ORDINES
Per un sapere interdisciplinare sulle istituzioni europee

ISSN 2421-0730
NUMERO 1 – GIUGNO 2021

ALESSANDRO MANFREDI

Big Tech e trattamento dei dati personali. Il caso WhatsApp e la sentenza Schrems II

ABSTRACT - Taking a cue from the grievances expressed by the Italian Data Protection Authority towards the updating of the WhatsApp privacy policy, the work will analyse the effective application of the GDPR on a case of large-scale personal data processing. Through the analysis of the WhatsApp privacy policy the main institutes and principles of the Regulation applied to the specific case will be identified, deepening their underlying philosophy. The study of the consent institution will be enhanced, identifying its legal basis, the founding elements and the applicative characteristics in the contractual context. Finally, through a look at the Facebook group's "global operations", the impact of the Schrems II judgement and the effects of the abolition of the Privacy Shield on the transfer of data outside the EU will be highlighted.

KEYWORDS - GDPR - WhatsApp - Privacy policy - Schrems II - consent to the processing of personal data

ORDINES
Per un sapere interdisciplinare sulle istituzioni europee

1/2021

ALESSANDRO MANFREDI*

Big Tech e trattamento dei dati personali. Il caso WhatsApp e la sentenza Schrems II**

SOMMARIO: *1. Il caso WhatsApp: aggiornamento dei termini di servizio e informativa privacy. L'intervento del Garante per la protezione dei dati personali. Posizioni contrastanti: gli obiettivi del Gruppo Facebook e i dubbi del Garante - 2. I principali punti d'interesse presenti nell'informativa privacy di WhatsApp, le considerazioni del Garante per la protezione dei dati personali. Il principio di trasparenza e il diritto di informazione, riferimenti alle principali norme di settore. Finalità di utilizzo dei dati, le comunicazioni di servizio e commerciali. Il diritto di accesso ai dati - 3. Il consenso al trattamento dei dati. Base giuridica di riferimento ed elementi caratterizzanti. Consenso e conclusione di un contratto: le principali disposizioni della Corte di Cassazione. Il principio di minimizzazione dei dati e le finalità di trattamento: il criterio di specificità. Liceità del Consenso - 4. Collaborazione con le altre aziende di Facebook e operazioni globali. Il dato personale, valore sociale ed economico. Trasposizione dei dati all'estero e collocazione fisica dei datacenter di WhatsApp fuori dall'Unione Europea. Privacy Shield: la sentenza Schrems II.*

1. Il caso WhatsApp: aggiornamento dei termini di servizio e informativa privacy. L'intervento del Garante per la protezione dei dati personali. Posizioni contrastanti: gli obiettivi del Gruppo Facebook e i dubbi del Garante

Con una nota inoltrata ai propri utenti l'applicazione di messaggistica WhatsApp, facente parte del gruppo Facebook, ha illustrato i nuovi termini di servizio e la nuova informativa privacy legata all'utilizzo dell'applicazione. Aggiornare i propri utenti sui cambiamenti cui è posta la privacy policy è prassi ed obbligo di ogni entità giuridica che faccia uso di dati personali, sia essa pubblica sia essa privata, in ossequio ai parametri previsti dal Regolamento n. 2016/679 General Data Protection Regulation (GDPR). Tuttavia, nel caso preso in esame le particolarità riguardano la genericità delle informazioni inerenti ai nuovi criteri di trasposizione e condivisione dei dati tra WhatsApp e le diverse aziende del gruppo Facebook.

L'azienda afferma che i cambiamenti riguardino in modo particolare la crescente piattaforma WhatsApp Business, specificando come i dati dei cittadini europei non vengano in alcun modo condivisi per il

* Dottore in Giurisprudenza.

** Contributo sottoposto a valutazione anonima.

miglioramento dei prodotti e delle pubblicità forniti da Facebook[1]. Nonostante ciò, è stato manifestato riserbo dal Garante per la protezione dei dati personali avverso alle novità introdotte da WhatsApp. Attraverso una nota, il Garante ha affermato come i dati inseriti nell'informativa privacy dell'applicazione siano poco chiari e intelligibili, specificando come questi debbano essere valutati attentamente alla luce della disciplina in materia di protezione dei dati personali[2]. Inoltre, a riprova del carattere emergenziale della situazione, la nota del Garante specifica la notifica del caso all'attenzione dell'European Data Protection Board (EDPB)[3].

La situazione fin qui prospettata evidenzia una palese dicotomia di intenti tra il Gruppo Facebook e l'autorità Garante per la privacy. Da un lato Facebook vorrebbe ampliare il bacino informativo delle sue società controllate entro un termine ristretto posto dalla deadline dell'8 febbraio 2021 (successivamente posticipato a maggio per rimostranze da parte di utenti e autorità) e relativo all'entrata in vigore dei nuovi termini di servizio, dall'altro la limitazione delle attività di trattamento maggiormente incisive poste dai cd. Big Tech da parte dei Garanti europei.

2. I principali punti d'interesse presenti nell'informativa privacy di WhatsApp, le considerazioni del Garante per la protezione dei dati personali. Il principio di trasparenza e il diritto di informazione, riferimenti alle principali norme di settore. Finalità di utilizzo dei dati, le comunicazioni di servizio e commerciali. il diritto di accesso ai dati.

[1] ANSA, *WhatsApp, in Europa nessuna modifica a condivisione dati con Facebook,* 11 gennaio 2021. Consultabile presso: https://www.ansa.it/sito/notizie/tecnologia/internet_social/2021/01/07/whatsapp-in-europa-nessuna-modifica-a-condivisione-dati-con-facebook_bd29bb96-d6c2-46a3-98fd-2d2ceec57ccf.html.

[2] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, nota del 14 gennaio 2021: WhatsApp: Garante privacy, informativa agli utenti poco chiara. L'Autorità intenzionata ad intervenire anche in via d'urgenza.

[3] L'European Data Protection Board (RDPB) è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE. È composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati. Ne fanno altresì parte le autorità di controllo degli Stati senza però che i loro rappresentanti godano del diritto di voto o di essere eletti presidente o vicepresidenti.

Il comunicato del Garante rileva l'opacità della privacy policy di WhatsApp definendola poco chiara, e risultando perciò di ostacolo ad una libera e consapevole accettazione dei termini da parte degli utenti (ovvero gli interessati dall'attività di trattamento).

Con tale affermazione il Garante sottolinea la possibile inidoneità dell'informativa posta da WhatsApp, la quale risulterebbe inefficace a garantire una completa e aggiornata esposizione delle novità presenti nell'informativa. Presentare all'interessato una corretta informazione è il primo passo per poter effettuare un trattamento idoneo alle regole poste dal GDPR. L'informativa ha il compito di elencare all'interessato i suoi diritti e le finalità cui il trattamento aspira, il tutto in derivazione del principio di trasparenza introdotto dall'art. 5 del GDPR. Detto principio mira a creare in capo al soggetto interessato una serie di poteri, tali da consentire una completa capacità cognitiva riguardante il contesto di trattamento.

La prima forma di trasparenza trova concretezza nel menzionato obbligo di informazione. Questo viene introdotto all'art. 13 e stabilisce che i soggetti interessati, principalmente le persone fisiche, debbano essere necessariamente informati circa le modalità, le finalità e i diritti che le riguardano, in modo da sensibilizzarle ai rischi cui potrebbero essere esposte. Ciò avviene mediante un'informativa che deve contenere al suo interno tutte le informazioni necessarie all'interessato, al fine di renderlo edotto sulle attività svolte[4].

L'impossibilità di rintracciare con certezza i compiti cui l'informativa assolve, come affermato dal Garante nel caso della privacy policy di WhatsApp, impedisce il rispetto del principio di trasparenza e la corretta applicazione del menzionato art. 13. Per allineare l'informativa ai parametri del GDPR è necessario rendere agevole la fruizione delle informazioni presentate dall'informativa, redigendole in modo semplice e sintetico e rendendole visualizzabili e acquisibili attraverso vari tipi di strumenti, ovvero mediante: forma scritta, banner o apposite pagine web[5], con messaggi audio o video[6].

[4] Tra le quali rientrano: l'identità e i contatti del titolare del trattamento (se presente anche del suo rappresentante); i dati di contatto del responsabile; le finalità e la base giuridica del trattamento; eventuali interessi legittimi; i destinatari terzi dei dati o l'eventuale trasposizione di essi verso un paese terzo all'UE; infine, le informazioni successive all'acquisizione dei dati (es: tempistiche di conservazione, accesso ai dati, revoca del consenso, reclamo).

[5] Considerando n. 58, GDPR: «Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile

La chiarezza con cui le informazioni devono essere presentate è stata ulteriormente evidenziata dal Gruppo di Lavoro ex Art. 29[7]. Nella presentazione delle linee guida sulla prestazione del consenso, il Working Party ribadisce come le privacy policy debbano essere redatte in modo semplice e facilmente comprensibile, evitando stesure pregne di tecnicismi tali da poter nascondere informazioni rilevanti attraverso termini e condizioni[8].

In relazione ai parametri indicati dalle norme del Regolamento GDPR la policy proposta da WhatsApp presenta alcune opacità. Queste sono principalmente attinenti alla collaborazione con le aziende del gruppo Facebook, soprattutto se relazionate alla sentenza Schrems II.

La policy di WhatsApp oltre ad elencare le tipologie dei dati acquisiti[9], specifica le finalità per cui questi verranno utilizzati. Tra le varie sono elencate nell'informativa: fornitura di servizi, ovvero i dati necessari per erogare materialmente il servizio (tra cui rientra il numero di telefono); per motivi di sicurezza, per cui si può presuppore l'utilizzo di dati per finalità relative al legittimo interesse[10]; metadati, utilizzati per inviare messaggi e chiamate.

---

comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web».

[6] WP259, *Guidelines on Consent under Regulation 2016/679*, in https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849», p. 13: «*This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages*». In argomento: E. BASSOLI, *La nuova Privacy GDPR. Dopo il D.lgs. 10 agosto 2018, n. 101. Guida teorico-pratica con schemi riassuntivi e formulario dei principali adempimenti*, Dike Giuridica, Roma, 2018, 98.

[7] Il Gruppo di Lavoro ex Art. 29 è l'organo predecessore dell'attuale EDPB. Il nome del Gruppo scaturisce dall'art. 29 della Direttiva 95/46/CE che lo istituì.

[8] WP259, loc. cit.: «Controllers cannot use long illegible privacy policies or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions».

[9] Tra i quali rientrano: numero di telefono, nome, immagine del profilo, stato, posizione, informazioni sul dispositivo, sulla connessione e informazioni reperite mediante l'uso di cookie.

[10] Descritto dall'art. 6 del GDPR, per legittimo interesse si intende la base giuridica attraverso cui il titolare, o terzi qualificati, possono trattare i dati in assenza non solo del consenso ma anche in mancanza di un obbligo giuridico. Tale prospettiva si applica a quella serie di situazioni in cui il titolare, per salvaguardare un proprio interesse, effettua una raccolta dati slegata dai fini dell'attività principale. Il trattamento per legittimo

Oltre ai citati fini, la privacy policy presenta due ulteriori eventualità di utilizzo dei dati: l'utilizzo per comunicazioni di servizio e per fini commerciali.

L'informativa identifica nel marketing, nella futuribile introduzione di banner pubblicitari e nella comunicazione per finalità di servizio le tre fattispecie di utilizzo dei dati per le comunicazioni verso l'utente (tra cui rientrano i nuovi aggiornamenti sulle novità introdotte dall'applicazione attraverso la condivisione di stati). In tal senso non appare casuale la menzione nella sezione riguardante le comunicazioni all'interessato dei diritti e delle procedure esperibili dall'utente per poter gestire il proprio patrimonio informativo. Tra questi vi rientra in particolare il diritto di accesso ai dati, il quale è strettamente legato al principio di trasparenza e al diritto di informazione.

Il diritto di accesso ai dati, diritto derivante dal principio di trasparenza, permette al soggetto interessato di richiedere determinate informazioni riguardanti l'attività di trattamento svolta in suo capo, attraverso un'apposita richiesta al titolare. L'articolo di riferimento, ossia l'art. 15 del Regolamento, descrive a quali notizie relative alle attività svolte dal titolare l'utente può avere accesso[11].

L'accesso ai dati risulta essere snodato in due differenti corollari, che ne favoriscono il funzionamento: il diritto a conoscere l'esistenza di dati riguardanti l'interessato e il diritto a riceverne comunicazione[12]. A tal proposito, appare curiosa la mancanza, rispetto alla Direttiva 95/46/CE, del requisito dell'intelligibilità dei dati forniti. L'intellegibilità risulta essere un parametro essenziale per poter ricevere dati comprensibili e la sua mancanza potrebbe portare ad un'informazione non pienamente

interesse è comunque subordinato all'obbligo di informazione verso l'interessato oltre che ad un'attenta opera di bilanciamento con i diritti e gli interessi che lo riguardano.

[11] Queste sono: le finalità del trattamento; le categorie dei dati trattati; i destinatari dei dati (anche terzi), il periodo della loro conservazione o i parametri per determinarlo; l'esistenza del diritto a opporsi, a limitare, rettificare o cancellare i dati; la possibilità di proporre reclamo e richiedere informazioni circa l'esistenza di un processo decisionale automatizzato (es: profilazione).

Nel caso in cui le informazioni siano ricollegate a processi di raccolta automatizzati, queste possono essere richieste solo se il processo di raccolta sia preordinato all'assunzione di una decisione con effetti giuridici verso l'interessato. Segue quindi la possibilità di poter richiedere qual è la logica presente dietro tale processo come descritto dal paragrafo 1, lettera h dell'art. 15. Sul punto, V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo,* Giappichelli, Torino, 2019, p. 702.

[12] E. BASSOLI, *La nuova privacy GDPR dopo il D. lgs. 10 agosto 2018, n.101,* cit., 132-134.

trasparente[13]. Una volta richiesti i dati, senza ledere altrui diritti, il titolare può fornirne una copia degli stessi, richiedendo eventualmente un contributo spese per le copie successive, equipollente a quello dei normali costi amministrativi. Per favorire lo sviluppo dell'economia digitale, si dovrebbe ritenere che tale richiesta possa essere effettuata elettronicamente, in modo da permettere al titolare di adempiere alla richiesta con gli stessi mezzi[14]. È questo il caso di WhatsApp, la cui applicazione permette di richiedere una copia digitale dei propri dati direttamente attraverso il proprio smartphone.

Quanto esplicato dall'informativa, come già evidenziato, adempie ad una funzione preparatoria e cognitiva dell'interessato. Infatti, l'interessato dovrà necessariamente prestare il proprio consenso per poter permettere a WhatsApp e alle società collegate di avviare il trattamento dei propri dati. Perciò il consenso risulta essere l'elemento cardine di tutta l'attività di trattamento. La comprensione del predetto istituto richiedere un'approfondita analisi, soprattutto con riguardo alle modalità di prestazione dello stesso e sul ruolo che ricopre durante la fruizione di un servizio e la conclusione di un contratto.

3. Il consenso al trattamento dei dati. Base giuridica di riferimento ed elementi caratterizzanti. Consenso e conclusione di un contratto: le principali disposizioni della Corte di Cassazione. Il principio di minimizzazione dei dati e le finalità di trattamento: il criterio di specificità. Liceità del Consenso

[13] Un esempio concreto che raffigura l'importanza dell'intelligibilità dei dati, può essere rintracciato nell'esame effettuato dall'Autorità Garante relativamente ad un ricorso presentato nel 2001 (Garante Privacy, 26 marzo 2001, cod. web n. 41910, in www.garanteprivacy.it). Dopo aver effettuato un accertamento presso un'azienda ospedaliera, un paziente presentava ricorso presso l'Autorità Garante. Tra le interrogazioni, il paziente chiedeva di ricevere informazioni riguardanti il significato di alcuni codici diagnostici utilizzati dall'azienda ospedaliera. L'AG (riunitasi nelle persone di: Stefano Rodotà, presidente, Giuseppe Santaniello, vicepresidente, Gaetano Rasi e Mauro Paissan) ha accolto tale richiesta, ribadendo che i dati forniti debbano essere redatti secondo parametri di intelligibilità degli stessi (secondo quando descritto, in quel tempo, dall' art. 13 della L. 31 dicembre 1996, n. 675).

[14] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione.* Giappichelli, Torino, 2018, 25.

Il consenso al trattamento deve essere presentato secondo il Considerando n. 32 del GDPR, attraverso un atto positivo inequivocabile[15] in forma scritta, attraverso mezzi elettronici o oralmente. A livello normativo viene introdotto dalla definizione fornita dall'art. 4 n. 11 del GDPR, il quale si riferisce testualmente a qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato. Appare evidente, dalla norma citata, che il consenso al trattamento può essere figurativamente considerato come la linea rossa che rende lecite o illecite eventuali attività che fanno uso di dati[16].

Essendo presenti diritti irrinunciabili, strettamente collegati alla dignità e alla libertà personale, è necessario che ci sia una riflessione libera, specifica e informata, da parte dell'interessato che deve prestare il consenso[17]. Questi, unitamente a quella che viene definita «manifestazione inequivocabile», sono i fondamenti del consenso al trattamento[18].

Analizzare questi caratteri singolarmente risulta fondamentale per consentire una precisa conoscenza del già menzionato istituto.

Partendo dal primo, occorre considerare che il concetto di libera manifestazione può essere estrapolato dall'art 7, par. 4 del Regolamento, il quale afferma che il consenso prestato deve essere libero da vincoli[19], per

[15] «Il consenso al trattamento è atto diretto a definire le modalità e le condizioni del trattamento stesso vincolando fortemente l'attività del titolare» (In questo senso, A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, Torino, 2018, 59, la quale si richiama a F. CAFAGGI, *Qualche appunto su circolazione, appartenenza e riappropriazione nella disciplina dei dati personali*, cit., 613 ss.; A. FICI, E. PELLECCHIA, *Il consenso al trattamento*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, cit., 502 ss.; S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Tomo I, Giuffrè, Milano, 2006, 994 ss.

[16] Ritengono che il consenso sia fondamento di legittimità per il trattamento stesso, S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, in *Europa e diritto privato*, 2004, p. 2 ss.; S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Rivista di diritto civile*, 2, 2001, 621 ss.

[17] R. IMPERIALI, *Codice della Privacy. Commento alla normativa sulla protezione dei dati personali.* Il Sole 24 Ore, Milano, 2004, 169.

[18] Considerando n. 32 GDPR: «Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano».

[19] Art 7, par. 4 «Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto».

cui non è possibile condizionare al consenso l'erogazione di un servizio o la conclusione del contratto[20].

La norma così posta mitiga un'eventuale costrizione attuabile verso l'interessato. Infatti, questi deve essere libero di poter fruire di un determinato servizio o di siglare un contratto, senza dover essere obbligato a fornire i propri dati per attività di trattamento.

Quanto affermato dall'art. 7, par. 4 trova inoltre riscontro in una pronuncia effettuata dalla Suprema Corte di Cassazione. La Corte di Cassazione ribadisce che in nessun caso, anche in presenza di clausole contrattuali, è possibile vincolare un soggetto alla prestazione del consenso al trattamento di quei dati che non risultano necessari ai fini degli adempimenti preposti. La Corte stessa ribadisce inoltre la natura imperativa delle norme a tema privacy il cui contrasto con le stesse, a norma dell'art. 1418 c.c., rende nulli eventuali termini avversi[21].

Inoltre, tale eventualità si scontrerebbe con il principio di minimizzazione dei dati. Detto principio, enunciato dal Regolamento GDPR all'art. 5 lett. c, afferma che i dati raccolti in sede di trattamento debbano necessariamente essere: adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Il principio di minimizzazione permette di effettuare una selezione accurata dei dati, in modo da evitare trattamenti superflui che potrebbero danneggiare gli interessati. L'importanza del principio di minimizzazione

[20] Tale previsione normativa risulta particolarmente importante rispetto al tema trattato. Spesso siti web o altri sistemi multimediali, vincolano la loro fruizione ad un eventuale consenso ad attività di trattamento di dati superflui alle finalità di trattamento. In questo modo il soggetto fruitore non può usufruire dei servizi e quindi prendere visione, ad esempio, di una pagina web, se prima non accetta di essere sottoposto ad attività di trattamento.

[21] Cass. Civile Sez. I, Sentenza n. 26778, ottobre 2019. «In conclusione, la clausola con cui la banca ha subordinato il dar corso alle operazioni richieste dal cliente al consenso al trattamento dei dati sensibili è affetta da nullità in quanto contraria a norme imperative, a norma dell'art. 1418 c.c. Ne consegue che la condotta con cui lo stesso istituto di credito ha successivamente provveduto al "blocco" del conto corrente e del deposito titoli, proprio perché trova il proprio titolo in una clausola nulla dalla stessa inserita, non lo esonera da responsabilità per inadempimento contrattuale».
La vicenda riguarda un contenzioso sorto tra un cliente e la propria banca. Dopo aver concluso un contratto con il cliente e aver permesso a questo di fruire per diverso tempo dei servizi offerti, la banca decise di bloccare il conto del cliente in quanto questo non diede il consenso al trattamento dei propri dati personali ulteriori rispetto ai fini previsti dalle operazioni da questo svolte.

è stata inoltre ribadita dalla Corte di Cassazione che ne afferma la centralità in un contesto di trattamento lecito[22].

Secondo quanto emerge dal Considerando n. 32, oltre a essere libero il consenso deve essere specifico. Esso deve infatti applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità[23], e qualora vi siano più finalità, il consenso deve essere prestato per ciascuna di esse. Il medesimo Considerando descrive i caratteri della richiesta di consenso fatta attraverso mezzi elettronici, la quale deve essere chiara, concisa e non deve interferire con il servizio per il quale il consenso è stato espresso. Inoltre, qualora dovessero cambiare le finalità, sarebbe necessario valutarne la compatibilità con quelle rispetto alle quali era stato in precedenza prestato il consenso, in modo da stabilire se esso debba essere rinnovato.

Il criterio di specificità viene ribadito non solo dall'art. 7 par. 2 del Regolamento, che ne evidenzia un'eventuale presentazione scritta[24], ma anche dal Gruppo di Lavoro ex Articolo 29. Il Gruppo dei Garanti europei ha ritenuto opportuno specificare che è la finalità a dover essere oggetto di un distinguo relativamente alla prestazione del consenso e non le operazioni che la compongono. Ad esempio, se il titolare volesse utilizzare i dati per finalità di marketing, il consenso prestato dovrebbe essere

[22] Cass. Civile Ordinanza 34113, dicembre 2019: «Il trattamento dei dati personali effettuato nell'ambito dell'attività di recupero crediti è lecito purché avvenga nel rispetto del principio di minimizzazione dovendo essere utilizzati solo i dati indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti potendo essere comunicate informazioni riguardanti il debitore persona fisica funzionali alla cessione del credito, quali la situazione debitoria e l'ubicazione dell'immobile.».
La suddetta ordinanza è stata emanata dalla Corte di Cassazione per rigettare un ricorso, ritenuto generico, presentato da un cliente avverso al proprio istituto di credito per violazione della legge sulla privacy nel corso di attività di recupero crediti. Il rigetto da parte della Corte è avvenuto in quanto la parte ricorrente non ha evidenziato quali dati sensibili siano stati effettivamente ceduti dalla banca, ritendendo dunque il ricorso generico.

[23] Sul principio di finalità, F. PIRAINO, *Il codice della privacy e la tecnica del bilanciamento d'interessi*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, cit., 715 ss.

[24] Art. 7 Par. 2 GDPR: «Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante».

distinto rispetto a quello richiesto per l'attività di profilazione, in quanto mirano a obiettivi differenti. Se invece le diverse operazioni di trattamento mirano alla stessa finalità, come ad esempio la trasposizione dei dati all'estero, allora il consenso da prestare sarà unico[25].

Infine, il consenso è strettamente collegato alla liceità del trattamento, perciò, per renderlo legalmente valido, è necessario che sia inequivocabile e verificabile. A tal fine il Considerando n. 32 precisa che l'apposizione del consenso può essere effettuata mediante qualsiasi dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto[26].

Da ciò si desume che l'interessato può mantenere una duplice condotta: una attiva, prestando esplicitamente il consenso al trattamento dei dati; ed una passiva, consistente in una dichiarazione desumibile da un comportamento chiaro e senza alcuna possibilità di smentita, tenuto dall'interessato.

Inoltre, il Considerando richiamato precisa che non possano essere qualificate come modalità lecite di prestazione del consenso: l'inerzia, assimilabile al mancato compimento di qualsiasi tipo di azione; il silenzio; l'utilizzo di form precompilati o caselle già spuntate[27] [28], che potrebbero

[25] S. BORGHI, *Il consenso nel GDPR: le linee guida dei Garanti europei,* in AA.VV. *Privacy e Dati Personali. Problemi e casi pratici.* Key, Milano, 2018, 188 ss.

[26] Considerando n. 32: «la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto».

[27] Tale concetto viene ribadito dalla Corte di Giustizia Europea con sentenza del 1° ottobre 2019 (Planet49 C-673/17), con la quale ha dichiarato che il consenso all'archiviazione di informazioni o all'accesso a informazioni, attraverso cookie installati nell'apparecchiatura terminale dell'utente di un sito Internet, non è validamente espresso quando l'autorizzazione risulta da una casella di spunta preselezionata, e ciò indipendentemente dal fatto che le informazioni di cui trattasi costituiscano o meno dati a carattere personale. Maggiori info in: M. IASELLI, *Cookie, per il consenso non basta una casella di spunta preselezionata. 10 ottobre 2019,* in https://www.altalex.com/documents/news/2019/10/24/cookie-per-il-consenso-non-basta-una-casella-di-spunta-preselezionata.

[28] C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH: «Il consenso attivo è ora, dunque, espressamente previsto dal regolamento 2016/679. Si deve rilevare, a tal riguardo, che, secondo il Considerando 32 di tale Regolamento, la manifestazione del consenso potrebbe comprendere, in particolare, la selezione di un'apposita casella in un sito Internet. Il suddetto Considerando esclude invece espressamente che «il silenzio, l'inattività o la preselezione di caselle» configurino consenso».

indurre ad una scelta forzata. In tale prospettiva andrebbe valutata l'eventuale liceità dell'apposizione di un termine perentorio di prestazione implicita del consenso, cui unico metodo di diniego risulterebbe l'opt-out da parte dell'interessato, come nel caso dell'informativa di WhatsApp.

Con riguardo invece alla verifica dell'effettiva apposizione del consenso, il titolare deve essere in grado di dimostrare che vi è stato un effettivo rilascio da parte dell'interessato[29]. Il Regolamento non specifica in tal senso l'obbligo di una prova scritta per poter dimostrare la liceità del trattamento. È comunque palese che la forma scritta sia da preferire per avere maggior evidenza probatoria[30].

Infine, l'art. 7 par. 1 del GDPR precisa che l'interessato prima di procedere con l'apposizione del consenso, è informato circa la revocabilità dello stesso. Il soggetto interessato deve essere quindi informato della sua facoltà di revocare il consenso con la stessa facilità con cui è accordato. Ivi, inoltre, si specifica che l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento[31]. La revoca del consenso non pregiudica la liceità del trattamento effettuato sulla base del consenso prestato prima della revoca, perciò il trattamento precedente risulta essere comunque lecito, mentre il successivo diventa illecito[32].

4. Collaborazione con le altre aziende di Facebook e operazioni globali. Il dato personale, valore sociale ed economico. Trasposizione dei dati all'estero e collocazione fisica dei datacenter di WhatsApp fuori dall'Unione Europea. Privacy Shield: la sentenza Schrems II

Come già affermato, il punto nodale del cd. caso WhatsApp riguarda la collaborazione che l'azienda effettuerà con le altre controllate del gruppo Facebook. I timori che scaturiscono da tale collaborazione

[29] Art. 7, par. 1, GDPR: «Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali».

[30] F. DE STEFANI, *Le regole della privacy. Guida pratica al nuovo GDPR.* Hoepli, Milano, 2018, Cap. 4, consultato in formato digitale.

[31] Sulla revoca, intesa come «atto ablativo degli effetti di un atto precedentemente caratterizzato dalla unilateralità, dalla provenienza dall'autore dell'atto revocato, dall'attuabilità in via stragiudiziale, dalla superfluità del sopraggiungere di circostanze o fatti nuovi», L. FERRI, *Revoca in generale (diritto privato)*, in *Enciclopedia del diritto*, XL, Giuffrè, Milano, 1989, 198 ss.

[32] F. PIZZETTI, *Intelligenza artificiale,* cit., 18.

riguardano la possibile creazione di un bacino informativo di ragguardevole imponenza che le aziende di Facebook andrebbero a generare. Le modalità di collaborazione, unitamente alle operazioni che WhatsApp definisce di «livello globale», possono essere individuate nella privacy policy e nelle FAQ ad essa correlate.

Da una prima analisi, la collaborazione tra WhatsApp e Facebook risulterebbe incentrata sull'utilizzo di infrastrutture, mezzi e servizi per permettere il potenziamento e l'espansione dell'applicazione. Le FAQ[33] indicano con specifica menzione, che i dati condivisi attraverso la piattaforma di messagistica non sono utilizzati per migliorare i prodotti o i servizi forniti da Facebook. Nonostante quanto indicato, le modalità di collaborazione prevedono comunque uno scambio di informazioni, seppur minime, tra le varie aziende del gruppo. Tali informazioni sono utilizzate per creare identificativi univoci al fine di valutare come e quali applicazioni, di proprietà del gruppo, vengano utilizzate dagli utenti. Il reperimento di questa tipologia di informazioni e il confronto con i dati in possesso di Facebook, anche se per il solo proposito di fornire i servizi, potrebbero portare ad una profilazione[34] dell'utente.

Quanto testé prospettato, deve essere necessariamente accostato ad alcuni elementi che consentano di individuare i motivi per cui l'attività di trattamento posta da WhatsApp crea rimostranze nei Garanti europei. Tali rimostranze sono individuabili in tre differenti elementi: nella qualificazione giuridica del trattamento dei dati quale attività pericolosa, nel valore socio-economico dei dati, nella trasposizione transfrontaliera dei dati personali.

Con riguardo al primo elemento, precedentemente all'avvento del GDPR e del D.lgs. del 10 agosto 2018, n. 101[35], il D.lgs. 30 giugno 2003, n.196 cd. Codice Privacy prevedeva l'applicazione dell'art 2050 c.c. ovvero la responsabilità per l'esercizio di attività pericolosa, per i danni cagionati attraverso il trattamento dei dati. Successivamente l'articolo di

[33] FAQ di WhatsApp, *Come collaboriamo con le altre aziende di Facebook*. Consultabile presso: https://faq.whatsapp.com/general/security-and-privacy/how-we-work-with-the-facebook-companies

[34] L'art. 4 del GDPR identifica nella profilazione qualsiasi forma di trattamento automatizzato di dati personali, consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, tra cui le preferenze personali e il comportamento.

[35] Il D.lgs. del 10 agosto 2018, n. 101 è il decreto attraverso il quale è avvenuto l'adeguamento del Codice Privacy al GDPR.

riferimento, ossia l'art. 15 [36], è stato abrogato, per cui non è più presente un richiamo esplicito all'art. 2050 c.c. Tale abrogazione risulta consequenziale all'emanazione del GDPR, in quanto lo stesso Regolamento inserisce all'interno dell'art. 82 parametri più precisi nell'individuare i profili di responsabilità, garantendo un adeguato diritto al risarcimento in caso di danni[37].

L'identificazione del trattamento quale attività pericolosa può essere considerata come una conseguenza del valore sociale ed economico che il dato personale ha acquisito nel corso del tempo, come evidenziato da recente giurisprudenza. Secondo il TAR del Lazio da un punto di vista economico e contrattuale, i dati personali possono essere parificati ad un «asset negoziale» economicamente apprezzabile, perciò secondo tale impostazione l'utilizzo, ad esempio, di un social network o il download di un'applicazione potrebbe essere considerato come una controprestazione di matrice contrattuale[38]. Con riguardo invece all'aspetto sociale, il dato

[36] Art.15 D.lgs. 196/2003 antecedente al D.lgs. n. 101/2018: «Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del Codice civile.»

[37] L'art. 82 stabilisce che il titolare del trattamento è responsabile per la violazione delle disposizioni presenti nel GDPR. Di contro, il responsabile risponderà delle violazioni relative alle mansioni a lui affidate dal GDPR ovvero comportamenti contrari alle istruzioni fornite dal titolare del trattamento. Altresì è prevista la responsabilità solidale tra più titolari e responsabili. Con la possibilità, in caso di pagamento di una delle parti, per tutte le altre, di rivalersi per le somme dovute. Il danno causato da una violazione delle norme presenti nel regolamento, verso cui può essere richiesto un risarcimento, può essere sia materiale che immateriale e deve essere necessariamente richiesto con azioni presso l'autorità giudiziaria. Solo in tale sede, con le modalità semplificate del rito del lavoro, l'interessato può vedersi riconoscere il risarcimento, in quanto in sede amministrativa può ottenere solo una limitazione o un divieto al trattamento. Una particolarità relativa alla responsabilità per violazione delle norme del Regolamento è rintracciabile nell'inversione dell'onere probatorio, prevista dal terzo punto dell'art. 82, in virtù del quale il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2, se dimostra che l'evento dannoso non gli sia in alcun modo imputabile.

[38] TAR Lazio Sez. I Sentenza n.261, gennaio 2020: «Le tesi di parte ricorrente presuppongono che l'unica tutela del dato personale sia quella rinvenibile nella sua accezione di diritto fondamentale dell'individuo, e per tale motivo F. era tenuta esclusivamente al corretto trattamento dei dati dell'utente ai fini dell'iscrizione e dell'utilizzo del "social network". Tuttavia, tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto».

personale, soprattutto di tipo particolare[39], risulterebbe meritevole di tutela in quanto ad essi sono ricollegati diritti e libertà fondamentali che potrebbero essere posti a serio rischio in sede di trattamento, come descritto nel Considerando n. 51 del Regolamento.

La sensibilità delle attività di trattamento dati e il valore che il dato personale possiede, richiedono necessariamente una tutela adeguata degli stessi, relazionata al contesto territoriale in cui questi vengono utilizzati dopo la loro acquisizione. Tale necessità si rafforza quando i dati lasciano i territori europei tutelati dal GDPR. In tal senso, il Regolamento pone un netto cambiamento rispetto alla Direttiva 95/46/CE nella tutela dei dati esportati e importati dall'Unione. Infatti, mentre la Direttiva riteneva episodi singoli e sporadici l'importazione e l'esportazione dei dati oltre confini, il Regolamento invece li considera come dei flussi derivanti dal commercio e dalla cooperazione internazionale e per cui facenti parte di una realtà globalizzata[40].

Nel caso di WhatsApp i dati vengono spesso esportati verso gli Stati Uniti come conseguenza delle «Operazioni globali» intraprese dall'azienda, il tutto avvalendosi degli strumenti di Facebook[41]. In particolare, è necessario menzionare come i datacenter del gruppo siano fisicamente collocati fuori dall'Unione, rendendo perciò materialmente improbabile il trattamento all'interno della stessa.

Il transito dei dati fuori dall'Europea rappresenta con riguardo a WhatsApp un problema principalmente di natura legale, oltre che fulcro principale delle problematiche emerse con la nuova privacy policy. Infatti, con la sentenza della Corte di Giustizia Europea relativa al processo C-311/18 (cd. Schrems II) e avversa a Facebook Ireland e Maximilian Schrems, è stato dichiarato invalido il Privacy Shield.

Il Privacy Shield è un accordo UE-Stati Uniti introdotto attraverso la Decisione 2016/1250 della Commissione Europea a seguito dell'abolizione post sentenza C-362/14 del «Safe Harbor», ovvero, l'accordo tra Unione Europa e Stati Uniti che consentiva alle imprese americane di conservare i dati personali degli utenti europei sia in Europa e sia negli Stati Uniti. Il

---

Sentenza riguardante un provvedimento dell'AGCM avverso F. inc e F.I. ltd.

[39] I dati particolari sostituiscono la categoria dei cd. dati sensibili. Introdotti dall'art. 9 del GDPR includono: opinione politica, religiosa, sindacale, origine etnica, orientamento sessuale, dati biometrici, genetici e relativi alla salute.

[40] F. PIZZETTI, *Il Regolamento europeo 2016/679*, Giappichelli, Torino, 2018, 76-78.

[41] «WhatsApp utilizza l'infrastruttura globale e i data center di Facebook, inclusi quelli negli Stati Uniti» in *Operazione globali.* Consultabile presso: https://www.whatsapp.com/legal/updates/privacy-policy-eea.

Privacy Shield prevedeva l'introduzione di una serie di principi[42] relativi alla trasparenza, alla gestione e alla vigilanza dei dati personali importati ed esportati tra Europa e Stati Uniti. L'abolizione del Privacy Shield avvenuto attraverso la sentenza Schrems II è espressione di uno scontro di forza tra i Big Tech e i giudici comunitari. Nella sua analisi, la Corte ha individuato nella normativa interna degli Stati Uniti alcuni programmi che consentono alle autorità di accedere ai dati personali trasferiti e importati dall'Unione. Secondo la Corte, l'accesso ai dati da parte delle autorità, oltre alla mancanza di strumenti giudiziari esperibili verso le stesse, comporterebbe limitazioni alla protezione dei dati personali, per cui le norme statunitensi non risulterebbero, nei requisiti, equivalenti alle regole dell'Unione[43].

Questo secondo la Corte renderebbe il trasferimento dei dati verso gli Stati Uniti pericoloso, in quanto non vi sarebbe equivalenza con la qualità delle norme poste dal GDPR.

Sempre con riguardo alle operazioni globali di WhatsApp merita menzione la citazione nell'informativa dell'utilizzo delle clausole contrattuali standard, utilizzate dall'azienda per il trasferimento dei dati dallo Spazio economico europeo (SEE). Tali clausole introdotte dall'art. 46 del Regolamento, prevedono, secondo il Considerando n.108, la presenza di garanzie che dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione. Inoltre, dovrebbe essere presente la disponibilità di diritti azionabili dagli interessati unitamente a mezzi di ricorso effettivi, fra cui il ricorso amministrativo o giudiziale oltre alla richiesta di

[42] Tra cui rientrano: principio sull'informativa, principio sull'integrità dei dati e la limitazione delle finalità, principio di scelta, principio di sicurezza, accesso e ricorso oltre un controllo sulle responsabilità.

[43] C-673/17 Data Protection Commissioner contro Facebook Ireland Ltd, Maximillian Schrems: «In base alle constatazioni contenute nella decisione «scudo per la privacy», è vero che i programmi di sorveglianza fondati sull'articolo 702 del FISA devono essere attuati nel rispetto dei requisiti risultanti dalla PPD-28. Tuttavia, sebbene la Commissione abbia sottolineato, ai punti 69 e 77 della decisione «scudo per la privacy», che siffatti requisiti sono vincolanti per i servizi di intelligence statunitensi, il governo degli Stati Uniti ha ammesso, in risposta ad un quesito della Corte, che la PPD-28 non conferisce agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici. Pertanto, essa non è idonea a garantire un livello di protezione sostanzialmente equivalente a quello risultante dalla Carta, contrariamente a quanto richiesto dall'articolo 45, paragrafo 2, lettera a), del RGPD, secondo il quale la constatazione di tale livello dipende, in particolare, dall'esistenza dei diritti effettivi e azionabili di cui godono le persone i cui dati sono stati trasferiti verso il paese terzo di cui trattasi».

risarcimento, nell'Unione o in un Paese terzo. Quanto affermato, delinea un'estensione delle garanzie proprie dello SEE alle attività di trattamento poste da organismi e autorità pubbliche di Paesi terzi[44]. Tale estensione, se relazionata alla sentenza Schrems II, dovrebbe necessariamente portare ad una rivalutazione degli strumenti di adeguatezza posti da WhatsApp a garanzia dei dati esportati all'estero, valutando le ulteriori alternative alle clausole standard proposte ed elencate dall'art. 46.

Gli eventi descritti mostrano come gli interventi del Garante e della Corte di Giustizia Europea siano considerabili come diretta espressione dei nuovi parametri introdotti dal Regolamento 2016/679. Tale imposizione può essere considerata come una prova di maturità a dimostrazione che il cambiamento apportato dal GDPR è stato quantomeno necessario per mitigare le lacune presenti nella precedente Direttiva 95/46/CE.

In conclusione, l'analisi fin qui proposta permette di individuare alcune delle criticità emerse. Innanzitutto, appare evidente, nonostante gli interventi dei garanti europei e della giurisprudenza, la difficoltà dei vari soggetti attivi coinvolti nel trattamento dei dati alla stesura di policy di semplice fruizione. Con troppa frequenza i titolari presentano agli interessati privacy policy esageratamente complesse, generiche e spesso contraddittorie, le quali si affiancano in molti casi ad una mancata frammentazione delle varie tipologie di consenso, portando così ad un'unica manifestazione di volontà utilizzata per ogni tipo di attività. Tale condotta è conseguenza dell'introduzione del principio di accountability all'interno della normativa privacy; principio che impone al titolare una gestione responsabile del trattamento, effettuata attraverso l'adozione di un piano che permetta di adottare politiche adatte a trattare i dati raccolti, in base alla finalità e al contesto da cui questi vengono estrapolati. Si ha perciò un passaggio da un modello di trattamento statico tipico dei parametri della Direttiva 95/46/CE, in cui la semplice adesione ai parametri posti dalla legge è sufficiente a rendere un trattamento dati lecito, ad un modello «proattivo»[45], dove il titolare è vincolato dai principi stabiliti dal Regolamento e dal piano da questi predisposto, in base ai criteri di privacy by default/by design e al rischio connesso all'attività di trattamento. Per cui la frequente difficoltà o la mancata e colpevole volontà di indicare con chiarezza tutti gli elementi presenti nella privacy policy sono conseguenza di tale impostazione introdotta dal GDPR.

[44] F. PIZZETTI, *Il Regolamento europeo 2016/679.* cit., 82-84

[45] F. DI RESTA, *La nuova "Privacy Europea"*, Giappichelli, Torino, 2018, 124-125.

Comunque, nonostante i rischi che tale impostazione presenta, l'infinità dei settori che richiedono l'utilizzo di dati e di conseguenza la loro gestione, rendono tale modello maggiormente idoneo allo scopo, in quanto affidarsi ad uno strumento dinamico basato su principi generali rispetto ad uno strumento statico, come può esserlo un apparato normativo di settore, rende più agevole la creazione di policy adattabili ai diversi contesti di trattamento. Non solo, il passaggio ad un modello dinamico permette di effettuare un alleggerimento del carico di lavoro in capo al Garante, il quale potrà eventualmente intervenire in un secondo momento.

Ulteriori spunti di riflessione sono ravvisabili nell'attività di trasposizione dei dati verso gli Stati Uniti. Alla luce delle sentenze Schrems il trasferimento dei dati verso gli Stati Uniti appare inidoneo se effettuato con i parametri previsti in precedenza dal Privacy Shield. Non a caso un primo passo, successivo all'emanazione delle citate sentenze, è stato effettuato dalla Data Protection Commission irlandese (DPC). La DPC è stata tra le prime autorità europee ad ingiungere Facebook per il trasferimento di dati all'estero, non solo in quanto Lead Supervisory Authority chiamata in causa nei menzionati processi, ma soprattutto in veste di autorità del Paese europeo in cui è presente la sede legale di Facebook. L'ingiunzione di Facebook da parte della DPC e riguardante il blocco al trasferimento dei dati verso gli Stati Uniti, mette in risalto il problema relativo alla mancanza di server e data center in cui processare i dati del gruppo all'interno dell'area Schengen. La collocazione dei data center all'interno dell'Unione garantirebbe la collocazione fisica dei dati processati in Europa, permettendo un diretto controllo da parte delle autorità e dei garanti europei.

Inoltre, un altro aspetto da considerare è l'utilizzo da parte di WhatsApp delle clausole contrattuali standard, volte a garantire l'idoneità del trattamento dei dati da questa effettuato. Tali clausole nonostante siano state ritenute idonee dalla della Corte di Giustizia Europea, al fine di garantire un corretto trattamento transfrontaliero, non possono assolvere ai medesimi compiti di un accordo similare al Privacy Shield. Ciò è ovviamente desumibile, come anche rilevato dalla Corte, dalla natura contrattuale di tali clausole che non vincolano il Paese terzo verso cui i dati vengono trasferiti a rispettarle. Perciò, in ossequio ai parametri di equivalenza sostanziale relativi alle garanzie di cui all'art. 46 del GDPR, andrebbe individuato un ulteriore strumento, differente dalle clausole

contrattuali standard, idoneo a tutelare i dati oggetto di trattamento transfrontaliero su vasta scala come nel caso preso in esame.