



OSSERVATORIO  
TMT·DATA PROTECTION

*di Morri Rossetti*

# Monthly Roundup

Ottobre 2023

## MONTHLY ROUNDUP

*Ottobre 2023*

I principali aggiornamenti in materia di TMT & Data Protection del mese

---

### NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

#### Provvedimenti del Garante Privacy

- Sanità: decalogo del Garante Privacy sull'uso dell'intelligenza artificiale [\[Link\]](#)
- Lavoro: il dipendente ha diritto di accedere ai dati sulla geolocalizzazione [\[Link\]](#)
- Sms promozionali senza consenso: sanzionato un ateneo telematico [\[Link\]](#)
- Il Garante Privacy multa una società energetica per 10 milioni di euro per l'attivazione di contratti non richiesti con dati inesatti e non aggiornati [\[Link\]](#)

#### Provvedimenti EU

- New EU rules needed to make digital platforms less addictive [\[Link\]](#)
- EDPS' Final Recommendations on the AI Act [\[Link\]](#)
- EDPS Opinion 42/2023 on the Proposal for two Directives on AI liability rules [\[Link\]](#)
- Digital euro: ensuring the highest data protection and privacy standards [\[Link\]](#)

### PRINCIPALI AGGIORNAMENTI

- Data Governance Act: vantaggi e profili aperti
- Orientarsi tra le norme sulla responsabilità dell'IA: Le istituzioni europee si focalizzano sulla tutela dei consumatori
- Influencer Marketing: nuove regole dell'AGCOM
- Possible Simplifications to Data Transfers Outside of China - CAC proposes new draft Regulations: What Potential Impact for Companies?



## Data Governance Act: vantaggi e profili aperti

Il 24 settembre 2023 ha segnato l'avvento di un nuovo capitolo nella storia della condivisione dei dati, grazie all'entrata in vigore del Regolamento UE 2022/868, conosciuto come "Data Governance Act" ("DGA" o il "Regolamento"). Il DGA è stato pensato per aumentare la fiducia nella condivisione dei dati, superare gli ostacoli tecnici e creare spazi comuni europei di dati, coinvolgendo attori privati e pubblici, in settori cruciali quali la sanità, l'ambiente, l'energia, l'agricoltura, la mobilità, la finanza, l'industria manifatturiera, la pubblica amministrazione e le competenze.

L'obiettivo è favorire la libera circolazione dei dati a livello internazionale, adottando i principi FAIR (Facili da trovare, Accessibili, Interoperabili e Riutilizzabili), garantendo al tempo stesso un alto livello di cybersicurezza.

Come affermato dalla Commissione europea, per lo sviluppo di un mercato unico che sia equamente concorrenziale, è necessario che *"le imprese competano sulla qualità dei servizi e non sulla quantità dei dati che controllano"*.

Il DGA offre, quindi, l'opportunità per tutti coloro che vogliono accedere alla data economy, di utilizzare dati personali e non, che legittimamente detengono, e costituisce un pilastro fondamentale della strategia europea per i dati.

Il DGA è, inoltre, strettamente correlato e connesso con la proposta di regolamento sulle norme armonizzate in materia di accesso equo ai dati e uso dei dati, noto anche come "Data Act" (il cui iter di approvazione non è ancora tuttavia terminato<sup>1</sup>).

Mentre il DGA regola i processi e le infrastrutture giuridiche che agevolano la condivisione dei dati tra imprese, individui e il settore pubblico promuovendo e rafforzando i meccanismi di data sharing, il Data Act è orientato, invece, alla creazione di valore attraverso i dati e stabilisce le condizioni in cui questo processo può avvenire.

### I Pilastri del DGA: Riutilizzo, Intermediazione e Altruismo dei Dati

Il DGA è strutturato su tre pilastri fondamentali:

1. **Riutilizzo dei dati pubblici:** il Regolamento stabilisce condizioni chiare per il riutilizzo dei dati detenuti dagli enti pubblici. Questi dati possono ora essere accessibili a enti pubblici e privati, purché vengano adottate specifiche tecniche e misure di protezione e svolte specifiche valutazioni che consentono di rendere disponibili i dati nel rispetto delle normative vigenti.

L'articolo 5 del DGA detta le condizioni per consentire il riutilizzo garantendo la tutela della natura protetta dei dati: quando si tratta di dati personali, i dati dovranno essere anonimizzati in modo da impedire o da non consentire più l'identificazione dell'interessato; nel caso di informazioni commerciali riservate, compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale, potranno essere modificati, aggregati o trattati mediante qualsiasi altro metodo di controllo della divulgazione. L'accesso e il riutilizzo dovranno avvenire altresì all'interno di un ambiente di trattamento sicuro e

---

<sup>1</sup> A seguito, infatti, dell'approvazione del testo di proposta da parte della Commissione il 23 febbraio 2022, il 28 giugno 2023, il Parlamento europeo e il Consiglio dell'UE hanno

raggiunto un accordo politico sul Data Act; la legge è ora soggetta ad approvazione formale e, una volta adottata, entrerà in vigore 20 giorni dopo la pubblicazione della Gazzetta ufficiale, diventando applicabile dopo 20 mesi.

controllato nel rispetto di rigorose norme di sicurezza.

Gli enti pubblici depositari dei dataset hanno, inoltre, la facoltà di valorizzare il patrimonio informativo imponendo delle tariffe, tariffe ridotte ed esenzioni al pagamento delle tariffe per l'accesso e l'utilizzo dei dati, a condizione che le stesse siano trasparenti, eque, competitive e che consentano l'accesso alle PMI, le start-up e le istituzioni di ricerca scientifica.

L'iter per l'ottenimento dell'accesso e del riutilizzo dei dati risulta semplificato dal DGA attraverso la creazione di **sportelli unici responsabili della ricezione di richieste di informazioni e di riutilizzo**, per conto degli enti pubblici competenti.

Da ultimo, la facoltà di riutilizzo, da parte di soggetti privati, dei dati detenuti dagli enti pubblici e messi a disposizione da questi ultimi alle condizioni dettate dal DGA, consente alle imprese di accedere a dati anonimizzati o aggregati, preservando la privacy dei cittadini e la tutela dei diritti di proprietà intellettuale, determinando, così, una riduzione delle responsabilità e delle procedure necessarie per gestire i dati in conformità con le leggi applicabili e un maggior controllo sui dati ottenuti e trattati.

**2. Servizi di Intermediazione:** il secondo pilastro è rappresentato dai **fornitori dei servizi di intermediazione dei dati**. Gli intermediari dei dati giocheranno un ruolo chiave nel facilitare la condivisione volontaria dei dati tra imprese, fungendo da ponti affidabili, collegando titolari dei dati, utenti dei dati e interessati, consentendo un flusso più agevole delle informazioni. Il ruolo di intermediario può essere assunto dai soggetti che svolgono le attività di cui all'articolo 10 del DGA, risultando esclusi, in generale, *"i servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per*

*l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati"*.

A titolo di esempio, quale fornitore di servizi di intermediazione dei dati, la Commissione menziona Deutsche Telekom, il quale assume il ruolo di fiduciario neutrale e che, tramite il suo Data Intelligence Hub, offre un mercato dei dati in cui le aziende possono gestire, fornire e monetizzare in modo sicuro informazioni di buona qualità, ad esempio i dati di produzione, al fine di ottimizzare i processi o l'intera catena del valore, garantendo la sovranità dei dati attraverso la gestione decentralizzata dei dati. Altro esempio è Dawex, azienda francese che si descrive come un "mercato globale di dati" che non acquista né vende dati, ma riunisce aziende interessate a monetizzare e riutilizzare i dati e promuove la trasparenza tra fornitori di dati e utenti, garantendo che comunichino e conducano la transazione direttamente sulla propria piattaforma, anche attraverso la creazione automatica di modelli contrattuali.

Per poter essere qualificati come "intermediari di dati", i soggetti interessati dovranno essere sottoposti alla procedura di valutazione e notifica da parte delle competenti autorità nazionali, nel rispetto delle condizioni stabilite dall'articolo 12 del DGA.

La normativa in esame prevede, quindi, che gli intermediari dei dati fungano da organizzatori affidabili della condivisione o della messa in comune dei dati all'interno degli spazi comuni europei di dati, offrendo servizi che collegano i diversi soggetti coinvolti (titolari dei dati, utenti dei dati e interessati – come individuati dalle definizioni del DGA) e migliorando le possibilità di accesso e riutilizzo dei dati. I servizi contemplati prevedono l'instaurazione, attraverso strumenti tecnici, giuridici o di altro tipo, di rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di

titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche per l'esercizio dei diritti degli interessati in relazione ai dati personali.

**3. Altruismo dei Dati:** il terzo pilastro su cui si basa il Regolamento contribuisce, infine, alla creazione di pool di dati messi a disposizione sulla base dell'altruismo dei dati ovvero, l'utilizzo di dati per obiettivi di interesse generale messi a disposizione su base volontaria dagli interessati stessi, sulla base del loro consenso informato. Tali obiettivi di interesse generale comprendono l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche europee, il miglioramento della fornitura dei servizi pubblici, o delle politiche pubbliche. Anche il sostegno alla ricerca scientifica dovrebbe essere considerato un obiettivo di interesse generale.

Gli articoli da 16 a 25 del DGA disciplinano le condizioni per facilitare l'altruismo dei dati da parte degli Stati membri. Il DGA, in particolare, istituisce le "Organizzazioni per l'altruismo dei dati", inserite in un registro pubblico e finalizzate alla creazione di repository di dati che fungono da intermediari tra i titolari dei dati e coloro che li utilizzano.

L'obiettivo del DGA è quello di creare organizzazioni conformi ai requisiti del Regolamento stesso che possano infondere fiducia quanto al fatto che i dati messi a disposizione a fini altruistici servano un obiettivo di interesse generale.

A tal fine, le Organizzazioni devono essere senza scopo di lucro, devono rispettare determinati obblighi di trasparenza e adottare tutele specifiche volte a proteggere i diritti e gli interessi degli interessati e delle imprese. Un modulo europeo di consenso all'altruismo dei dati, ovvero un documento personalizzabile, anche in base al settore o all'obiettivo del trattamento, permetterà

di ottenere (e revocare) il consenso ai sensi del Regolamento (UE) 2016/679 da parte degli interessati, in un formato standard valido in tutti gli Stati Membri.

Ulteriori tutele dovrebbero comprendere la possibilità di trattare i dati pertinenti in un ambiente di trattamento sicuro gestito dalle organizzazioni per l'altruismo dei dati riconosciute, meccanismi di sorveglianza quali consigli o comitati etici, compresi i rappresentanti della società civile, per garantire che il titolare del trattamento mantenga standard elevati di etica scientifica e di protezione dei diritti fondamentali, strumenti tecnici efficaci e comunicati con chiarezza per revocare o modificare il consenso in qualsiasi momento, sulla base degli obblighi di informazione dei responsabili del trattamento dei dati a norma del Regolamento (UE) 2016/679, nonché strumenti che consentano agli interessati di essere informati circa l'utilizzo dei dati che hanno messo a disposizione.

### **Quali sono i vantaggi?**

Il DGA mira a creare e a regolamentare sistemi e meccanismi funzionali a rendere disponibili più dati e a ottenere una maggior libertà nella condivisione di dati, riconoscendo, quale presupposto fondamentale, le potenzialità economiche e sociali derivanti da un corretto ed efficiente uso dei dati.

La Commissione europea ha fornito già esempi pratici sugli effettivi obiettivi che possono essere perseguiti grazie al nuovo framework introdotto dal DGA:

- lo sviluppo di prodotti e servizi innovativi da parte delle aziende tali da rendere molti settori dell'economia più efficienti e sostenibili;
- l'utilizzo dei dati per la formazione dei sistemi di intelligenza artificiale nel

rispetto delle previsioni normative applicabili nell'Unione europea;

- lo sviluppo di politiche migliori nel settore pubblico, portando a una governance più trasparente e a servizi pubblici più efficienti, grazie al maggior numero di dati disponibili.

### **Quali sono i dubbi interpretativi e le principali problematiche?**

Il DGA è una normativa intersettoriale che tocca profili e ambiti già ampiamente regolati da diverse altre normative specifiche, tra le quali, ad esempio: il Regolamento UE 2016/679 in materia di protezione dei dati personali ("**GDPR**"); il Regolamento UE 2018/1807 sui dati non-personali, la normativa sugli Open Data della Pubblica Amministrazione (quali, il recente Regolamento di esecuzione 2023/138 e la Direttiva 2019/1024), nonché la normativa per la tutela giuridica delle banche dati (i.e. la Direttiva 96/9/CE).

Se da una parte, il DGA lascia impregiudicati tali normative così come ogni altra disciplina settoriale dell'Unione che regolamenta l'accesso ai dati e il loro riutilizzo, dall'altro, la coesistenza con altre normative europee e nazionali, come il GDPR e le leggi nazionali sulla protezione dei dati che disciplinano profili comuni potrebbe dare adito a sovrapposizioni o discrepanze tra normative, generando confusione per gli operatori chiamati ad applicarle e incertezza.

In materia di protezione dei dati personali, ad esempio, sono già stati sollevati numerosi dubbi interpretativi circa le previsioni del DGA, in primis dall'EDPB e dall'EDPS che con il [Parere congiunto 03/2021](#) *"sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati"*, avevano sottolineato l'importanza primaria di *"evitare nel testo legislativo della proposta eventuali incoerenze e possibili conflitti con il GDPR"*.

Mentre alcuni dei dubbi espressi dalle citate Autorità sono stati chiariti, alcune delle incongruenze o incertezze rimangono ancora irrisolte (si pensi, ad esempio, ad alcune definizioni contenute all'interno del DGA, come quella di *"titolare dei dati"*, che potrebbero risultare ambigue o troppo ampie, creando incertezze sulle persone o entità che ricadono effettivamente nell'ambito di applicazione del DGA; o ai meccanismi volti ad assicurare l'implementazione del principio di *"altruismo dei dati"* che potrebbero apparire ancora poco chiari, causando problemi nell'attuazione pratica; così come al ruolo degli Intermediari dei dati rispetto ai quali andrebbero forniti maggiori dettagli su come queste entità dovrebbero operare e interagire con i titolari dei dati e gli utenti dei dati).

### **Concludendo**

Se da una parte si auspica che una maggiore chiarezza e certezza venga fornita dalle competenti autorità nell'ambito dell'applicazione pratica del nuovo regime introdotto dal DGA, dall'altra si può tuttavia affermare che il rispetto della normativa in materia di protezione dei dati personali da parte di tutti i soggetti coinvolti nel DGA assumerà sempre più maggiore importanza e costituirà, quindi, un presupposto necessario per poter trarre vantaggio dalle previsioni del DGA. Le misure tecniche e organizzative richieste dal GDPR, tra cui le misure di pseudonimizzazione e/o anonimizzazione così come le modalità per la raccolta e gestione dei consensi secondo i parametri indicati dall'art. 7 GDPR diverranno elementi essenziali per gli obiettivi di libera circolazione dei dati garantendo il rispetto delle previsioni in materia nonché il controllo da parte di interessati e titolari sui dati che li riguardano.

Le imprese che si sono già adoperate per conformare le proprie attività alle previsioni del GDPR e delle altre disposizioni vigenti in materia di protezione dei dati personali saranno quindi in

grado di prepararsi più facilmente e in anticipo al DGA e di sfruttare il potenziale di questa nuova normativa.

\* \* \*

### **Orientarsi tra le norme sulla responsabilità dell'IA: le istituzioni europee si focalizzano sulla tutela dei consumatori**



Il 28 settembre 2022, la Commissione europea ha adottato due proposte mirate ad armonizzare le normative nazionali riguardanti la responsabilità nel campo dell'intelligenza artificiale ("IA"). Queste proposte affrontano le sfide legate ai sistemi di IA per quanto riguarda la gestione delle richieste di risarcimento in caso di danni causati da prodotti e servizi che utilizzano sistemi di IA.

Le due proposte sono:

- la proposta di direttiva sulla responsabilità per danno da prodotti difettosi, la quale si concentra sulla responsabilità dei produttori per i prodotti difettosi. La proposta mira a modernizzare il quadro giuridico attuale includendo i software e i file per la fabbricazione digitale nella definizione di "prodotto". Inoltre, chiarisce che anche i servizi digitali integrati in un prodotto o interconnessi ad esso sono considerati componenti del prodotto stesso;
- la proposta di direttiva relativa all'adeguamento delle norme in materia

di responsabilità civile extracontrattuale all'intelligenza artificiale (c.d. direttiva sulla responsabilità da IA), la quale mira ad adattare le norme nazionali in materia di responsabilità civile, in considerazione delle caratteristiche specifiche di determinati sistemi di IA come l'opacità, il comportamento autonomo e la complessità che possono rendere eccessivamente oneroso per il danneggiato identificare i soggetti responsabili, nonché soddisfare l'onere della prova.

Tali proposte fanno parte della strategia digitale dell'UE, che mira a regolamentare l'IA al fine di promuovere lo sviluppo responsabile ed efficace delle tecnologie di IA nell'Unione Europea. La strategia digitale include anche la proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (il c.d. "AI Act").

### **Parere dell'European Data Protection Supervisor ("EDPS")**

Ai sensi dell'art. 57 del Regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione Europea e sulla libera circolazione di tali dati, l'EDPS ha il compito di fornire, di propria iniziativa o su richiesta, consulenza a tutte le istituzioni e organi dell'Unione Europea in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche per quanto riguarda il trattamento dei dati personali.

Conformemente, l'EDPS ha accolto favorevolmente le due proposte di direttiva, con la pubblicazione del Parere 42/2023. Secondo l'EDPS, tali proposte riusciranno a garantire ai soggetti che subiscono danni scaturenti da

sistemi coinvolgenti l'IA lo stesso livello di tutela dei soggetti danneggiati in altre circostanze.

Nello specifico, la direttiva sulla responsabilità per danno da prodotti difettosi mira a garantire che il sistema a livello dell'UE per il risarcimento delle persone che subiscono lesioni fisiche o danni patrimoniali dovuti a prodotti difettosi sia aggiornato all'attuale evoluzione digitale e, in particolare, alla diffusione di sistemi di IA e di *smart product*.

Inoltre, la proposta di direttiva sulla responsabilità da IA mira a adattare in modo mirato alcune norme nazionali in materia di responsabilità civile al fine di poter gestire le azioni di responsabilità per danni causati da prodotti e servizi basati sull'IA o, comunque, a situazioni in cui sono coinvolti sistemi di IA. L'EDPS ha riconosciuto che le caratteristiche specifiche dell'IA, tra cui la complessità, l'autonomia e l'opacità, possono creare ostacoli significativi per i soggetti danneggiati che intendono chiedere il risarcimento dei danni.

Secondo il Parere, pubblicato l'11 ottobre 2023, l'EDPS raccomanda quanto segue:

- posto che l'AI Act si applica alle istituzioni, gli uffici, gli organi e le agenzie dell'UE quando agiscono come fornitori o utenti di sistemi di IA, dovrebbe essere garantito un livello di tutela equivalente per i soggetti che hanno subito danni causati dai sistemi di IA prodotti e/o utilizzati dalle istituzioni, gli organi e le agenzie dell'UE, analogamente alle persone danneggiate dai sistemi di IA prodotti e/o utilizzati da soggetti privati o autorità nazionali. Allo stato attuale risulta che le due proposte non si applichino alle istituzioni dell'UE;
- assicurarsi che le proposte non siano in contrasto con la normativa europea sulla protezione dei dati e statuire

espressamente che le due proposte non sostituiscono la normativa europea in materia di protezione dei dati personali;

- estendere le garanzie procedurali delineate negli artt. 3 e 4 della direttiva sulla responsabilità da IA, che prevedono la divulgazione degli elementi di prova, la presunzione relativa di non conformità e la presunzione relativa del nesso di causalità in caso di colpa, a tutti i casi di danni causati da un sistema di IA, indipendentemente dalla loro classificazione come sistemi di IA ad alto rischio o non ad alto rischio;
- assicurarsi che le informazioni divulgate ai sensi dell'art. 3 della direttiva sulla responsabilità da IA siano accompagnate da spiegazioni chiare e comprensibili;
- valutare ulteriori misure volte a ridurre ulteriormente l'onere della prova in capo ai soggetti danneggiati dai sistemi di IA.

\* \* \*



## **Influencer Marketing: nuove regole dell'AGCOM**

### **Introduzione**

Negli ultimi anni, l'attività imprenditoriale degli influencer si è sempre più intensificata, grazie all'importanza e alla pervasività dei social media e del mondo digitale nelle esperienze dei consumatori. Nel solo 2022, questo fenomeno ha creato un mercato pari a circa 308 milioni di euro in Italia e di 16,4 miliardi nel mondo.



## Ma chi sono esattamente gli influencer? e quali regole devono rispettare nell'ambito della propria attività?

Gli influencer (conosciuti, nel linguaggio comune, anche come "vlogger", "streamer", "creator", "uploder", etc.) sono individui che **creano, producono e diffondono contenuti audiovisivi** (di cui esercitano la responsabilità editoriale) **tramite l'utilizzo di piattaforme per la condivisione di video o di social media** al fine di influenzare il comportamento di acquisto dei consumatori. Sempre più spesso, i *brand* collaborano con gli influencer per aumentare la visibilità del marchio e, di conseguenza, incrementare le proprie vendite.

Dato che l'Italia rappresenta, nel mercato europeo, il paese con la maggiore percentuale di influencer, l'Autorità per le garanzie nella comunicazione ("Autorità" o "AGCOM") ha ritenuto essenziale affrontare il tema della loro regolamentazione, anche al fine di favorire una maggiore trasparenza e consapevolezza tra tutti gli interessati.

Dopo le recenti iniziative dell'Istituto dell'Autodisciplina Pubblicitaria ("IAP") volte a delineare nuove regole per un corretto e trasparente esercizio del digital advertising, l'AGCOM, con la Delibera n. 178/23/CONS (la "**Delibera**"), ha aperto quindi una consultazione pubblica della durata di 60 giorni - terminata lo scorso 21 settembre 2023 -, per valutare l'applicabilità delle disposizioni del decreto legislativo 208/2021 (noto come "*Testo Unico dei servizi di media audiovisivi*" o "**TUSMA**") all'attività degli influencer.

Lo scopo principale della Delibera dell'Autorità è quello di elaborare apposite Linee Guida al fine di evidenziare alla comunità d'interesse le regole del TUSMA applicabili anche agli influencer e i casi in cui la loro attività sia assimilabile alla fornitura di servizi di media audiovisivi.

## Quadro normativo applicabile

La Direttiva (UE) 2018/1808 ("**Direttiva SMAV**"), recepita in Italia con il TUSMA, ha aggiornato il precedente quadro regolatorio europeo del settore dei servizi media audiovisivi (i.e. Direttiva (UE) 2010/13), includendo anche le attività svolte attraverso i social media. Ciò si è reso necessario a causa dell'evoluzione delle realtà del mercato dei servizi media audiovisivi, che include la diffusione di attività attraverso i social media, che gradualmente ha concorso con i tradizionali servizi media audiovisivi in termini di audience, ricavi e influenza sull'opinione degli utenti.

Come chiarito, infatti, dal Considerando 4 della Direttiva SMAV, oltre ai contenuti audiovisivi forniti attraverso piattaforme per la condivisione di video, anche i servizi social media sono diventati un importante mezzo per condividere informazioni, intrattenere e istruire, dando anche accesso a programmi e video generati dagli utenti ("**Servizi Social Media**") e, per tale ragione, il legislatore europeo ha ritenuto necessario includerli nell'ambito di applicazione della Direttiva SMAV.

Questi servizi non solo competono con i servizi di media audiovisivi tradizionali, ma facilitano anche il processo di influenzabilità degli utenti a fronte di pareri di altri utenti (come, ad esempio, gli influencer). Per tale ragione, l'inclusione dei Servizi Social Media nell'ambito di applicazione della Direttiva SMAV è sembrata funzionale, tra l'altro, anche alla protezione dei minori da contenuti nocivi e di tutti i cittadini dall'istigazione all'odio, alla violenza e al terrorismo.

Inoltre, facendo riferimento anche al Considerando 3 della Direttiva SMAV, ai sensi del quale "[...] *I canali o altri servizi audiovisivi sotto la responsabilità editoriale di un fornitore possono essi stessi costituire servizi di media audiovisivi, anche se sono offerti su una piattaforma per la*

condivisione di video caratterizzata dall'assenza di responsabilità editoriale. In questi casi spetterà ai fornitori la responsabilità editoriale di conformarsi alla direttiva 2010/13/UE".

Dall'esame dei Considerando richiamati si comprende che l'attività svolta dagli *influencer* debba rientrare nell'ambito della fornitura di servizi di media audiovisivi, laddove la stessa soddisfi i requisiti fissati dalla Direttiva SMAV, così come recepiti, a livello nazionale, dal TUSMA.

### **La posizione dell'AGCOM e la proposta di specifiche Linee Guida**

Nella propria Delibera, l'AGCOM ritiene che i soggetti qualificabili come "influencer", nell'esercizio delle attività di creazione, selezione e organizzazione dei contenuti che diffondono, possono essere considerati fornitori di servizi di media audiovisivi <sup>2</sup> a richiesta sotto la giurisdizione nazionale, ai sensi dell'art. 3, comma 1, lett. a), b) e q), del TUSMA. In quanto tali, sono direttamente responsabili del rispetto delle disposizioni ivi contenute, a condizione che siano soddisfatti i seguenti requisiti:

- il servizio offerto costituisce attività economica;
- lo scopo principale del servizio offerto è la fornitura di contenuti, creati o selezionati dall'influencer, che informano, intrattengono o istruiscono;
- l'influencer ha la responsabilità editoriale, la quale include il controllo effettivo sulla creazione, selezione e organizzazione dei contenuti;
- il servizio è accessibile al grande pubblico, raggiunge un numero significativo di utenti sul territorio italiano, ha un impatto rilevante su una porzione significativa di pubblico ed è

alimentato con continuità da nuovi contenuti;

- i contenuti sono trasmessi tramite un servizio di piattaforma di condivisione di video o di social media;
- il servizio consente la visualizzazione dei contenuti su richiesta dell'utente;
- il servizio è prestato nel rispetto dell'ordinamento giuridico nazionale ed è caratterizzato da un legame stabile ed effettivo con l'economia italiana;
- i contenuti sono offerti tramite l'utilizzo della lingua italiana o sono esplicitamente rivolti agli utenti sul territorio italiano.

Tuttavia, stante la peculiare natura degli influencer e dei servizi audiovisivi dagli stessi erogati, l'AGCOM ha ritenuto opportuno diversificare gli influencer in due categorie, prevedendo l'applicazione del TUSMA a seconda della natura dell'attività da questi prestata e la sovrapposibilità della stessa con la fornitura di un servizio di media audiovisivo.

#### **Prima categoria di influencer**

Il primo gruppo riguarda i soggetti che propongono contenuti audiovisivi in modo continuo con una modalità di offerta e organizzazione degli stessi tale da renderli sovrapposibili a un catalogo di un servizio di media on-demand (ad esempio, i canali Youtube).

Per questi soggetti, l'Autorità ritiene opportuna l'applicazione della totalità degli obblighi previsti dal TUSMA, ivi inclusi, a titolo esemplificativo, l'iscrizione al ROC, la disciplina in materie di opere europee e indipendenti, la SCIA (segnalazione certificata di inizio attività).

<sup>2</sup> Ai sensi dell'art. 3(1)(d) del TUSMA: "la persona fisica o giuridica cui è riconducibile la responsabilità editoriale della

scelta del contenuto audiovisivo del servizio di media audiovisivo e che ne determina le modalità di organizzazione [...]"

## Seconda categoria di influencer

Il secondo gruppo comprende invece i soggetti che operano in maniera meno continuativa e strutturata, ai quali, di contro, sempre a parere dell'Autorità, non appare giustificata l'applicazione nella sua interezza del regime giuridico previsto per i servizi di media audiovisivi a richiesta.

Sulla base di questa distinzione, l'AGCOM si è posta l'obiettivo di elaborare specifiche Linee-guida volte ad evidenziare quali disposizioni del TUSMA siano applicabili anche agli influencer, a seconda che rientrino in una categoria o nell'altra, in modo da assicurare un livello minimo di tutela anche da parte dei soggetti rientranti nella seconda categoria sopra menzionata.

Infine, l'Autorità, a prescindere dalle specificità dell'attività svolta dall'influencer, ritiene che tutti gli influencer debbano rispettare, in quanto compatibili, le norme a tutela dei diritti fondamentali della persona, dei minori e dei valori dello sport, oltre a quelle in tema di comunicazioni commerciali, televendite, sponsorizzazioni e inserimento dei prodotti, adottando misure operative quali, ad esempio, l'inserimento di hashtag o di diciture "adv", nonché il "tag" che rimanda al partner pubblicitario.

## Conclusioni

La consultazione pubblica, conclusasi il 21 settembre 2023, è stata sicuramente uno strumento efficace per acquisire i contributi di tutti i soggetti del mercato interessati e garantire il rispetto delle disposizioni del TUSMA, da parte degli influencer.

Detto ciò, l'AGCOM ritiene che lo strumento delle Linee-guida sia il modo migliore per regolamentare le attività degli influencer, applicando le normative esistenti in modo compatibile con il contesto degli influencer.

Per maggiori approfondimenti sul tema, si attende quindi la pubblicazione del testo delle Linee-guida e, nel frattempo, si raccomanda a tutti i soggetti interessati di impostare il proprio business tenendo a mente le indicazioni dell'AGCOM.

\* \* \*



## Possible Simplifications to Data Transfers Outside of China - CAC proposes new draft Regulations: What Potential Impact for Companies?

In our previous articles, we analyzed numerous provisions (and restrictions) concerning the transfer of personal information outside the borders of the People's Republic of China. These include the Measures for data export security assessment (available [here](#)), the Guidelines for the application of such Measures (available [here](#)), the implementation rules for personal information protection certification (available [here](#)) and the guidelines for the submission of the standard contract (available [here](#)).

To reduce the restrictions on cross-border data transfers, the Cyberspace Administration of China ("CAC") recently published the draft regulations aimed at regulating and standardizing such transfers (the "Draft Regulations"). If passed, these regulations should ease the compliance burden imposed on international companies intending to engage in cross-border data transfer activities. The CAC requests for public comments,

which can be submitted via email until 15th October 2023.

In this article, we will briefly analyze the content of the Draft Regulations, its potential impact if adopted, and provide some tips for companies intending to transfer personal information outside the borders of the People's Republic of China.

### **The Draft Regulations: content and exemptions**

Currently, under the "Measures for data export security assessment" (the "**Measures**", effective as of September 1, 2022), a controller of personal information that intends to transfer important data overseas must undergo a security assessment conducted by the CAC.

It is worth noting that, pursuant to Article 19 of these Measures, "important data" refers to data that, once tampered with, destroyed, leaked, or illegally obtained or used, may endanger national security, economic operation, social stability, public health and safety, etc.

As the definition of "important data" remains unclear, the Draft Regulations specify that companies will not need to self-identify its meaning; instead, the government will provide clarification through public announcements or specific notices.

Moreover, according to the Draft Regulations, a controller that intends to transfer personal information overseas is not subject to the mechanisms provided by the Personal Information Protection Law ("**PIPL**"), such as passing the security assessment conducted by the CAC, obtaining a certification from a specialized body, or entering into a contract (in accordance with the standard contract formulated by the CAC) with the foreign receiving party, when:

- The data to be transferred does not contain personal information or important data and is generated in activities such as international trade, academic cooperation, transnational manufacturing and marketing, and other similar activities;
- The personal information is not collected within the Chinese territory, but is provided overseas and is transferred in China for processing before being exported;
- The personal information must be transferred overseas for the establishment and performance of a contract with data subjects, such as online shopping, cross-border remittances, flight booking, hotel reservations, and visa applications;
- Personal information must be transferred overseas in emergency situations to protect the life, health, and safety of natural persons; and
- Employee personal information (including sensitive personal information) must be provided overseas for human resources management purposes, in conjunction with a collective contract signed in accordance with the law. It is worth noting that regarding this point, there are still some issues such as how to prove that exporting employees' personal information is "necessary" for the implementation of human resources management, and what happens if the exemption is met but the amount of employees' personal information to be exported exceeds 10,000 or 1 million.

The Draft Regulations also clarify that when personal information of less than 10,000 individuals is expected to be provided overseas within one year, the controller is exempt from the aforementioned mechanisms. However, the Draft Regulations specify that if personal information

transfer is based on an individual consent, the controller must obtain separate consent from individuals.

Also in this case, there are still some issues, such as how to calculate the starting point of “within one year”, whether it is necessary to consider both the number of personal information transfers in the past year and the number of transfers in the next year, whether, when calculating the amount of personal information to be exported overseas, the controller should include employee personal information provided overseas for the purpose of human resources management.

Nonetheless, the Draft Regulations provide that when:

- the personal information of more than 10,000 but less than 1 million individuals is expected to be transferred overseas, the controller must enter into a standard contract for the export of personal information;
- the personal information of more than more than 1 million individuals is expected to be exported, the controller must pass the security assessment.

Even in case of an exemption, the controller must conduct a personal information protection impact assessment (“**PIPIA**”).

Finally, the Draft Regulations also specify that pilot free trade zones<sup>3</sup> will have the authority to independently formulate a data list, which is considered a negative list. If a controller transfers data falling outside the negative list, such cross-border data transfer is exempt from the abovementioned mechanisms.

The press release and the draft regulations are available [here](#), only in Chinese.

### **Tips for companies**

Considering that the Draft Regulations could have a significant impact on data transfer, companies should pay attention to the release of the official regulations and take some measures, such as:

- Evaluate the amount of the personal information that a company expects to transfer overseas within a year;
- Monitor the negative list to determine if the personal information to be exported falls outside the list, especially if the company is located within a free trade pilot zone;
- comply with other requirements (such as obtain the separate consent);
- verify if the company can export employee personal information according to the regulations;
- stay updated on the progress of these regulations;
- seek legal counsel for compliance.

---

<sup>3</sup> China’s Pilot Free Trade Zones are some designated areas within the country that implement innovative policies and

reforms to promote international trade and investment, in order to attract foreign businesses, investors and companies.

\* \* \*

Per maggiori informazioni, potete contattare:

**Carlo Impalà**

*Partner e Responsabile Dip. TMT e Data Protection  
(Carlo.Impala@MorriRossetti.it)*

---

Linked 

Morri Rossetti



Osservatorio TMT&DP





OSSERVATORIO  
TMT·DATA PROTECTION

*di Morri Rossetti*

Morri Rossetti  
Piazza Eleonora Duse, 2  
20122 Milano

MorriRossetti.it  
Osservatorio-dataprotection.it