione dei dati personali sostanzialmente equivalente a quello previsto dal Regolamento (cfr. Raccomandazione n. 1/2020, cit., paragrafi 50-57, che reca l'indicazione dei criteri ai fini dell'individuazione delle misure da adottare).

Al riguardo, in ordine alle misure supplementari di natura tecnica, ma anche contrattuale e organizzativa, adottate nell'ipotesi in esame, merita rilevare quanto segue.

Le misure di natura tecnica consistono nell'adozione di meccanismi di cifratura dei dati, durante il trasferimento fra sistemi (in transit) e quando sono memorizzati nei sistemi (at rest).

La cifratura in transito è adottata ove i dati siano trasferiti fra diversi sistemi, servizi o data center attraverso reti o infrastrutture non controllate dalla Società (es.: reti geografiche).

La cifratura at rest riguarda invece i dati dell'utente che sono memorizzati su unità disco o in unità di backup e si basa sulla cifratura dei dati mediante algoritmi standard (in genere tramite AES256) e sulla cifratura, a diversi livelli, a partire dalla cifratura a livello hardware, in base al tipo di applicazione e ai rischi specifici. L'accesso ai data center di Google LLC è protetto da 6 livelli di

misure di sicurezza fisica.

In merito, si evidenzia che, tenuto conto delle indicazioni rese dall'EDPB nella Raccomandazione n. 1/2020, le misure tecniche summenzionate non risultano adeguate.

In ordine ai meccanismi di cifratura dei dati sopra evidenziati, esse, infatti, non sono sufficienti ad evitare i rischi di un accesso, ai fini di sicurezza nazionale, ai dati trasferiti dall'Unione europea da parte delle Autorità pubbliche degli Stati Uniti, in quanto le tecniche di cifratura adottate prevedono che la disponibilità della chiave di cifratura sia in capo a Google LLC che la detiene, in qualità di importatore, in virtù della necessità di disporre dei dati in chiaro per effettuare elaborazioni e fornire servizi.

Merita inoltre evidenziare che l'obbligo di consentire l'accesso, da parte delle Autorità statunitensi, ricade su Google LLC non solo con riferimento ai dati personali importati, ma anche in ordine alle eventuali chiavi crittografiche necessarie per renderli intelligibili (v. anche Raccomandazione 1/2020, cit., par. 81).

Da ciò ne consegue che, contrariamente a quanto sostenuto dalla Società (v. supra punto d); cfr. anche verbale del 28 marzo 2022, pag. 3), fintanto che la chiave di cifratura rimanga nella disponibilità dell'importatore, le misure adottate non possono ritenersi adeguate (v. Raccomandazione 1/2020, cit., par. 95).

Ciò anche tenuto conto di alcune misure contrattuali e organizzative consistenti nello specifico nell'impegno a:

> verificare, ai sensi della normativa statunitense, la legittimità di ogni singola richiesta di accesso ai dati degli utenti oggetto di trasferimento da parte delle Autorità pubbliche, valutandone la proporzionalità; non accogliere la stessa ove, a seguito di un'attenta valutazione, si concluda che non sussistano i presupposti in base alla normativa di riferimento;
>
> comunicare tempestivamente all'interessato le richieste di accesso provenienti dalle Autorità pubbliche statunitensi, salvo che tale comunicazione sia vietata dalla relativa normativa, informando ad ogni modo l'interessato qualora il divieto di cui sopra venga revocato;
>
> pubblicare un "Transparency Report" recante una sintesi delle richieste di accesso ai dati ricevute da parte delle Autorità pubbliche statunitensi, nella misura in cui tale pubblicazione sia consentita dalla relativa normativa;
>
> pubblicare la policy di gestione delle richieste di accesso ai dati degli utenti oggetto di trasferimento da parte delle Autorità pubbliche statunitensi.

In merito infatti si rileva che, come considerato dall'EDPB, in assenza di misure tecniche idonee –circostanza accertata nel caso di specie– le misure contrattuali e organizzative sopra indicate, di per sé, non possono ridurre o impedire le possibilità di accesso ai dati oggetto di trasferimento da parte delle Autorità statunitensi (cfr. Raccomandazione 1/2020, cit., par. 53).

Alla luce di quanto complessivamente sopra rappresentato, pertanto, le misure supplementari adottate nel caso di specie non possono considerarsi adeguate con conseguenziale illiceità, ai sensi dell'art. 44 e dell'art. 46 del Regolamento, dei relativi trasferimenti di dati personali verso gli Stati Uniti.

2.4 Accountability del titolare

Il titolare è tenuto a mettere in atto "misure tecniche e organizzative adeguate per garantire, ed

essere in grado di dimostrare, che il trattamento è effettuato conformemente al [Regolamento]" (c.d. principio di accountability; cfr. art. 5, par. 2 e art. 24, par. 1 del Regolamento).

Spetta dunque proprio al titolare il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto della normativa rilevante in materia.

Il Regolamento, infatti, pone con forza l'accento sulla "responsabilizzazione" del titolare, ossia, sull'adozione di comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione della disciplina di protezione dei dati personali (si veda, in particolare l'art. 24 del Regolamento).

L'attuazione del principio di accountability con riferimento ai trasferimenti di dati verso paesi terzi, pone, in capo al titolare in qualità di esportatore, la responsabilità di verificare, caso per caso e, ove necessario, in collaborazione con l'importatore nel paese terzo, se la legge o la prassi di quest'ultimo incidano sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento di cui all'articolo 46 del Regolamento.

In tali casi, l'esportatore è tenuto ad adottare, in applicazione di tale principio, misure supplementari che consentano all'importatore di rispettare gli obblighi previsti dallo strumento adottato a sensi dell'art. 46 del Regolamento; tutto ciò al fine di assicurare che il livello di protezione delle persone fisiche garantito dal Regolamento non sia pregiudicato (v. art. 44 del Regolamento; cfr. al riguardo, Raccomandazione 1/2020, cit., paragrafi 1-5).

Per tutte le ragioni su esposte, ferma restando la rilevata inidoneità delle misure supplementari adottate nel caso di specie, non può essere accolto quanto sostenuto da Fastweb S.p.A. in ordine alla mancanza di autonomia della stessa rispetto alle decisioni da assumere in merito al trasferimento di dati verso paesi terzi (v. supra, par. 1, punto e); ciò considerato che la Società, in ragione del ruolo rivestito ai sensi della disciplina di protezione dei dati personali, è tenuta, come già chiarito, a mettere in atto, anche nel contesto dei trasferimenti transfrontalieri, misure adeguate ed efficaci a tutela dei diritti e delle libertà degli interessati e ad essere in grado di dimostrare la conformità delle stesse al Regolamento.

Alla luce delle considerazioni di cui sopra, nel porre in essere la condotta descritta, Fastweb S.p.A. ha quindi violato gli artt. 5, par. 2, e 24, del Regolamento.

2.5. Inidoneità dell'informativa resa ai sensi dell'art. 13 del Regolamento.

Con riferimento alle informazioni che devono essere rese all'interessato, ai sensi dell'art. 13 del Regolamento, si fa presente che l'informativa fornita al reclamante sul sito www.fastweb.it, all'atto della raccolta dei dati che lo riguardano (v. nota del 13 gennaio 2021, pag. 14) non era pienamente conforme alle disposizioni contenute nell'art. 13, par. 1, lett. f) del Regolamento.

Invero, in considerazione del fatto che i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" (art. 5, par. 1, lett. a), del Regolamento), il titolare del trattamento, qualora sia posto in essere un trasferimento di dati personali, ha l'obbligo, nel rispetto del principio di trasparenza, di rendere edotti gli interessati anche in ordine "all'intenzione di trasferire dati personali a un paese terzo" nonché "all'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili" (art. 13, par. 1, del Regolamento).

Al riguardo, nel prendere comunque atto dell'avvenuto aggiornamento nei termini suddetti dell'informativa da rendere agli utenti sul sito www.fastweb.it (v. allegato "Cookie policy del portale Fastweb" al verbale del 28 marzo 2022 e cfr. supra par. 1, punto f), si rileva che il modello a suo

tempo fornito da Fastweb S.p.A. al reclamante nel caso di specie, non definiva chiaramente tutti gli elementi di cui all'art. 13, par. 1, lett. f) del Regolamento concernenti il trasferimento.

Ne consegue, pertanto, con riferimento a tale modello, la violazione dell'art. 5, par. 1, lett. a) e dell'art. 13, par. 1, lett. f), del Regolamento.

3. Conclusioni: dichiarazione di illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2 del Regolamento.

Per i suesposti motivi l'Autorità ritiene che le dichiarazioni, la documentazione e le ricostruzioni fornite dal titolare del trattamento nel corso dell'istruttoria, non consentano di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e che risultino pertanto inidonee a disporre l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali effettuato dalla Società risulta quindi illecito, nei termini complessivamente sopra indicati, in relazione all'art. 5, par. 1, lett. a) e par. 2, all'art. 13, par. 1, lett. f), all'art. 24, e agli artt. 44 e 46, del Regolamento.

La violazione delle disposizioni sopra richiamate comporta l'applicazione delle sanzioni amministrative previste dall'art. 83, par. 5, lettere a), b) e c), del Regolamento.

Al riguardo, con riferimento agli elementi da prendere in considerazione al fine di valutare se infliggere una sanzione amministrativa pecuniaria (art. 83, par. 2, del Regolamento), si rileva in primis che, in relazione alla natura e alla gravità della violazione, le operazioni di trattamento oggetto di contestazione non hanno avuto ad oggetto categorie particolari di dati personali.

Con riguardo all'elemento soggettivo del trasgressore, occorre considerare che Fastweb S.p.A. –stante l'asimmetria di potere contrattuale derivante dalla primaria posizione di mercato assunta da Google nel settore dei servizi di web analytics– ha erroneamente assunto come idonee, sulla base delle informazioni rese da Google, le misure supplementari adottate da quest'ultima senza esercitare alcun potere decisionale in merito alle stesse.

Relativamente alle misure adottate dalla Società per attenuare il danno subito dagli interessati, si prende altresì atto delle iniziative intraprese dal titolare del trattamento, concernenti l'aggiornamento del testo dell'informativa presente sul sito internet della Società e l'adesione all'opzione di "IP-Anonymization" messa a disposizione da Google (v. nota del 13 gennaio 2021, pag. 11 e nota del 18 ottobre 2021, pag. 19, 20 e 25; cfr. anche verbale del 28 marzo 2022, pag. 3).

Rileva, inoltre, ai fini delle valutazioni dell'Autorità, l'attività di leale collaborazione con il Garante nel corso del procedimento.

La natura e la gravità della violazione, il carattere colposo della stessa, nonché gli ulteriori elementi sopra richiamati inducono pertanto a qualificare la fattispecie in esame come "violazione minore" (v. art. 83, par. 2, e cons. 148 del Regolamento).

Si ritiene, quindi, che, relativamente al caso di specie, occorra ammonire il titolare del trattamento, ai sensi degli artt. 143 del Codice e 58, par. 2, lett. b), del Regolamento, per aver effettuato un trattamento in violazione dell'art. 5, par. 1, lett. a) e par. 2, dell'art. 13, par. 1, lett. f), dell'art. 24, e degli artt. 44 e 46, del Regolamento.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento del Garante n. 1/2019, concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

TUTTO CIÒ PREMESSO IL GARANTE:

a) ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, dichiara l'illiceità del trattamento dei dati personali degli utenti del sito www.fastweb.it posto in essere, per il tramite di Google Analytics, da Fastweb S.p.A. con sede in Milano, P.I. 12878470157, in ordine alla violazione degli artt. 5, par. 1, lett. a) e par. 2, dell'art. 13, par. 1, lett. f), dell'art. 24, e degli artt. 44 e 46, del Regolamento;

b) ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, ingiunge a Fastweb S.p.A. di conformare al Capo V del Regolamento entro il termine di novanta giorni dalla notifica del presente provvedimento, il trattamento di dati personali degli utenti del sito www.fastweb.it effettuato per il tramite di Google Analytics, adottando misure supplementari adeguate;

c) ai sensi dell'art. 58, par. 2, lett. j), del Regolamento, ordina la sospensione dei flussi, verso Google LLC con sede negli Stati Uniti, dei dati personali sopra individuati, ove Fastweb S.p.A. non ottemperi a quanto stabilito al punto b) del presente dispositivo entro il termine ivi previsto;

d) ai sensi del considerando 148 e dell'art. 58, par. 2, lett. b), del Regolamento ammonisce Fastweb S.p.A. per aver effettuato un trattamento di dati personali in violazione degli artt. 5, par. 1, lett. a) e par. 2, dell'art. 13, par. 1, lett. f), dell'art. 24, e degli artt. 44 e 46, del Regolamento;

e) ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019, concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

Ai sensi del 157 del Codice, richiede a Fastweb S.p.A. di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto disposto nel presente provvedimento e di fornire comunque riscontro adeguatamente documentato, entro il termine di novanta giorni dalla data della notifica della presente decisione; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. e) del Regolamento.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. del 1° settembre 2011, n. 150, avverso il presente provvedimento è possibile proporre ricorso dinanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 21 luglio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Mattei