Dati personali: la nozione di "responsabile del trattamento" include il gestore di una *fanpage* presente su un *social network*

di Angela Correra

Title: Personal Data: the concept of 'controller' within the meaning of that provision encompasses the administrator of a fan page hosted on a social network

Keywords: Personal data; Controller responsible for the processing of personal data; Powers of intervention of national supervisory authorities.

1. – Con la sentenza in epigrafe la Corte di Giustizia torna a pronunciarsi sul delicato tema della tutela dei dati personali, offrendo un nuovo importante contributo nella risoluzione delle complesse questioni interpretative che la società odierna pone.

All'aumento della varietà di dati elettronici relativa a ciascun individuo, in parte dovuta alla comparsa dei social media e in parte dovuta alla crescita dei dispositivi mobili, dei dispositivi di sorveglianza e dei sensori collegati in Rete, si accompagna sempre più spesso il fenomeno del *webtracking* comportamentale, fondato su una tecnica di monitoraggio a fini commerciali e di marketing del comportamento degli utenti di Internet (frequentazione ripetuta di certi siti, interazione, parole chiave, produzione di contenuti on line), fino alla elaborazione di un vero e proprio profilo specifico per inviare messaggi pubblicitari perfettamente corrispondenti agli interessi dedotti (per un approfondimento sulla tecnologia del *tracking cookie*, si veda il parere 2/2010 del gruppo di lavoro «Articolo 29» per la protezione dei dati, del 22 giugno 2010, sulla pubblicità comportamentale). In particolare, attraverso l'impiego di *cookie (i.e.* file di controllo attivati sul computer dell'internauta all'apertura di un sito web), è possibile osservare le abitudini di navigazione degli utenti e identificare i loro interessi, permettendo così ai pubblicitari di ottimizzare le funzionalità dei siti web e di rivolgersi in maniera più mirata alle diverse fasce di utenti.

Affinché tali operazioni di tracciamento del comportamento di navigazione degli internauti siano conformi alle disposizioni dettate dalla normativa in materia di protezione dei dati personali è, però, necessario che sussistano gli specifici presupposti individuati dal legislatore europeo e, cioè, che gli utenti siano adeguatamente informati in ordine alla raccolta e all'utilizzo dei loro dati personali e che gli stessi prestino il previo consenso al trattamento dei propri dati personali.

Proprio la valutazione di conformità delle operazioni di monitoraggio comportamentale degli utenti alla normativa in materia di protezione dei dati personali, impone la necessità di chiarire l'ampiezza della nozione di responsabile del trattamento, l'individuazione del diritto nazionale applicabile e dell'autorità chiamata ad esercitare poteri di intervento.

In tale contesto si inserisce la recente pronuncia della CGUE del 5 giugno 2018, con la quale è stato statuito che l'amministratore di una fanpage su Facebook è responsabile assieme al social network del trattamento dei dati dei visitatori della sua pagina e che l'autorità per la protezione dei dati dello Stato membro, in cui tale amministratore ha la propria sede, può agire, in forza della direttiva 95/46, sia nei confronti di quest'ultimo sia nei confronti della filiale di Facebook stabilita in tale Stato.

2. – In dettaglio, la CGUE è stata investita, attraverso lo strumento del rinvio pregiudiziale di cui all'art. 267 TFUE, dalla Corte amministrativa federale tedesca della risoluzione di ben sei questioni di massimo rilievo relative alla interpretazione della direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (ad oggi sostituita dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 o "GDPR").

L'occasione della pronuncia è stata offerta dalla controversia sorta tra l'Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (autorità di vigilanza regionale indipendente per la protezione dei dati dello Schleswig-Holstein) (in prosieguo, «ULD») e la Wirtschaftsakademie Schleswig-Holstein GmbH, società di diritto privato specializzata nel settore della formazione (in prosieguo, «Wirtschaftsakademie»), avente ad oggetto la legittimità di un provvedimento emesso dall'ULD, motivato dall'asserita violazione della normativa tedesca attuativa della direttiva 95/46, con cui si intimava alla Wirtschaftsakademie di disattivare una fanpage presente sul sito del social network «Facebook». L'ULD aveva, infatti, rilevato che gli utenti della fanpage non erano informati della circostanza che Facebook raccogliesse i loro dati personali attraverso *cookie* attivati sul loro disco rigido, per realizzare statistiche destinate al gestore di detta pagina e permettere allo stesso Facebook di diffondere pubblicità mirate.

Come opportunamente ricordato dall'Avvocato generale, nelle proprie conclusioni, i gestori delle fanpage possono servirsi, gratuitamente e nel quadro di condizioni d'uso non modificabili, di statistiche realizzate grazie allo strumento di «Facebook Insights» per poi personalizzarle sulla base di vari criteri, come il sesso o l'età, e ricavarne informazioni dettagliate sulle abitudini e sui comportamenti degli utenti a cui inviare comunicazioni più mirate.

Ma, nel caso sottoposto all'esame della CGUE nè Facebook nè la Wirtschaftsakademie informavano i clienti della circostanza che i loro dati personali, raccolti per mezzo di *cookie*, venivano sottoposti ad un successivo trattamento. Da qui la decisione dell'ULD di intimare alla Wirtschaftsakademie, in qualità di responsabile del trattamento dei dati compiuto da Facebook e dei *cookie* attivati dallo stesso social network, la disattivazione della fanpage.

Alla decisione da ultimo menzionata la società di formazione si opponeva a mezzo reclamo e successivamente a mezzo ricorso dinanzi al Tribunale amministrativo tedesco, adducendo di non poter essere considerata responsabile del trattamento dei dati realizzato esclusivamente da Facebook e che, in quanto tale, esulava dalla propria sfera di controllo o di influenza. L'autorità, pertanto, avrebbe dovuto agire direttamente nei confronti di Facebook e non contro di essa.

É in tale contesto che la Corte amministrativa federale tedesca ha sollecitato l'intervento della CGUE, affinché chiarisse se un provvedimento di disattivazione di una pagina web, come quello adottato dalla ULD, possa essere disposto anche nei confronti di un organismo (la Wirtschaftsakademie) che, in fatto e in diritto, non corrisponde ai criteri fissati dalla richiamata disposizione di cui all'art. 2, lettera d), della direttiva 95/46: infatti, sebbene il giudice del rinvio riconosca che, in nome di una tutela efficace della vita privata e della vita familiare, di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, che costituiscono, come la CGUE ha più volte ribadito (in tal senso, ex multis, *Digital Rights Ireland*, punto 53; *Google Spain*, punti 53, 66 e 74 nonché *Schrems*, punto 39), la base per l'interpretazione della direttiva

95/46/CE, la nozione giuridica di «responsabile del trattamento» elaborata dal legislatore europeo, debba essere interpretata in maniera estensiva, tuttavia dubita che la società tedesca possa essere qualificata come tale. In realtà, essa non eserciterebbe alcuna influenza in ordine alle modalità con cui Facebook elabora i dati degli utenti in piena autonomia, nè assumerebbe rilievo la circostanza che la società tragga un vantaggio dalla raccolta di quei dati, effettuata a mezzo dello strumento di «Facebook Insights», gestito dallo stesso social network, che le sono trasmessi per il funzionamento della sua fanpage.

La CGUE, nella sentenza in esame, osserva che anche un amministratore quale la Wirtschaftsakademie deve essere considerato responsabile, all'interno dell'Unione, assieme alla Facebook Ireland del trattamento dei dati interessati, dopo aver rilevato che nessun dubbio sussiste in ordine al fatto che la società americana Facebook e, per quanto riguarda l'Unione, la sua filiale irlandese Facebook Ireland debbano essere considerate «responsabili del trattamento» dei dati personali degli utenti di Facebook, nonché delle persone che hanno visitato le fanpage presenti su Facebook, in quanto esse determinano, in via principale, le finalità e gli strumenti del trattamento di tali dati.

La Corte trae l'abbrivio del proprio convincimento dalla considerazione per cui la Wirtschaftsakademie e Facebook determinerebbero congiuntamente le finalità e le modalità di trattamento dei dati personali degli utenti della fanpage, che, nel caso di specie, avevano la possibilità di accedere a dati demografici, di geo-localizzazione e ad informazioni sullo stile di vita e sugli interessi di questi ultimi. Pur non essendo l'ideatore di «Facebook Insights», infatti, il gestore, permettendo il trattamento dei dati personali degli utenti della fanpage, aderisce al sistema introdotto da Facebook, accetta gli strumenti e le finalità del trattamento elaborato dal social network ed è, dunque, coinvolto nella loro determinazione. Inoltre, così come dispone di un potere di influenza determinante nell'avvio del trattamento dei dati personali degli utenti della pagina, il gestore ha anche il potere di farlo cessare, appunto disattivando la fanpage.

Per le ragioni suesposte, conclude la Corte, la circostanza che un amministratore di una fanpage utilizzi la piattaforma realizzata da Facebook per beneficiare dei servizi a essa collegati non può esonerarlo dal rispetto degli obblighi che su di esso gravano in materia di protezione dei dati personali.

A ben vedere, la scelta della CGUE di riconoscere una responsabilità congiunta del gestore del social network e dell'amministratore di una fanpage presente su tale network, in relazione al trattamento dei dati personali dei visitatori di tale fanpage, appare coerente con lo spirito della direttiva 95/46/CE, perchè contribuisce a garantire una più completa tutela dei diritti di cui godono le persone che visitano una fanpage.

A tanto si aggiunga che è ormai pacifico nella giurisprudenza della Corte che, affinchè un soggetto possa essere considerato come responsabile del trattamento dei dati personali, ai sensi e per gli effetti della direttiva richiamata, non è necessario che disponga di un potere di controllo completo su tutti i singoli aspetti del trattamento medesimo. La CGUE, sul punto, già in occasione della nota sentenza del 13 maggio 2014, *Google Spain e Google*, ha evidenziato la natura ormai complessa dei trattamenti, che coinvolgono diversi soggetti che, a loro volta, esercitano diversi gradi di controllo. Anche in quest'ultima occasione, si ricorda che i giudici di Lussemburgo, accogliendo una nozione ampia di «responsabile del trattamento», avevano statuito che il gestore di un motore di ricerca, in quanto soggetto che determina gli strumenti e le finalità della sua attività, «deve assicurare, nell'ambito delle sue responsabilità, possibilità e competenze che quella attività soddisfi le prescrizioni della direttiva 95/46/CE».

Ad ogni modo, il riconoscimento di una corresponsabilità non comporta un automatico ed equivalente grado di responsabilità dei diversi operatori nell'ambito delle operazioni di trattamento. Invero, come chiarisce la CGUE, secondo un approccio funzionale e sostanziale, esso deve essere valutato, di volta in volta, attraverso la puntuale valutazione delle circostanze del caso concreto e, in particolare, del livello di coinvolgimento dei singoli operatori nell'ambito dei trattamenti condotti dagli stessi.

3. - Con la terza e con la quarta questione pregiudiziale, il giudice del rinvio ha chiesto alla CGUE di pronunciarsi in ordine alla interpretazione degli articoli 4, paragrafo 1, lettera a), e 28, paragrafi 1, 3 e 6, della direttiva 95/46 quando una società controllante stabilita al di fuori dell'Unione europea, come Facebook Inc., fornisce servizi di social network nel territorio dell'Unione servendosi di vari stabilimenti. Nella sostanza ha chiesto alla Corte se l'autorità di controllo di uno Stato membro è autorizzata a esercitare i poteri che le conferisce l'articolo 28, paragrafo 3, di tale direttiva, nei confronti di una filiale situata nel territorio di tale Stato membro anche se, come nella fattispecie in esame, in base alla ripartizione delle funzioni all'interno del gruppo, da un lato, tale filiale è competente solamente per la vendita di spazi pubblicitari e per altre attività di marketing nel territorio di detto Stato membro e, dall'altro, la responsabilità esclusiva per la raccolta e per il trattamento dei dati personali grava, per l'intero territorio dell'Unione, su una filiale situata in un altro Stato membro, o se spetti all'autorità di controllo di tale ultimo Stato membro esercitare detti poteri nei confronti della seconda filiale.

In via preliminare, la CGUE ricorda (v., in tal senso, sentenza del 1° ottobre 2015, *Weltimmo*, C - 230/14, EU:C:2015:639, punto 51) che, ai sensi dell'articolo 28, paragrafi 1 e 3, della direttiva 95/46, ciascuna autorità di controllo esercita tutti i poteri che le sono stati conferiti dal diritto nazionale nel territorio dello Stato membro cui appartiene, per assicurare in tale territorio il rispetto delle norme in materia di protezione dei dati. Dal combinato disposto di quest'ultima norma con il paragrafo 1, lettera a), dell'articolo 4 della richiamata direttiva, la CGUE desume che, per il fatto che il trattamento in oggetto è effettuato nell'ambito delle attività di uno stabilimento del responsabile del trattamento nel territorio di detto Stato membro, tale autorità di controllo può esercitare tutti i poteri che tale diritto le conferisce nei confronti di tale stabilimento, e ciò indipendentemente dal fatto che il responsabile del trattamento disponga di stabilimenti anche in altri Stati membri.

Sulla nozione di «stabilimento» (per un approfondimento, v. G. Caggiano, *L'interpretazione del «contesto delle attività di stabilimento» dei responsabili del trattamento dei dati personali*, in Dir. Inf. 2014, p. 605 ss), la CGUE ha più volte ribadito la necessità di aderire ad una interpretazione estensiva, chiarendo che lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale di un'attività mediante un'organizzazione stabile e che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante (sul punto si veda la già richiamata sentenza del 1° ottobre 2015, *Weltimmo*, C - 230/14, EU:C:2015:639, punto 28 e giurisprudenza ivi citata). In tali precedenti, si legge altresì che l'articolo 4, paragrafo 1, lettera a), svolgerebbe una duplice funzione, consentendo da un lato, l'applicazione del diritto dell'Unione, attraverso il diritto di uno dei suoi Stati membri quando il trattamento dei dati abbia luogo esclusivamente 'nel contesto' delle attività di uno stabilimento situato nel loro territorio, e ciò anche se il trattamento dei dati 'in senso proprio' viene effettuato in un terzo Stato (come accadeva nella causa *Google Spain e Google*) e consentendo, dall'altro lato, di determinare la legge applicabile, in quanto norma di conflitto tra le leggi dei diversi Stati membri (come appunto nel caso *Weltimmo*, in tal senso, cfr. Giusella Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, nell'ambito del PRIN 2010 - 2011, «La regolamentazione giuridica delle Tecnologie dell'Informazione e della Comunicazione (TIC) quale strumento di potenziamento delle società inclusive, innovative e sicure»).

Orbene, come rilevato dall'avvocato generale nelle sue conclusioni, dato che Facebook, trae una parte considerevole delle sue entrate segnatamente dalla pubblicità diffusa sulle pagine web che gli utenti creano e a cui essi accedono e che la filiale di Facebook ubicata in Germania è destinata a garantire, in tale Stato membro, la promozione e la vendita di spazi pubblicitari che servono a rendere redditizi i servizi offerti dallo stesso social network, le attività di tale filiale devono essere ritenute

inscindibilmente connesse al trattamento di dati personali del procedimento principale, di cui la Facebook Inc. è il responsabile assieme alla Facebook Ireland. Di conseguenza, conclude la Corte, un siffatto trattamento deve essere considerato come effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento, ai sensi del citato articolo 4, paragrafo 1, lettera a), della direttiva 95/46.

Ne segue che il diritto tedesco era applicabile nel caso di specie e che l'autorità di vigilanza era competente ad esercitare tutti i poteri di intervento che il diritto nazionale e quello sovranazionale le riconoscono nei confronti del responsabile del trattamento, anche se quest'ultimo è situato in un altro Stato membro o in uno Stato terzo.

4. - Infine, con la quinta e la sesta questione, il giudice del rinvio chiede, in sostanza, se l'articolo 4, paragrafo 1, lettera a), e l'articolo 28, paragrafi 3 e 6, della direttiva 95/46 debbano essere interpretati nel senso che, qualora l'autorità di controllo di uno Stato membro intenda esercitare, nei confronti di un organismo stabilito nel territorio di tale Stato membro, i poteri d'intervento di cui all'articolo 28, paragrafo 3, di tale direttiva a motivo di violazioni delle disposizioni relative alla protezione dei dati personali, commesse da un terzo responsabile del trattamento di tali dati, che ha la propria sede in un altro Stato membro, tale autorità di controllo è competente a valutare, in modo autonomo rispetto all'autorità di controllo di quest'ultimo Stato membro, la liceità di un siffatto trattamento di dati e può esercitare i suoi poteri d'intervento nei confronti dell'organismo stabilito sul proprio territorio senza previamente richiedere l'intervento dell'autorità di controllo dell'altro Stato membro.

Anche in quest'ultimo caso, la CGUE risponde positivamente. Specificatamente, secondo la Corte, dalla direttiva 95/46 non discende alcun criterio di priorità che disciplini l'intervento delle autorità di vigilanza le une rispetto alle altre, nè l'obbligo per ciascuna di esse di conformarsi alle posizioni eventualmente espresse dalle autorità di altri Stati membri.

Pertanto, la Corte conclude che l'Autorità di controllo procedente (*i.e.* l'autorità dello Stato membro in cui si trova lo stabilimento del responsabile del trattamento) può autonomamente agire nei confronti di un titolare per illeciti commessi da terzi nello Stato membro in cui questa esercita i propri poteri di intervento, senza necessità di consultare preventivamente o agire di concerto, con l'Autorità di controllo di un altro Stato membro.

5. – Come evidenziato, non di rado accade che gli internauti, senza esserne a conoscenza, producano informazioni che vengono a loro volta conservate e frequentemente impiegate per finalità diverse da quelle per le quali erano state originariamente raccolte. Ciò ha inevitabilmente evidenziato, soprattutto nell'ultimo decennio, l'inadeguatezza di quel modello di tutela statico, proprio del web 1.0, modellato sui cd. "small data", rispetto ai *Big Data* propri del web 2.0. (in tal senso, S.Faro, N.Lettieri *Big Data e Internet delle cose: opportunità, rischi e nuove esigenze di tutela per gli utenti della Rete*, in L.Ruggeri,C.Perlingieri (a cura di),Internet e diritto civile, Napoli, 2015, 279), rendendo necessario l'intervento riformatore puntuale e scrupoloso del legislatore europeo e quello appunto chiarificatore e costante della CGUE.

La previsione dell'utilizzo delle nuove tecnologie e delle nuove circuitazioni dei flussi informativi e documentali ha comportato, sotto il profilo normativo, un implemento qualitativo del livello di tutela, oltre che l'accresciuta consapevolezza del valore fondamentale della valutazione della tipologia, della qualità e/o della quantità dei dati oggetto del trattamento e la necessità della scelta di adeguate policy di *risk management*.

Non da ultimo, si è posta per le legislazioni nazionali la sfida per la realizzazione di uno standard di tutela uniforme, in grado di proiettarsi verso la dimensione di quello che è stato già definito come l'imminente avvento del web 3.0 con il quale si apre un

panorama ancora più complesso in cui entrano in gioco direttamente gli oggetti e gli strumenti tecnici attraverso i quali le informazioni ed i dati vengono raccolti. Infatti, questi apparati non sono solo capaci di accumulare un considerevole flusso di informazioni riguardanti coloro che li utilizzano, ma riescono addirittura ad entrare in collegamento in modo del tutto autonomo, con altri dispositivi ed interagire fra di loro per cambiarsi ed aggiornare tutte le informazioni in loro possesso (in questi termini, G. Marini, *Diritto alla Privacy*, in *Commentario al Codice Civile* (a cura di Gabrielli), *Delle Persone. Vol. III. Leggi collegate* (a cura di V. Barba, S.Pagliantini), Milano, 2013, p. 199 (ma spec. p. 252 ss., *Web 3.0. La Nuvola e le altre frontiere tecnologiche*).

La sentenza della CGUE in esame costituisce, dunque, un contributo rilevante per fare chiarezza sulla portata della normativa applicabile in materia di protezione dei dati personali, collocandosi coerentemente in quel processo di evoluzione della tutela dei dati personali, fondato sul crescente coinvolgimento della persona nella gestione dei propria sfera individuale, iniziato già da oltre un decennio, da quando cioè l'integrazione europea ha smesso di guardare solo al mercato unico per volgere lo sguardo anche verso il più ampio orizzonte dei diritti della persona. In tale prospettiva, nella Carta dei diritti fondamentali della persona dell'Unione, il diritto alla protezione dei dati personali (art. 8) è riconosciuto come diritto autonomo, separato da quello al rispetto della propria vita privata e familiare di cui all'art. 7. Inoltre, l'art. 16 TFUE espressamente attribuisce ad ogni persona il diritto alla protezione dei propri dati personali.

Si tratta della manifestazione più pregnante di quel "*right to be let alone*" individuato come il frutto del passaggio da un modello di tutela statica e negativa della riservatezza, che, costruita sul prototipo della proprietà privata, si esaurisce nell'esclusione delle ingerenze altrui alla protezione dei dati personali, ad un modello di tutela dinamica, fatta di regole rigorose da cui discendono le modalità del trattamento e di conferimento di poteri di controllo e di intervento alla persona interessata e alle preposte autorità di vigilanza (così, S. Rodotà, *Il diritto di avere diritti* (Roma 2012), 397).