NOMOS
Le attualità nel diritto

Quadrimestrale di Teoria generale,
Diritto pubblico comparato e Storia costituzionale

FLAVIA ZORZI GIUSTINIANI*

L'ENTRATA IN VIGORE DELLA CONVENZIONE DI MALABO SULLA SICUREZZA INFORMATICA E LA PROTEZIONE DEI DATI PERSONALI E LA PRONUNCIA DELLA CORTE DI GIUSTIZIA EUROPEA NEL CASO META PLATFORMS (CAUSA C-252/21)**

SOMMARIO: 1. La Convenzione di Malabo. – 2. Il caso Meta Platforms.

1. La Convenzione di Malabo

Tra gli sviluppi più interessanti avvenuti nel quadrimestre in rassegna deve annoverarsi in primo luogo l'entrata in vigore, l'**8 giugno** scorso, della convenzione dell'Unione Africana sulla sicurezza informatica e la protezione dei dati personali (cd. Convenzione di Malabo). L'entrata in vigore è effetto del deposito, effettuato dalla Mauritania il **9 maggio** 2023, del quindicesimo ed ultimo strumento di ratifica necessario a tal uopo ai sensi dell'art. 36 della Convenzione in discorso[1].

La Convenzione era stata adottata in seno all'Unione africana nel lontano 2014, dopo un negoziato durato tre anni, al fine di dotare il continente africano di uno strumento normativo *ad hoc* sul digitale che fosse capace di rispondere alla crescente diffusione delle tecnologie digitali. Il testo del trattato - unica convenzione internazionale a disciplinare nel contempo sicurezza informatica, crimine informatico, transazioni elettroniche e protezione dei dati - è stato redatto con l'ausilio sia di esperti africani del settore che di grandi potenze quali gli USA e l'Unione europea. La Convenzione di Malabo, peraltro, per molti aspetti è ispirata alla Convenzione del Consiglio d'Europa sulla sicurezza informatica (c.d. Convenzione di Budapest) e, per quanto concerne la protezione dei dati personali, alla Convenzione del Consiglio d'Europa per la protezione delle persone in materia di trattamento dei dati personali (c.d. Convenzione 108+) e alla direttiva 46/95 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera

* Professoressa associata di Diritto dell'Unione europea – Università degli Studi "Link Campus University" di Roma.

** Contributo sottoposto a *peer review*.

[1] Oltre alla Mauritania, la Convenzione é stata ratificata dai seguenti Stati membri dell'Unione africana: Benin, Capo Verde, Costa D'Avorio, Congo, Ghana, Guinea, Mozambico, Mauritius, Namibia, Niger, Ruanda, Senegal, Togo e Zambia.

ISSN 2279-7238

circolazione di tali dati (abrogata e sostituita, a partire dal 25 maggio 2018, dal Regolamento (UE) 2016/679 sulla protezione dei dati personali (c.d GDPR)).

I punti cardine della Convenzione di Malabo possono così riassumersi: in tema di criminalità informatica, vengono criminalizzate un'ampia gamma di attività quali la pirateria informatica, la frode informatica e il furto di identità e si stabiliscono apposite procedure di inchiesta; in materia di protezione dei dati personali, il trattamento di questi ultimi è assoggettato a sei principi fondamentali (consenso, legittimità, pertinenza, accuratezza, trasparenza e confidenzialità)[2] e gli Stati parti devono istituire apposite autorità per la protezione dei dati e garantire che i dati personali siano raccolti, elaborati e archiviati in modo sicuro[3].

Il recente impulso al processo di ratifica, che ha infine permesso l'entrata in vigore della Convenzione, si deve alla riluttanza di diversi Stati africani ad aderire ad un trattato – nella specie la Convenzione di Budapest – che non hanno contribuito a negoziare[4]. Al pari della Convenzione di Budapest, tuttavia, la Convenzione di Malabo sconta la sopravvenuta inattualità di molte sue parti, *in primis* le disposizioni relative alla condivisione transfrontaliera dei dati, che appaiono del tutto inadeguate dinanzi all'attuale mole e velocità dei flussi di dati transfrontalieri, come pure la mancata considerazione di problematiche cruciali quali la giurisdizione. Inoltre, essendo un trattato quadro, non pone una disciplina di dettaglio e dovrebbe essere integrato da un'ulteriore normativa che definisca la portata di molte sue norme. Nondimeno, la sua entrata in vigore segna una tappa fondamentale verso la progressiva armonizzazione delle legislazioni nazionali africane nel settore digitale.

2. Il caso Meta Platforms

Un altro sviluppo degno di nota ci è offerto dalla Corte di Giustizia dell'Unione Europea (CGUE) che, il **4 luglio** 2023, riunita in Grande Sezione, ha reso un importante pronuncia nella causa C-252/21 (Meta Platforms e altri (condizioni generali d'uso di un social network)) in tema di rapporti tra diritto della concorrenza e normativa sulla protezione dei dati personali. All'origine di questa sentenza vi è la richiesta di rinvio pregiudiziale depositata dal Tribunale regionale superiore di Düsselfdorf (Oberlandesgericht Düsseldorf) a margine di una controversia tra l'autorità federale tedesca garante della concorrenza (Bundeskartellamt) e Meta Platforms Inc., Meta Platforms Ireland Ltd. nonché Facebook Deutschland GmbH. La Bundeskartellamt aveva infatti deciso di vietare alle suddette società il trattamento di alcuni dati personali previsti dalle condizioni generali d'uso del social network Facebook. Il Tribunale regionale superiore di Düsseldorf ha pertanto interrogato la CGUE in merito, in primo luogo, alla competenza dell'autorità federale

[2] Cfr. l'art. 13 della Convenzione.
[3] Cfr. gli artt. 11-12 della Convenzione.
[4] La Convenzione di Budapest, infatti, seppur negoziata nell'ambito del Consiglio d'Europa, annovera tra i suoi membri vari Paesi extraeuropei quali il Brasile, gli Stati Uniti d'America e il Giappone.

garante della concorrenza ad emettere una siffatta decisione e, in secondo luogo, circa la conformità di diversi aspetti del trattamento effettuato da Meta.

Per quanto concerne il primo punto, la Corte europea ha concluso che, nell'ambito dell'esame dell'abuso di posizione dominante di un'impresa, un'autorità nazionale garante della concorrenza può rilevare l'illegittimità dei relativi trattamenti[5]. Si tratta di una interpretazione indubbiamente evolutiva, che è però temperata dal richiamo all'obbligo di leale cooperazione ex art. 4 par. 3 TUE. Difatti, pur in assenza di specifiche norme unionali in tema di cooperazione tra gli organismi deputati al controllo della protezione dei dati e quelli dedicati alla concorrenza, la Corte ha sancito l'esistenza di un chiaro obbligo in capo alle autorità nazionali garanti della concorrenza, allorché debbano esaminare nell'esercizio delle loro competenze la conformità di un comportamento di un'impresa al GDPR, di "concertarsi e cooperare lealmente con le autorità nazionali di controllo interessate oppure con l'autorità di controllo capofila"[6]. Quanto al contenuto concreto delle misure di concertazione/cooperazione da adottare, questo è rimesso alle due tipologie di autorità nazionali, alle quali la CGUE affida il compito "to coordinate their respective competences and interpretations of the law" [7].

Quanto alle diverse questioni sollevate dal giudice del rinvio con riguardo alla conformità dei trattamenti dei dati effettuati da Meta con il GDPR, i punti fondamentali posti all'attenzione della CGUE sono essenzialmente tre. Il primo consiste nell'individuare se avvenga un trattamento di dati personali sensibili e, in caso affermativo, se si tratti di dati chiaramente pubblici[8]. Il secondo è volto a stabilire su quali basi giuridiche possa fondarsi un tale trattamento ai sensi dell'art. 6 GDPR[9]. Il terzo punto, infine, attiene al consenso e alla sua capacità di essere "libero" in caso di posizione dominante del titolare del trattamento[10].

In merito al primo aspetto, la Corte ritiene che i dati "off-Facebook" consentano in particolare di vedere quali pagine web sono visitate dagli utenti. Ciò è tecnicamente possibile quando tali pagine integrano Facebook Business Tools o altre tecnologie di tracciamento. La CGUE evidenzia poi che la consultazione di determinate pagine web, quali siti medici, religiosi o su tematiche relative ad un particolare orientamento sessuale, può rivelare dati sensibili anche senza l'inserimento di informazioni in siffatti siti, in particolare informazioni attinenti alle particolari categorie di dati personali di cui all'art. 9 GDPR[11]. Partendo da questa premessa, la CGUE esamina poi l'eventuale natura "pubblica" dei dati personali. L'art. 9 par. 2 GDPR prevede una specifica deroga al generale divieto di trattamento di particolari categorie di dati personali nel caso in cui detti dati sono "resi manifestamente

[5] Cfr. il par. 48 della sentenza della Corte.

[6] Cfr. il par. 53 della sentenza della Corte.

[7] Cfr. I. GRAEF, *The European Court of Justice in Meta Platforms leaves competition and data protection authorities with an assignment*, in *EuropeanLawBlog.eu*, n. 30/2023.

[8] Cfr. la seconda questione pregiudiziale.

[9] Cfr. la terza, quarta e quinta questione pregiudiziale.

[10] Cfr. la sesta questione pregiudiziale.

[11] Si tratta, in particolare, di dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose nonché di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.

pubblici dall'interessato"[12]. Qualora risulti che la consultazione di pagine web è idonea a rivelare dati sensibili, tale consultazione da sola non consente di dedurre l'intenzione di rendere pubbliche informazioni sensibili da parte dell'internauta. Nel caso in cui siano utilizzati i social plug-in, come i pulsanti di selezione "mi piace" o "condividi", è compito del giudice verificare che l'utente possa effettivamente decidere, sulla base di un'impostazione di parametri effettuata con cognizione di causa, di rendere o meno i dati inseriti nei siti Internet o nelle applicazioni in questione, nonché i dati risultanti dall'attivazione dei pulsanti di selezione in essi integrati, accessibili al grande pubblico. Per rientrare nella suddetta eccezione è dunque necessario che l'utente "abbia inteso, in modo esplicito e con un atto positivo chiaro, rendere accessibili al pubblico i dati personali in questione"[13].

Quanto al secondo punto, concernente le basi giuridiche che, ai sensi dell'art. 6 GDPR, possono essere utilizzate per trattamenti relativi alla pubblicità mirata, la CGUE esamina singolarmente il consenso, il contratto, l'interesse legittimo, la tutela degli interessi vitali e l'interesse pubblico. Al riguardo la Corte stabilisce anzitutto che se il trattamento comprende dati sensibili oltre ai dati personali "normali", senza dissociazione tra le due tipologie di dati, il trattamento è in linea di principio vietato sulla base dell'art. 9 par. 1 GDPR. Da ciò discende che, qualora un insieme di dati contenga anche una sola informazione sensibile, esso viene "contaminato" e si trova soggetto a severi requisiti relativi al trattamento di dati di categorie speciali. In secondo luogo, la CGUE fornisce chiarimenti in merito all'esame del trattamento basato sulla necessità relativa all'esecuzione di un contratto (art. 6 par. 1 lett. b GDPR). Il trattamento dei dati in questione, infatti, deve essere "oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale"[14]. Il trattamento deve quindi essere essenziale, senza che siano presenti altre soluzioni meno invasive. Ad avviso della CGUE, la personalizzazione della pubblicità mediante cui è finanziato il social network non è idonea a giustificare il trattamento dei dati in quanto "legittimo interesse" del titolare del trattamento stesso. Meta deve pertanto richiedere ed ottenere il consenso espresso e libero del soggetto interessato dal trattamento ai sensi dell'art. 6, par. 1, lett. f) GDPR.

In terzo luogo, nel controllo dei legittimi interessi invocati da Meta per giustificare il trattamento, previsto dall'art. 6 par. 1 lett. c) GDPR, la CGUE esamina, tra l'altro, l'interesse alla personalizzazione della pubblicità. Nella sua argomentazione, la CGUE tiene conto delle "ragionevoli aspettative" dell'interessato nonché della portata del trattamento e del suo impatto. Ritiene che, nonostante la gratuità del servizio offerto, l'interessato non può pretendere che i suoi dati vengano trattati senza il suo consenso. Inoltre, un trattamento esteso e illimitato avrebbe un impatto significativo sull'internauta, potendo suscitare in esso "la sensazione di una continua sorveglianza della sua vita privata"[15]. Quest'ultimo

[12] Cfr. art. 9 par. 2 lett. e) GDPR.
[13] Cfr. il par. 77 della sentenza della Corte.
[14] Cfr. il par. 98 della sentenza della Corte.
[15] Cfr. par. 118 della sentenza della Corte.

riferimento evidenzia l'importanza che la Corte attribuisce alla percezione del trattamento da parte dell'interessato nel determinare la legittimità degli interessi del titolare.

Quanto al terzo punto, relativo alla libertà del consenso in un contesto di posizione dominante, la CGUE ha ritenuto che nella fattispecie il fatto che il social network occupi una posizione dominante sul mercato non pregiudica la possibilità per gli utenti di acconsentire al trattamento dei loro dati personali. Tuttavia, giacché la suddetta posizione dominante incide sulla libertà di scelta dell'internauta, è necessario un accertamento più stringente della manifestazione di un consenso libero e validamente prestato, il cui onere della prova grava sul titolare del trattamento.

Degno di rilievo è il fatto che la Corte suggerisca altresí la possibilità, per l'utente che rifiuta di prestare il proprio consenso, di usufruire ugualmente dei servizi digitali dietro pagamento di un corrispettivo[16]. Nel caso poi dei dati "off-Facebook", in base al principio che il trattamento di questi non è necessario all'esecuzione del contratto, la CGUE ritiene che debba essere prestato un consenso specifico a tale trattamento. Sembra quindi che l'unica base giuridica che può essere mantenuta nel contesto di un'attività pubblicitaria mirata sia il consenso.

[16] Cfr. il par. 150 della sentenza della Corte. Come é stato osservato, ciò potrebbe contribuire a rendere consapevoli gli internauti che l'utilizzo dei servizi in questione non é affatto «for free» (cfr. H. RUSCHEMEIER, *Competition law as a powerful tool for effective enforcement of the GDPR*, in *Verfassungsblog.de.*