Gli obblighi dei gatekeeper e la tutela dei dati personali

1. Il contesto

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 inattese con la disciplina di protezione dati. Il legame tra questi plessi normativi deriva anzitutto dall'identità di contesto (il digitale) che determina, spesso, sovrapposizioni tra gli obblighi imposti allo stesso soggetto (piattaforma come titolare del trattamento), con un rischio di sovraqualificazione della fattispecie tanto più rilevante in ragione del carattere punitivo in senso convenzionale di molte delle sanzioni previste[1].

Ma il legame tra questi plessi normativi si esprime anche nel tentativo, iniziato con il Reg. Ue 2016/679 (*infra*: GDPR) e proseguito con il pacchetto digitale, di responsabilizzare le piattaforme, con obblighi (anche di carattere preventivo) funzionali rispettivamente alla tutela di diritti fondamentali e della concorrenza, nella consapevolezza di come l'anomia, lungi dal garantire libertà, determini invece assenza di tutele.

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.

Vicende come quelle di Cambridge Analytica – e, prima, di Apple-Fbi, sia pur sul diverso terreno delle "servitù di giustizia" – o della sospensione degli account di Donald Trump dopo i fatti di Capitol Hill hanno, infatti, dimostrato come i grandi attori della *new economy* esercitino poteri riconducibili non più al solo piano commerciale ma tali invece da incidere, in misura rilevante, su ambiti pubblicistici per definizione, quale in primo luogo quello dell'esercizio delle libertà e dei suoi limiti. La l*ex mercatoria* ha così rappresentato una parte significativa del codice normativo del digitale, lasciando emergere istanze di tutela cui si è tanto di rispondere, progressivamente, soprattutto sul piano della co- (e auto-) regolamentazione (codici di condotta in particolare, come nel settore dell'*hate speech).*

Parallelamente a interventi settoriali più rigorosi (ad esempio con gli obblighi imposti dalla direttiva antiterrorismo 2017/541), si è dunque complessivamente promossa, almeno negli anni più recenti e anche grazie all'impulso fornito dal GDPR, una più marcata responsabilizzazione dei soggetti privati a vario titolo coinvolti in posizione di primazia nel mercato digitale. 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, estesi poi dalla giurisprudenza della Cgue addirittura alla verifica della "sostanziale equivalenza", rispetto a quelle accordate in Europa, delle garanzie sancite dall'ordinamento di destinazione in caso di trasferimento di dati all'estero (sent. 16 luglio 2020, Schrems II, C 311-18), oltre che ai gestori dei motori di ricerca rispetto all'indicizzazione delle notizie in rete (sent. 13 maggio 2014, Costeja c. Google Spain, C 131-12, sent. 24 settembre 2019, C 136-17) .

Questa tendenza alla responsabilizzazione di soggetti, quali in particolare le piattaforme, privati ma esercenti un ruolo centrale nel contesto digitale, si è profondamente radicata negli assetti regolatorii dell'Unione e degli Stati membri, estendendosi poi dal settore privacy ad altri già prima del pacchetto digitale: si pensi alla direttiva (UE) 2018/1808 sui servizi di media audiovisivi, alla direttiva 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale (soprattutto, art. 17), al regolamento relativo alla prevenzione della diffusione di contenuti terroristici *online (*2021/784).

Al di là dei settori specifici, la normativa europea più recente sembra aver fatto tesoro del modello, sperimentato in particolare nel settore privacy, della responsabilizzazione delle piattaforme per introdurre alcune minime garanzie per i diritti degli utenti, altrimenti esposti a una sorta di autodichia dei poteri privati.

Non è un rischio così remoto, se si pensa alle vicende dell'oscuramento di profili Facebook di movimenti politici come Forza Nuova e, soprattutto Casapound. In questi casi la giurisprudenza si è

[1] Per quelle previste dalla disciplina di protezione dati, cfr. Trib. Palermo, sent. sent. 3563 del 18 luglio 2019.

misurata con la difficoltà di stabilire il confine oltre il quale l'autonomia privata (di cui il contratto che regola il servizio di social network è, pur sempre, espressione), esiga invece una peculiare forma di eteroregolazione funzionale alla garanzia dei diritti e delle libertà incise da questi contratti.

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[2], 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".*

Il tema sollevato dalla vicenda Casapound – significativamente risolto in modo molto diverso nel caso, affine, di Forza Nuova (Trib. Roma, ord. 24.2.2020, RG 64894/2019, confermata in sede di reclamo) – ripropone, del resto, le questioni già emerse rispetto al bilanciamento tra oblio e informazione sul terreno della deindicizzazione, le cui decisioni sono affidate, in prima istanza, ai motori di ricerca, o anche riguardo al cyberbullismo con la l. 71 del 2017 (nonché, pur con profili diversi, in relazione al *revenge porn ex* art. 144-bis d.lgs. 196 del 2003) . Il ruolo arbitrale attribuito alle piattaforme era del resto plasticamente emerso, in tutta la sua complessità, con la sentenza del 3 ottobre 2019 (Glawischnig-Piesczek c. Facebook, C 18-2018), con cui la Corte di giustizia UE 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 stia onerando le piattaforme di valutazioni talora complesse e tutt'altro che 'automatiche' o automatizzabil[3]i.

In linea generale era, dunque, emersa 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[4]; secondo una concezione sempre pubblicista delle piattaforme ma di tipo protezionistico nei confronti della dignità, soggetto comunque tenuti alla rimozione di contenuti lesivi o istigativi (è la tesi della sentenza di merito del Trib. Roma su Casapound[5]), anche secondo i vincoli di cui all'art. 41 Cost; secondo la concezione privatistica (maggioritaria) soggetti privati le cui azioni ablative si giustificano in termini di recesso a fronte della violazione delle clausole contrattuali da parte dell'utente[6].

---

[2] Sent.17909/2022 del 5.12.2022.

[3] Si tratta di un modello normativo molto diverso da quello adottato, ad esempio, dal dlgs 107 del 2023 di adeguamento al Regolamento UE 2021/784 sui contenuti terroristici on line, ove il ruolo dell'a.g. è centrale ai fini dell'adozione, da parte delle piattaforme, di provvedimenti ablativi.

[4] Con la difficoltà, che ne consegue, di far discendere da una situazione di mero fatto obblighi pubblicistici che, tuttavia, non hanno fondamento normativo espresso. Cfr. G.E. VIGEVANI, *Dal "caso Casapound" del 2019 alla "sentenza Casapound" del 2022: piattaforme digitali, libertà di espressione e odio online nella giurisprudenza italiana*, in *Medialaws* 2/23, 142.

[5] Con il rischio, tuttavia, di delegare l'*enforcement* delle politiche pubbliche a soggetti privati senza le necessarie garanzie

[6] Tesi sostenuta, ad es., dal Trib. di Siena, ord. 19.1.20, sempre rispetto a una vicenda relativa a Casapound, con il rischio tuttavia di ammettere una tutela dei diritti a geometria variabile in ragione delle singole clausole contrattuali.

2. Il "pacchetto digitale"

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. E 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..

Anche da questo punto di vista (criterio del t*argeting* ai fini della temperata extraterritorialità della disciplina, tassonomia degli obblighi, approccio proceduralista, rimedi attivabili da parte del soggetto, *accountability* ma anche *governanc*e e sistema sanzionatorio), le affinità con il modello del GDPR sono significative, come lo sono le intersezioni per gli obblighi che coinvolgano, a vario titolo, la gestione dei dati.

Naturalmente gli obiettivi cui tali obblighi tendono sono 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; 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).

2.1.Il DMA

Per quanto riguarda il **DMA**, esso 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.

Gli obblighi specifici, di *facere e non facere*, sono volti a:

a) promuovere la contendibilità dei mercati e la *fairness* delle loro dinamiche;

b) favorire l'accesso al mercato e la pluralità dei suoi attori;

c) contrastare la concentrazione del potere[7].

Tutte le misure funzionali all'osservanza degli obblighi e dei divieti devono rispettare il GDPR (art. 8, p.1, u.p.), incluse le raccolte dati funzionali all'interoperabilità dei servizi offerti (art.7.8).

Ma soprattutto il DMA, muovendo dalla consapevolezza del valore anche economico dei dati, introduce misure volte a evitare comportamenti anticoncorrenziali o concentrazioni di potere per via del possesso dei dati in capo alle piattaforme, tali da creare barriere all'ingresso.

In particolare, il C 36 rileva come spesso i gatekeeper raccolgano direttamente i dati personali degli utenti finali che utilizzino 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

[7] Vds. V. FALCE, *Regolazione delle piattaforme e antitrust* in R. BOCCHINI (a cura di), *Manuale di diritto privato dell'informatica giuridica*, Napoli, 2023.

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.

Una forte interrelazione con la protezione dati (la cui disciplina è fatta salva in via generale e, in particolare, rispetto alla tutela remediale dal C 37) si ha, in particolare, rispetto agli artt. 5, paragrafo 2, e 6, paragrafi 9 e 10.

La prima disposizione vieta ai *gatekeeper* l'utilizzo dei dati ottenuti dagli utenti aziendali per scopi pubblicitari e la combinazione o l'utilizzo di tali dati in diversi servizi senza l'espresso consenso, non revocato, dell'interessato. Precisamente, la piattaforma:

a) non tratta, ai fini della fornitura di servizi pubblicitari online, i dati personali degli utenti finali che utilizzano servizi di terzi che si avvalgono di servizi di piattaforma di base del gatekeeper;

b) non combina dati personali provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi;

c) non utilizza in modo incrociato dati personali provenienti dal pertinente servizio di piattaforma di base in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base, e viceversa; e

d) non fa accedere con registrazione gli utenti finali ad altri servizi del gatekeeper al fine di combinare dati personali.

Il C 37 precisa che il consenso in questione dovrebbe essere prestato mediante dichiarazione o azione positiva inequivocabile, con cui l'utente finale esprime una manifestazione di volontà libera, specifica, informata e inequivocabile.

Tra le norme antielusione (art. 13) è, inoltre, previsto che 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.

Naturalmente in un contesto, quale quello del rapporto tra utente e piattaforma, così fortemente caratterizzato dall'asimmetria nelle posizioni (e nella forza dispositiva) delle parti, non sembra agevole garantire l'effettiva libertà (intesa come opzionalità e non condizionalità) del consenso, prescritta per la sua validità dall'art. 7 GDPR. Lo stesso esercizio della facoltà di revoca, da parte dell'interessato, del consenso inizialmente prestato potrebbe ingenerare difficoltà applicative sulle quali, però, la Commissione e l'European data protection Board potrebbero ipotizzare di fornire indicazioni, anche con uno strumento di *soft law*. Tali misure contribuirebbero anche ad evitare l'eterogenesi dei fini della *consent fatigue* (che determina un sostanziale svuotamento della funzione e del valore autodeterminativo del consenso), valorizzando anche le disposizioni sugli obblighi di trasparenza delle piattaforme.

Un argine al rischio della *consent fatigue* è correttamente previsto all'art. 5, p.2, secondo cui: "*Se l'utente finale ha negato o revocato il consenso prestato ai fini del primo comma, il gatekeeper non ripete la sua richiesta di consenso per la stessa finalità più di una volta nell'arco di un anno"*.

In ogni caso, andrebbero valorizzate le indicazioni del C 37, volte a ridurre il rischio di condizionalità del consenso, imponendo in particolare 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 revocabilità del consenso dovrebbe godere delle stesse agevolazioni previste per la prestazione del consenso, con divieto di presentazione delle proprie interfacce in modo decettivo rispetto all'autodeterminazione informativa *("I gatekeeper non dovrebbero progettare, organizzare o gestire le loro interfacce online in modo tale da ingannare, manipolare ovvero compromettere o*

falsare in altro modo, in misura rilevante, la capacità degli utenti finali di prestare liberamente il proprio consenso").

Il C 38 ricorda la tutela rafforzata di cui godono i dati dei minori, precisando che "*Nessuna disposizione del presente regolamento esonera i gatekeeper dai loro obblighi in materia di protezione dei minori previsti dal diritto dell'Unione applicabile.".*

Si ammette comunque la possibilità per la piattaforma di avvalersi, al fine del trattamento dei dati degli utenti finali, dei presupposti di liceità di tipo pubblicistico (obbligo legale, esercizio di un compito di interesse pubblico) e dell'interesse vitale. Si esclude invece (C 36) il ricorso al legittimo interesse, non solo per ragioni di bilanciamento ma anche, correttamente, per evitare l'elusione della volontà dell'utente.

L'art. 6, p.9 e 10 impone, invece, di garantire agli utenti finali la portabilità dei dati generati sui servizi della piattaforma principale. Come si evince dal Considerando 59- che ravvisa in proposito il carattere integrativo di questa forma di portabilità rispetto a quella di cui all'art. 20 del GDPR- sembra delinearsi un istituto giuridico diverso e più ampio rispetto a quest'ultimo, 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) relativi ai dati inferiti dallo stesso titolare del trattamento (quale, ad esempio ,un profilo utente realizzato mediante analisi di dati grezzi).

Sul punto, il Garante europeo con i pareri 1 e 2/2021 e lo stesso Garante italiano in sede interna (audizione in IX Commissione, Camera dei deputati, sugli schemi di regolamento DSA e DMA, 23.6.2021), avevano suggerito di prevedere l'obbligo, per le piattaforme, di garantire l'effettiva anonimizzazione dei dati derivati dall'attività on line, nonché di adottare misure adeguate ad impedire rischi di reidentificazione dei dati derivati degli utenti. Pur in assenza di tale previsione, ad esiti analoghi potrà comunque pervenirsi anche in virtù di un'interpretazione delle norme adottate che valorizzi i principi di minimizzazione e di responsabilizzazione.

I gatekeeper dovranno, inoltre, garantire l'interoperabilità dei servizi di terzi con il loro hardware e software gratuitamente: allo stesso modo, gli utenti dovranno poter avanzare richieste di portabilità dei dati generati su un dispositivo o un'applicazione in via gratuita.

In termini di *enforcement*, il rispetto della protezione dati degli utenti assume un ruolo determinante nell'ambito dell'oggetto del controllo della Commissione. Come rileva il C 72, infatti, la trasparenza delle pratiche di profilazione di cui si avvalgono i gatekeeper (mediante audit indipendente), agevola la contendibilità di questi servizi.

Significativo, in tal senso, l'art. 15, relativo all'obbligo, sancito 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. La trasparenza esercita infatti una pressione esterna sui gatekeeper affinché non rendano la profilazione approfondita dei consumatori una norma del settore, dato che i potenziali concorrenti o le start-up non possono accedere ai dati in una misura e con un'accuratezza analoghe, né su una scala paragonabile. La protezione dati può rappresentare, così, un fattore di vantaggio competitivo.

Le interrelazioni tra protezione dati e attuazione del DMA (la cui autorità di controllo nazionale è AGCM secondo il ddl concorrenza) imporranno, ovviamente, un coordinamento delle sue azioni con il Garante, conformemente alla clausola di salvaguardia sancita dall'art. 18 del ddl concorrenza (AC 1555). L'esigenza di tale coordinamento è, del resto, stata affermata in linea generale dalla Cgue nella sentenza del 4 luglio scorso (C 252/21), secondo cui le prime devono consultare le seconde laddove, nell'ambito di proprie istruttorie, vengano in rilievo profili incidenti sulla protezione dei dati. Come ha ricordato il Garante in sede di audizione al Senato sul ddl concorrenza, la connessione procedimentale così resa possibile è, del resto, tanto più necessaria per evitare il *bis in idem* censurato, rispetto al diritto punitivo in senso convenzionale, dalla Corte stessa e richiamato nei considerando tanto del DMA quanto del DSA.

Il ddl ha tuttavia omesso di coordinare – come sottolineato dal Garante in sede di audizione parlamentare il 5 settembre 2023 in prima lettura - le azioni di Garante e AGCM rispetto ai pp. 10 ultimo periodo e 11 dell'art. 6, relativi all'accesso, che i gatekeepers devono consentire agli utenti commerciali e ai terzi da questi autorizzati, ai dati personali connessi con l'uso effettuato dagli utenti finali, con il loro consenso, in relazione a prodotti o servizi offerti dall'utente commerciale mediante la piattaforma e ai dati, anonimizzati, relativi a ricerche, click e visualizzazioni cui devono poter accedere i motori di ricerca.

Gli obblighi descritti presuppongono, infatti, altrettanti doveri di correttezza nel trattamento dei dati degli utenti finali, il cui rispetto deve poter essere accertato dal Garante. In assenza di una clausola di salvaguardia espressa, si imporrà dunque un'interpretazione sistematica delle norme di adeguamento, coerente con i poteri riservati al Garante dal GDPR.

2.2.Il DSA

Il DSA muove invece dall'esigenza di responsabilizzare le piattaforme per assicurare quella che potremmo definire "c*ybersafety*", intesa come garanzia di un ambiente *on line* sicuro per la tutela dei diritti degli utenti, attraverso una serie di obblighi asimmetrici (differenziati cioè in ragione della natura dell'intermediario on line, che se ascrivibile alle piattaforme o motori di ricerca molto grandi perché con più di 45 milioni di utenti al mese, assume obblighi supplementari).

Si tratta, in particolare[8], di obblighi relativi alla definizione di termini e condizioni, alla predisposizione di meccanismi di notice and action tali da consentire la rimozione di contenuti illeciit e di sistemi interni di decisione dei reclami, alla gestione dei rischi sistemici, alla soggezione ad audit indipendenti, all'istituzione di una specifica funzione aziendale di *compliance*.

Il crinale stretto su cui si muove il Digital Services Act è il mantenimento dell'opzione di fondo sottesa alla direttiva 2000/31, ovvero il regime generale di responsabilità (solo) condizionata del gestore – con il correlativo divieto di monitoraggio generale dei contenuti – coniugato, tuttavia, con una serie di obblighi procedurali e sostanziali espressivi tanto del principio di a*ccountability* quanto del canone di r*esponsibility* .

In un momento di accentuata esigenza di ascrizione alle grandi piattaforme di responsabilità almeno pari alla rilevanza del potere (non solo economico) dalle stesse esercitato, è significativa la scelta della Commissione di non cedere al modello (affermato ad esempio nel caso Bolger[9]) della responsabilità oggettiva della piattaforma per i servizi intermediati o i contenuti diffusi dagli utenti . E questo, pur non rinunciando a una revisione della disciplina in senso maggiormente rigorista (si pensi al principio del *know your business customer*, che impone alle piattaforme di valutare adeguatamente l'affidabilità dei professionisti cui concedono spazi bloccando le società fraudolente che utilizzano i loro servizi per vendere prodotti e contenuti illegali e non sicuri.) analogamente allo statunitense Shop Safe Act 2020, che incentiva le piattaforme a monitorare adeguatamente prodotti e venditori ospitati per garantire ai consumatori informazioni più complete e maggiore trasparenza nell'effettuazione di acquisti on line.

Tali norme sembrano mettere a sistema alcune delle più riuscite soluzioni normative sperimentate a livello nazionale, soprattutto tedesco e francese (dalla distinzione degli obblighi gravanti sulle piattaforme in ragione della loro dimensione espressa dal numero degli utenti, sino al ruolo degli organismi di monitoraggio, pur sempre privati ma assistiti da requisiti stringenti d'indipendenza) e

[8] E con significative assonanze anche rispetto al (draft di) Regolamento europeo sul targeting politico ((COM(2021) 731 final)..

[9] Sentenza del 13 agosto 2020 del Quarto Distretto della Corte d'appello della California. Essa innova rispetto a una giurisprudenza consolidata, espressa ad es, dalla sentenza della US District Court, N.D. California, nel caso Carpenter v.Amazon,com Inc., 2019 WL 1259158, che ha escluso la responsabilità di Amazon da prodotto difettoso pubblicizzato, ritenendola non qualificabile né come venditore né come distributore di questi prodotti. La sentenza Bolger radica, invece, la responsabilità della piattaforma sull'affidamento riposto dagli utenti nella qualità dei prodotti ospitati.

taluni degli istituti-cardine di discipline, quale quella di protezione dati, che intervengono sul settore del digitale.

Si pensi, in tal senso, al criterio del t*argeting* per l'ambito applicativo della disciplina (art.2.1), alla valutazione d'impatto del rischio sistemico connesso alla propria attività, a un'architettura di governance che prevede anche il Comitato europeo dei servizi digitali quale gruppo consultivo indipendente di coordinatori dei servizi digitali, alla figura del *compliance officer* mutuata dal *data protection officer* o alla stessa struttura delle norme sanzionatorie, modulate su cornici edittali ampie ancorate al fatturato dell'impresa[10]).

Rilevanti sul rapporto con la protezione dati sono, in particolare, oltre la generale clausola di salvaguardia ex C 10, il divieto di profilazione fondata su dati particolari (art. 26.3); il divieto di profilazione fondata su dati di minori quali utenti finali (28.2) che non deve essere attuato con misure che impongano raccolte ulteriori di dati per la verifica dell'età dell'utente; 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, non basata sulla profilazione (38); 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 del GDPR (art. 40.8).

L'eventuale violazione di tali obblighi, da parte dei soggetti tenutivi potrebbe almeno in ipotesi determinare un concorso di illeciti ogniqualvolta essa integri anche gli estremi della violazione della disciplina di protezione dati (si pensi, ad esempio, alla profilazione fondata su un trattamento illecito di dati personali, tanto più se appartenenti alle categorie particolari di cui all'art. 9 GDPR). In tal caso pare difficilmente configurabile un concorso apparente di norme o, comunque, l'applicazione del principio di consunzione, se non altro in ragione della diversità dei beni giuridici protetti dalle norme (e dai rispettivi plessi normativi)[11].

Le norme interne di adeguamento (contenute nel "dl Caivano", n. 123 del 2023, conv, mod. l. 159 del 2023) non delineano in maniera netta il confine tra competenze di Agcom quale Digital Service Coordinator e Garante limitatamente alle sue attribuzioni sul trattamento dati, ma si limitano a prevederne la collaborazione, da delineare anche mediante protocolli di intesa.

Rispetto agli obblighi di *notice and action* gravanti sulle piattaforme in caso di segnalazione di contenuti illeciti, l'attuazione del Dsa andrà effettuata, peraltro, tenendo conto degli specifici rimedi previsti dalla l. 71/17 e dall'art. 144-bis dlgs 196/03 e s.m.i., rispettivamente per il cyberbullismo e per il revenge porn, con legittimazione del minore ultraquattordicenne e il sistema di tutela amministrativa e giurisdizionale[12] previsto in generale dalla disciplina privacy.

2.3.Il DGA (cenni)

Infine, 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.

Gli intermediari dei dati sono assistiti da specifici requisiti di neutralità rispetto ai soggetti coinvolti nel flusso di dati e sono tenuti a particolari obblighi di trasparenza e responsiveness. L'adeguamento dell'ordinamento interno a tale normativa è previsto da un'apposita delega legislativa

---

[10] Per un'interessante analisi dei criteri di commisurazione infraedittale delle sanzioni previste dalla disciplina di protezione dati cfr., in particolare, *Cass.,o* rd. 21789/23 su cui, volendo, F. RESTA, *Sanzioni privacy e poteri del giudice: i principi affermati dalla Corte di cassazione, in Giustiziainsieme*

[11] E quindi anche, del resto, *un bis in* idem: per l'affermazione della "doppia barriera" in materia antitrust proprio in ragione della diversità di beni giuridici protetti cfr., in particolare, CGUE, Grande Sezione, 14 febbraio 2012, C-17/10, *Toshiba*, §§ 81-83 e 97.

[12] Con giurisdizione, peraltro, del giudice ordinario (art. 152 d.lgs. 196 del 2003) a fronte, invece, della giurisdizione del g.a. prevista nel caso di impugnazione dei provvedimenti Agcom

all'esame della Commissione XIV della Camera dei deputati in prima lettura (ddl di delegazione europea, AC 1342, art. 13), ove pure si 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"*.

Tale ultimo criterio di delega coglie un'esigenza di adeguamento e razionalizzazione sistematica delle norme introdotte con una disciplina trasversale ai vari settori quale, appunto, quella di protezione dati.

3. Osservazioni conclusive

Complessivamente, il pacchetto digitale compie una scelta importante nell'*an* (delineare un modello di innovazione tecnologica non limitato all'autoregolazione capitalistica), per garantire un governo sostenibile del digitale. Ma la scelta è importante anche nel q*uomodo*, nella misura in cui introduce una cornice regolatoria essenziale per l'economia delle piattaforme, fondata su alcuni obblighi, di trasparenza, collaborazione e gestione dei contenuti ospitati, nella logica della *corporate compliance*, idonei a rafforzare le garanzie tanto in favore degli utenti quanto della sostenibilità della *data economy*.

Così, se il DMA onera le piattaforme di alcuni adempimenti funzionali a evitare restrizioni nell'accesso al mercato, il DSA introduce vincoli importanti all'esercizio del potere di azione sui contenuti e, quindi, anche sulla libertà di espressione, rendendolo più trasparente e sindacabile e, per ciò, non (o, se non altro, meno) arbitrario.

Di contro, il DGA intende promuovere, anche grazie a obblighi di *compliance* dei principali soggetti coinvolti, la circolazione dei dati (personali e non), a fini di promozione dell'iniziativa economica, della competitività del sistema economico europeo, ma anche e soprattutto a fini solidaristici e di utilità sociale.

Ed è proprio il paradigma della *complian*ce a rappresentare l'elemento comune a queste normative, comprensive anche di soluzioni innovative quali quelle di natura negoziale sul terreno dell'e*nforcemen*t, in parte sperimentate sul terreno della *corporate criminal liability*, 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. 45 DSA e impegni nel DMA, art.25), tali da valorizzare il ravvedimento operoso.

Anche la governance risente di questo doppio livello di controllo, nazionale ed europeo, che tuttavia se più centralistico nel DMA, si fa più reticolare nel DSA e, in parte, anche nel DGA.

Le soluzioni proposte rispondono alle caratteristiche che distinguono i nuovi poteri privati dal paradigma tradizionale (weberiano) del potere[13]: formale, operante in una dimensione causale, verticale e coercitiva.

In questo senso, gli obblighi di trasparenza e la *due diligenc*e fondata sulla valutazione e prevenzione del rischio assolvono una funzione compensativa e remediale rispetto alla natura non formale di questi poteri; l'articolazione[14] delle tutele, amministrativa ma anche giurisdizionale (di

[13] Vds. G. RESTA, voce *Poteri privati e regolazione*, in *Enciclopedia del diritto*, I tematici, vol. V: Potere e costituzione, Giuffrè, Milano, 2023, pp. 1026-1027

[14] Anche innovativa, considerando ad es. la previsione di azioni rappresentative nel DMA (art. 42) a fronte di violazioni da parte dei gatekeeper che ledano interessi collettivi dei consumatori; la possibilità di ricorso alla tutela amministrativa anche in forma collettiva secondo quanto previsto, in particolare, dal DGA (art. 27) e, sia pur in modo diverso, dal DSA (art. 53),)

natura anche risarcitoria nel DSA, centrale sul lato del *private enforcement*) così come, nel DGA, il supporto offerto all'interessato da soggetti collettivi quali le organizzazioni per l'altruismo dei dati rafforzano le garanzie del singolo nell'ambito di una relazione inevitabilmente asimmetrica quale quella con le piattaforme.

Se, dunque, il disegno europeo è complessivamente ambizioso e lungimirante, tuttavia la rilevanza delle scelte regolatorie imporrà un adeguato coordinamento, in primo luogo in sede interna, tra le discipline in vario modo intersecantesi nel settore: a partire, appunto, dalla 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 (rilevante in termini amministrativi, civili o finanche penali) secondo la disciplina di protezione dei dati personali. 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.

Le norme di adeguamento adottate (per il DSA) o in fase di esame parlamentare (per il DMA e il DGA) non tracciano un confine netto tra le competenze delle autorità coinvolte ma, certamente, forniscono gli elementi per consentire – anche attraverso protocolli d'intesa espressamente previsti, ad esempio, dal d.l. "Caivano" per il DSA- un'applicazione armonizzata e sostenibile delle norme.