

Gli obblighi dei gatekeeper e la tutela dei dati personali

Il “pacchetto digitale” (Regg. Ue 2022/2065, *infra*: DSA; 2022/1925, *infra*: DMA; 2022/868 (*infra*: DGA) ha introdotto significative innovazioni nella regolazione dell’economia delle piattaforme, che rivelano interrelazioni importanti con la disciplina di protezione dati (Reg UE 2016/679; d.lgs. 196/2003; d.lgs. 51/ 2018).

Il complesso normativo realizzato con gli interventi (in certa misura anche complementari) del DSA, DMA ma anche del DGA completano il percorso di regolazione della dimensione “virtuale” iniziato, già nel 2016, con il GDPR, per **responsabilizzare** i nuovi poteri privati.

Sul piano della tutela dei dati personali raccolti da queste aziende, il GDPR ha imposto, appunto, un approccio preventivo e proattivo fondato sull'assunzione di obblighi di diligenza specifici (applicabili, secondo il criterio del *targeting*, con una parziale extraterritorialità della disciplina), sull'adozione di misure di valutazione e prevenzione del rischio, di tutele remediali e prerogative di intervento dei singoli, nonché su un articolato sistema di public e private enforcement, con sanzioni punitive in senso convenzionale (Trib. Palermo, 3563/19) estese anche alla violazione dei meri principi, distinti dai precetti.

Obiettivo del GDPR è la responsabilizzazione di chiunque tratti dati personali (ivi incluse le piattaforme) rispetto al «rischio sociale» connesso alla gestione dei dati.

- Un ambito in cui le piattaforme (motori di ricerca) sono state destinatarie di obblighi specifici ante litteram è stato quello dell'oblio (CGUE sent.Costeja, 13.5.2014; poi art. 17 Gdpr) ovvero del delisting di contenuti obsoleti o inesatti
- Norme settoriali (l. 71/17 per il cyberbullismo e, più recentemente, dl 139/21 per il revenge porn), muovendo dall'esigenza di responsabilizzazione "secondaria" delle piattaforme rispetto agli user generated content hanno poi imposto loro specifici obblighi ablativi o inibitori, il controllo sui quali è attribuito in prima istanza al Garante

- Gli obblighi sanciti da queste norme e, in particolare, relativamente all'oblio, hanno evidenziato il ruolo arbitrale attribuito alle piattaforme anche rispetto all'esercizio di libertà fondamentali quali quella di espressione. Ciò era plasticamente emerso con la sentenza 3.10.2019 (Glawischnig-Piesczek c. Facebook, C 18-2018), con cui la CGUE ha ammesso **l'ingiunzione giudiziale di rimozione di contenuti equivalenti** a quelli dichiarati illeciti perché lesivi della dignità.
- Per quanto la Corte abbia circoscritto l'ammissibilità di tale ingiunzione "dinamica" ai casi di **effettiva equivalenza** dei contenuti, che non lasci residuare in capo al gestore margini significativi di valutazione discrezionale, è evidente come si siano onerate le piattaforme di valutazioni talora complesse e tutt'altro che 'automatiche' o automatizzabili.

La difficoltà di qualificazione del ruolo delle piattaforme è emersa in particolare rispetto all'oscuramento di profili Facebook di movimenti politici come Casapound o FN, per stabilire il confine oltre il quale l'autonomia privata esiga una forma di eteroregolazione funzionale alla garanzia dei diritti incisi.

Fino a che punto, insomma, l'oscuramento della pagina di un movimento politico può ridursi a mero recesso dal contratto di fornitura del servizio di social network? O deve, questa libertà negoziale, essere esercitata tenendo conto delle implicazioni che ha sui diritti di partecipazione politica dei singoli e dei gruppi?

Ed è davvero ammissibile onerare soggetti privati, che agiscono secondo logiche commerciali, della valutazione di liceità dei contenuti diffusi, alla stregua di *policies* interne che riflettono bilanciamenti tra diritti e libertà, complessi persino per il giudice?

Su questo punto l'ordinanza cautelare del Tribunale di Roma del 29 aprile 2020 (RG 80961/19), poi revocata nel 2022 in sede di merito, sulla vicenda Casapound, è netta nell'escludere la possibilità di *“riconoscere ad un soggetto privato, quale Facebook Ireland, sulla base di disposizioni negoziali e quindi in virtù della disparità di forza contrattuale, poteri sostanzialmente incidenti sulla libertà di manifestazione del pensiero e di associazione, tali da eccedere i limiti che lo stesso legislatore si è dato nella norma penale”*.

Osserva del resto, in linea generale, il Tribunale, come la *“qualificazione del rapporto in termini contrattuali e l'assenza di disposizioni normative speciali non implicano che la sua disciplina sia rimessa senza limiti alla contrattazione fra le parti ed al rapporto di forza fra le stesse né che l'esercizio dei poteri contrattuali sia insindacabile”*.

Queste vicende (risolte in modo diverso ad esempio nel caso di FN) hanno dimostrato la difficoltà di qualificazione del ruolo della piattaforma:

- per alcuni (Tribunale Roma, ordinanza cautelare su Casapound) *essential facility* rispetto all'esercizio di diritti fondamentali, fori pubblici in cui garantire il pluralismo, sulla base di un'applicazione orizzontale delle norme costituzionali a rapporti tra privati;
- secondo una concezione sempre pubblicista delle piattaforme ma di tipo protezionistico nei confronti della dignità, soggetto comunque tenuto alla rimozione di contenuti lesivi o istigativi (è la tesi della sentenza di merito del Trib. Roma su Casapound), anche secondo i vincoli di cui all'art. 41 Cost;
- secondo la concezione privatistica (maggioritaria; es. trib. Siena ma anche Trib. Roma su Forza Nuova) soggetti privati le cui azioni ablativo si giustificano in termini di recesso a fronte della violazione delle clausole contrattuali da parte dell'utente.

Da questa difficoltà di qualificazione della natura della piattaforma è derivata anche la difficoltà di tracciare i confini della sua responsabilità alla luce dell'ampia (benché condizionata) esenzione dell'art. 14 della direttiva sul commercio elettronico.

Come dimostra anche la giurisprudenza *sull'host provider attivo e sugli indici di interferenza* tali da escludere l'esenzione da responsabilità, l'esigenza di una maggiore *responsiveness* delle piattaforme, a fronte del loro crescente potere, ha rappresentato la ragione fondante il pacchetto digitale.

Le norme del DSA, del DMA e in parte anche del DGA hanno introdotto, ciascuna, un tassello importante in questo percorso, con significative affinità con il GDPR.

Non si è trattato, certo, di un rovesciamento radicale di prospettiva rispetto all'assetto precedente, ma di un passaggio **dalla responsabilità (primaria e secondaria) alla responsabilizzazione** attuata mediante la previsione di obblighi (di trasparenza, di prevenzione, di analisi dei rischi) in capo al gestore e rimedi attivabili dall'utente, pur con una generale conferma del *safe harbour* della direttiva 2000/31..

Gli obblighi imposti alle piattaforme hanno fini diversi:

- nel caso del DMA assicurare la contendibilità del mercato e la correttezza delle sue dinamiche evitando concentrazioni di potere (con ovvie ricadute positive per gli utenti: cfr., ad es., art.42);
- per il DSA impedire lo sfruttamento delle posizioni dominanti per veicolare contenuti illeciti e, in genere, responsabilizzare gli intermediari rispetto ai contenuti ospitati;
- per il DGA essenzialmente favorire la circolazione e condivisione dei dati, a fini tanto solidaristici quanto d'iniziativa economica, responsabilizzando gli attori principali (servizi di intermediazione dei dati e organizzazioni per l'altruismo dei dati).

Il DMA

- Introduce obblighi e divieti in capo ai soggetti economici designati dalla Commissione (con possibilità di riesame) quali gatekeeper, ovvero piattaforme di grandi dimensioni che rivestono all'interno del mercato digitale **un ruolo strategico di collegamento tra le aziende e i consumatori**, in ragione della posizione economica, commerciale, di intermediazione, definita con indici qualitativi e quantitativi tra cui il numero di utenti, il controllo di altri soggetti, la capitalizzazione e il fatturato.
- Tutte le misure funzionali all'osservanza degli obblighi e dei divieti (volte a evitare comportamenti anticoncorrenziali o **concentrazioni di potere per via del possesso dei dati**) **devono rispettare il GDPR (art. 8, p.1, u.p.), incluse le raccolte dati funzionali all'interoperabilità dei servizi offerti (art.7.8).**

C 36

- Spesso i gatekeeper raccolgono direttamente i dati personali degli utenti finali che utilizzano siti e app di terzi, per fornire servizi pubblicitari online. I terzi forniscono inoltre ai gatekeeper i dati personali dei loro utenti finali per avvalersi di determinati servizi offerti dai primi nel contesto dei loro servizi di piattaforma di base, come per esempio il pubblico personalizzato.
- Le piattaforme dovrebbero quindi offrire agli utenti finali, rileva il C 36, **alternative meno personalizzate ma equivalenti**, senza per ciò limitare l'uso del servizio offerto dalla piattaforma stessa.

Art. 5, p.2 (utilizzo dei dati su consenso)

- Vieta ai *gatekeeper* :
- l'utilizzo dei dati ottenuti dagli utenti aziendali per scopi pubblicitari e senza l'espresso consenso, non revocato, dell'interessato; **la combinazione o l'utilizzo incrociato di tali dati in diversi servizi**
- l'iterazione della richiesta di consenso (negato o revocato) per lo stesso fine più di una volta l'anno
- Il trattamento dati degli utenti finali può comunque fondarsi su presupposti di liceità di tipo pubblicistico (obbligo legale, esercizio di un compito di interesse pubblico) e sull'interesse vitale; si esclude invece (C 36) il ricorso al legittimo interesse.

Caratteristiche (e limiti) del consenso

- Il consenso dovrebbe essere prestato mediante **dichiarazione o azione positiva inequivocabile**, con cui l'utente finale esprime una manifestazione di volontà libera, specifica, informata e inequivocabile (C 37); *dubbi sull'asimmetria del rapporto e sulla natura effettivamente opzionale e non condizionale del consenso, che il C 37 contrasta indicando l'esigenza di mantenere eguali livelli di qualità delle alternative meno personalizzate, salvo che le differenze siano dettate dall'impossibilità per la piattaforma di trattare i dati, con corrispondente informazione all'utente.*
- Anche la revoca dovrebbe essere agevolata con divieto di presentazione delle proprie interfacce in modo decettivo rispetto all'autodeterminazione informativa dell'utente

C 38

Ricorda la tutela rafforzata di cui godono **i dati dei minori:**

“Nessuna disposizione del presente regolamento esonera i gatekeeper dai loro obblighi in materia di protezione dei minori previsti dal diritto dell'Unione applicabile»

Art. 6, p. 9 (portabilità)

- Impone di garantire agli utenti finali la **PORTABILITÀ dei «dati» forniti o generati sui servizi** della piattaforma principale.
- C 59: questa forma di portabilità ha **carattere integrativo** rispetto a quella di cui all'art. 20 del GDPR, delineando un istituto giuridico diverso e più ampio, esteso sino a ricomprendere **anche i dati non personali** e quelli (ulteriori rispetto a quelli forniti dagli interessati o risultanti dall'osservazione delle loro attività) inferiti dallo stesso titolare del trattamento (quale, ad esempio ,un profilo utente realizzato mediante analisi di dati grezzi).

Art. 6, p.10

(accesso su consenso)

- Il gatekeeper fornisce agli utenti commerciali e a terzi autorizzati **ACCESSO:**
 - a dati aggregati e non, **compresi i dati personali** e, nel caso di questi ultimi...
 - ne garantisce l'uso **solo se i dati sono direttamente connessi con l'uso effettuato** dagli utenti finali in relazione ai prodotti o servizi offerti dal pertinente utente commerciale mediante il pertinente servizio di piattaforma di base e
 - nel caso in cui gli utenti finali accettano tale condivisione esprimendo il **loro CONSENSO**

Art. 6, p.11 (accesso a dati su ricerche)

- Obbligo del gatekeeper di **anonimizzazione** dei dati (personali) relativi a ricerca, click e visualizzazione cui consente l'accesso da parte delle imprese terze che forniscono motori di ricerca online

Art.7, p.8 (Interoperabilità)

- A fronte di una richiesta di interoperabilità da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero, il gatekeeper fornisce solo:
- **i dati personali degli utenti finali strettamente necessari** per fornire un'effettiva interoperabilità (principio di minimizzazione)

Art. 8 p.1 (accountability)

- La norma sancisce, in capo alla piattaforma, l'obbligo di garantire (e dimostrare) l'osservanza degli obblighi impostigli dal DMA e
- la **conformità delle relative misure, tra gli altri, al GDPR**

Art. 13, p.5 (norme antielusione)

- Ove sia richiesto un consenso per la raccolta, il trattamento, l'utilizzo in modo incrociato e la condivisione dei dati personali, la piattaforma **consente agli utenti commerciali di ottenere direttamente il consenso necessario**, anche fornendo loro, ove opportuno, dati debitamente anonimizzati.
- **E' vietato** alla piattaforma rendere l'acquisizione di tale consenso da parte dell'utente commerciale **più onerosa** di quanto sia previsto per i propri servizi

Art. 15

(tecniche di profilazione)

- Sancisce uno specifico obbligo, in capo alla Commissione, di trasmissione, al Comitato europeo per la protezione dei dati, della **descrizione delle tecniche di profilazione dei consumatori** applicate dai gatekeepers ai servizi di base da loro offerti
- Questo perché la trasparenza sul profiling può promuovere una reale competitività ed evitare concentrazione di potere (informativo)
- La privacy può rappresentare un fattore di vantaggio competitivo

Adeguamento dell'ordinamento (ddl concorrenza, AC 1555, seconda lettura)

- Le norme di adeguamento dell'ordinamento interno al DMA recano una clausola di salvaguardia (non del tutto esaustiva) in favore delle competenze del Garante sul controllo del trattamento dati da parte delle piattaforme
- Anche a tal fine sarà tanto più opportuno normare, anche con atti convenzionali, quella connessione procedimentale tra AGCM (autorità interna designata per il DMA) e Garante, suggerita da CGUE, sent. 4.7.23

Il DSA

- Sancisce obblighi in capo agli intermediari on line per garantire un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e tuteli i diritti sanciti dalla CDFUE
- Si tratta di obblighi asimmetrici, differenziati in ragione della natura dell'intermediario on line, che se ascrivibile alle piattaforme o motori di ricerca molto grandi (**con più di 45 milioni di utenti al mese**), assume obblighi supplementari
- C 10: generale clausola di salvaguardia rispetto al GDPR

Artt. 26, p.3; 28, p.2 (profilazione e dati a tutela rafforzata)

- La prima sancisce, in capo alle piattaforme on line, un divieto di **profilazione fondata su dati particolari** (art 9 GDPR) funzionale a scopi pubblicitari
- La seconda vieta alle piattaforme on line **la profilazione, a scopi pubblicitari, basata su dati** dei destinatari del servizio, in presenza **della ragionevole certezza della loro minore età ;**
- **tale divieto** non deve essere attuato con misure che impongano **raccolte ulteriori di dati per la verifica dell'età dell'utente**

Art. 38

(opzioni scevre da profilazione)

- Sancisce l'obbligo per le very large online platform e per i motori di ricerca, di **assicurare almeno un'opzione**, per ciascuno dei loro sistemi di raccomandazione, che non sia basata sulla profilazione

Art. 40

Accesso dei ricercatori abilitati

- La norma legittima **l'accesso dei ricercatori abilitati ai dati in possesso** delle very large online platform o dei motori di ricerca, pur con l'impegno dei primi a rendere disponibili gratuitamente al pubblico i risultati delle loro ricerche, **in conformità al GDPR**

Norme di adeguamento interno

- Il **dl «Caivano»** (n. 123 del 2023, conv, mod. l. 159 del 2023) non sancisce clausole di salvaguardia ma dispone la **cooperazione**, tra gli altri del Garante, con Agcom quale DSC **anche mediante protocolli d'intesa**
- Anche in tale ambito è opportuno prevedere una connessione procedimentale adeguata, pure per esigenze di rispetto delle condizioni richieste dalla CGUE in caso di configurabilità di un *bis in idem*

Il DGA

- Tocca marginalmente il ruolo delle piattaforme in quanto costituiscano **servizi di intermediazione dei dati (anonimizzati se personali)**, per mettere in contatto utenti e titolari dei dati, promuovere fiducia nella condivisione e coadiuvando l'interessato nelle scelte dispositive sui suoi dati.
- Le organizzazioni per l'altruismo dei dati hanno invece un ruolo essenzialmente di sostegno rispetto alle scelte dispositive dell'interessato

Norme di adeguamento

- L'adeguamento dell'ordinamento interno è nella delega legislativa all'esame della Commissione XIV della Camera dei deputati in prima lettura (ddl di delegazione europea, AC 1342, art. 13) e prevede l'introduzione di:
- **norme di raccordo con il sistema sanzionatorio** vigente per garantire proporzionalità tipizzando, conformemente alla previsione e ai criteri di cui all'art. 34, sanzioni, di natura amministrativa e, nei casi più gravi, penale, per le violazioni degli obblighi previsti dal regolamento,
- adeguando anche il sistema delle tutele, amministrativa e giurisdizionale, vigente (anche, è da intendere, nella materia dei dati personali)
- e garantendo *“conformemente alla normativa in materia di protezione dei dati personali, i presupposti di liceità per la trasmissione di dati personali a terzi, ai fini del riutilizzo di cui all'articolo 5, sulla base di quanto disposto dall'articolo 1, paragrafo 3, del regolamento (UE) 2022/868”*.

Complessivamente...

- Il pacchetto digitale introduce una cornice regolatoria fondata su obblighi di trasparenza, collaborazione e gestione dei contenuti ospitati, nella logica della *corporate compliance*, idonei a rafforzare tanto le garanzie degli utenti quanto la sostenibilità della *data economy*.
- Si introducono soluzioni innovative quali quelle di natura negoziale sul terreno dell'*enforcement*, con un'articolazione complessa di misure che comprendono sanzioni punitive, penalità di mora in funzione deterrente rispetto agli oneri di cooperazione con la Commissione nell'esercizio dei suoi poteri di controllo e impegni (*action plan*: art. 75 DSA e impegni nel DMA, art.25), tali da valorizzare il ravvedimento operoso.

Esigenze di coordinamento

- La vastità e trasversalità degli interventi imporrà tuttavia un adeguato coordinamento con le discipline convergenti come ad es. la protezione dati
- Potranno, infatti, ipotizzarsi casi nei quali la violazione degli obblighi sanciti in capo alle piattaforme che incida sulla sfera giuridica soggettiva dell'utente finale (cfr. artt. 42 DMA, 53 DSA) e riguardi la gestione dei loro dati integri, anche, gli estremi di un illecito privacy (rilevante in termini amministrativi, civili o finanche penali). In tali casi, a fronte della concorrenza dei rimedi esperibili, almeno sul piano del *public enforcement* si imporrà quantomeno quel coordinamento procedimentale imposto dalla CGUE, da ultimo, nella citata sentenza del 4 luglio 2023.