APPROFONDIMENTO CIVILE

Diritto digitale europeo: enforcement digitale nell'EU tra GDPR, DSA e AI Act per una governance efficace

Data pubblicazione: 04/09/2025

Autore: Avv. Roberto Francesco Iannone

Categoria: Civile

Contenuto

Negli ultimi anni l'Unione Europea ha adottato un insieme di **atti normativi strategici nel settore digitale**, che segnano un cambio di paradigma nella regolazione delle tecnologie:

- il **Regolamento generale sulla protezione dei dati (GDPR)**;
- il **Digital Services Act (DSA)**;
- l'**Artificial Intelligence Act (AI Act)**.

Queste norme hanno **rafforzato i diritti dei cittadini online** e, al tempo stesso, ampliato i poteri delle autorità pubbliche in materia di vigilanza e controllo. Tuttavia, mentre l'attenzione politica e accademica si è concentrata prevalentemente sul contenuto delle nuove disposizioni, meno spazio è stato dedicato al tema centrale dell'**enforcement**, ossia alle modalità concrete con cui queste regole trovano applicazione.

Enforcement frammentato: il cuore del problema

Il sistema regolatorio europeo del digitale presenta oggi un **mosaico complesso e frammentato**. Le piattaforme online si trovano a operare in un contesto in cui si intrecciano:

- **obblighi di moderazione dei contenuti** (DSA);
- **regole sulla profilazione e tutela della privacy** (GDPR);
- **norme sull'intelligenza artificiale** (AI Act);
- **disposizioni settoriali su comunicazione audiovisiva, cybersicurezza e concorrenza**.

Ne deriva che un singolo comportamento di una piattaforma può rientrare **simultaneamente**

nell’ambito applicativo di più normative, richiamando competenze di autorità diverse.

Moltiplicazione delle autorità: tra sovrapposizione e conflitti di competenza

L’architettura europea prevede un enforcement distribuito tra:

- la **Commissione europea**;
- le **autorità nazionali garanti della privacy**;
- le **autorità di regolazione dei media**;
- le **autorità antitrust**;
- le **agenzie nazionali ed europee per la cybersicurezza**.

Questa moltiplicazione istituzionale, pur teoricamente arricchente, genera rischi di **disallineamento decisionale** e di **conflitti di competenza**. Un esempio significativo è rappresentato dal **caso Meta Platforms**, in cui la **Corte di giustizia dell’Unione europea** è intervenuta per chiarire i rapporti tra autorità antitrust e autorità per la protezione dei dati personali.

Frammentazione orizzontale e verticale

La frammentazione si sviluppa:

- **orizzontalmente**, tra autorità con competenze parallele (ad es. Garante Privacy, AGCOM e Antitrust in Italia);
- **verticalmente**, nei rapporti tra istituzioni europee e autorità nazionali.

Nei casi transfrontalieri, la situazione si complica ulteriormente: interpretazioni divergenti tra Stati membri aumentano l’incertezza giuridica per imprese e cittadini.

Governance digitale europea: rischi e prospettive

L’Unione Europea ha costruito una solida impalcatura normativa che mira a tutelare **diritti fondamentali, concorrenza leale e valori democratici** nello spazio digitale. Tuttavia, senza un **rafforzamento del coordinamento tra autorità**, questa architettura rischia di trasformarsi in una struttura incompiuta. Non è tanto la **semplificazione normativa** a rappresentare la priorità, quanto piuttosto la definizione di **meccanismi efficaci di cooperazione e coordinamento istituzionale**. Solo così sarà possibile garantire **certezza del diritto** e **coerenza applicativa**, elementi imprescindibili per imprese, utenti e investitori.

Conclusioni

Il **futuro della governance digitale europea** dipenderà dalla capacità di superare le attuali criticità dell’enforcement.

A cura dell'avv. Fabrizio Valerio Bonanni Saraceno