AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

26 September 2024, Davide Gallino

# Back to school/DSA

# Sommario

Sfide per i regolatori (dalle tlc/post regolamentazione ai servizi digitali, alle piattaforme, alla lotta alla disinformazione e alla garanzia dei diritti fondamentali)

Il Digital Services Act in breve

Implementazione pratica in EU e in Italia

# Challenges for regulators

Il modello di business adottato dalle telco e poi sfruttato dagli OTT (servizi separati dalle reti) ha aperto nuove sfide per l'industria delle telecomunicazioni e dei media

Ha reso sempre più necessario lo sviluppo di un quadro normativo per le grandi piattaforme.

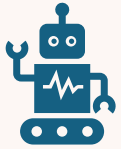
Un sistema orizzontale di divieti e obblighi applicabili a tali soggetti (come quelli di trasparenza e di non discriminazione) e con rimedi specifici, da definire caso per caso,

sulla base delle tematiche presentate dalle piattaforme dotate di un significativo potere di intermediazione che consente loro di controllare l'accesso a un numero significativo di utenti finali o di servizi, beni o contenuti

# Il network layer è (solo) un fattore abilitante

Ultra broadband

4G- 5G networks, software defined radio, etc



Artificial intelligence for network management (10-15 yrs old)

Cloud/-→edge computing

BYOD

# Inoltre: Direttiva sui servizi di media audiovisivi modificata

- Disposizioni per la coregolamentazione delle piattaforme per la condivisione di video (linee guida (2020/C 223/02))
- Fornitori di servizi di media, comprese le piattaforme social, tenuti a fornire agli utenti informazioni sufficienti in merito ai contenuti, compresa la pubblicità, che possono nuocere allo sviluppo fisico, mentale o morale dei minori;
- Limiti alla pubblicità del gioco d'azzardo;
- Misure specifiche nei confronti di chi utilizza profili fittizi di soggetti inesistenti o attraverso l'appropriazione di identità altrui, al fine di alterare lo scambio di opinioni, generare allarmi, sfruttare la diffusione di notizie false.

# 3 pilastri – linee di lavoro presenti e future nella regolamentazione dei mercati e dei servizi digitali

- **Digital Services Act (**Regulation of 19 Oct. 2022 on a Single Market For Digital Services ( Digital Services Act) and amending Directive 2000/31/EC**)**
- Digital Markets Act
- Artificial Intelligence Act

- *Digital Fairness Act on unfair commercial practices ??*

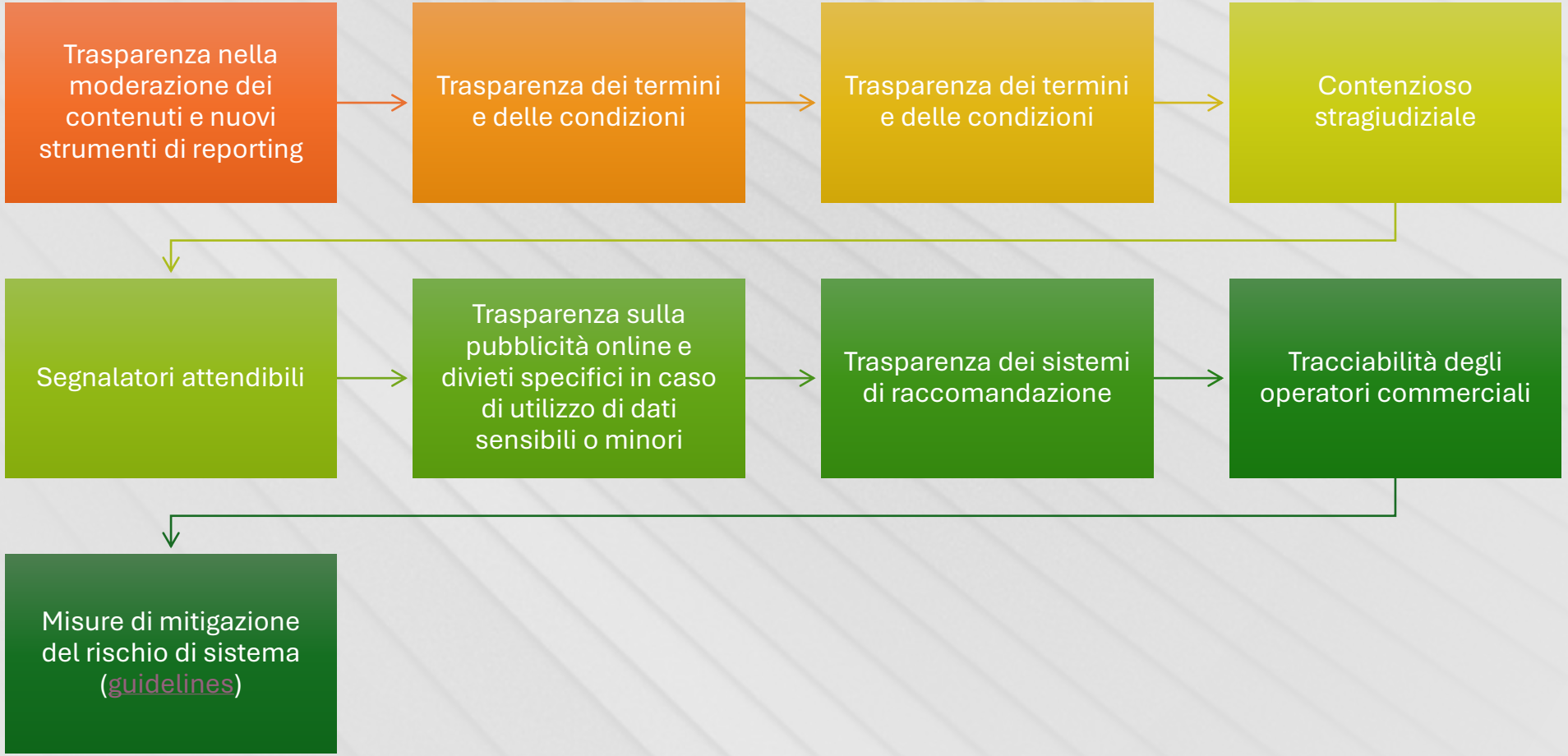
# DSA roll-out e governance

- Il DSA è entrato in vigore nel novembre 2022.
- Il regolamento sui servizi digitali si applica a tutti i prestatori intermediari di servizi a partire dal 17 febbraio 2024.
- Dal 25 agosto 2023, il DSA è già applicabile alle piattaforme di dimensioni molto grandi e ai motori di ricerca online di dimensioni molto grandi, con oltre 45 milioni di utenti attivi nell'UE (10% della popolazione europea), designati dalla Commissione europea (VLOP e VLOSE).
- La legge sui servizi digitali ha istituito una complessa struttura di governance che prevede una stretta cooperazione tra la Commissione europea e le autorità nazionali, al fine di garantire l'applicazione, il monitoraggio e la supervisione degli obblighi:
- La Commissione ha competenza esclusiva per l'applicazione della legge sui servizi digitali e sulla vigilanza delle VLOP e delle VLOSE in relazione agli obblighi supplementari loro imposti;
- A livello nazionale, il coordinatore dei servizi digitali (DSC) è responsabile della supervisione e dell'applicazione del regolamento nello Stato membro ed esercita funzioni di coordinamento con le altre autorità nazionali competenti;
- Il DSA ha inoltre istituito il Comitato europeo per i servizi digitali, un organismo indipendente costituito dai DSC e presieduto dalla Commissione europea, con compiti di consulenza e assistenza per l'applicazione coerente del regolamento e un'efficace cooperazione tra il DSC e la Commissione.

# DSA is the new key focus for ex-ante regulators

- La legge sui servizi digitali (DSA) è una nuova serie di norme rivolte agli intermediari online, comprese piattaforme come le reti di social media e i mercati online.  Stabilisce chiari obblighi di dovuta diligenza per le piattaforme in base ai loro ruoli, alle loro dimensioni e al loro impatto sul mondo online.
- Introduzione di meccanismi per la rimozione dei contenuti illegali e l'efficace protezione dei diritti fondamentali degli utenti online, compresa la libertà di parola.
- Trasparenza e obblighi di comunicazione nella legge sui servizi digitali = opportunità per un maggiore controllo pubblico degli intermediari online; + una serie di obblighi per le piattaforme online e i motori di ricerca che raggiungono in media più di 45 milioni di utenti mensili, che corrispondono a circa il 10% della popolazione dell'UE.
- Questi intermediari sono formalmente designati dalla Commissione come piattaforme online di dimensioni molto grandi (VLOP) e motori di ricerca online di dimensioni molto grandi (VLOSE).

# Principali misure in fase di attuazione:



# Orientamenti per la riduzione dei rischi sistemici (elezioni).....

b) **ccess to official i**
improve voter t
misinformation, d
process itself, be
VLOSEs is to fa
concerning the el
how and where to
the electoral auth
Such information
of information
interventions, link
specific election in
platform. When
mitigation measu
providers of VLO
inclusiveness and

**Media literacy initiatives.** Best practice for providers of VLO

c) **Measures to provide users with more contextual information** on the
Examples include:

i. **Fact-checking labels** on identified disinformation and FIMI content pro
fact-checking teams of independent media organisations. Fact-checkin
and its languages, inter alia through strengthening the cooperation
periods, integrating and showcasing election-related fact-checking conti
help increase the impact of these on audiences. Fact-checking labels s
understandable language.

ii. **Prompts and nudges** urging users to read content and evaluate its accu

iii. Clear, visible, and non-deceptive **indications of official accounts,** as
information on the electoral process, such as the accounts of electoral
such verification is established. The criteria that lead to an "official" lab
available and provided in easily understandable language, to prevent s
accounts impersonating official accounts, such as those of electoral autl

iv. Clear, visible, and non-deceptive **labelling of accounts** controlled by Me
controlled or financed by entities controlled by third countries.

v. **Tools and information to help users assess the trustworthiness** of i
focused on the integrity of the source based on transparent methodolo
parties.

vi. **Other tools to assess the provenance**, edit history, authenticity, or accu
to check the authenticity or identify the provenance or source of conter

vii. Establish effective internal measures to **counter misuse** of any of the a
the abuse of the verification process for labelled accounts and content.

adapting mitigation measures to the **relevant national context an**

d) **Recommender systems** can play a significant role in shaping the information landscape and public opinion, as recognised in recitals 70, 84, 88, and 94, as well as Article 34(2) of Regulation (EU) 2022/2065. To mitigate the risk that such systems may pose in relation to electoral processes, providers of VLOPs and VLOSEs should consider:

i. Ensuring that recommender systems are designed and adjusted in a way that gives users meaningful choices and controls over their feeds, with due regard to media diversity and pluralism;

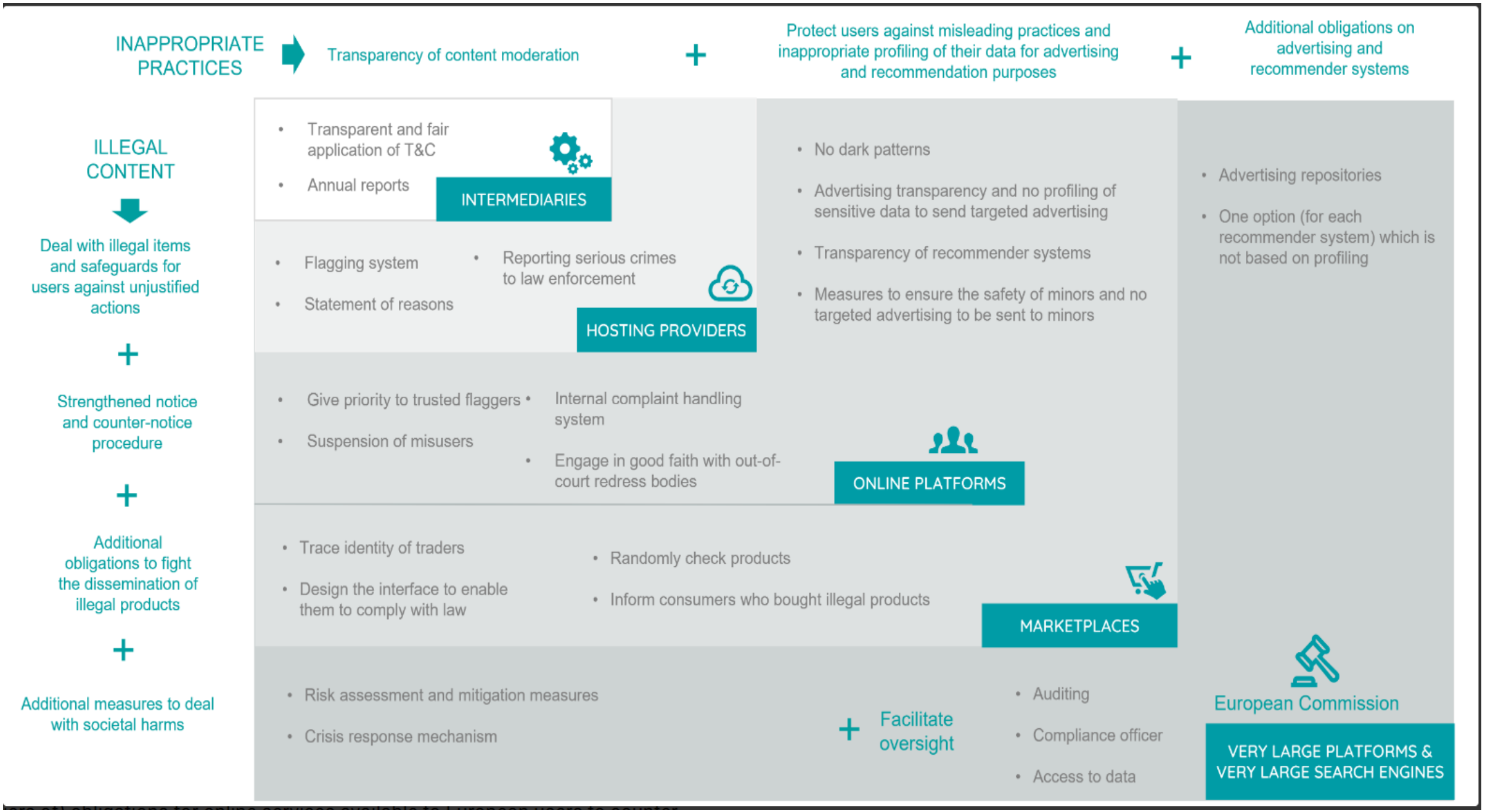
ii. Establishing measures to reduce the prominence of disinformation in the context of elections based on clear and transparent methods, e.g. regarding deceptive content that has been fact-checked as false or coming from accounts that have been repeatedly found to spread disinformation;

iii. Establishing measures to limit the amplification of deceptive, false or misleading content generated by AI in the context of elections through their recommender systems;

iv. Regularly assessing the performance and impact of recommender systems and addressing any emerging risks or issues related to electoral processes, including by updating and refining policies, practices, and algorithms;

# VLOP/VLOSE designati a partire dal 19 settembre 2024

- AliExpress International (Netherlands) B.V., Amazon Services Europe S.à.r.l, Apple Distribution International Limited,  Aylo Freesites Ltd. Booking.com B.V.
- Google Ireland Ltd., Google Play, Infinite Styles Services Co, Ltd, LinkedIn Ireland Unlimited Company, Meta Platforms Ireland Limited (MPIL)
- Microsoft Ireland Operations Limited , NKL Associates s.r.o, Pinterest Europe Ltd.
- Snap B.V., Technius Ltd. , TikTok Technology Limited, Twitter International Unlimited Company (TIUC)
- Whaleco Technology Limited, WebGroup Czech Republic, Wikimedia Foundation Inc 3****, Zalando SE




Source: Cullen International

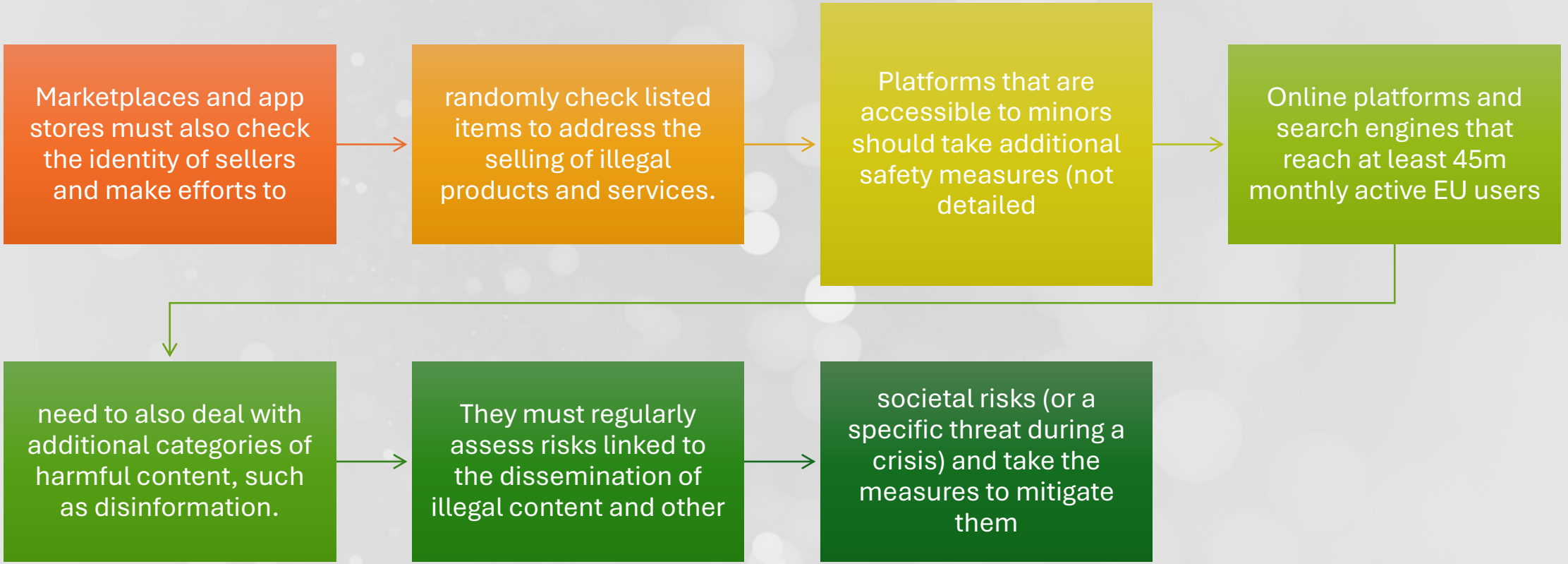
# Due diligence in DSA

Il regolamento mantiene l'attuale esenzione di responsabilità per gli intermediari e il divieto per gli Stati membri di imporre obblighi generali di monitoraggio, ma stabilisce (diversi livelli di) obblighi per i servizi online a disposizione degli utenti europei per contrastare la diffusione di contenuti illegali (compresi prodotti, servizi e attività) e in alcuni casi anche di contenuti dannosi.

I servizi di hosting devono prevedere una procedura di notifica e azione in base alla quale trattano le segnalazioni di articoli illegali che ricevono attraverso un sistema di segnalazione vincolante e segnalano alle autorità di contrasto qualsiasi sospetto di reati gravi.

Anche il sistema di segnalazione dei social media, degli app store e dei marketplace (piattaforme online) deve dare la priorità ai segnalatori attendibili. Tali piattaforme online hanno inoltre l'obbligo di sospendere gli utenti che forniscono frequentemente contenuti o prodotti manifestamente illegali

# Age/product/information verification



# Article 39, Ulteriore trasparenza della pubblicità online- the Digital Services Act (DSA)

- 1. I fornitori di VLOPS/VLOSE che presentano annunci pubblicitari sulle loro interfacce online compilano e mettono a disposizione del pubblico in una sezione specifica della loro interfaccia online, attraverso uno strumento consultabile e affidabile che consente interrogazioni multicriterio e attraverso interfacce per programmi applicativi, un repository:
- Essi garantiscono che il repertorio non contenga dati personali dei destinatari del servizio ai quali l'annuncio è stato o avrebbe potuto essere presentato e compiono ogni ragionevole sforzo per garantire che le informazioni siano accurate e complete.
- 2. Il repertorio contiene almeno tutte le seguenti informazioni:
- (a) il contenuto dell'annuncio, compreso il nome del prodotto, del servizio o del marchio e l'oggetto dell'annuncio;
- b) la persona fisica o giuridica per conto della quale è presentato l'annuncio;
- c) la persona fisica o giuridica che ha pagato per l'annuncio, se diversa dalla persona di cui alla lettera b);
- d) il periodo durante il quale l'annuncio è stato presentato;
- e) se l'annuncio pubblicitario era destinato ad essere presentato specificamente a uno o più gruppi particolari di destinatari del servizio e, in caso affermativo, i principali parametri utilizzati a tal fine, compresi, se del caso, i principali parametri utilizzati per escludere uno o più di tali gruppi specifici;
- f) le comunicazioni commerciali pubblicate sulle piattaforme online di dimensioni molto grandi e individuate a norma dell'articolo 26, paragrafo 2;
- g) il numero totale di destinatari del servizio raggiunti e, se del caso, il numero aggregato ripartito per Stato membro per il gruppo o i gruppi di destinatari specificamente destinatari dell'annuncio.

# Applicazione DSA e fasi più recenti/successive

**APPLICAZIONE**

La legge è entrata in vigore nel novembre 2022, ma gli obblighi di due diligence hanno iniziato ad applicarsi a tutti gli intermediari online solo a partire dal 17 febbraio 2024.

I fornitori designati come piattaforme di dimensioni molto grandi (VLOP) o motori di ricerca (VLOSE) devono rispettare gli obblighi stabiliti dalla sezione 5 (solo per VLOP e VLOSE) quattro mesi dopo la notifica della loro designazione.

**ULTIMI PASSAGGI**

10 luglio 2024: designazione di XNXX come VLOP

31 maggio 2024: designazione di Temu come VLOP

26 aprile 2024: designazione di Shein come VLOP

17 febbraio 2024: applicazione degli obblighi a tutti gli intermediari online

**PASSAGGI SUCCESSIVI**

4 ottobre 2024: Temu inizierà ad applicare la Sezione 5 e fornirà una prima valutazione del rischio

Novembre 2024: XNXX inizierà ad applicare la Sezione 5 e fornirà una prima valutazione del rischio

1° trimestre 2025: la Commissione pubblicherà orientamenti sulla designazione dei segnalatori attendibili

1H 2025: la Commissione pubblicherà orientamenti sulla protezione dei minori

Febbraio 2027: la Commissione valuterà l'impatto sulle piccole e medie imprese

# Dibattito del 17 settembre 2024 – Parlamento europeo

- La signora Vestager ha dato il via al dibattito chiarendo che il DSA non regola i contenuti online, né limita la libertà di parola. La legge sui servizi digitali impone alle piattaforme online di disporre di sistemi per contrastare la diffusione di contenuti illegali e per valutare e attenuare i gravi rischi per la società, come la disinformazione. Richiede inoltre loro di adeguare i loro sistemi di raccomandazione per evitare la diffusione di contenuti dannosi e "ha aperto la scatola nera dei loro algoritmi".
- Il DSA non richiede alle piattaforme di rimuovere i contenuti dannosi che non sono illegali, ha aggiunto. Al contrario, impedisce alle piattaforme online di prendere decisioni arbitrarie o di rimuovere  i contenuti legittimi, stabilendo solide garanzie per proteggere la libertà di espressione degli utenti.
- Ha spiegato come il lavoro della Commissione (nella fase di attuazione e di applicazione) si concentri su cinque settori prioritari: la protezione dei minori (ha menzionato in particolare la loro salute mentale), la lotta contro i contenuti illegali, la pubblicità, l'integrità delle elezioni e i mercati.

Online platforms and search engines that reach at least 45m monthly active EU users need to also deal with additional categories of harmful content, such as disinformation.

They must regularly assess risks linked to the dissemination of illegal content and other societal risks (or a specific threat during a crisis) and take the measures to mitigate them.

To protect users against the unjustified moderation of their content, the regulation requires all intermediaries to clearly provide information in their T&Cs of their content moderation activities. Hosting providers must also inform users when and why their

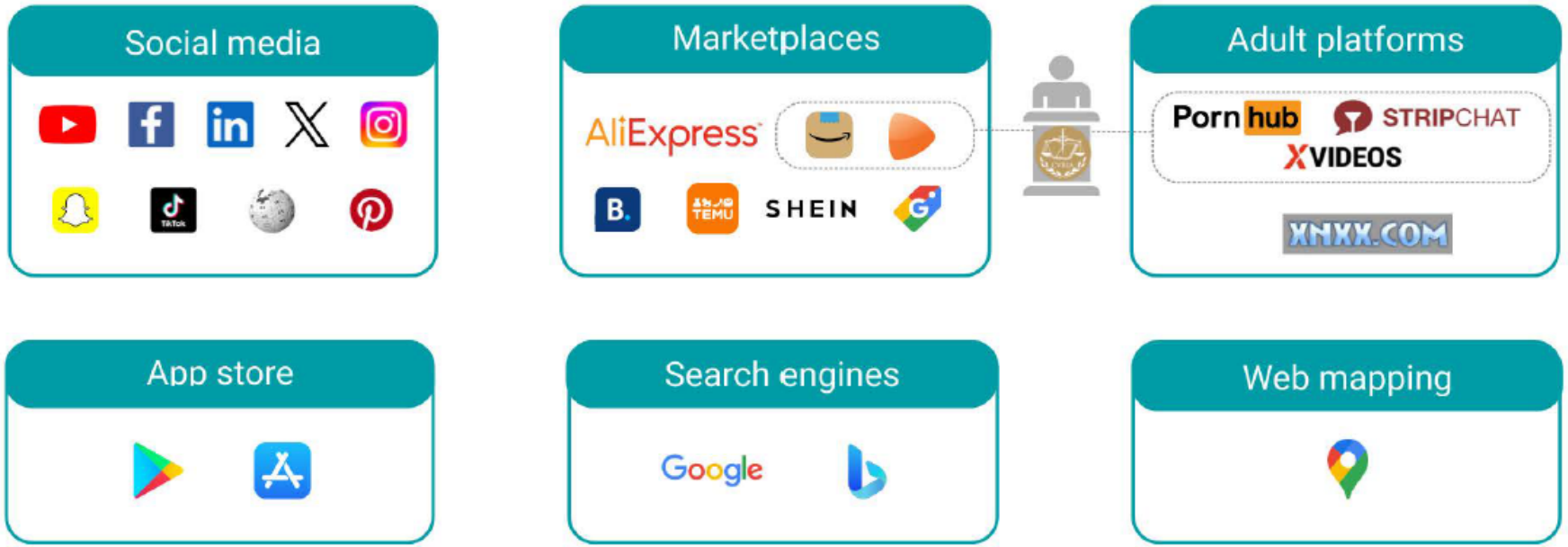
content is removed or restricted (including in relation to its monetisation or visibility), and of the redress options they have. Users are entitled to lodge internal complaints within online platforms and to seek redress before out of court dispute resolution bodies.

No special treatment is provided for the moderation of journalistic content but intermediaries must apply T&C so as to respect freedom and pluralism of the media and VLOPs and VLOSEs must assess (and eventually mitigate) related systemic risks.

Additional transparency obligations apply for advertising and for parameters used for targeting advertising or for recommending content to specific users. Advertising targeted to minors and advertising targeted to all users based on sensitive data are prohibited, as well as the use of dark patterns to manipulate users' choices..

# Designation of very large platforms and search engines

The Commission has so far designated 23 very large online platforms (VLOPs) and two very large online search engines (VLOSEs). Those that were most recently designated have not delivered their first risk assessment yet. Five platforms have so far challenged their designation as VLOPs before the EU Court. All online platforms must update the information on the number of users by Feb. 2025.




**Oct. 2024**
Temu to submit first risk assessment

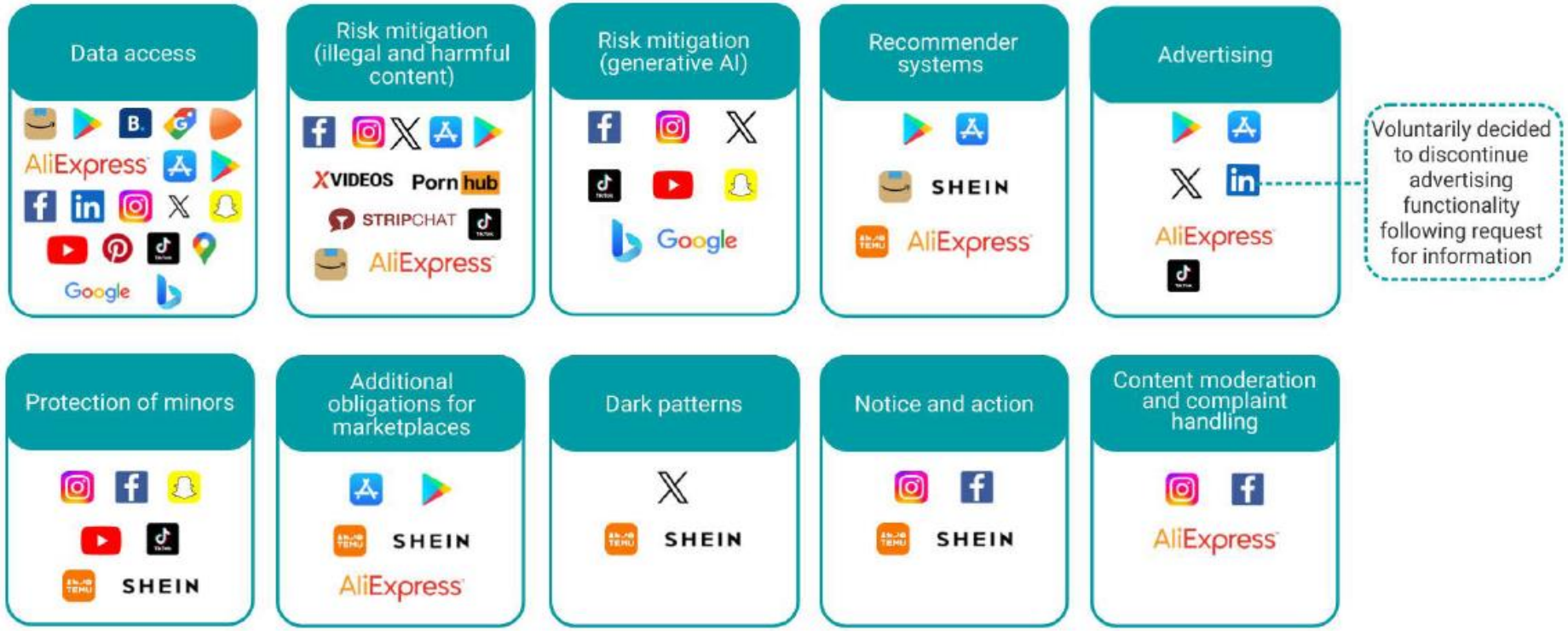
**Nov. 2024**
XNXX to submit first risk assessment

**Feb. 2025**
All online platforms to update number of users

Source: Cullen International

# Formal requests for information

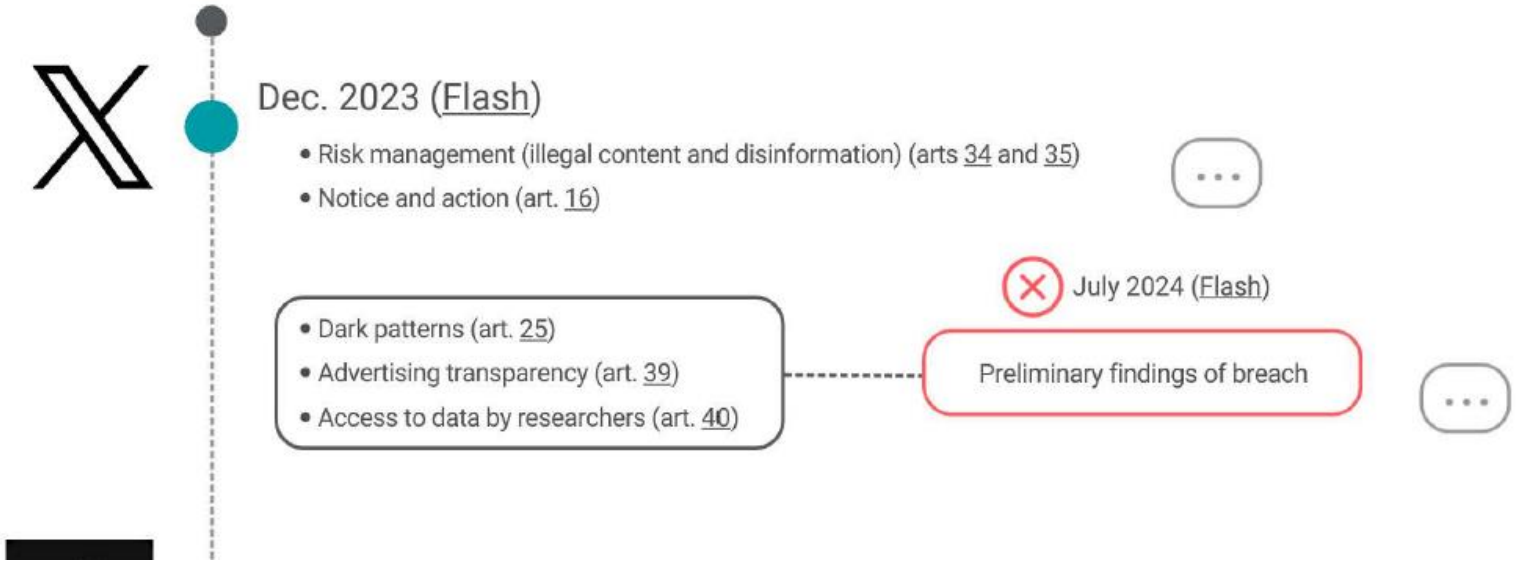
The Commission has so far requested information from 23 VLOPs and VLOSEs to understand if they are complying with different provisions of the regulation. Only two very large providers have not been formally questioned yet.




Source: Cullen International

# Formal proceedings

The Commission has so far opened formal proceedings against four VLOPs. In August 2024 it closed one proceeding against TikTok by accepting its commitment to permanently withdraw a service feature from the EU. In July 2024 the Commission issued preliminary findings that X is in breach of some obligations. X, which can exercise its rights of defence, could face fines of up to 6% of its total worldwide annual turnover if the findings are confirmed. Other investigations are pending.




Source: Cullen International

**Sono stati resi vincolanti gli impegni della piattaforma sulla cancellazione del programma che consentiva agli utenti di guadagnare punti svolgendo specifiche attività**

TikTok

Feb. 2024 (Flash)

- Risk management (addictive design and harmful content) (arts 34 and 35)
- Protection of minors (art. 28)
- Advertising transparency (art. 39)
- Data access for researchers (art. 40)

...

April 2024 (Flash)

- Risk management (Lite Reward programme) (arts 34 and 35)

Aug. 2024 (Flash)

Proceeding closed by accepting TikTok's commitments to permanently withdraw the feature from the EU (and not to launch others)

AliExpress

March 2024 (decision, Flash)

- Risk management (illegal content) (arts 34 and 35)
- Notice and action (art. 16)
- Internal complaint handling (art.20)
- Advertising transparency (arts 26 and 39)
- Recommender systems (arts 27 and 38)
- Traders' traceability (art. 30)
- Data access for researchers (art. 40)

...

# POV:


https://www.tiktok.com/transparency/en/covert-influence-operations

https://www.tiktok.com/transparency/en/dsa-transparency?tc_version=2024

- During Q4 2023, we proactively removed approximately 13 million items of violative content under our Policies (defined below).
- In the same time period we also received around 131,000 illegal content reports corresponding to approximately 63,000 unique pieces of content. We estimate 38% of those were found to violate our Policies or local law and were actioned.
- TikTok has more than 6,000 people dedicated to moderating content, covering at least one official language for each of the 27 European Union Member States.

# Case study: content moderation, TikTok

- We place considerable emphasis on proactive detection to remove violative content. Content that is uploaded to the
- platform is first reviewed by our automated moderation technology, which aims to identify content that violates our
- Policies before it is viewed or shared by other people on the platform or reported to us. While undergoing this review,
- the content is visible only to the uploader.
- If our automated moderation technology identifies content that is a potential violation, it will either be automatically
- removed from the platform or flagged for further review by our human moderation teams. In line with our safeguards
- to help ensure accurate decisions are made, automated removal is applied when violations are the most clear-cut.
- We use a variety of automated tools, including:
- ● Computer Vision models, which help to detect objects (for example visual signals, emblems, logos and
- objects that are known to be associated with extremist and hate groups) so it can be determined whether
- the content likely contains material which violates our Policies.
- ● Keyword lists and models are used to review text and audio content to detect material in violation of our
- Policies. We work with various external experts, like our fact-checking partners, to inform our keyword lists.
- ● Where we have previously detected content that violates our Policies, we use de-duplication and hashing
- technologies that enable us to recognise copies or near copies of such content. This is used to prevent
- further re-distribution of violative content on the platform. We work with external groups, such as Tech
- Against Terrorism on hate or violent extremist content, who help us to more quickly detect and remove
- violative content that has already been identified off the platform.
- We are continuing to invest in improving the precision of our automated moderation systems so that we can more
- effectively remove violative content at scale, while also reducing the number of incorrect removals. If users or
- advertisers believe we have made a mistake, they can appeal the removal of their content

## April 2024 (decision, Flash)

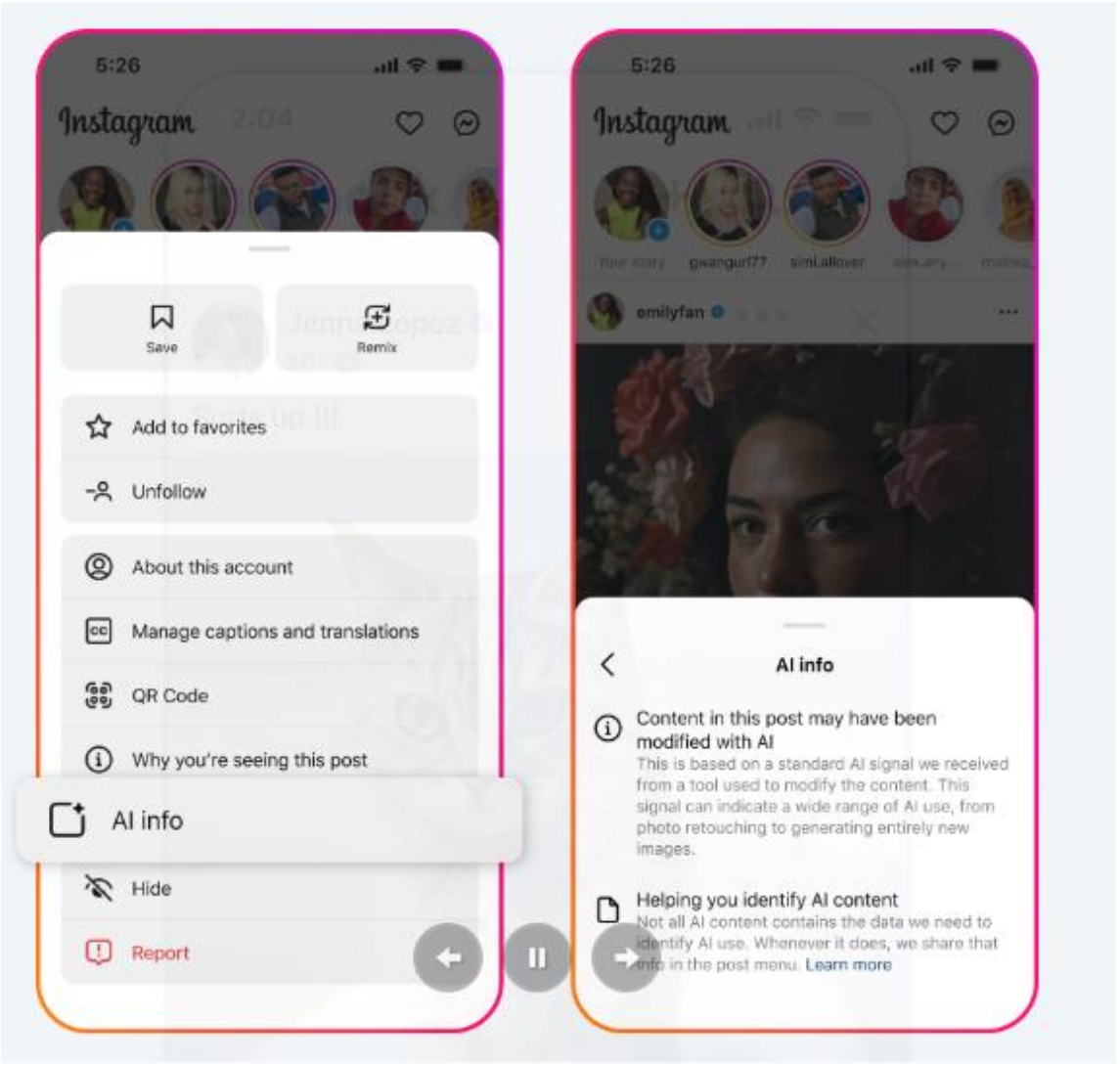
- Risk management: integrity of elections and dissemination of harmful content (arts 34 and 35)
- Notice-and-action (art. 16)
- Content moderation transparency (arts 14, 17 and 24)
- Internal complaint handling (art. 20)
- Dark patterns (art. 25)
- Data access for researchers (art. 40)

## May 2024 (Flash)

- Risk management (addictive design and harmful content) (arts 34 and 35)
- Protection of minors (art. 28)

# POV META

- https://about.fb.com/news/2024/04/metas-approach-to-labeling-ai-generated-content-and-manipulated-media/



## Implementing rules and guidelines

According to the DSA, the Commission must adopt additional implementing rules and can publish non-binding guidelines for providers or digital services coordinators, DSCs (DSA implementing rules and guidelines Tracker). While some acts and guidelines are already adopted, others are in the process of adoption. There is no indication yet if the Commission will issue guidelines on dark patterns and on online advertising repositories, or implementing rules on the calculation on the number of users.

Act Guidelines

| FOR PROVIDERS | FOR ENFORCEMENT AUTHORITIES |
| --- | --- |
| • Independent external audits (art. 37) (Flash) | • Calculation of supervisory fee (art. 43) (Flash) |
| • Risk mitigation for the integrity of elections (Flash)<br>• Calculation of average monthly active users (art. 33) (Flash) | • Information sharing system between DSCs, Commission and the EU Board for digital services (EBDS) (art. 85) (Flash)<br>• Commission's monitoring and investigatory procedures (arts 69, 72 and 79) |

Source: Cullen International

- Access to data (art. 40)
- Transparency reports (arts 15 and 24)

4Q 2024

- Designation of trusted flaggers (art. 22)

1Q 2025

- Protection of minors (art. 28)

2Q 2025

- Dark patterns (art. 25)
- Advertising repositories (art. 39)
- Possible rules to calculate the average monthly active users (art. 33)
- Rules to adjust the number of users threshold when EU population increases or decreases (art. 33)

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI

AGCOM

# AGCOM è il DSC italiano

- I coordinatori dei servizi digitali (DSC) sono autorità indipendenti nominate da ciascuno Stato membro dell'UE.
- I DSC sono responsabili della vigilanza sulla conformità ai DSA dei servizi intermediari stabiliti nel loro paese.
- Un'altra responsabilità è quella di valutare le domande dei ricercatori per l'accesso ai dati. Fungeranno anche da collegamento tra i ricercatori e i VLOP/VLOSE.

# Cooperazione tra CE ed ERGA nell'applicazione dei DSA

- La cooperazione si concentrerà sulla supervisione delle piattaforme online di dimensioni molto grandi (VLOP) e dei motori di ricerca (VLOSE) designati.
- L'esperienza dell'ERGA, che riunisce le autorità nazionali di regolamentazione dei media ai sensi della direttiva sui servizi di media audiovisivi, è una preziosa fonte di informazioni per il lavoro quotidiano della Commissione in qualità di autorità di regolamentazione per le VLOP e le VLOSE.
- L'ERGA fungerà da facilitatore per raccogliere informazioni pertinenti a livello nazionale e produrre rapporti su questioni relative al pluralismo dei media, alla disinformazione e alla protezione dei minori, tra le altre. La cooperazione con l'ERGA sosterrà l'individuazione e la valutazione dei rischi sistemici in questi settori da parte della Commissione.
- Lo sviluppo di competenze e capacità attraverso la cooperazione con l'ERGA aiuterà anche il Comitato europeo per i servizi digitali, composto da coordinatori dei servizi digitali, a raggiungere gli obiettivi stabiliti dal DSA.
- La Commissione ha già concluso accordi amministrativi bilaterali con le autorità nazionali di regolamentazione di Francia, Irlanda, Italia e Paesi Bassi. La cooperazione attiva con gli Stati membri, le autorità nazionali di regolamentazione e gli organismi dell'UE è fondamentale per attuare efficacemente la legge sui servizi digitali e adoperarsi per creare un ambiente online sicuro e affidabile nell'UE.

# EC/AGCOM administrative agreement

L'accordo mira a sviluppare competenze e capacità che aiuteranno la Commissione a individuare e valutare i rischi sistemici nell'ambito della legge sui servizi digitali, compresi i rischi connessi alla diffusione di contenuti illegali e alla disinformazione, nonché gli effetti negativi sui minori. Contribuirà a organizzare lo scambio pratico di informazioni, dati, buone pratiche, metodologie, sistemi e strumenti tecnici con l'autorità di regolamentazione.

L'AGCOM è stata nominata Coordinatore dei Servizi Digitali per l'Italia ed è quindi entrata a far parte del Consiglio per i Servizi Digitali, composto da un'autorità competente per Stato membro.

# Punto di contatto ai sensi dell'art. 11 DSA

- Conformemente all'articolo 11 della legge sui servizi digitali, i prestatori di servizi intermediari designano un punto di contatto unico che consenta loro di comunicare direttamente, per via elettronica, con le autorità degli Stati membri, con la Commissione e con il Comitato europeo per i servizi digitali.
- L'AGCOM, in qualità di Coordinatore dei Servizi Digitali, richiede a tutti i prestatori intermediari di servizi, di comunicare il proprio punto di contatto tramite l'indirizzo di posta elettronica dsa@agcom.it, o indirizzo di posta elettronica certificata (PEC) agcom@cert.agcom.it, ove possibile, specificando nell'oggetto "PUNTO DI CONTATTO COMUNICAZIONE ai sensi dell'art. 11 DSA".

# Due decisioni applicative dell'AGCOM (contenzioso stragiudiziale e istituzione di segnalatori attendibili)

- L'Autorità per le Garanzie nelle Comunicazioni, nella seduta del Consiglio del 24 luglio 2024, ha approvato il Regolamento interno per la certificazione degli organismi di risoluzione extragiudiziale delle controversie tra fornitori di piattaforme online e destinatari di servizi (delibera n. 282/24/CONS) e per il rilascio della qualifica di segnalatore attendibile (delibera n. 283/24/CONS), in attuazione degli articoli 21 e 22 del Regolamento (UE) 2022/2065 (Digital Services Act o DSA).
- I Regolamenti, entrati in vigore il 15 settembre, costituiscono i primi interventi messi in atto dall'AGCOM, nell'esercizio delle funzioni di Coordinatore dei Servizi Digitali per l'Italia, per garantire l'applicazione efficace e coordinata del DSA.
- Il Regolamento è stato adottato a seguito della consultazione pubblica, alla quale hanno partecipato 11 soggetti, tra cui organismi di mediazione, associazioni di categoria e dei consumatori e piattaforme online.
- A partire dal 15 settembre, gli organismi stabiliti in Italia che svolgono attività di risoluzione non giurisdizionale delle controversie (ADR) potranno richiedere all'Autorità la certificazione necessaria per poter gestire le controversie relative a decisioni assunte dalle piattaforme in merito alla pubblicazione di "contenuti illeciti", in quanto contrarie alle norme del diritto europeo o nazionale,  o più in generale rispetto alla gestione degli account dei destinatari del servizio.

# Consultazione sulla risoluzione alternativa delle controversie

Gli organismi ADR partecipanti hanno presentato osservazioni più specifiche in merito alla proposta di regolamentazione, mentre le associazioni di categoria hanno espresso soprattutto preoccupazione in merito al funzionamento, all'indipendenza e alle decisioni degli organi ADR, con particolare riguardo al criterio dell'indipendenza finanziaria, auspicando regole armonizzate.

Il contributo dell'unica piattaforma partecipante alla consultazione (Meta) ha più volte evidenziato la necessità di procedure standard e

l'applicazione di regole omogenee da parte degli organismi ADR, al fine di evitare il proliferare di procedure non uniformi (nella gestione delle diverse fasi della procedura e/o nell'applicazione delle disposizioni in materia di contenuti illeciti) e il rischio di abusi.

# Delibera n. 282/24/CONS dell'AGCOM

- Disposizioni volte a garantire la trasparenza, l'imparzialità e l'efficienza:
- Indipendenza: gli organismi devono essere finanziariamente e operativamente indipendenti dalle piattaforme online e dagli altri attori economici coinvolti.
- Trasparenza: devono fornire informazioni chiare e accessibili sulle procedure di risoluzione delle controversie, compresi i costi e i tempi previsti.
- Competenza: gli organismi devono dimostrare di disporre di personale qualificato ed esperto nella risoluzione digitale delle controversie.
- Imparzialità: devono garantire che le decisioni siano prese in modo imparziale e senza conflitti di interesse.
- Efficienza: le procedure devono essere rapide ed efficaci, con l'obiettivo di risolvere le controversie nel minor tempo possibile.

# Gestione delle controversie

Le controversie devono essere risolte entro un massimo di 90 giorni dalla data di presentazione del reclamo. Questo termine può essere prorogato in casi eccezionali, ma l'organo di risoluzione delle controversie deve informare le parti interessate dei motivi della proroga e della nuova data prevista per la risoluzione.

# Segnalatori attendibili

- Il secondo Regolamento (delibera n. 283/24/CONS), relativo alle procedure per il rilascio della qualifica di segnalatore attendibile, è stato adottato a seguito di una consultazione pubblica nazionale in cui hanno partecipato 19 soggetti (industria dei media, nonché fornitori di servizi di piattaforme online e altri stakeholder
- Il Regolamento definisce le modalità operative per il rilascio della qualifica di segnalatore attendibile a qualsiasi organismo stabilito in Italia che dimostri di possedere i requisiti – previsti dall'art. 22 del DSA – di capacità e competenza, indipendenza dalle piattaforme online e qualità nell'attività di segnalazione.
- I soggetti interessati devono presentare apposita richiesta e indicare l'ambito di competenza in cui intendono svolgere l'attività. Il titolo avrà durata triennale ed è rinnovabile previa presentazione di apposita richiesta prima della scadenza.

# La delibera dell'AGCOM (agosto 2024) e le iniziative di supporto

- Requisiti e applicazione per diventare un segnalatore attendibile

+

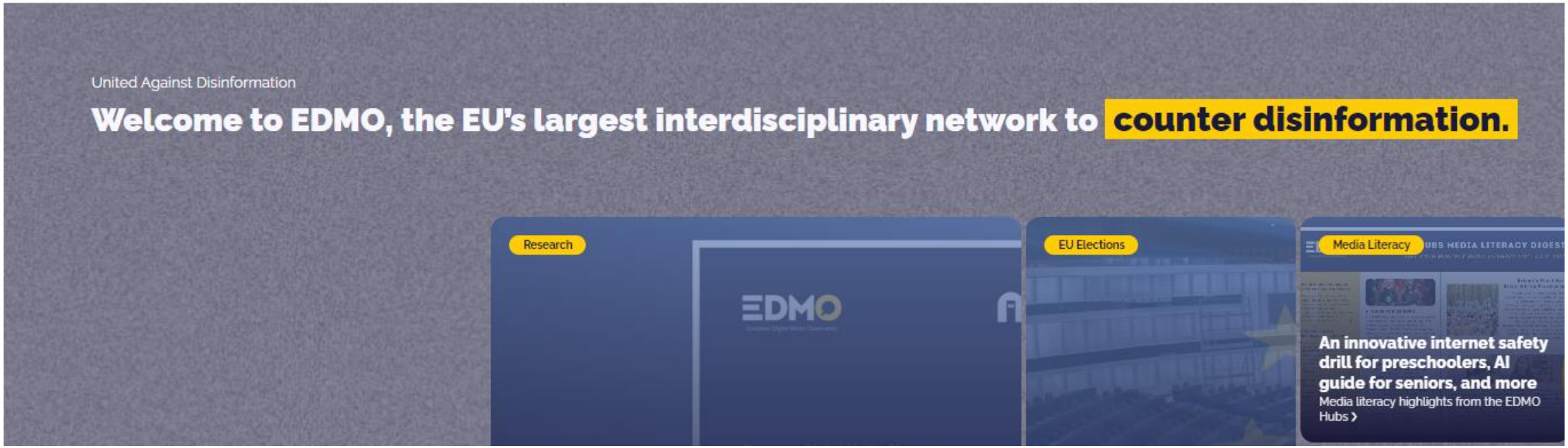
- Gruppo di lavoro EDMO per la creazione di un organismo intermediario indipendente a sostegno della ricerca sulle piattaforme digitali e la bozza del codice di condotta su come le piattaforme possono condividere i dati con ricercatori indipendenti tutelando nel contempo i diritti degli utenti

# Recepimento italiano del DSA – segnalatore attendibile

- Allegato A alla delibera n. 283/24/CONS Regolamento di procedura per il riconoscimento della qualifica di segnalatore attendibile ai sensi dell'art. 22 del Regolamento Servizi Digitali
- Questioni giurisdizionali (la maggior parte delle piattaforme, in particolare VLOP, ha la propria sede europea in Irlanda) – questo limita le richieste di accesso dall'Italia.

**Ruolo del DSC ruolo nell'aiutare i ricercatori ad accedere ai dati?**

- I ricercatori possono presentare la loro domanda di accesso ai dati al DSC dello Stato membro dell'istituto di ricerca a cui sono affiliati o direttamente al DSC in cui è stabilito il fornitore del VLOP o del VLOSE a cui desiderano accedere. In entrambi i casi, la decisione di richiedere l'accesso ai dati per conto del ricercatore spetta al DSC di stabilimento del rispettivo fornitore del VLOP o del VLOSE. Quando un ricercatore si rivolge al proprio DSC "locale", tale DSC trasmette la domanda, unitamente a una valutazione iniziale di tale domanda, al DSC di stabilimento. Es. dall'Italia, i ricercatori potranno chiedere di accedere ai dati in Irlanda (sede di molte piattaforme)


https://edmo.eu
EDMO
European Digital Media Observatory
About Us
Our Activities
Thematic Areas
Resources
United Against Disinformation
Welcome to EDMO, the EU's largest interdisciplinary network to counter disinformation.
Research
EDMO
EU Elections
Media Literacy
An innovative internet safety drill for preschoolers, AI guide for seniors, and more
Media literacy highlights from the EDMO Hubs ›

# Richiesta di accesso ai dati delle piattaforme

- Rapporto EDMO (Set 24) : 📄 Trova il rapporto completo qui sotto o sul sito web EDMO: https://lnkd.in/eCSwcq9g
- Nonostante l'entrata in vigore della legge sui servizi digitali, in pratica l'attuale accesso ai dati da parte dei ricercatori dalle piattaforme rimane limitato, con alcune API di piattaforma che funzionano meglio di altre, mentre permangono una serie di carenze significative che sono presentate nella relazione.
- Tra queste limitazioni, i ricercatori segnalano l'accessibilità limitata, i processi di candidatura complessi che comportano rischi significativi in termini di responsabilità e multe e il requisito che le applicazioni siano collegate a progetti specifici piuttosto che approvate a tutti i livelli organizzativi.

# Quali argomenti di ricerca ?

- **Quali temi di ricerca sono sostenuti dall'articolo 40 della legge sui servizi digitali?**
- **Per ottenere l'accesso ai dati VLOP e VLOSE in qualità di "ricercatore controllato", la ricerca proposta nella domanda al DSC deve contribuire all'individuazione, all'identificazione e alla comprensione dei rischi sistemici nell'UE e/o alla valutazione dell'adeguatezza, dell'efficienza e dell'impatto delle misure di mitigazione del rischio.**
- **I rischi sistemici in esame, come indicato all'articolo 34, paragrafo 1, sono:**
- **La diffusione di contenuti illegali**
- **Effetti negativi per l'esercizio dei diritti fondamentali, in particolare:**
- **Dignità umana**
- **Rispetto della vita privata e familiare**
- **Protezione dei dati personali**
- **Libertà di espressione e di informazione**
- **Non discriminazione**
- **Rispetto dei diritti del minore**
- **Un elevato livello di protezione dei consumatori**
- **Effetti negativi sul discorso civico e sui processi elettorali e sulla sicurezza pubblica**
- **Effetti negativi in relazione a**
- **Violenza di genere**
- **Tutela della salute pubblica e dei minori**
- **Gravi conseguenze negative per il benessere fisico e mentale personale.**

# Ricercatori in Europa e in Italia

- EDMO.eu and Vera.ai projects,
- The Integrity Institute,
- Digital Forensic Research Lab,
- Center for Digital Governance, Hertie School

- Inoltre: utilizzare un bot di debunking per ridurre la credulitànelle cospirazioni

# Alcuni aspetti positivi

- In questo settore si possono notare anche alcuni sviluppi positivi. Tra queste, le dichiarazioni pubbliche della CE secondo cui l'interpretazione dell'articolo 40, paragrafo 12, sembra consentire lo scraping non autorizzato1 e il fatto che le disposizioni sull'accesso ai dati dei ricercatori di cui all'articolo 40, paragrafo 12, esistono ora per la stragrande maggioranza dei VLOP, almeno sulla carta, anche se in molti casi mancano ancora i dettagli dei programmi concreti e dei dati disponibili.
- Ciò sottolinea la necessità di un'entità indipendente che possa testare e garantire la qualità dei dati ai sensi dell'articolo 40, paragrafo 12, della legge sui servizi digitali e, potenzialmente, dell'articolo 40, paragrafo 4; 40, paragrafo 8, in quanto è chiaro che ciò non può essere fatto dai singoli ricercatori

# EDMO - Raccomandazioni

la necessità di implementare rapidamente gli strumenti e le interfacce della piattaforma per l'accesso ai dati;

• La necessità di aumentare la consapevolezza sulle API di nuova concezione, anche rendendo le informazioni chiare e di facile utilizzo e fornendo formazione e supporto alla comunità di ricerca su questi strumenti; Rapporto sul workshop EDMO sull'accesso ai dati delle piattaforme per i ricercatori 7 www.edmo.eu

• la necessità che le procedure di candidatura siano chiare e che le domande dei ricercatori siano approvate rapidamente;

• La proposta di approvare le candidature a livello organizzativo, anziché essere legate a progetti specifici;

• I dati forniti dovrebbero soddisfare le esigenze della comunità di ricerca consentendo un accesso incrementale e quasi in tempo reale ai dati, che dovrebbe includere anche la fornitura ai ricercatori di informazioni sui dati contrassegnati come disinformativi;

• Consentire l'accesso alle API anche ai ricercatori della società civile;

• Fornire sostegno ai ricercatori che stipulano contratti legali, ad esempio l'istituzione di un sistema di protezione/assicurazione legale per gli istituti di ricerca pubblici, le ONG e i ricercatori indipendenti;

• Una maggiore standardizzazione delle API consentirà alla comunità di ricerca di utilizzarle più ampiamente, piuttosto che dover acquisire competenze specifiche per ciascuna piattaforma;

• In futuro potrebbe essere sollevata la questione se sia possibile sviluppare strumenti specifici che potrebbero consentire l'uso di API da parte di ricercatori provenienti da diversi background disciplinari oltre ai data scientist

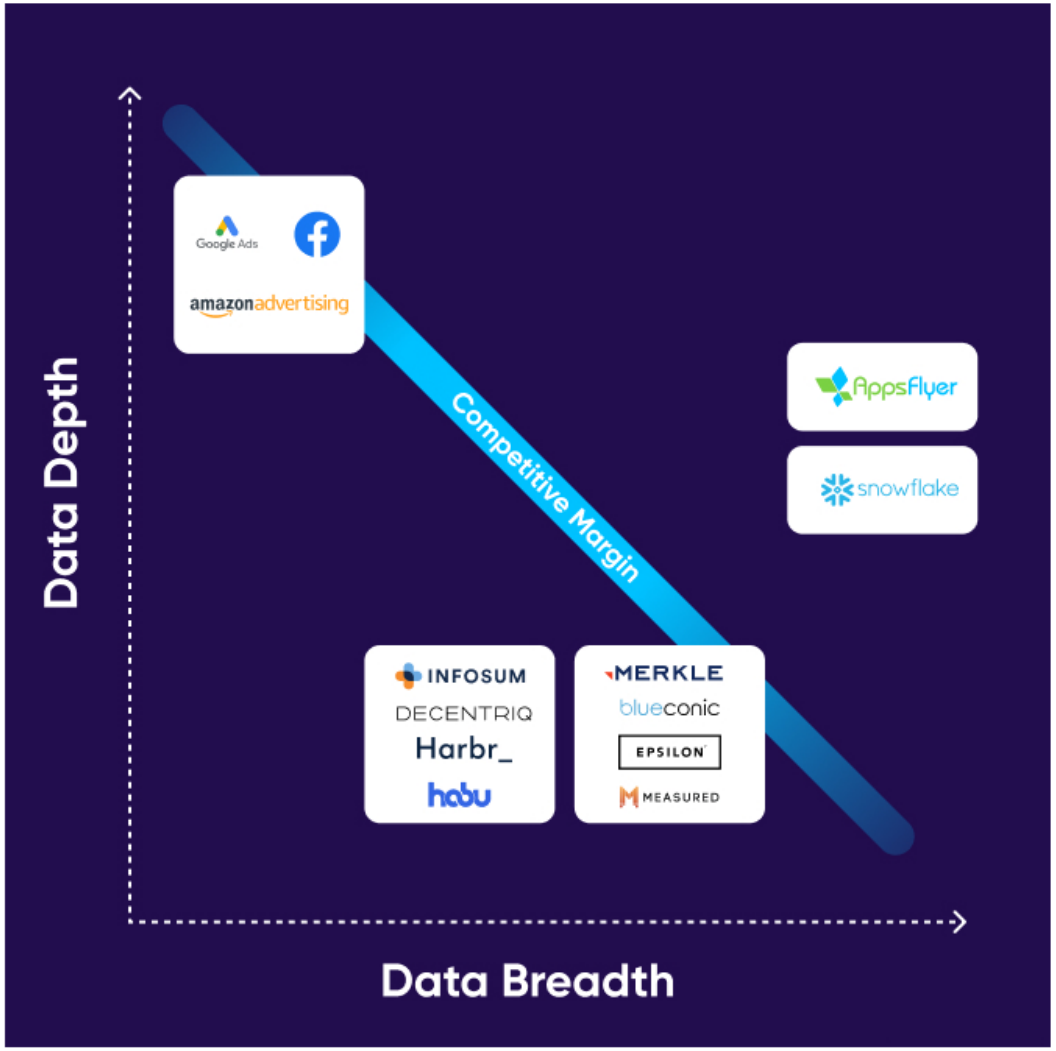
# Non permissioned scraping

- If I scrape a site and the data remains on my PC/phone, ok (the cache does it to speed up use); if I use that data to offer services, they might ask me where I got it and I would have to prove that I obtained it through legitimate methods

# Handling  data in the «clean data room»

| | Data Granularity | Ingestion | Connect & Enrich | Query & Actions |
|---|---|---|---|---|
| **MMPs** | • User-level & cross-channel (cornered resource)<br>• Restrictions imposed by SRNs | • Conversion data ingested at the source (DSPs, in-app SDK) and in real-time<br>• No existing CDP architecture | • Best in class analytics features (both in-house and via rich partner ecosystem) | • Flexible integrations for marketing actions<br>• Best in class aggregated reporting<br>• Business users / marketers<br>• Restrictions imposed by SRNs |
| **Independent Marketing Incumbents** | • Maximum flexibility<br>• No access to Walled Garden data | • Leverages existing CDP / CEP functionality; potential movement of data issues | • Complete flexibility to users<br>• Small partner ecosystem<br>• Less sophisticated compute / data manipulation tools | • Targeted at business users / marketers<br>• Limited downstream integrations |
| **Pure-play** | | • Reliant on 3rd party infrastructure (CDPs, cloud storage etc.) for data ingestion<br>• Data storage may be distributed (e.g. Infosum's Bunker Technology) | | |
| **Enterprise Cloud** | | • Full distributed (no copying of data into one place)<br>• Leverages existing data piping and storage infrastructure | • Access to rich ecosystem of Snowflake's integrated partners | • Access to rich ecosystem of Snowflake's integrated partners |
| **Walled Gardens** | • Unrivalled access to native ecosystem data<br>• No cross-channel access | • Ads data hub built on top of BigQuery; approach of Facebook is unclear<br>• Lacks scalability | • Unrivalled depth but lacks breadth (no cross-channel enrichment) | • Requires a data scientist / engineer<br>• Limited flexibility (walled garden moat) |

- The volume and quality of the data – referred to as depth
- And the variety of received data – referred to as breadth



# Algorithmic transparency

- https://algorithmic-transparency.ec.europa.eu/news/faqs-dsa-data-access-researchers-2023-12-13_en
- Caso X (Twitter) Inoltre, sono stati resi noti i risultati preliminari del procedimento contro X, che include la constatazione che X non riesce a fornire l'accesso ai suoi dati pubblici ai ricercatori. In particolare, X vieta ai ricercatori idonei di accedere in modo indipendente ai suoi dati pubblici, ad esempio tramite scraping, come indicato nei suoi termini di servizio. Inoltre, il processo di X per concedere ai ricercatori idonei l'accesso alla sua interfaccia di programmazione delle applicazioni (API) sembra dissuadere i ricercatori dal portare avanti i loro progetti di ricerca o lasciarli senza altra scelta se non quella di pagare tariffe sproporzionatamente elevate.

# EDMO

- Per quanto riguarda le modalità di accesso ai dati tramite API specifiche, le API di streaming/in tempo reale (ad esempio, le precedenti API di Twitter) che consentono di ottenere continuamente nuovi set di dati possono essere preferibili alle API in cui è richiesto il download periodico (YouTube e TikTok) in quanto ciò potrebbe anche limitare il tipo di ricerca possibile.
- Modello di Data Sharing Agreement:
- Model-Data-Sharing-Agreement-Final.pdf (edmo.eu)