

Codice di condotta sulla disinformazione - Rapporto di TikTok per il periodo 1° luglio 2024 - 31 dicembre 2024

Indice dei contenuti

Riassunto esecutivo	12
II. Controllo delle inserzioni pubblicitarie	18
Impegno 1.....	19
Misura 1.1.....	21
Misura 1.2.....	30
Misura 1.3.....	31
Misura 1.4.....	32
Misura 1.5.....	33
Misura 1.6.....	34
Impegno 2.....	34
Misura 2.1.....	35
Misura 2.2.....	38
Misura 2.3.....	39
Misura 2.4.....	42
Impegno 3.....	45
Misura 3.1.....	45
Misura 3.2.....	46
Misura 3.3.....	46
III. Pubblicità politica	47
Impegno 4.....	48
Misura 4.1.....	48
Misura 4.2.....	48
Impegno 5.....	49
Misura 5.1.....	50
Impegno 6.....	50
Misura 6.1.....	51
Misura 6.2.....	51
Misura 6.3.....	52
Misura 6.4.....	52
Misura 6.5.....	52
Impegno 7.....	52
Misura 7.1.....	53
Misura 7.2.....	54
Misura 7.3.....	54
Misura 7.4.....	54
Impegno 8.....	55
Misura 8.1.....	55
Misura 8.2.....	55
Impegno 9.....	56
Misura 9.1.....	56
Misura 9.2.....	56
Impegno 10.....	57
Misura 10.1.....	57
Misura 10.2.....	57
Impegno 11.....	58
Misura 11.1.....	59
Misura 11.2.....	59

Misura 11.3.....	59
Misura 11.4.....	59
Impegno 12.....	59
Misura 12.1.....	60
Misura 12.2.....	60
Misura 12.3.....	60
Impegno 13.....	60
Misura 13.1.....	61
Misura 13.2.....	61
Misura 13.3.....	61
IV. Integrità dei servizi	62
Impegno 14.....	63
Misura 14.1.....	65
Misura 14.2.....	74
Misura 14.3.....	101
Impegno 15.....	102
Misura 15.1.....	103
Misura 15.2.....	105
Impegno 16.....	105
Misura 16.1.....	106
Misura 16.2.....	107
V. Responsabilizzare gli utenti	109
Impegno 17.....	110
Misura 17.1.....	114
Misura 17.2.....	141
Misura 17.3.....	161
Impegno 18.....	163
Misura 18.1.....	164
Misura 18.2.....	172
Misura 18.3.....	181
Impegno 19.....	182
Misura 19.1.....	183
Misura 19.2.....	185
Impegno 20.....	187
Misura 20.1.....	188
Misura 20.2.....	188
Impegno 21.....	189
Misura 21.1.....	191
Misura 21.2.....	202
Impegno 22.....	204
Misura 22.1.....	204
Misura 22.2.....	205
Misura 22.3.....	205
Misura 22.4.....	205
Misura 22.5.....	206
Misura 22.6.....	207
Misura 22.7.....	207
Impegno 23.....	207
Misura 23.1.....	208
Misura 23.2.....	212
Impegno 24.....	214
Misura 24.1.....	214
Impegno 25.....	222
Misura 25.1.....	223



Misura 25.2	223
VI. Responsabilizzare la comunità di ricerca	224
Impegno 26	225
Misura 26.1	226
Misura 26.2	227
Misura 26.3	232
Impegno 27	232
Misura 27.1	233
Misura 27.2	233
Misura 27.3	234
Misura 27.4	234
Impegno 28	234
Misura 28.1	235
Misura 28.2	238
Misura 28.3	239
Misura 28.4	239
Impegno 29	239
Misura 29.1	240
Misura 29.2	240
Misura 29.3	241
VII. Potenziare la comunità di fact-checking	242
Impegno 30	243
Misura 30.1	244
Misura 30.2	250
Misura 30.3	251
Misura 30.4	251
Impegno 31	252
Misura 31.1	253
Misura 31.3	260
Misura 31.4	261
Impegno 32	261
Misura 32.1	262
Misura 32.2	262
Misura 32.3	262
Impegno 33	263
Misura 33.1	263
VIII. Centro per la trasparenza	264
Impegno 34	265
Misura 34.1	265
Misura 34.2	265
Misura 34.3	265
Misura 34.4	266
Misura 34,5	266
Impegno 35	266
Misura 35.1	266
Misura 35.2	267
Misura 35.3	267
Misura 35.4	267
Misura 35,5	267
Misura 35.6	267
Impegno 36	267
Misura 36.1	268
Misura 36.2	268
Misura 36.3	268



IX. Task-Force permanente	269
Impegno 37	270
Misura 37.1	270
Misura 37.2	270
Misura 37.3	270
Misura 37.4	271
Misura 37,5	271
Misura 37,6	271
X. Monitoraggio del codice	272
Impegno 38	273
Misura 38.1	273
Impegno 39	274
Impegno 40	275
Misura 40.1	276
Misura 40.2	276
Misura 40.3	276
Misura 40.4	276
Misura 40.6	276
Impegno 41	276
Misura 41.1	277
Misura 41.2	277
Misura 41.3	277
Impegno 42	277
Impegno 43	278
Impegno 44	279
Guerra di aggressione della Russia all'Ucraina	281
Conflitto Israele - Hamas	295
Elezioni francesi 2024	309
Elezioni presidenziali rumene del 2024	319

Impegni	Misure	Servizio A
II. Controllo delle inserzioni pubblicitarie		
1	Misura 1.1	<input checked="" type="checkbox"/>
	Misura 1.2	<input checked="" type="checkbox"/>
	Misura 1.3	<input checked="" type="checkbox"/>
	Misura 1.4	<input checked="" type="checkbox"/>
	Misura 1.5	<input checked="" type="checkbox"/>
	Misura 1.6	<input checked="" type="checkbox"/>
2	Misura 2.1	<input checked="" type="checkbox"/>
	Misura 2.2	<input checked="" type="checkbox"/>
	Misura 2.3	<input checked="" type="checkbox"/>
	Misura 2.4	<input checked="" type="checkbox"/>
3	Misura 3.1	<input checked="" type="checkbox"/>
	Misura 3.2	<input checked="" type="checkbox"/>
	Misura 3.3	<input checked="" type="checkbox"/>
III. Pubblicità politica		
4	Misura 4.1	<input checked="" type="checkbox"/>
	Misura 4.2	<input checked="" type="checkbox"/>
5	Misura 5.1	<input checked="" type="checkbox"/>
6	Misura 6.1	<input checked="" type="checkbox"/>
	Misura 6.2	<input checked="" type="checkbox"/>
	Misura 6.3	<input checked="" type="checkbox"/>
	Misura 6.4	<input checked="" type="checkbox"/>
	Misura 6.5	<input type="checkbox"/>
7	Misura 7.1	<input checked="" type="checkbox"/>
	Misura 7.2	<input checked="" type="checkbox"/>
	Misura 7.3	<input checked="" type="checkbox"/>
	Misura 7.4	<input checked="" type="checkbox"/>



8	Misura 8.1	<input checked="" type="checkbox"/>
	Misura 8.2	<input checked="" type="checkbox"/>
9	Misura 9.1	<input checked="" type="checkbox"/>
	Misura 9.2	<input checked="" type="checkbox"/>
10	Misura 10.1	<input checked="" type="checkbox"/>
	Misura 10.2	<input checked="" type="checkbox"/>
11	Misura 11.1	<input checked="" type="checkbox"/>
	Misura 11.2	<input checked="" type="checkbox"/>
	Misura 11.3	<input checked="" type="checkbox"/>
	Misura 11.4	<input checked="" type="checkbox"/>
12	Misura 12.1	<input type="checkbox"/>
	Misura 12.2	<input type="checkbox"/>
	Misura 12.3	<input type="checkbox"/>
13	Misura 13.1	<input checked="" type="checkbox"/>
	Misura 13.2	<input checked="" type="checkbox"/>
	Misura 13.3	<input checked="" type="checkbox"/>
IV. Integrità dei servizi		
14	Misura 14.1	<input checked="" type="checkbox"/>
	Misura 14.2	<input checked="" type="checkbox"/>
	Misura 14.3	<input checked="" type="checkbox"/>
15	Misura 15.1	<input checked="" type="checkbox"/>
	Misura 15.2	<input checked="" type="checkbox"/>
16	Misura 16.1	<input checked="" type="checkbox"/>
	Misura 16.2	<input checked="" type="checkbox"/>
V. Responsabilizzare gli utenti		
17	Misura 17.1	<input checked="" type="checkbox"/>
	Misura 17.2	<input checked="" type="checkbox"/>
	Misura 17.3	<input checked="" type="checkbox"/>
18	Misura 18.1	<input checked="" type="checkbox"/>

	Misura 18.2	<input checked="" type="checkbox"/>
	Misura 18.3	<input checked="" type="checkbox"/>
19	Misura 19.1	<input checked="" type="checkbox"/>
	Misura 19.2	<input checked="" type="checkbox"/>
20	Misura 20.1	<input type="checkbox"/>
	Misura 20.2	<input type="checkbox"/>
21	Misura 21.1	<input checked="" type="checkbox"/>
	Misura 21.2	<input checked="" type="checkbox"/>
	Misura 21.3	<input checked="" type="checkbox"/>
22	Misura 22.1	<input type="checkbox"/>
	Misura 22.2	<input type="checkbox"/>
	Misura 22.3	<input type="checkbox"/>
	Misura 22.4	<input type="checkbox"/>
	Misura 22.5	<input type="checkbox"/>
	Misura 22.6	<input type="checkbox"/>
23	Misura 22.7	<input checked="" type="checkbox"/>
	Misura 23.1	<input checked="" type="checkbox"/>
24	Misura 23.2	<input checked="" type="checkbox"/>
	Misura 24.1	<input checked="" type="checkbox"/>
25	Misura 25.1	<input type="checkbox"/>
	Misura 25.2	<input type="checkbox"/>
VI. Responsabilizzare la comunità di ricerca nità		
26	Misura 26.1	<input checked="" type="checkbox"/>
	Misura 26.2	<input checked="" type="checkbox"/>
	Misura 26.3	<input checked="" type="checkbox"/>
27	Misura 27.1	<input checked="" type="checkbox"/>
	Misura 27.2	<input checked="" type="checkbox"/>
	Misura 27.3	<input checked="" type="checkbox"/>
	Misura 27.4	<input checked="" type="checkbox"/>

28	Misura 28.1	<input checked="" type="checkbox"/>
	Misura 28.2	<input checked="" type="checkbox"/>
	Misura 28.3	<input checked="" type="checkbox"/>
	Misura 28.4	<input checked="" type="checkbox"/>
29	Misura 29.1	<input type="checkbox"/>
	Misura 29.2	<input type="checkbox"/>
	Misura 29.3	<input type="checkbox"/>
VII. Potenziamento della comunità di fact-checking		
30	Misura 30.1	<input checked="" type="checkbox"/>
	Misura 30.2	<input checked="" type="checkbox"/>
	Misura 30.3	<input checked="" type="checkbox"/>
	Misura 30.4	<input checked="" type="checkbox"/>
31	Misura 31.1	<input checked="" type="checkbox"/>
	Misura 31.2	<input checked="" type="checkbox"/>
	Misura 31.3	<input checked="" type="checkbox"/>
	Misura 31.4	<input checked="" type="checkbox"/>
32	Misura 32.1	<input checked="" type="checkbox"/>
	Misura 32.2	<input checked="" type="checkbox"/>
	Misura 32.3	<input checked="" type="checkbox"/>
33	Misura 33.1	<input type="checkbox"/>
VIII. Centro per la trasparenza		
34	Misura 34.1	<input checked="" type="checkbox"/>
	Misura 34.2	<input checked="" type="checkbox"/>
	Misura 34.3	<input checked="" type="checkbox"/>
	Misura 34.4	<input checked="" type="checkbox"/>
	Misura 34.5	<input checked="" type="checkbox"/>
35	Misura 35.1	<input checked="" type="checkbox"/>
	Misura 35.2	<input checked="" type="checkbox"/>
	Misura 35.3	<input checked="" type="checkbox"/>

	Misura 35.4	<input checked="" type="checkbox"/>
	Misura 35.5	<input checked="" type="checkbox"/>
	Misura 35.6	<input checked="" type="checkbox"/>
36	Misura 36.1	<input checked="" type="checkbox"/>
	Misura 36.2	<input checked="" type="checkbox"/>
	Misura 36.3	<input checked="" type="checkbox"/>
IX. Task-Force permanente		
37	Misura 37.1	<input checked="" type="checkbox"/>
	Misura 37.2	<input checked="" type="checkbox"/>
	Misura 37.3	<input checked="" type="checkbox"/>
	Misura 37.4	<input checked="" type="checkbox"/>
	Misura 37.5	<input checked="" type="checkbox"/>
	Misura 37.6	<input checked="" type="checkbox"/>
X. Monitoraggio del Codice		
38	Misura 38.1	<input checked="" type="checkbox"/>
39	-	<input checked="" type="checkbox"/>
40	Misura 40.1	<input checked="" type="checkbox"/>
	Misura 40.2	<input checked="" type="checkbox"/>
	Misura 40.3	<input checked="" type="checkbox"/>
	Misura 40.4	<input checked="" type="checkbox"/>
	Misura 40.5	<input checked="" type="checkbox"/>
	Misura 40.6	<input checked="" type="checkbox"/>
41	Misura 41.1	<input checked="" type="checkbox"/>
	Misura 41.2	<input checked="" type="checkbox"/>
	Misura 41.3	<input checked="" type="checkbox"/>
42	-	<input checked="" type="checkbox"/>
43	-	<input checked="" type="checkbox"/>
44	-	<input checked="" type="checkbox"/>



Sintesi

Informazioni su TikTok

La missione di TikTok è ispirare la creatività e portare gioia. In una comunità globale come la nostra, con milioni di utenti, è naturale che le persone abbiano opinioni diverse, quindi cerchiamo di operare sulla base di un insieme condiviso di fatti e realtà quando si tratta di argomenti che hanno un impatto sulla sicurezza delle persone. Garantire un ambiente sicuro e autentico per la nostra comunità è fondamentale per raggiungere i nostri obiettivi, anche per assicurare che i nostri utenti abbiano un'esperienza affidabile su TikTok. Per creare un ambiente affidabile, la trasparenza è essenziale per consentire alle comunità online e alla società in generale di valutare l'approccio di TikTok ai suoi obblighi normativi. TikTok si impegna a fornire informazioni sulle azioni intraprese in qualità di firmatario del Codice di condotta sulla disinformazione (il Codice).

Prendiamo molto sul serio la disinformazione. Ci impegniamo a prevenirla, a promuovere informazioni autorevoli e a investire in iniziative di alfabetizzazione mediatica che creino resistenza nella nostra comunità contro la disinformazione. Su TikTok diamo priorità alla moderazione proattiva dei contenuti e siamo orgogliosi del fatto che la stragrande maggioranza dei contenuti violativi venga identificata e rimossa in modo proattivo prima che riceva visualizzazioni o ci venga segnalata. Nel periodo H2 2024 di questo rapporto, oltre il 98% dei video che violavano le nostre politiche di disinformazione sull'integrità e l'autenticità sono stati rimossi in modo proattivo a livello globale.

Ci impegniamo inoltre a tenere il passo con i comportamenti e i rischi nuovi e in evoluzione che riguardano i nostri utenti. Nell'ambito del programma di conformità al Digital Services Act (DSA), in base al quale il Codice opererà a partire dal luglio 2025, abbiamo implementato una serie di misure volte a garantire la sicurezza dei nostri utenti in una serie di aree chiave, tra cui la disinformazione. Per ulteriori informazioni su queste misure, compreso il modo in cui utilizziamo la tecnologia e impieghiamo i nostri team, consultare il nostro [Hub europeo alla sicurezza online](#) dedicato.

Il nostro lavoro nell'ambito del Codice continua a riflettere il nostro forte impegno a combattere la disinformazione sulla nostra piattaforma e ad essere trasparenti e responsabili nei confronti della nostra comunità in generale sulle misure che adottiamo.

La nostra quinta relazione ai sensi del Codice - dal 1° luglio al 31 dicembre 2024

TikTok è stata fortemente coinvolta e impegnata nel processo del Codice dal 2020. Continuiamo a partecipare attivamente alla task force del Codice e ai suoi gruppi e sottogruppi di lavoro attivi, in particolare all'H2 per quanto riguarda la conversione del COPD in un codice di condotta ai sensi della DSA e lo sviluppo/attivazione dell'RRS per le elezioni. Continuiamo a co-presiedere il gruppo di lavoro sulle elezioni e ricopriamo la posizione di co-presidente del gruppo di lavoro sulla trasparenza dal settembre 2023.

In linea con i nostri rapporti precedenti, questo quinto rapporto continua a fornire informazioni dettagliate sulle misure che attuiamo per combattere la disinformazione in conformità con i nostri impegni, insieme a dati completi e granulari a sostegno di tali misure. Alcune delle misure descritte sono state attuate al di fuori degli Stati membri dell'UE, ad esempio nei Paesi candidati all'adesione all'UE e nelle nazioni con significative comunità di diaspora residenti nell'UE. Pur fuori dai confini dell'UE, queste azioni dovrebbero avere un impatto positivo nel limitare la diffusione della disinformazione all'interno dell'UE stessa.

Con oltre la metà della popolazione mondiale che si reca alle urne, il 2024 rappresenta un anno significativo per le elezioni e i processi civici. Le elezioni comportano un'intensificazione del discorso civico sulle piattaforme online. Siamo quindi consapevoli dei rischi elevati che si corrono in questi periodi elettorali, compresi i tentativi di promuovere in modo non autentico narrazioni polarizzanti o di influenzare l'opinione pubblica. Durante questi processi civici, TikTok si concentra sulla sicurezza delle persone e sulla protezione dell'integrità della piattaforma TikTok.

Lo facciamo applicando una serie di politiche solide volte a prevenire la diffusione della disinformazione, valorizzando le informazioni autorevoli provenienti da fonti attendibili e collaborando con esperti che ci aiutano



valutare e migliorare il nostro approccio. Questo rapporto fornisce informazioni sulle risorse significative che abbiamo dedicato alla protezione dell'integrità della nostra piattaforma durante questo periodo. Include anche due rapporti specifici post-elettorali per le elezioni lampo francesi e le elezioni presidenziali rumene.

Tra le misure di mitigazione che abbiamo attuato in questo periodo critico, ricordiamo: la gestione di Centri di controllo della missione per fornire una copertura coerente e dedicata a potenziali questioni legate alle elezioni; la partecipazione al Sistema di risposta rapida del Codice per semplificare lo scambio di informazioni tra le organizzazioni della società civile, i fact-checker e le piattaforme; l'espansione del nostro Programma di verifica dei fatti (ora collaboriamo strettamente con 14 organizzazioni di verifica dei fatti accreditate dall'IFCN nell'UE); il lancio di campagne di alfabetizzazione mediatica localizzate.

Sono inoltre in corso due conflitti (Israele/Hamas e Russia/Ucraina), con la condivisione online di una quantità significativa di dialoghi e di opinioni politiche contrastanti relative ai conflitti, e con ciò la potenziale diffusione di disinformazione. Vengono forniti rapporti di crisi individuali con informazioni specifiche sulla nostra risposta al conflitto tra Israele e Hamas e alla guerra in Ucraina.

Siamo orgogliosi dei nostri continui sforzi per proteggere la nostra comunità dalla disinformazione, dotandola degli strumenti per orientarsi tra le tendenze emergenti della disinformazione e delle competenze necessarie per valutare l'accuratezza delle informazioni che incontra.

Le nostre politiche

Le nostre politiche di integrità e autenticità sono state concepite per contribuire a promuovere un'esperienza affidabile e autentica per i nostri utenti. Abbiamo politiche rigorose su specifici tipi di disinformazione¹ e comportamenti ingannevoli, nonché su contenuti ingannevoli generati dall'intelligenza artificiale, teorie cospirative, reti di Covert Influence Operations (CIO) ed eventi di sicurezza pubblica come i disastri naturali. Non permettiamo contenuti falsi o fuorvianti che possano causare danni significativi agli individui o alla società, indipendentemente dalle intenzioni. Le nostre politiche sono state elaborate con cura per coprire un'ampia gamma di contenuti e la natura in costante evoluzione delle tendenze della disinformazione, spesso basate su ciò che sta accadendo nel mondo. Affrontiamo anche i comportamenti ingannevoli rimuovendo gli account che cercano di ingannare le persone o che si impegnano nella manipolazione della piattaforma.

Continuiamo a rivedere e sviluppare le nostre politiche. Nella seconda metà del 2024 abbiamo introdotto una nuova politica granulare per gli annunci di disinformazione sul clima e abbiamo perfezionato le politiche esistenti, tra cui le nostre politiche sul Fake Engagement, le linee guida sulla Deceptive Personas e abbiamo ampliato le nostre politiche sull'impersonalità.

Applicare le nostre politiche

La moderazione della disinformazione online è complessa e ricca di sfumature. Per moderare efficacemente i contenuti in lingua europea su scala, continuiamo a rafforzare il nostro processo di revisione automatica e a investire nella formazione dei nostri team Trust e Safety. Forniamo trasparenza alla nostra comunità su [come moderiamo](#) e su quali [azioni di moderazione intraprendiamo](#). Questo include informazioni dettagliate sui contenuti che rendiamo [non ammissibili per il feed For You](#). In questo rapporto rendiamo note le metriche sottostanti.

Ci affidiamo alla moderazione automatica quando i nostri sistemi hanno un alto grado di certezza che il contenuto sia violativo, ma la disinformazione presenta sfide uniche. È molto complessa, si evolve rapidamente e può richiedere un contesto, per cui il contesto e il fact-checking sono fondamentali. Sebbene utilizziamo modelli di apprendimento automatico per individuare la potenziale disinformazione, il nostro approccio prevede che il nostro team specializzato nella moderazione della disinformazione valuti, confermi e rimuova le violazioni dannose della disinformazione. I nostri moderatori hanno accesso a [partner indipendenti di fact-checking](#) e al nostro database globale di affermazioni precedentemente verificate per valutare l'accuratezza dei contenuti.

¹ Su TikTok interveniamo per moderare o rimuovere i contenuti contenenti disinformazione dannosa, a prescindere dall'intento (ossia se il contenuto in questione sia o meno una disinformazione), in conformità alle nostre Linee guida della comunità. Ai fini dell'allineamento con il Codice, in questa relazione utilizziamo "disinformazione" e "disinformazione". "disinformazione" in modo intercambiabile.



Ci occupiamo anche di disinformazione rimuovendo gli account che pubblicano ripetutamente informazioni errate che violano le nostre politiche e disponiamo di team di esperti che monitorano costantemente le campagne di disinformazione, i comportamenti non autentici e le operazioni di influenza.

Trasparenza e controllo della pubblicità

Siamo lieti di aver lanciato una nuova politica di annunci di disinformazione sul clima nel SEE alla fine del 2024. Questa si aggiunge alle [politiche](#) esistenti che vietano comportamenti fuorvianti, non autentici e ingannevoli e, in particolare, alla nostra [politica sulla disinformazione](#) che copre la disinformazione pericolosa, la disinformazione medica, le teorie cospirative pericolose e i media sintetici e manipolati. Lavoriamo costantemente per migliorare l'implementazione e l'applicazione delle nostre politiche pubblicitarie e valutiamo costantemente nuove aree di interesse per le quali sviluppare ulteriori politiche.

Come tutti gli utenti della nostra piattaforma, i partecipanti ai programmi di monetizzazione dei contenuti devono attenersi alle nostre Linee guida della comunità, comprese le nostre politiche di integrità e autenticità. Tali politiche chiariscono che non consentiamo attività che possano minare l'integrità della nostra piattaforma o l'autenticità dei nostri utenti. Esse chiariscono inoltre che rimuoviamo i contenuti o gli account, compresi quelli dei creatori, che contengono informazioni fuorvianti che causano danni significativi o comportamenti ingannevoli. In alcuni casi, possiamo rimuovere l'accesso di un creatore a una funzione di monetizzazione dei creatori. Il nostro [Codice di per i creatori condotta](#) definisce gli standard che ci aspettiamo dai creatori coinvolti nei programmi, nelle funzionalità, negli eventi e nelle campagne di TikTok, sia sulla piattaforma che al di fuori di essa, anche in relazione alle attività di disinformazione.

Continuiamo a collaborare con le parti interessate esterne per aumentare l'efficacia del nostro controllo degli inserimenti pubblicitari su TikTok. Abbiamo continuato ad ampliare le funzionalità (comprese le possibilità di scelta e le abilità) del filtro TikTok Inventory, il nostro strumento interno di sicurezza pre-campagna (che ora è disponibile in 29 giurisdizioni del SEE), continuiamo a offrire soluzioni di brand safety e suitability di terze parti ai nostri inserzionisti (come DoubleVerify, Integral Ad Science e Zefr) e abbiamo migliorato la nostra certificazione IAB Swedish Gold Standard portandola a 2.0.

Vietare gli annunci politici

TikTok è prima di tutto una piattaforma di intrattenimento e siamo orgogliosi di essere un luogo che riunisce le persone attraverso contenuti creativi e divertenti. Sebbene la condivisione di convinzioni politiche e la partecipazione a conversazioni politiche siano consentite come contenuti organici su TikTok, le nostre politiche vietano alla nostra comunità, compresi gli account di politici e partiti politici, di inserire [annunci politici](#) o pubblicare [contenuti politici a marchio](#). Inoltre, impediamo [ai governi, ai politici e agli account dei partiti politici](#) di accedere alle nostre funzioni di monetizzazione e di raccolta fondi per le campagne (con un'eccezione limitata agli annunci di servizio pubblico gestiti dal governo, come le campagne sanitarie).

Ci siamo concentrati sull'applicazione del nostro divieto di pubblicità politica prima dell'entrata in vigore della maggior parte delle disposizioni del Regolamento UE sulla trasparenza e l'orientamento della pubblicità politica a partire dall'ottobre 2025.

Vietando la pubblicità politica, la raccolta di fondi per le campagne e limitando l'accesso ad alcune funzioni di monetizzazione, cerchiamo di trovare un equilibrio tra il permettere alle persone di discutere le questioni rilevanti per la loro vita e il proteggere la piattaforma creativa e divertente che la nostra comunità desidera.

Garantire l'integrità dei servizi

Le nostre politiche di Integrità e Autenticità ([politiche I&A](#)) vietano rigorosamente i comportamenti ingannevoli e ci impegniamo a ridurre al minimo le pratiche di manipolazione non consentite. Rimaniamo estremamente vigili di fronte all'evoluzione delle tattiche, delle tecniche e delle procedure di disinformazione impiegate da attori malintenzionati, come illustrato in dettaglio nell'Impegno 14. Per combattere efficacemente queste minacce, valutiamo e perfezioniamo continuamente le nostre politiche. Per combattere efficacemente queste minacce, valutiamo e perfezioniamo continuamente le nostre politiche, assicurandoci che rimangano solide e rispondenti alle sfide emergenti nel settore dell'informazione.



ecosistema. Attraverso un monitoraggio e un'applicazione proattivi, miriamo a salvaguardare l'integrità della nostra piattaforma e a proteggere gli utenti da operazioni di influenza dannose.

In particolare, notiamo che se da un lato l'intelligenza artificiale (AI) consente incredibili opportunità creative, dall'altro può potenzialmente confondere o fuorviare gli spettatori se non sono consapevoli che il contenuto è stato generato o modificato con l'AI. La nostra politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC) riguarda l'uso di contenuti creati o modificati dall'intelligenza artificiale sulla nostra piattaforma. Per favorire esperienze autentiche e trasparenti per la nostra comunità, incoraggiamo i creatori a etichettare i contenuti completamente generati o modificati dall'IA e a dichiarare quando i loro contenuti mostrano scene realistiche. Oltre all'[etichetta generata dall'IA](#) che consente ai creatori di divulgare l'AIGC, implementiamo la tecnologia [Content Credentials](#) della Coalition for Content Provenance and Authenticity (C2PA), che consente ai nostri sistemi di riconoscere ed etichettare automaticamente l'AIGC che ha avuto origine su altre importanti piattaforme.

Continuiamo inoltre a lottare contro le operazioni di influenza occulta (CIO) e non permettiamo tentativi di influenzare l'opinione pubblica ingannando i sistemi o la comunità della nostra piattaforma sull'identità, l'origine, la sede operativa, la popolarità o lo scopo dell'account. Per contrastare le minacce emergenti e rimanere al passo con l'evoluzione delle sfide, disponiamo di team di esperti che si concentrano interamente sull'individuazione, l'investigazione e l'interruzione delle operazioni di influenza occulta. Questi team seguono e analizzano i segnali di comportamento ingannevole presenti sulla piattaforma, nonché gli indizi provenienti da fonti esterne. Collaborano anche con fornitori esterni di intelligence per supportare indagini specifiche caso per caso. Per fornire aggiornamenti più regolari e dettagliati sulle CIO che distruggiamo, abbiamo un rapporto di trasparenza dedicato alle CIO, [disponibile nel Centro per la trasparenza di TikTok](#), in cui pubblichiamo informazioni sulle operazioni che abbiamo precedentemente rimosso e che hanno tentato di tornare sulla nostra piattaforma con nuovi account.

TikTok è inoltre orgogliosa di partecipare attivamente al sistema di risposta rapida del Codice, al fine di semplificare lo scambio di informazioni tra le organizzazioni della società civile, i verificatori e le piattaforme online.

Responsabilizzare gli utenti

Oltre a intervenire sui contenuti generati dagli utenti che violano le nostre linee guida, lavoriamo costantemente per scoraggiare la disinformazione in modo proattivo, mettendo a disposizione della nostra comunità risorse che li aiutino a riconoscere la disinformazione, a valutare i contenuti in modo critico e a fare segnalazioni sui contenuti violati. In Europa offriamo alla nostra comunità strumenti di segnalazione online e all'interno dell'app facili da usare, in modo che possano segnalarci contenuti o account che ritengono possano violare le nostre Linee guida della comunità o infrangere la legge. I contenuti segnalati come illegali saranno esaminati in base alle nostre politiche e, se viene rilevata una violazione, i contenuti potranno essere rimossi a livello globale.

Abbiamo dedicato risorse significative ad aumentare il numero di strumenti di intervento in-app che forniscono agli utenti un contesto aggiuntivo su determinati contenuti, li invitano a riconsiderare la condivisione di certi contenuti, li reindirizzano verso informazioni autorevoli e li incoraggiano a segnalarci direttamente qualsiasi potenziale disinformazione. Continuiamo a rivedere gli argomenti per i quali sviluppiamo interventi, tra cui le elezioni, il cambiamento climatico, la guerra in Ucraina e il conflitto tra Israele e Hamas. Questi strumenti sono disponibili in 23 lingue ufficiali dell'UE e in norvegese e islandese per gli utenti del SEE.

Siamo impegnati in una serie di campagne di alfabetizzazione mediatica su e fuori piattaforma in stretta collaborazione con partner esterni, ad esempio i nostri partner per il fact-checking e l'alfabetizzazione mediatica in relazione alle elezioni. Durante il periodo di riferimento, abbiamo condotto 14 campagne temporanee di alfabetizzazione mediatica, tutte con Centri elettorali in-app, prima delle elezioni regionali. I Centri elettorali sono stati visitati più di 4,1 milioni di volte durante il periodo di riferimento.

Crediamo che la collaborazione contribuisca a rafforzare i nostri sforzi per mitigare i danni e gli abusi sulla nostra piattaforma. Per informare meglio il nostro approccio alle prossime elezioni, abbiamo organizzato 9 Election Speaker Series, 7 negli Stati membri dell'UE e 2 in Georgia e Moldavia, invitando esperti esterni, anche comunità di fact-checking, a condividere le loro intuizioni e la loro esperienza di mercato con i nostri team interni.



Durante la COP29 è stata inoltre lanciata una campagna globale di alfabetizzazione mediatica per sensibilizzare gli utenti e dotarli di capacità di pensiero critico, indipendentemente da qualsiasi partnership specifica. Abbiamo anche introdotto delle guide di ricerca sull'alfabetizzazione mediatica, adattate alle regioni colpite da eventi significativi. Queste guide sono state lanciate in Europa centrale e orientale in risposta alle inondazioni, coprendo Paesi come la Cechia, la Polonia, la Romania, l'Austria, l'Ungheria, la Slovacchia, la Germania e la Moldavia. Iniziative simili sono state intraprese in Portogallo per gli incendi, in Spagna per le inondazioni e a Mayotte per un ciclone.

Continuiamo inoltre a [contrastare i tentativi di influenza](#), anche rendendo gli account dei media affiliati allo Stato che tentano di raggiungere le comunità al di fuori del loro Paese di origine su eventi e questioni globali di attualità non ammissibili alla raccomandazione nei feed "Per te" dei nostri utenti e vietando agli account dei media affiliati allo Stato in tutti i mercati in cui sono disponibili le nostre etichette dei media controllati dallo Stato, compresa l'UE, di fare pubblicità al di fuori del Paese con cui sono principalmente affiliati. Ci impegniamo a fornire ai nostri utenti trasparenza sui nostri sistemi e sulle nostre attività di I&A. Continuiamo a espandere il nostro Centro per la trasparenza con risorse come il nostro primo Hub per l'integrità delle elezioni negli Stati Uniti, l'Hub per l'integrità delle elezioni in Europa, rapporti dedicati sull'influenza occulta e un nuovo blog del Centro per la trasparenza.

Responsabilizzare i ricercatori

Riconosciamo l'importanza del ruolo dei ricercatori nel contribuire a identificare le tendenze e le pratiche di disinformazione. Pubblichiamo [rapporti sull'applicazione delle linee guida della comunità](#) trimestrali per fornire informazioni continue sulle azioni che intraprendiamo contro i contenuti e gli account che violano le nostre linee guida della comunità, i termini di servizio e le politiche pubblicitarie. Nell'ambito dei nostri continui sforzi per semplificare lo studio della piattaforma TikTok, il report offre anche l'accesso a dati aggregati in un file scaricabile. Manteniamo, e continuiamo a perfezionare, la nostra [API di ricerca](#) (che fornisce ai ricercatori in Europa l'accesso ai dati pubblici sui contenuti e sugli account della nostra piattaforma), nonché la nostra [API di contenuti commerciali](#) (che porta trasparenza alla pubblicità a pagamento e ad altri contenuti di natura commerciale su TikTok) e la Biblioteca di contenuti commerciali (un database di annunci dell'UE ricercabile pubblicamente con informazioni sugli annunci a pagamento e metadati sugli annunci). Continuiamo inoltre a perfezionare il [Virtual Compute Environment](#) (VCE), che offre un accesso più ampio ai dati degli utenti per qualificare i ricercatori non accademici senza scopo di lucro a interrogare e analizzare i dati applicabili, garantendo al contempo solide protezioni di sicurezza e privacy.

Ci impegniamo a garantire la trasparenza su come operiamo, moderiamo e raccomandiamo i contenuti, diamo potere agli utenti e proteggiamo la nostra piattaforma. Per questo motivo abbiamo aperto i nostri Transparency and Accountability Centers (TAC) globali per consentire agli ospiti invitati di vedere in prima persona il nostro lavoro per proteggere la sicurezza della piattaforma TikTok. I TAC offrono l'opportunità a ricercatori e altri esperti di vedere in prima persona come i team di TikTok svolgono il lavoro importantissimo di garantire la sicurezza, i dati e la privacy della nostra comunità.

Potenziare la comunità del Fact-Checking

TikTok riconosce l'importante contributo dei nostri partner di fact-checking nella lotta contro la disinformazione. Nel corso dell'anno H2 abbiamo accolto due nuovi partner di fact-checking e abbiamo ampliato la nostra copertura di fact-checking a una serie di paesi europei e candidati all'UE con i partner di fact-checking esistenti. Ora lavoriamo a stretto contatto con 14 organizzazioni di fact-checking [accreditate dall'IFCN](#) in tutta l'UE, il SEE e l'Europa in generale, che dispongono di formazione tecnica, risorse e conoscenze di settore per valutare in modo imparziale la disinformazione online.

Il nostro programma di fact-checking incorpora il contributo dei fact-checker nel nostro più ampio impegno di moderazione dei contenuti. I fact-checker non moderano direttamente i contenuti su TikTok, ma valutano se un'affermazione è vera, falsa o non comprovata. Inoltre, condividono rapporti di approfondimento proattivi che ci aiutano a individuare la disinformazione dannosa e ad anticipare le tendenze della disinformazione. Il feedback dei fact-checker viene trasmesso ai team di moderazione di TikTok, che possono così assicurarsi che sia preso in considerazione nel loro lavoro di moderazione e adottare le azioni pertinenti in base alle nostre linee guida della comunità. Questo approccio produce di fatto un moltiplicatore di forze per il risultato del fact-checking, assicurando che il contenuto o la tendenza alla disinformazione siano affrontati in modo più completo e ampio. Il nostro archivio di fact-checking in espansione garantisce che i nostri team e sistemi utilizzino appieno le informazioni fornite dai nostri partner di fact-checking su TikTok.



Guardare avanti

TikTok mantiene il suo impegno nei confronti del Codice, che entrerà in vigore come Codice di condotta nell'ambito delle DSA a partire da luglio 2025.

Ci auguriamo una collaborazione continua e significativa con l'industria, la società civile e le autorità dell'UE per salvaguardare insieme l'integrità delle nostre piattaforme. Condividendo le competenze, rafforzando le politiche e migliorando i meccanismi di applicazione, intendiamo impedire ai cattivi attori di sfruttare gli spazi digitali attraverso comportamenti ingannevoli e la diffusione di disinformazione dannosa.



II. Controllo degli annunci su Impegni 1 - 3



II. Controllo delle inserzioni pubblicitarie	
Impegno 1	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Si/No]	Si



<p>Se sì, elencare queste misure di attuazione [brevi punti elenco].</p> <p>Guida all'identificazione delle politiche. Migliorare l'identificazione. Miglioramento dell'applicazione delle politiche stesse (non della loro formulazione).</p>	<ul style="list-style-type: none"> ● Per migliorare la granularità delle politiche pubblicitarie esistenti, è stata sviluppata una politica pubblicitaria specifica per la disinformazione sul clima. ● Abbiamo continuato ad applicare le nostre quattro politiche per gli annunci di disinformazione dannosa nel SEE. Come indicato nel nostro rapporto H2 2023, le politiche riguardano: <ul style="list-style-type: none"> ○ Misinformazione medica ○ Pericolosa disinformazione ○ Media sintetici e manipolati ○ Pericolose teorie cospiratorie ● Ampliamento delle funzionalità (comprese la scelta e la capacità) nel SEE del nostro strumento interno di brand safety pre-campagna, il TikTok Inventory Filter. ● Abbiamo migliorato la nostra certificazione IAB per lo Sweden Gold Standard portandola a 2.0. ● Continuiamo a partecipare alla task force e ai suoi gruppi e sottogruppi di lavoro, come il sottogruppo di lavoro sulle elezioni (risposta alle crisi).
--	---



Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Si/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto.
Misura 1.1	



QRE 1.1.1

Per mantenere la nostra piattaforma accogliente e autentica per tutti, ci impegniamo a garantire che sia priva di disinformazione dannosa.

(I) Le nostre politiche e il nostro approccio

Le nostre politiche di Integrità e Autenticità (I&A) all'interno delle nostre CG sono la prima linea di difesa per combattere la disinformazione dannosa e i comportamenti ingannevoli sulla nostra piattaforma. Tutti gli utenti sono tenuti a rispettare le nostre CG, che stabiliscono le circostanze in cui rimuoveremo o limiteremo in altro modo la disponibilità dei contenuti.

Anche gli annunci a pagamento sono soggetti alle nostre [politiche sugli annunci](#) e vengono esaminati rispetto a tali politiche prima di essere ammessi sulla nostra piattaforma. Le nostre politiche sugli annunci vietano specificamente i contenuti imprecisi, fuorvianti o falsi che possono causare danni significativi agli individui o alla società, indipendentemente dalle intenzioni. Vietano inoltre altri comportamenti fuorvianti, non autentici e ingannevoli. Gli annunci ritenuti in violazione di queste politiche non saranno consentiti sulla nostra piattaforma e gli account ritenuti in grave o ripetuta violazione potranno essere sospesi o bannati.

Nel 2023, al fine di migliorare le nostre politiche pubblicitarie esistenti, abbiamo lanciato quattro politiche granulari nel SEE. Le politiche riguardano:

- Misinformazione medica
- Pericolosa disinformazione
- Media sintetici e manipolati
- Pericolose teorie cospiratorie

Abbiamo lavorato costantemente per migliorare l'implementazione di queste politiche e per riflettere sull'opportunità di sviluppare nuove politiche in altre aree mirate. Alla fine del 2024 abbiamo lanciato una quinta politica pubblicitaria granulare che riguarda la disinformazione sul clima. Essa vieta le affermazioni false o fuorvianti relative al cambiamento climatico, come ad esempio negare l'esistenza e gli impatti del cambiamento climatico, affermare falsamente che gli impatti a lungo termine delle strategie di mitigazione del clima sono peggiori di quelli dei cambiamenti climatici o minare la validità o la credibilità di dati o ricerche che documentano un consenso scientifico consolidato.

Le nostre [politiche pubblicitarie](#) richiedono agli inserzionisti di soddisfare una serie di requisiti relativi alla pagina di destinazione. Ad esempio, la pagina di destinazione deve essere funzionante e deve contenere informazioni complete e accurate, anche sull'inserzionista. Gli annunci rischiano di non essere approvati se il prodotto o il servizio pubblicizzato sulla pagina di destinazione non corrisponde a quello incluso nell'annuncio.

In linea con il nostro approccio di costruire una piattaforma che unisca le persone e non le divida, da tempo [vietiamo gli annunci politici](#) e i [contenuti a marchio politici](#). In particolare, [non sono consentiti annunci a pagamento](#) (né landing page) che promuovano o si oppongano a un candidato, a un leader in carica, a un partito o a un gruppo politico, né contenuti che sostengano una posizione (favorevole o contraria) su una questione locale, statale o federale di importanza pubblica al fine di influenzare una decisione o un risultato politico. Regole simili si applicano ai contenuti di marca. Abbiamo inoltre classificato alcuni account come [account governativi, politici e di partiti politici \(GPPPA\)](#) e abbiamo introdotto restrizioni a livello di account. Ciò significa che gli account appartenenti a governi, politici e partiti politici vedranno automaticamente disattivato l'accesso alle funzioni pubblicitarie. Facciamo eccezioni per i governi in determinate circostanze, ad esempio per promuovere la salute pubblica. Mettiamo a disposizione degli inserzionisti diversi strumenti per la sicurezza del marchio, per aiutarli a garantire che i loro annunci non vengano inseriti in un sito web.



	<p>adiacenti a contenuti che non ritengono in linea con i valori del loro marchio. Sebbene i contenuti che violano le nostre CG, comprese le nostre politiche di I&A, vengano rimossi, gli strumenti di brand safety sono pensati per aiutare gli inserzionisti a proteggere ulteriormente il loro marchio. Ad esempio, un marchio orientato alla famiglia potrebbe non voler apparire accanto a video contenenti contenuti di attualità. A sostegno di questi principi abbiamo adottato il quadro di riferimento accettato dal settore.</p> <p>(II) Verifica nel contesto delle inserzioni pubblicitarie</p> <p>Forniamo badge verificati su alcuni account, compresi alcuni inserzionisti. I badge verificati aiutano gli utenti a fare scelte informate sugli account che scelgono di seguire. È un modo semplice per le figure di spicco di far sapere agli utenti stanno vedendo contenuti autentici e contribuisce a creare fiducia tra gli account di alto profilo e i loro follower. Per i singoli, le organizzazioni non profit, le istituzioni, le aziende o le pagine ufficiali dei marchi, questo badge crea un importante livello di chiarezza con la comunità di TikTok. Prima di assegnare un badge verificato, consideriamo una serie di fattori, come il fatto che l'account di rilievo sia autentico, unico e attivo.</p> <p>Rafforziamo il nostro approccio per contrastare i tentativi di influenza</p> <ul style="list-style-type: none"> • Rendere gli account dei media affiliati allo Stato che tentano di raggiungere le comunità al di fuori del loro Paese su eventi e questioni globali attuali non ammissibili alla raccomandazione, il che significa che i loro contenuti non appariranno nel feed "Per te". • Vietare agli account dei media affiliati allo Stato in tutti i mercati in cui sono disponibili le nostre etichette dei media controllati dallo Stato di fare pubblicità al di fuori del Paese con cui sono principalmente affiliati. • Investire nelle nostre capacità di rilevamento degli account dei media affiliati allo Stato. • Collaborare con esperti esterni di terze parti per definire la nostra politica sui media affiliati allo Stato e la valutazione delle etichette dei media controllati dallo Stato.
<p>SLI 1.1.1 - Numeri da azioni che applicano le politiche di cui sopra (specificare se a livello di pagina e/o di dominio)</p>	<p>Metodologia di misurazione dei dati:</p> <p>Abbiamo indicato il numero di annunci che sono stati rimossi dalla nostra piattaforma per violazione delle nostre politiche sui contenuti politici, nonché le nostre politiche più granulari sulla disinformazione medica, sulla disinformazione pericolosa, sui media sintetici e manipolati e sulle teorie cospirative pericolose. Abbiamo lanciato la nostra politica di disinformazione climatica granulare verso la fine del periodo di riferimento e ci auguriamo di poter condividere i dati su di essa una volta che avremo un periodo di riferimento completo.</p> <p>La maggior parte degli annunci che violano le nostre precedenti quattro, ora cinque, politiche sulla disinformazione granulare, sarebbero stati rimossi in base alle nostre politiche esistenti. Nei casi in cui un annuncio è ritenuto violativo per altre politiche e anche per le nostre più recenti politiche di disinformazione granulare, la rimozione viene conteggiata in base alla politica esistente. Pertanto, la seconda colonna qui sotto mostra solo il numero di annunci rimossi quando l'unico motivo era una delle quattro politiche di disinformazione aggiuntive segnalate, e non include gli annunci già rimossi in base alle nostre politiche esistenti o quando le politiche di disinformazione non sono state il fattore trainante della rimozione.</p>



	<p>Ci siamo concentrati sull'applicazione del nostro divieto di pubblicità politica e sulla nostra capacità di rilevamento interno dei contenuti politici sulla nostra piattaforma, che ha incluso il lancio di strategie di formazione e automoderazione dei moderatori di contenuti politici. I dati riportati di seguito suggeriscono che le nostre politiche esistenti (come quella sui contenuti politici e altre aree di policy come quella sui contenuti inaccurati, fuorvianti o falsi) coprono già la maggior parte degli annunci di disinformazione dannosi, grazie alla loro natura espansiva di copertura.</p> <p>Si noti che i numeri sono stati forniti solo per i mercati monetizzati e si basano su dove sono stati visualizzati gli annunci. Notiamo che il periodo H2 2024 ha coperto un ciclo elettorale molto intenso in Europa, anche in Romania, Francia e Irlanda.</p>	
	Numero di rimozioni di annunci in base alla politica degli annunci a contenuto politico	Numero di rimozioni di annunci in base alle <u>quattro</u> politiche sugli annunci di disinformazione <u>granulari</u>
Stati membri		
Austria	746	3
Belgio	1,152	1
Bulgaria	328	7
Croazia	3	0
Cipro	128	0
Repubblica Ceca	111	0
Danimarca	409	0
Estonia	90	0
Finlandia	235	0
Francia	4,621	7
Germania	6,498	63



Grecia	911	8
Ungheria	512	2
Irlanda	565	1
Italia	2,781	8
Lettonia	131	4
Lituania	19	0
Lussemburgo	86	0
Malta	N/D	N/D
Paesi Bassi	1,179	3
Polonia	1,118	4
Portogallo	438	1
Romania	10,698	2
Slovacchia	145	4
Slovenia	52	0
Spagna	2,558	17
Svezia	752	0
Islanda	N/D	N/D
Liechtenstein	N/D	N/D
Norvegia	474	2



Totale UE	36,266	135
Totale SEE	36,740	137

Questo indicatore aggiuntivo del livello di servizio fornisce una stima del valore finanziario delle azioni intraprese dai Firmatari per demonetizzare le fonti di disinformazione (ai sensi dello SLI 1.1.1). Si basa sulle metriche dei media a disposizione dei Firmatari (query/bid² o impression³) e sull'applicazione di un fattore di conversione concordato fornito da una terza parte designata dalla task force del Codice (Ebiquity plc.).

² Richiesta posta tra un venditore e un acquirente di pubblicità che può specificare, tra l'altro, sito web, contenuto specifico, dati di targeting comprensivi di pubblico o contenuto.
³ Calcolo completo del numero di persone che sono state raggiunte da un contenuto mediatico tramite esposizione passiva (visualizzazione di un) o coinvolgimento attivo (visita di una destinazione).



SLI 1.1.2 -	<p>La task force permanente del Codice di condotta dell'UE ha incaricato Ebiquity Plc di svolgere il ruolo di "stimatore terzo", responsabile di fornire fattori di conversione periodici del Costo per Mille ("CPM") che i firmatari potranno utilizzare per ricavare stime finanziarie esclusivamente in relazione a questa SLI. Questo SLI applica il fattore di conversione sviluppato da Ebiquity alle impressioni degli annunci che sono stati rimossi dalla nostra piattaforma e mira a fornire una stima del valore non realizzato dei ricavi legati alla demonetizzazione della disinformazione.</p> <p>I dati CPM sono forniti su base specifica per i mercati dell'UE, ove disponibili, e attualmente coprono 26 dei 27 mercati dell'UE (escluso il Lussemburgo). Si noti che abbiamo fornito i numeri solo per i mercati monetizzati, in base a dove sono stati visualizzati gli annunci.</p> <p>Ebiquity crea le stime del CPM sulla base di dati aggregati e anonimizzati sugli investimenti media provenienti dal Media Data Vault, l'infrastruttura di database proprietaria utilizzata per servire i propri clienti. Ebiquity ha sviluppato tre CPM dedicati ai canali (Programmatic - Display, Programmatic - Online Video e Paid Social) e un CPM misto, che può essere utilizzato per applicazioni generali e non è identificabile con alcun cliente, agenzia, fornitore, piattaforma o formato pubblicitario specifico.</p> <p>Abbiamo calcolato il valore finanziario approssimativo utilizzando il valore "Blended CPM" fornito da Ebiquity. Notiamo che questo SLI fornisce solo un valore finanziario approssimativo e non riflette il modo in cui TikTok monetizza i contenuti pubblicitari nella pratica. Non è quindi una rappresentazione accurata delle entrate effettive di TikTok.</p> <p>TikTok non ha partecipato allo sviluppo del fattore di conversione e non può quindi approvarlo, né la metodologia e i dati sottostanti. Rimaniamo impegnati ad aumentare la trasparenza in questo capitolo, anche partecipando al gruppo di lavoro per comprendere meglio la metodologia sottostante e garantire che il fattore di conversione fornisca, nel modo più accurato possibile, un'approssimazione del valore finanziario delle azioni intraprese per demonetizzare la disinformazione. Si noti che la maggior parte dei fattori di conversione forniti da Ebiquity sono aumentati rispetto all'ultimo rapporto.</p>			
	Valore in euro degli annunci demonetizzati			
	Numero di impressioni per gli annunci rimossi in base all'informativa sugli annunci di contenuto politico	Numero di impressioni per gli annunci rimossi in base alle politiche di disinformazione granulari	Conversione di Ebiquity	Euro Valore di Annunci Demonetizzati/1000 (conteggio del costo per mille)



Austria	2,405,688	0	4	9622.752
Belgio	414,078	16,971	5.5	2370.7695
Bulgaria	21,839	0	1.5	32.7585
Croazia	69	0	3.5	0.2415
Cipro	10,838	0	2.5	27.095
Repubblica Ceca	187,494	0	4	749.976
Danimarca	1,333,325	12,268	4.5	6055.1685
Estonia	14,889	0	2.5	37.2225
Finlandia	7,543,943	0	4	30175.772
Francia	14,427,406	510	4	57711.664
Germania	45,161,261	0	4.5	203225.6745
Grecia	512,170	12,873	1.5	787.5645
Ungheria	3,675,505	0	2	7351.01
Irlanda	1,341,419	0	3	4024.257



Italia	6,836,564	12,029	3.5	23970.0755
Lettonia	4,551	0	3	13.653
Lituania	59,348	0	2.5	148.37
Lussemburgo	5,472	0	0	0
Malta	N/D	N/D	3	0
Paesi Bassi	879,250	1,048	5	4401.49
Polonia	610,009	0	1.5	915.0135
Portogallo	409,358	0	2.5	1023.395
Romania	27,208,895	0	1.5	40813.3425
Slovacchia	52,215	0	2.5	130.5375
Slovenia	53,989	0	2	107.978
Spagna	9,622,981	8,551	3	28894.596
Svezia	4,565,753	0	4.5	20545.8885
Islanda	N/D	N/D	3	0



Liechtenstein	N/D	N/D	0	0
Norvegia	120,449	1,367	5.5	669.988
Totale UE	127,358,309	64,250	N/D	443,136.27
Totale SEE	127,478,758	65,517	N/D	443,806.25

Misura 1.2	
QRE 1.2.1	<p>Tutti i creatori devono rispettare le Linee guida della community di TikTok, comprese le nostre politiche I&A. La mancata osservanza delle Linee guida della community da parte dei creatori può comportare la perdita dell'accesso alla monetizzazione e/o la perdita dell'accesso all'account. Gli utenti di tutti gli Stati membri dell'Unione Europea vengono avvisati tramite una notifica in-app nella loro lingua locale in caso di limitazione della loro capacità di monetizzare, di limitazione dell'accesso a una funzione, di rimozione o comunque di limitazione dell'accesso ai loro contenuti o di ban del loro account.</p> <p>Le nostre politiche vietano agli account verificati come appartenenti a un governo, a un politico o a un partito politico di accedere alle funzioni di monetizzazione. Ad esempio, non potranno partecipare ai programmi di monetizzazione dei contenuti, come il nostro Creator Rewards Program. Oltre al divieto esistente di pubblicità politica, ciò significa che gli account appartenenti a politici, partiti politici e governi non potranno dare o ricevere denaro attraverso le funzioni di monetizzazione di TikTok, né spendere denaro per promuovere i loro contenuti (sebbene siano previste esenzioni per i governi in determinate circostanze, come ad esempio per la salute pubblica).</p> <p>Nell'aprile 2024 abbiamo lanciato il Codice di condotta dei creatori. Questi sono gli standard che ci aspettiamo che i creatori coinvolti nei programmi, nelle funzionalità, negli eventi e nelle campagne di TikTok seguano sia sulla piattaforma che al di fuori di essa, oltre alle nostre Linee guida della comunità e ai Termini di servizio. Partecipare a questi programmi per creatori è un'opportunità che comporta ulteriori responsabilità e questo codice contribuirà a rassicurare i creatori sul fatto che anche gli altri partecipanti rispettino questi standard. Stiamo migliorando attivamente le nostre linee guida e i nostri processi di applicazione, anche per quanto riguarda la segnalazione proattiva di attività al di fuori della piattaforma.</p>
SLI 1.2.1	Metodologia di misurazione dei dati:



	Le nostre politiche di I&A all'interno delle nostre CG sono la prima linea di difesa per combattere la disinformazione dannosa e i comportamenti ingannevoli sulla nostra piattaforma. Tutti i creatori sono tenuti a rispettare le nostre CG, che stabiliscono le circostanze in cui rimuoveremo o limiteremo in altro modo la disponibilità dei contenuti. I creatori che violano le Linee guida della community o i Termini di servizio non possono ricevere ricompense. Nella SLI 1.1.1 abbiamo indicato il numero di annunci che sono stati rimossi dalla nostra piattaforma per violazione delle nostre politiche sui contenuti politici e delle nostre quattro politiche più dettagliate sulla disinformazione medica, sulla disinformazione pericolosa, sui media sintetici e manipolati e sulle teorie cospirative pericolose. Inoltre, la SLI 1.1.2 mira a fornire una stima del potenziale impatto sui ricavi della demonetizzazione della disinformazione. Stiamo lavorando per essere in grado di fornire più dati per questo SLI.			
Stati membri	N/D	N/D	N/D	N/D
Totale UE				
Totale SEE				

Misura 1.3	
------------	--



<p>QRE 1.3.1</p>	<p>Collaboriamo con una serie di leader del settore per fornire una serie di controlli e strumenti di trasparenza agli acquirenti di pubblicità per quanto riguarda l'inserimento degli annunci:</p> <p>Controlli: Offriamo soluzioni pre-campagna agli inserzionisti, in modo che possano mettere in atto ulteriori misure di salvaguardia prima che la loro campagna venga avviata, per ridurre il rischio che la loro pubblicità venga visualizzata accanto a determinati tipi di contenuti generati dagli utenti. Queste misure si aggiungono alle CG, che forniscono regole generali sui tipi di contenuti che possono apparire su TikTok e sono idonei per il feed For You:</p> <ul style="list-style-type: none"> ● Filtro inventario TikTok: È il nostro sistema proprietario che consente agli inserzionisti di scegliere il profilo dei contenuti a cui vogliono che i loro annunci siano adiacenti. Abbiamo ampliato il nostro Filtro inventario che ora è disponibile in 29 giurisdizioni del SEE ed è incorporato direttamente in TikTok Ads Manager, il sistema attraverso il quale gli inserzionisti acquistano gli annunci. Abbiamo ampliato la funzionalità di questo inventario in vari Paesi del SEE. Ulteriori dettagli sono disponibili qui. Il Filtro inventario è informato dagli Standard di settore e le politiche includono argomenti che possono essere suscettibili di disinformazione. ● TikTok Pre-bid Brand Safety Solution di Integral Ad Science ("IAS"): Gli inserzionisti possono filtrare i contenuti in base a categorie standard del settore con tutti i livelli di rischio (disponibili in Francia e Germania). Alcuni contenuti di disinformazione possono essere catturati e filtrati da queste categorie standard del settore, come "Questioni sociali sensibili". <p>Trasparenza: Abbiamo collaborato con terze parti per offrire soluzioni post-campagna che consentono agli inserzionisti di valutare l'idoneità dei contenuti degli utenti immediatamente adiacenti al loro annuncio nel feed For You, in base ai parametri di idoneità del marchio da loro scelti:</p> <ul style="list-style-type: none"> ● Zefr: Grazie alla nostra partnership con Zefr, gli inserzionisti possono ottenere informazioni sulle campagne in merito all'idoneità e alla sicurezza del marchio sulla piattaforma (ora disponibile in 29 Paesi del SEE). Zefr è in linea con gli standard del settore. ● IAS: Gli inserzionisti possono misurare la sicurezza del marchio, la viewability e il traffico non valido sulla piattaforma con la piattaforma IAS Signal (la post-campagna è disponibile in 28 paesi del SEE). Come la soluzione di pre-bid di IAS descritta sopra, anche questa è conforme al GARM Framework. ● DoubleVerify: Stiamo collaborando con DoubleVerify per fornire agli inserzionisti la misurazione della qualità dei media per gli annunci. DoubleVerify sta lavorando attivamente con noi per espandere la sua suite di soluzioni per l'idoneità del marchio e la qualità dei media piattaforma. DoubleVerify è disponibile in 27 Paesi dell'UE.
<p>Misura 1.4</p>	



QRE 1.4.1	<p>Quando TikTok fa pubblicità, acquista spazi pubblicitari solo attraverso reti pubblicitarie (direttamente, tramite editori o agenzie) che consentono di misurare direttamente la sicurezza e l'idoneità del marchio, attraverso il tagging, utilizzando i principali strumenti di sicurezza del marchio su tutti i canali mediatici digitali. Questo ci permette di ridurre il rischio che gli annunci di TikTok appaiano accanto a fonti di disinformazione e di avere il controllo dell'ambiente in cui i nostri contenuti appaiono.</p> <p>Utilizziamo DoubleVerify per garantire che i nostri annunci vengano pubblicati su o in prossimità di contenuti idonei, mentre eseguiamo e monitoriamo la sicurezza del marchio e le metriche di idoneità in altri posizionamenti, aggiornando sempre il contesto e il contenuto delle nostre blocklist e garantendo che il marchio TikTok sia protetto in qualsiasi contesto.</p> <p>Ad esempio, monitoriamo molto attentamente il posizionamento dei nostri annunci, soprattutto nel contesto di eventi politicamente sensibili come la guerra in Ucraina o il conflitto tra Israele e Hamas, e nel caso in cui i nostri annunci appaiano adiacenti o su fonti di disinformazione, siamo in grado di identificare e indagare il contenuto in questione per valutare i rischi utilizzando i dashboard di DoubleVerify. Una volta individuati, modificheremo eventuali filtri o aggiungeremo la pubblicazione alla nostra blocklist (che viene regolarmente rivista e aggiornata) per evitare che si ripeta.</p>
Misura 1.5	
QRE 1.5.1	<p>Abbiamo ottenuto il sigillo TAG Brand Safety Certified e il sigillo TAG Certified Against Fraud dal Trustworthy Accountability Group ("TAG") nel SEE e a livello globale. Ciò ha richiesto un'adeguata verifica da parte di revisori esterni. I dettagli del nostro marchio TAG possono essere trovati cercando "TikTok" nel loro registro pubblico, disponibile qui.</p> <p>Siamo stati certificati dall'Interactive Advertising Bureau ("IAB") per lo IAB Ireland Gold Standard 2.1 (elencato qui) e IAB Sweden Gold Standard 2.0.</p>
QRE 1.5.2	<p>Abbiamo ottenuto i sigilli TAG Brand Safety Certified e TAG Certified Against Fraud e i marchi IAB Ireland Gold Standard e IAB Sweden Gold Standard 2.0.</p>



Misura 1.6	
QRE 1.6.1	<p>Offriamo una serie di strumenti di brand safety per evitare che gli annunci vengano inseriti accanto a determinati tipi di contenuti. Continuiamo a investire nelle partnership esistenti con i principali fornitori terzi di brand safety e suitability (tra cui DoubleVerify, Integral Ad Science e Zepr).</p> <p>Valutiamo costantemente se ci sono nuove potenziali partnership, anche con ricercatori, che potrebbero essere appropriate per la nostra piattaforma. Inoltre, le nostre politiche pubblicitarie contribuiscono a garantire che le categorie di contenuti che con maggiore probabilità richiedono tali controlli e l'integrazione delle informazioni non entrino nella piattaforma.</p>
QRE 1.6.2	Acquistiamo annunci solo attraverso reti pubblicitarie che mettono a nostra disposizione strumenti di brand safety solidi e affidabili. Tutti i nostri investimenti nei media sono quindi protetti da tali strumenti.
QRE 1.6.3	Abbiamo stretto una partnership con diverse terze parti (IAS, Double Verify e Zepr) per offrire soluzioni post-campagna che consentono agli inserzionisti di valutare l'idoneità dei contenuti degli utenti che sono stati visualizzati immediatamente accanto al loro annuncio in tutti i feed.
QRE 1.6.4	Non applicabile in quanto TikTok non valuta le fonti.
SLI 1.6.1	

II. Controllo delle inserzioni pubblicitarie	
Impegno 2	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve punti elenco].	<ul style="list-style-type: none"> Per migliorare la granularità delle politiche pubblicitarie esistenti, è stata sviluppata una politica pubblicitaria specifica per la disinformazione sul clima.



	<ul style="list-style-type: none"> ● Abbiamo continuato ad applicare le nostre quattro politiche per gli annunci di disinformazione dannosa nel SEE. Come indicato nel nostro rapporto H2 2023, le politiche riguardano: <ul style="list-style-type: none"> ○ Misinformazione medica ○ Pericolosa disinformazione ○ Media sintetici e manipolati ○ Pericolose teorie cospiratorie ● Ampliamento delle funzionalità (comprese la scelta e la capacità) nel SEE del nostro strumento interno di brand safety pre-campagna, il TikTok Inventory Filter. ● Abbiamo migliorato la nostra certificazione IAB per lo Sweden Gold Standard portandola a 2.0. ● Continuiamo a partecipare alla task force e ai suoi gruppi e sottogruppi di lavoro, come il sottogruppo di lavoro sulle elezioni (risposta alle crisi).
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto.
Misura 2.1	
QRE 2.1.1	<p>Gli annunci a pagamento sono soggetti alle nostre rigorose politiche sugli annunci, che vietano specificamente i comportamenti ingannevoli, inautentici e fuorvianti. Gli annunci vengono esaminati alla luce di queste politiche prima di essere ammessi sulla nostra piattaforma. Per migliorare le nostre politiche pubblicitarie esistenti, nel 2023 abbiamo lanciato nel SEE quattro politiche più dettagliate (che riguardano la disinformazione medica, la disinformazione pericolosa, i media sintetici e manipolati e le teorie cospirative pericolose) che anche gli inserzionisti devono rispettare. Verso la fine del 2024, abbiamo lanciato una quinta politica granulare che riguarda la disinformazione sul clima.</p>



SLI 2.1.1 - Numeri per azioni applicare le politiche di cui sopra	<p>Metodologia di misurazione dei dati:</p> <p>Abbiamo indicato il numero di annunci che sono stati rimossi dalla nostra piattaforma per violazione delle nostre politiche sui contenuti politici, nonché le nostre quattro politiche granulari sulla disinformazione medica, sulla disinformazione pericolosa, sui media sintetici e manipolati e sulle teorie cospirative pericolose. Abbiamo lanciato la nostra politica di disinformazione sul clima verso la fine del periodo di riferimento e ci auguriamo di poter condividere i dati su di essa e sulle altre quattro politiche di annunci di disinformazione granulari una volta che avremo un periodo completo di dati.</p> <p>La maggior parte degli annunci che violano le nostre nuove politiche di disinformazione sarebbero stati rimossi in base alle nostre politiche esistenti. Nei casi in cui un annuncio è ritenuto violativo per altre politiche e anche per queste politiche aggiuntive di disinformazione, la rimozione viene conteggiata in base alla politica più vecchia. Pertanto, la seconda colonna qui sotto mostra solo il numero di annunci rimossi quando l'unica ragione era una di queste quattro politiche aggiuntive di disinformazione, e non include gli annunci già rimossi in base alle nostre politiche esistenti o quando le politiche di disinformazione non erano il fattore trainante della rimozione.</p> <p>I dati che seguono suggeriscono che le nostre politiche esistenti (come quella sui contenuti politici) coprono già la maggior parte degli annunci di disinformazione dannosi, grazie alla loro natura espansiva di copertura.</p> <p>Si noti che i numeri sono stati forniti solo per i mercati monetizzati e si basano su dove sono stati visualizzati gli annunci.</p>	
	Numero di rimozioni di annunci in base alla politica degli annunci a contenuto politico	Numero di rimozioni di annunci in base alle quattro politiche sugli annunci di disinformazione granulari
Stati membri		
Austria	746	3
Belgio	1,152	1
Bulgaria	328	7
Croazia	3	0
Cipro	128	0
Repubblica Ceca	111	0



Danimarca	409	0
Estonia	90	0
Finlandia	235	0
Francia	4,621	7
Germania	6,498	63
Grecia	911	8
Ungheria	512	2
Irlanda	565	1
Italia	2,781	8
Lettonia	131	4
Lituania	19	0
Lussemburgo	86	0
Malta	N/D	N/D
Paesi Bassi	1,179	3
Polonia	1,118	4
Portogallo	438	1
Romania	10,698	2
Slovacchia	145	4
Slovenia	52	0

Spagna	2,558	17
Svezia	752	0
Islanda	N/D	N/D
Liechtenstein	N/D	N/D
Norvegia	474	2
Totale UE	36,266	135
Totale SEE	36,740	137

Misura 2.2	
QRE 2.2.1	<p>Per identificare i contenuti e le fonti che violano le nostre politiche pubblicitarie, gli annunci vengono sottoposti a moderazione prima di essere pubblicati piattaforma.</p> <p>TikTok pone una notevole enfasi sulla moderazione proattiva degli annunci. Gli annunci e gli account degli inserzionisti vengono esaminati in base alle nostre Politiche pubblicitarie nella fase di pre-posting e post-posting attraverso una combinazione di moderazione automatica e umana.</p> <p>La maggior parte degli annunci che violano le nostre politiche di disinformazione sarebbero stati rimossi in base alle nostre politiche esistenti. Attualmente le nostre politiche pubblicitarie granulari coprono:</p> <ul style="list-style-type: none">● Pericolosa disinformazione● Pericolose teorie cospiratorie● Misinformazione medica● Media manipolati● La disinformazione sul clima <p>Dopo che l'annuncio è stato pubblicato sulla piattaforma, gli utenti possono segnalare eventuali problemi utilizzando il pulsante "segna"; l'annuncio verrà riesaminato e, se necessario, verranno presi provvedimenti adeguati.</p>



	<p>TikTok opera anche un processo di "richiamo" in base al quale gli annunci già presenti su TikTok passano attraverso un'ulteriore fase di revisione se vengono soddisfatte determinate condizioni, tra cui il raggiungimento di determinate soglie di impression. TikTok effettua inoltre ulteriori revisioni su campioni casuali di annunci per garantire che i suoi processi funzionino come previsto.</p> <p>Collaboriamo con 14 partner di fact-checking che forniscono una copertura di fact-checking in 23 lingue del SEE, tra cui almeno una lingua ufficiale di ogni Stato membro dell'UE, oltre a georgiano, russo, turco e ucraino.</p>
Misura 2.3	
QRE 2.3.1	<p>Per identificare i contenuti e le fonti che violano le nostre politiche pubblicitarie, gli annunci vengono sottoposti a moderazione prima di essere pubblicati piattaforma.</p> <p>TikTok pone una notevole enfasi sulla moderazione proattiva degli annunci. Gli annunci e gli account degli inserzionisti vengono esaminati in base alle nostre Politiche pubblicitarie nella fase di pre-posting e post-posting attraverso una combinazione di moderazione automatica e umana.</p> <p>La maggior parte degli annunci che violano le nostre politiche di disinformazione sarebbero stati rimossi in base alle nostre politiche esistenti. Attualmente le nostre politiche pubblicitarie granulari coprono:</p> <ul style="list-style-type: none"> ● Pericolosa disinformazione ● Pericolose teorie cospiratorie ● Misinformazione medica ● Media manipolati ● La disinformazione sul clima <p>Dopo che l'annuncio è stato pubblicato sulla piattaforma, gli utenti possono segnalare eventuali problemi utilizzando il pulsante "segнала"; l'annuncio verrà riesaminato e, se necessario, verranno presi provvedimenti adeguati.</p> <p>TikTok opera anche un processo di "richiamo" in base al quale gli annunci già presenti su TikTok passano attraverso un'ulteriore fase di revisione se vengono soddisfatte determinate condizioni, tra cui il raggiungimento di determinate soglie di impression. TikTok effettua inoltre ulteriori revisioni su campioni casuali di annunci per garantire che i suoi processi funzionino come previsto.</p>
SLI 2.3.1	<p>Siamo lieti di poter riferire in merito agli annunci rimossi per violazione delle nostre policy sui contenuti politici, nonché alle nostre policy più granulari sugli annunci di disinformazione, includendo le impressioni di tali annunci in questo report. Abbiamo lanciato la nostra politica di disinformazione sul clima verso la fine del periodo di riferimento e non vediamo l'ora di condividere i dati relativi a questa politica e alle altre 4 politiche di disinformazione quando avremo un periodo completo di dati.</p>



	Numero di rimozioni di annunci in base alla politica degli annunci a contenuto politico	Numero di rimozioni di annunci nell'ambito delle quattro politiche di disinformazione granulare politiche sugli annunci	Numero di impressioni per gli annunci rimossi in base all'informativa sugli annunci di contenuto politico	Numero di impressioni per gli annunci rimossi in base alle quattro politiche pubblicitarie di disinformazione granulare
Stati membri				
Austria	746	3	2,405,688	0
Belgio	1,152	1	414,078	16,971
Bulgaria	328	7	21,839	0
Croazia	3	0	69	0
Cipro	128	0	10,838	0
Repubblica Ceca	111	0	187,494	0
Danimarca	409	0	1,333,325	12,268
Estonia	90	0	14,889	0
Finlandia	235	0	7,543,943	0
Francia	4,621	7	14,427,406	510
Germania	6,498	63	45,161,261	0
Grecia	911	8	512,170	12,873
Ungheria	512	2	3,675,505	0
Irlanda	565	1	1,341,419	0
Italia	2,781	8	6,836,564	12,029



Lettonia	131	4	4,551	0
Lituania	19	0	59,348	0
Lussemburgo	86	0	5,472	0
Malta	N/D	N/D	N/D	N/D
Paesi Bassi	1,179	3	879,250	1,048
Polonia	1,118	4	610,009	0
Portogallo	438	1	409,358	0
Romania	10,698	2	27,208,895	0
Slovacchia	145	4	52,215	0
Slovenia	52	0	53,989	0
Spagna	2,558	17	9,622,981	8,551
Svezia	752	0	4,565,753	0
Islanda	N/D	N/D	N/D	N/D
Liechtenstein	N/D	N/D	N/D	N/D
Norvegia	474	2	120,449	1,367
Totale UE	36,266	135	127,358,309	64,250
Totale SEE	36,740	137	127,478,758	65,617



Misura 2.4				
QRE 2.4.1	<p>Siamo chiari con gli inserzionisti sul fatto che i loro annunci devono essere conformi alle nostre rigorose politiche sugli annunci (vedere il Centro assistenza TikTok Business). Spieghiamo che tutti gli annunci vengono esaminati prima di essere caricati sulla nostra piattaforma, di solito entro 24 ore. Gli annunci già presenti su TikTok possono essere sottoposti a un'ulteriore fase di revisione se vengono segnalati, se vengono soddisfatte determinate condizioni (ad esempio, il raggiungimento di determinate soglie di impression) o a causa di un campionamento casuale condotto su iniziativa di TikTok.</p> <p>Se un inserzionista ha violato una politica sugli annunci, viene informato tramite una notifica. Questa è visibile nell'account TikTok Ads Manager e/o inviata via e-mail (se l'inserzionista ha fornito un indirizzo e-mail valido), oppure se l'inserzionista ha prenotato il proprio annuncio tramite un rappresentante TikTok, quest'ultimo informerà l'inserzionista di eventuali violazioni. Gli inserzionisti avvalersi della funzionalità di ricorso contro il rifiuto dei loro annunci in determinate circostanze.</p> <p>Nell'ambito del nostro programma generale di conformità alla DSA, abbiamo migliorato le modalità di notifica e aumentato la trasparenza nei confronti dei nostri inserzionisti. Le notifiche delle restrizioni includono la restrizione stessa, il motivo della restrizione, se la decisione è stata presa con mezzi automatici, come siamo arrivati a rilevare la violazione (ad esempio a seguito di una segnalazione di un utente o di iniziative proattive di TikTok) e quali sono i loro diritti di ricorso. Gli inserzionisti possono accedere alla funzionalità online per appellarsi alle restrizioni sul loro account o sugli annunci. Questi ricorsi vengono esaminati anche in base alle nostre politiche pubblicitarie e potrebbero essere fornite agli inserzionisti informazioni aggiuntive per aiutarli a comprendere la violazione e le azioni da intraprendere.</p>			
SLI 2.4.1	<p>Siamo lieti di poter condividere il numero di ricorsi per gli annunci rimossi in base alle nostre politiche sugli annunci di contenuto politico e alle nostre quattro politiche sugli annunci di disinformazione granulare, nonché il numero dei rispettivi annullamenti. I dati mostrano una riduzione del numero di ricorsi per annunci rimossi nell'ambito della policy sui contenuti politici, a dimostrazione del miglioramento dei nostri processi di moderazione e decisionali. Abbiamo lanciato la nostra politica di disinformazione sul clima verso la fine del periodo di riferimento e non vediamo l'ora di condividere i dati relativi a questa politica e alle altre quattro politiche di disinformazione granulare quando avremo un periodo di riferimento completo.</p>			
	Numero di ricorsi per annunci rimossi nell'ambito delle quattro politiche per gli annunci di disinformazione granulare	Numero di ricorsi per annunci rimossi in base alla politica sui contenuti politici	Numero di annullamenti di apparizioni in base alle quattro politiche di disinformazione più granulari politiche di disinformazione	Numero di respinti in base alla politica dei contenuti politici
Stati membri				
Austria	0	34	0	26



Belgio	0	18	0	8
Bulgaria	0	2	0	0
Croazia	0	2	0	2
Cipro	0	1	0	1
Repubblica Ceca	0	6	0	1
Danimarca	0	18	0	10
Estonia	0	6	0	4
Finlandia	0	15	0	7
Francia	0	84	0	50
Germania	0	78	0	45
Grecia	0	16	0	6
Ungheria	0	11	0	5
Irlanda	0	32	0	18
Italia	0	53	0	22
Lettonia	0	2	0	1
Lituania	0	6	0	2
Lussemburgo	0	0	0	0
Malta	N/D	N/D	N/D	N/D
Paesi Bassi	0	24	0	10



Polonia	0	9	0	3
Portogallo	0	15	0	7
Romania	0	75	0	31
Slovacchia	0	3	0	0
Slovenia	0	0	0	0
Spagna	0	90	0	35
Svezia	0	37	0	13
Islanda	N/D	N/D	N/D	N/D
Liechtenstein	N/D	N/D	N/D	N/D
Norvegia	0	27	0	11
Totale UE	0	637	0	307
Totale SEE	0	664	0	318

II. Controllo delle inserzioni pubblicitarie	
Impegno 3	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve elenco].	Continuiamo partecipare alla task force e a tutti i suoi gruppi e sottogruppi di lavoro, come il sottogruppo di lavoro sulle elezioni (risposta alle crisi).
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto.
Misura 3.1	



QRE 3.1.1	<p>Come illustrato più avanti nel presente rapporto, collaboriamo con una serie di terze parti per facilitare il flusso di informazioni che possono essere rilevanti per affrontare i fornitori di disinformazione dannosa. Queste informazioni vengono condivise internamente per garantire la coerenza dell'approccio all'interno della nostra piattaforma.</p> <p>Continuiamo inoltre a partecipare attivamente al gruppo di lavoro della Task-force per il Capitolo 2, in particolare al sottogruppo di lavoro sulle Elezioni (Risposta alle crisi) che abbiamo co-presieduto. Lavoriamo con altri firmatari per definire e delineare le metriche relative alla portata e all'impatto monetario della disinformazione dannosa. Siamo in stretta collaborazione con l'industria per garantire l'allineamento e la chiarezza sulla segnalazione di questi requisiti del codice.</p> <p>Collaboriamo con 14 partner di fact-checking che forniscono una copertura di fact-checking in 23 lingue del SEE, tra cui almeno una lingua ufficiale di ogni Stato membro dell'UE, oltre a georgiano, russo, turco e ucraino.</p>
Misura 3.2	
QRE 3.2.1	<p>Lavoriamo con i partner del settore per discutere standard e definizioni comuni a sostegno della coerenza della categorizzazione dei contenuti, dell'adiacenza e degli argomenti rilevanti per la misurazione, nelle sedi appropriate. Lavoriamo a stretto contatto con IAB Svezia, IAB Irlanda e altre organizzazioni come TAG nel SEE e a livello globale. Facciamo anche parte del consiglio di amministrazione del Brand Safety Institute.</p> <p>Continuiamo a condividere le informazioni e le metriche rilevanti all'interno dei nostri rapporti trimestrali sulla trasparenza, che mirano a informare i colleghi del settore e la comunità dei ricercatori. Continuiamo a partecipare ai sottogruppi istituiti per la condivisione di informazioni tra i firmatari e la Commissione.</p>
Misura 3.3	
QRE 3.3.1	<p>Continuiamo a lavorare a stretto contatto con IAB Svezia, IAB Irlanda e altre organizzazioni come TAG nel SEE e a livello globale.</p>



III. Impegni di pubblicità politica 4 - 13



III. Pubblicità politica	
Impegno 4	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	Poiché vietiamo la pubblicità politica, continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e l'orientamento della pubblicità politica e dell'applicazione della maggior parte delle disposizioni a partire dall'ottobre 2025.
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D
Misura 4.1	
Misura 4.2	
QRE 4.1.1 (per misure 4.1 e 4.2)	<p>TikTok è prima di tutto una piattaforma di intrattenimento e siamo orgogliosi di essere un luogo che riunisce le persone attraverso contenuti creativi e divertenti. Sebbene la condivisione di convinzioni politiche e la partecipazione a conversazioni politiche siano consentite come contenuti organici su TikTok, le nostre politiche vietano alla nostra comunità, compresi i politici e gli account di partiti politici, di inserire annunci politici o pubblicare contenuti a marchio politici .</p> <p>In particolare, la nostra politica su Politica, Cultura e Religione vieta annunci e pagine di destinazione che:</p> <ul style="list-style-type: none">● fare riferimento, promuovere o opporsi a candidati o candidati a cariche pubbliche, partiti politici o funzionari governativi eletti o nominati;



	<ul style="list-style-type: none">● riferimento a un'elezione, tra cui la registrazione degli elettori, l'affluenza alle urne e gli appelli al voto;● includere il patrocinio a favore o contro referendum passati, attuali o proposti, misure elettorali e risultati o processi legislativi, giudiziari o normativi (compresi quelli che promuovono o attaccano le politiche o i risultati del governo); e● fare riferimento, promuovere o vendere merce con persone, entità o contenuti vietati, compresi slogan, simboli o loghi di campagne elettorali. <p>Quando gli account sono designati come account di governo, politici e partiti politici ("GPPPA"), a tali account è vietato inserire annunci su TikTok, accedere alle funzioni di monetizzazione e raccogliere fondi per le campagne. Possiamo consentire alcune pubblicità basate su cause e servizi pubblici da parte di enti governativi, organizzazioni non profit e altre entità se soddisfano determinate condizioni e collaborano con un rappresentante commerciale di TikTok.</p> <p>Vietiamo i contenuti politici nei contenuti di marca, ossia quelli pubblicati in cambio di un pagamento o di qualsiasi altro incentivo da parte di terzi.</p> <p>Abbiamo rivisto le nostre politiche per garantire che il nostro divieto sia almeno altrettanto ampio di quello definito dal Regolamento UE 2024/900 sulla trasparenza e l'orientamento della pubblicità politica. Il nostro divieto di pubblicità politica è una parte dei nostri sforzi per l'integrità elettorale, di cui si può leggere di più nei rapporti sulla crisi elettorale.</p>
QRE 4.1.2 (per misure 4.1 e 4.2)	Non applicabile in questa fase.

III. Pubblicità politica	
Impegno 5	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No

Se sì, elencare queste misure di attuazione [breve punti elenco].		N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]		Vietiamo la pubblicità politica e continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e la targetizzazione della pubblicità politica, la cui maggior parte delle disposizioni si applicherà a partire dall'ottobre 2025.
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?		N/D
Misura 5.1		
QRE 5.1.1	Non è applicabile in quanto TikTok non consente la pubblicità politica, come indicato nella nostra su politica, cultura e religione . Non consentiamo la presentazione di contenuti politici in qualsiasi forma di pubblicità, estendendo questo divieto sia agli account di governi, politici o partiti politici sia agli inserzionisti non politici che esprimono opinioni politiche nella pubblicità.	

III. Pubblicità politica		
Impegno 6		
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No	
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D	



Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]		Vietiamo la pubblicità politica e continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e la targetizzazione della pubblicità politica, la cui maggior parte delle disposizioni si applicherà a partire dall'ottobre 2025.	
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?		N/D	
Misura 6.1			
QRE 6.1.1	Non applicabile in quanto TikTok non consente la pubblicità politica.		
Misura 6.2			
QRE 6.2.1	Non applicabile in quanto TikTok non consente la pubblicità politica.		
QRE 6.2.2	Non applicabile in quanto TikTok non consente la pubblicità politica.		
SLI 6.2.1 - numeri per le azioni applicazioni e delle politiche di cui sopra			
Stati membri	N/D	N/D	N/D
Totale UE			
Totale SEE			

Misura 6.3	
QRE 6.3.1	Non applicabile in quanto TikTok non consente la pubblicità politica.
Misura 6.4	
QRE 6.4.1	Non applicabile in quanto TikTok non consente la pubblicità politica.
Misura 6.5	
QRE 6.5.1	Questo impegno non è applicabile in quanto TikTok non è un'app di messaggistica.

III. Pubblicità politica	
Impegno 7	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	Vietiamo la pubblicità politica e continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e la targetizzazione della pubblicità politica, la cui maggior parte delle disposizioni si applicherà a partire dall'ottobre 2025.



Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?		N/D	
Misura 7.1			
QRE 7.1.1	<p>Quando gli account sono designati come account governativi, politici e di partiti politici ("GPPPA"), a tali account è vietato inserire annunci su TikTok (ad eccezione di alcune agenzie governative che possono avere un motivo specifico per fare pubblicità, ad esempio per promuovere iniziative di salute pubblica) e le funzioni di monetizzazione. Pubblichiamo i dettagli della nostra politica sulle GPPPA sul nostro sito web, dove indichiamo chi consideriamo una GPPPA e le restrizioni su questi tipi di account. Spieghiamo come l'attore di un'agenzia governativa deve agire sulla nostra piattaforma e cosa può pubblicizzare nel nostro Centro assistenza per le aziende di TikTok.</p> <p>Nell'UE, applichiamo un'etichetta interna agli account appartenenti a un governo, a un politico o a un partito politico. Una volta che un account è stato etichettato in questo modo, verranno applicate una serie di politiche che aiutano a prevenire l'uso improprio di alcune funzioni, ad esempio l'accesso alle funzioni pubblicitarie e la sollecitazione per la raccolta di fondi per le campagne elettorali non sono consentite.</p>		
SLI 7.1.1 - numeri per le azioni di applicazione delle politiche di cui sopra (metriche comparabili a quelle della SLI 6.2.1)			
Stati membri	N/D	N/D	

Totale UE				
Totale SEE				



Misura 7.2	
QRE 7.2.1	<p>Non applicabile in quanto TikTok non consente la pubblicità politica.</p> <p>La nostra Politica degli attori mira a proteggere l'integrità e l'autenticità della nostra comunità e a impedire agli attori di eludere i nostri strumenti e processi. Se un attore dimostra costantemente un comportamento che inganna, fuorvia o è inautentico nei confronti degli utenti e/o di TikTok, applichiamo un'applicazione a livello di account. Questo non riguarda esclusivamente gli annunci con contenuti politici.</p> <p>TikTok si impegna a indagare e interrompere i casi confermati di CIO sulla piattaforma. Le operazioni di influenza occulta (CIO) sono tentativi organizzati di manipolare o corrompere il dibattito pubblico, ingannando al contempo i sistemi o gli utenti di TikTok sull'identità, l'origine, la posizione operativa, la popolarità o lo scopo generale. La logica di sospensione dipende dagli scioperi, in cui si tiene conto delle violazioni a livello di annuncio e dei comportamenti dell'account dell'inserzionista. Le violazioni critiche confermate della policy portano alla sospensione permanente. Ulteriori informazioni sulla nostra politica sono disponibili nell'articolo Centro assistenza per le aziende del .</p>
QRE 7.2.2	Non applicabile in quanto TikTok non consente la pubblicità politica.
Misura 7.3	
QRE 7.3.1	Non applicabile in quanto TikTok non consente la pubblicità politica.
QRE 7.3.2	Non applicabile in quanto TikTok non consente la pubblicità politica.
Misura 7.4	
QRE 7.4.1	Non applicabile in quanto TikTok non consente la pubblicità politica.



III. Pubblicità politica	
Impegno 8	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	Vietiamo la pubblicità politica e continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e la targetizzazione della pubblicità politica, la cui maggior parte delle disposizioni si applicherà a partire dall'ottobre 2025.
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D
Misura 8.1	
Misura 8.2	
QRE 8.2.1 (per le misure 8.1 e 8.2)	Non applicabile in quanto TikTok non consente la pubblicità politica.



III. Pubblicità politica	
Impegno 9	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	Vietiamo la pubblicità politica e continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e la targetizzazione della pubblicità politica, la cui maggior parte delle disposizioni si applicherà a partire dall'ottobre 2025.
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D
Misura 9.1	N/D
Misura 9.2	N/D
QRE 9.2.1 (per le misure 9.1 e 9.2)	Non applicabile in quanto TikTok non consente la pubblicità politica.

III. Pubblicità politica	
Impegno 10	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	Vietiamo la pubblicità politica e continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e la targetizzazione della pubblicità politica, la cui maggior parte delle disposizioni si applicherà a partire dall'ottobre 2025.
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D
Misura 10.1	
Misura 10.2	
QRE 10.2.1 (per le misure 10.1 e 10.2)	<p>Non applicabile in quanto TikTok non consente la pubblicità politica.</p> <p>In ottemperanza ai nostri obblighi ai sensi del Digital Services Act, TikTok mantiene una libreria di annunci consultabile pubblicamente che presenta gli annunci che TikTok è stato pagato per mostrare agli utenti, compresi quelli che non sono attualmente attivi o sono stati messi in pausa dagli inserzionisti. Questo include informazioni sul numero totale di destinatari raggiunti, con numeri aggregati suddivisi per Stato membro per il gruppo o i gruppi di destinatari a cui l'annuncio era specificamente rivolto,</p>



	<p>compresi gli annunci politici che sono stati rimossi. Ogni annuncio è disponibile per tutto il tempo in cui viene mostrato su TikTok e per un anno dopo, in conformità con la legge sui servizi digitali.</p> <p>L'articolo 39, paragrafo 3, della legge sui servizi digitali prevede che tali biblioteche non includano il contenuto dell'annuncio, l'identità della persona per conto della quale è stato presentato o chi lo ha pagato nel caso in cui un annuncio sia stato <u>rimosso per incompatibilità</u> con i termini e le condizioni di una piattaforma. Poiché gli annunci politici sono vietati su TikTok, per ottemperare ai suoi obblighi legali TikTok deve rimuovere questi dettagli specifici di qualsiasi annuncio politico che sia stato rimosso dalla sua piattaforma (in quanto tale annuncio viola i suoi termini e condizioni). Per questo motivo, la libreria di annunci di TikTok è tenuta a visualizzare informazioni diverse in merito agli annunci politici rispetto alle piattaforme che li consentono.</p>
--	---

III. Pubblicità politica	
Impegno 11	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D

Misura 11.1	
Misura 11.2	
Misura 11.3	
Misura 11.4	
QRE 11.1.1 (per le misure 11.1-11.4)	
QRE 11.4.1	

III. Pubblicità politica	
Impegno 12	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	TikTok non ha sottoscritto questo impegno. L'impegno 12 e le misure associate sono applicabili solo alla società civile.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No



Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	TikTok non ha sottoscritto questo impegno. L'impegno 12 e le misure associate sono applicabili solo alla società civile.
Misura 12.1	
Misura 12.2	
Misura 12.3	
QRE 12.1.1 (per le misure 12.1-12.3)	L'impegno 12 e le misure 12.1, 12.2 e 12.3 si applicano solo alla società civile.

III. Pubblicità politica	
Impegno 13	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	N/D
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	Vietiamo la pubblicità politica e continuiamo a concentrarci sull'applicazione di questa politica alla luce dell'entrata in vigore del Regolamento UE 2024/900 sulla trasparenza e la targetizzazione della pubblicità politica, la cui maggior parte delle disposizioni si applicherà a partire dall'ottobre 2025.
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D

Misura 13.1	
Misura 13.2	TikTok non consente la pubblicità politica e questo continua nei periodi di blackout.
Misura 13.3	
QRE 13.1.1 (per le misure 13.1-13.3)	Pur non consentendo la pubblicità politica, continuiamo a partecipare alle discussioni che si tengono attraverso la task force e altri forum per garantire che le nostre politiche e i nostri processi rimangano aggiornati e che le minacce emergenti siano affrontate nelle nostre politiche e nell'applicazione.



IV. Integrità di Servizi

Impegni 14 - 16



IV. Integrità dei servizi

Impegno 14

Al fine di limitare i comportamenti e le pratiche manipolative inammissibili nei loro servizi, i Firmatari rilevanti si impegnano a mettere in atto o a rafforzare ulteriormente le politiche per affrontare sia la disinformazione che l'informazione scorretta nei loro servizi e a concordare una comprensione trasversale dei comportamenti, degli attori e delle pratiche manipolative non consentite nei loro servizi. Tali comportamenti e pratiche, che dovrebbero essere periodicamente rivisti alla luce delle più recenti evidenze sulle condotte e sui TTP impiegati dagli attori malintenzionati, come il Disinformation Tactics, Techniques and Procedures Framework dell'AMITT, includono:

I seguenti TTP riguardano la creazione di risorse ai fini di una campagna di disinformazione e i modi per farle sembrare credibili:

- 1. Creazione di account o botnet non autentici (che possono includere account automatizzati, parzialmente automatizzati o non automatizzati).
- 2. Uso di reazioni false/inautentiche (ad esempio, like, voti in alto, commenti).
- 3. Uso di falsi follower o abbonati
- 4. Creazione di pagine, gruppi, gruppi di chat, forum o domini non autentici.
- 5. Dirottamento o impersonificazione dell'account

I seguenti TTP riguardano la diffusione di contenuti creati nel contesto di una campagna di disinformazione, che può includere o meno alcune forme di bersagliamento o di tentativo di mettere a tacere le opinioni contrarie. I TTP rilevanti includono:

- 6. Puntare deliberatamente a destinatari vulnerabili (ad esempio, tramite pubblicità personalizzata, spoofing della posizione o offuscamento).
- 7. Impiego di mezzi di comunicazione manipolati e ingannevoli (ad esempio, "deep fakes", "cheap fakes"...).
- 8. Utilizzare l'operazione "hack and leak" (che può includere o meno contenuti falsificati).
- 9. Coordinamento non autentico della creazione o dell'amplificazione di contenuti, compresi i tentativi di ingannare/manipolare gli algoritmi delle piattaforme (ad esempio, keyword stuffing o posting/reposting non autentici progettati per ingannare le persone sulla popolarità dei contenuti, anche da parte degli influencer).
- 10. Uso di pratiche ingannevoli per ingannare/manipolare gli algoritmi della piattaforma, ad esempio per creare, amplificare o dirottare hashtag, vuoti di dati, bolle di filtraggio o camere d'eco.
- 11. Messaggi o promozioni non trasparenti e compensati da parte degli influencer
- 12. Segnalazione coordinata di massa di contenuti o account opposti non violenti.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]

Sì



<p>Se sì, elencare queste misure di attuazione [brevi punti elenco].</p>	<ul style="list-style-type: none"> ● Sulla base della nostra nuova etichetta generata dall'IA, che consente ai creatori di rivelare contenuti completamente generati dall'IA o modificati in modo significativo dall'IA, abbiamo ampliato i nostri sforzi nello spazio AIGC: <ul style="list-style-type: none"> ○ Implementazione delle credenziali di contenuto della Coalition for Content Provenance and Authenticity (C2PA), che consente ai nostri sistemi di riconoscere istantaneamente ed etichettare automaticamente l'AIGC. ○ Sostenere i gruppi di lavoro della coalizione come membro generale di C2PA. ○ Aderire alla Content Authenticity Initiative (CAI) per promuovere una più ampia adozione dello standard tecnico. ○ Pubblicazione di un nuovo articolo del Centro per la trasparenza Sostegno a contenuti generati dall'intelligenza artificiale responsabili e trasparenti. ○ Sulla base della nostra nuova etichetta per i contenuti generati dall'IA per i creatori e dell'implementazione delle C2PA Content Credentials, abbiamo lanciato una serie di campagne di alfabetizzazione mediatica con la guida di organizzazioni esperte come Mediawise e WITNESS, anche in Brasile, Germania, Francia, Messico e Regno Unito, che insegnano alla nostra comunità come individuare ed etichettare i contenuti generati dall'IA. Questa campagna di trasparenza dell'AIGC, informata da WITNESS, ha raggiunto 80 milioni di utenti a livello globale, di cui oltre 8,5 milioni e 9,5 milioni rispettivamente in Germania e in Francia. ● Ha continuato a unirsi ai partner del settore come parte del "Tech Accord to Combat Deceptive Use of AI in 2024 Elections", un impegno comune per combattere l'uso ingannevole dell'IA nelle elezioni. ● Ha continuato a partecipare ai gruppi di lavoro sull'integrità dei servizi e sull'IA generativa. ● Abbiamo continuato a migliorare la nostra capacità di individuare le operazioni di influenza occulta. Per fornire aggiornamenti più regolari e dettagliati sulle operazioni di influenza occulta che interrompiamo, abbiamo un rapporto di trasparenza dedicato alle operazioni di influenza occulta, disponibile nel centro di trasparenza di TikTok. In questo rapporto includiamo informazioni sulle operazioni che abbiamo precedentemente rimosso e che hanno tentato di tornare sulla nostra piattaforma con nuovi account.
<p>Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]</p>	<p>No</p>



Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto COPD.
Misura 14.1	



<p>QRE 14.1.1</p>	<p>Oltre alle politiche di I&A delle nostre CG, che tutelano dalla disinformazione dannosa (cfr. QRE 18.2.1), le nostre politiche di I&A vietano espressamente i comportamenti ingannevoli. Le nostre politiche sui comportamenti ingannevoli si riferiscono ai TTP come segue:</p> <p><i>TTP che riguardano la creazione di risorse allo scopo di una campagna di disinformazione e i modi per far sembrare tali risorse credibili:</i></p> <p>Creazione di account o botnet non autentici (che possono includere account automatizzati, parzialmente automatizzati o non automatizzati).</p> <p>Le nostre politiche I&A, che riguardano lo spam e i comportamenti ingannevoli dell'account, vietano espressamente i comportamenti dell'account che possono causare spam o ingannare la nostra comunità. È possibile creare più account su TikTok per creare diversi canali di espressione creativa autentica, ma non per scopi ingannevoli.</p> <p>Non sono ammessi messaggi di spam:</p> <ul style="list-style-type: none"> ● Gestione di grandi reti di conti controllati da un'unica entità o attraverso l'automazione; ● Distribuzione massiva di un elevato volume di spam; e ● Manipolazione dei segnali di coinvolgimento per amplificare la portata di determinati contenuti, o acquisto e vendita di follower, in particolare per scopi finanziari. <p>Inoltre, non sono consentite le impersonificazioni:</p> <ul style="list-style-type: none"> ● Account che si spacciano per un'altra persona o entità reale senza rivelare di essere un fan o un account parodia nel nome dell'account, ad esempio utilizzando il nome, i dettagli biografici, il contenuto o l'immagine di qualcuno senza rivelarlo. ● Presentarsi come una persona o un'entità che non esiste (una persona falsa) con intento dimostrato di ingannare gli altri sulla piattaforma. <p>Se riteniamo che qualcuno abbia messo in atto uno di questi comportamenti ingannevoli da parte dell', lo banneremo e potremo bannare qualsiasi nuovo account che venga creato.</p> <p>Uso di reazioni false/inautentiche (ad es. like, voti alti, commenti) e uso di falsi follower o abbonati</p>
--------------------------	--



	<p>Le nostre politiche I&A, che riguardano il falso impegno, non consentono il commercio o la commercializzazione di servizi che tentano di aumentare artificialmente l'impegno o di ingannare il sistema di raccomandazione di TikTok. Non consentiamo ai nostri utenti di:</p> <ul style="list-style-type: none"> • facilitare il commercio o la commercializzazione di servizi che aumentano artificialmente il coinvolgimento, come la vendita di follower o like; oppure • forniscono istruzioni su come aumentare artificialmente il coinvolgimento su TikTok. <p>Se veniamo a conoscenza di account o contenuti con metriche gonfiate in modo non autentico, rimuoveremo i falsi follower o like associati. I contenuti che ingannano o manipolano gli altri per aumentare le metriche di coinvolgimento, come le promesse di "like-for-like" e i falsi incentivi per il coinvolgimento nei contenuti (per aumentare i regali, i follower, i like, le visualizzazioni o altre metriche di coinvolgimento) non sono ammissibili per il nostro feed For You.</p> <p>Creazione di pagine, gruppi, gruppi di chat, forum o domini non autentici. TikTok non ha pagine, gruppi, gruppi di chat, forum o domini. Questo TTP non è pertinente alla nostra piattaforma.</p> <p>Dirottamento dell'account o impersonificazione Anche in questo caso, le nostre politiche vietano l'impersonificazione, che si riferisce ad account che si spacciano per un'altra persona o entità reale o che si presentano come una persona o un'entità che non esiste (una persona falsa) con l'intento dimostrato di ingannare gli altri sulla piattaforma. Ai nostri utenti non è consentito utilizzare il nome, i dati biografici o l'immagine del profilo di qualcun altro in modo fuorviante. Al fine di proteggere la libertà di espressione, consentiamo gli account che sono chiaramente parodistici, di commento o basati sui fan, ad esempio quando il nome dell'account indica che si tratta di un account di fan, di commento o di parodia e che non è affiliato all'oggetto dell'account. Continuiamo a sviluppare le nostre politiche per garantire che l'impersonificazione di entità (come aziende o istituzioni educative, ad esempio) sia vietata e che siano vietati anche gli account che impersonano persone o entità che non sono presenti sulla piattaforma. Inoltre, avvertiamo gli utenti di account sospetti di impersonificazione e non raccomandiamo tali account nel nostro Feed per voi.</p>
--	--



Abbiamo anche una serie di politiche che affrontano il problema del dirottamento degli account. Le nostre politiche sulla privacy e sulla sicurezza nell'ambito delle nostre CG vietano espressamente agli utenti di fornire l'accesso alle credenziali del proprio account ad altri o di consentire ad altri di condurre attività contro le nostre CG. Non consentiamo l'accesso a nessuna parte di TikTok attraverso metodi non autorizzati; tentativi di ottenere informazioni sensibili, riservate, commerciali o personali; o qualsiasi abuso della sicurezza, integrità o affidabilità della nostra piattaforma. Forniamo inoltre [indicazioni](#) pratiche agli utenti che temono che il loro account sia stato violato.

TTP che riguardano la diffusione di contenuti creati nel contesto di una campagna di disinformazione, che può includere o meno alcune forme di bersagliamento o di tentativo di mettere a tacere le opinioni contrarie:

targettizzazione deliberata di destinatari vulnerabili (ad esempio tramite pubblicità personalizzata, spoofing della posizione o offuscamento), coordinamento non autentico della creazione o amplificazione di contenuti, compresi i tentativi di ingannare/manipolare gli algoritmi delle piattaforme (ad esempio keyword stuffing o post/reposting non autentici progettati per ingannare le persone sulla popolarità dei contenuti, anche da parte degli influencer), uso di pratiche ingannevoli per ingannare/manipolare gli algoritmi delle piattaforme, come creare, amplificare o dirottare hashtag, vuoti di dati, bolle di filtraggio o camere dell'eco e segnalazione coordinata di massa di contenuti o account opposti non violenti.

Lottiamo contro i CIO in quanto le nostre politiche vietano i tentativi di influenzare l'opinione pubblica e di ingannare i nostri sistemi o utenti sull'identità, l'origine, la posizione approssimativa, la popolarità o lo scopo generale.



Quando indaghiamo e rimuoviamo queste operazioni, ci concentriamo sul comportamento e sulla valutazione dei collegamenti tra gli account e le tecniche per determinare se gli attori sono impegnati in uno sforzo coordinato per ingannare i sistemi di TikTok o la nostra comunità. In ogni caso, riteniamo che le persone dietro queste attività si coordinino tra loro per travisare chi sono e cosa stanno facendo. Sappiamo che i CIO continueranno a evolversi in risposta al nostro rilevamento e che le reti potrebbero tentare di ristabilire una presenza sulla nostra piattaforma: ecco perché intraprendiamo azioni continue contro questi tentativi, tra cui il ban degli account che risultano collegati a reti precedentemente interrotte. Continuiamo a ricercare e valutare in modo iterativo i comportamenti ingannevoli complessi sulla nostra piattaforma e a sviluppare soluzioni di prodotto e di policy adeguate a lungo termine. Pubblichiamo tutte le reti CIO che identifichiamo e rimuoviamo volontariamente in un rapporto dedicato all'interno del nostro centro di trasparenza.

Utilizzare l'operazione di "hack and leak" (che può includere o meno contenuti falsificati)

Abbiamo una serie di politiche che affrontano le minacce legate agli hack e alle fughe di notizie (alcuni esempi sono riportati di seguito):

- La nostra politica in materia di hack e leak, che mira a ridurre ulteriormente i danni inflitti dalla divulgazione non autorizzata di materiale hackerato agli individui, alle comunità e alle organizzazioni che possono essere coinvolti o esposti da tali divulgazioni.
- La nostra politica CIO affronta l'uso di documenti trapelati per influenzare l'opinione pubblica come parte di un'operazione più ampia.
- La nostra politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC) individua i materiali che sono stati modificati digitalmente senza un'adeguata divulgazione.
- Le nostre politiche di disinformazione dannosa combattono le teorie cospirative legate agli eventi in corso e la disinformazione pericolosa.
- La nostra politica sul commercio di beni e servizi regolamentati proibisce il commercio di beni violati.

Media manipolati in modo ingannevole (ad esempio "deep fakes", "cheap fakes" ...)



La nostra politica sui "Media modificati e contenuti generati dall'intelligenza artificiale (AIGC)" include un linguaggio comunemente usato e facilmente comprensibile quando ci si riferisce all'AIGC, e delinea i nostri divieti esistenti sull'AIGC che mostra false fonti autorevoli o eventi di crisi, o che mostra falsamente personaggi pubblici in determinati contesti, tra cui il bullismo, l'approvazione o l'essere sostenuti. Inoltre, non consentiamo contenuti che contengano le sembianze di giovani o di figure private adulte utilizzate senza il loro permesso.

Ai fini della nostra politica, AIGC si riferisce a contenuti creati o modificati dalla tecnologia di intelligenza artificiale (AI) o da processi di apprendimento automatico, che possono includere immagini di persone reali e possono mostrare scene dall'aspetto altamente realistico o utilizzare un particolare stile artistico, come un dipinto, cartoni animati o anime. Per "contenuti modificati in modo significativo" si intendono contenuti che mostrano persone che fanno o dicono qualcosa che non hanno fatto o detto, o che alterano il loro aspetto in modo da renderne difficile il riconoscimento o l'identificazione. I media fuorvianti o modificati sono contenuti audio o visivi che sono stati modificati, anche combinando insieme clip diverse, per cambiare la composizione, la sequenza o la tempistica in modo da alterare il significato del contenuto e da indurre gli spettatori in errore sulla verità degli eventi del mondo reale.

In conformità con la nostra politica, vietiamo l'AIGC che presenta:

- Persone dall'aspetto realistico di età inferiore ai 18 anni
- L'immagine di figure private adulte, se ci rendiamo conto che è stata utilizzata senza il loro permesso.
- Media fuorvianti dell'AIGC o modificati che mostrano falsamente:
 - Contenuti che sembrano provenire da una fonte autorevole, come ad esempio un'organizzazione giornalistica rinomata.
 - Un evento di crisi, come un conflitto o una catastrofe naturale
 - Un personaggio pubblico che è:
 - essere degradati o molestati, o assumere un comportamento criminale o antisociale
 - prendere posizione su una questione politica, su un prodotto commerciale o su una questione di importanza pubblica (come le elezioni)
 - essere appoggiato o condannato politicamente da un individuo o da un gruppo



Con l'evoluzione dell'IA, continuiamo a investire nella lotta contro l'AIGC dannosa, evolvendo i nostri modelli di rilevamento proattivo, consultando esperti e collaborando con i colleghi per soluzioni condivise.

Messaggi o promozioni non trasparenti e compensati da parte degli influencer

I nostri [Termini di servizio](#) e la nostra [Politica sui contenuti di marca](#) richiedono agli utenti che pubblicano su un **marchio o un prodotto in cambio di un pagamento o di un altro incentivo** di divulgare i loro contenuti attivando la levetta per i contenuti di marca che mettiamo a disposizione degli utenti. Forniamo inoltre una funzionalità per consentire agli utenti di segnalare i contenuti di marca sospetti e non divulgati, che ricorda all'utente che ha pubblicato i contenuti di marca sospetti e non divulgati i nostri requisiti e lo invita ad attivare la levetta per i contenuti di marca, se necessario. Nel nostro aggiornamento delle CG del marzo 2023 abbiamo reso questo requisito ancora più chiaro per gli utenti nella nostra politica di **divulgazione commerciale e promozione a pagamento**, aumentando le informazioni sulla nostra attività di controllo di questa politica e fornendo esempi specifici.

Oltre alle politiche sui contenuti di marca, la nostra politica CIO può essere applicata anche a messaggi o promozioni non trasparenti compensati da influencer, qualora scopra che tali messaggi o promozioni facevano parte di una campagna di influenza occulta.

**QRE 14.1.2**

In TikTok poniamo una notevole enfasi sulla moderazione proattiva dei contenuti e utilizziamo una combinazione di tecnologia e professionisti della sicurezza per individuare e rimuovere la disinformazione dannosa (cfr. QRE 18.1.1) e i comportamenti ingannevoli sulla nostra Piattaforma, *prima che* ci vengano segnalati dagli utenti o da terzi.

Ad esempio, adottiamo misure proattive per impedire la creazione di account non autentici o di spam. Per questo motivo, abbiamo creato e utilizziamo modelli di rilevamento e motori di regole che:

- impedire la creazione di account non autentici basati su modelli dannosi; e
- rimuovere gli account registrati in base a determinati segnali (ad esempio, comportamenti insoliti sulla piattaforma).

Inoltre, monitoriamo manualmente le segnalazioni di account inautentici da parte degli utenti per individuare cluster più ampi o comportamenti inautentici simili.

Tuttavia, data la natura complessa dei TTP, la moderazione umana è fondamentale per il successo in questo settore e i team di moderazione di TikTok svolgono quindi un ruolo chiave nel valutare e risolvere le violazioni individuate. Forniamo ai nostri team di moderazione una guida dettagliata su come applicare le politiche di I&A nelle nostre CG, fornendo anche banche di casi di affermazioni di disinformazione dannose per supportare il loro lavoro di moderazione, e consentiamo loro di indirizzare contenuti nuovi o in evoluzione ai nostri partner di fact-checking per la valutazione.

Inoltre, quando un contenuto raggiunge determinati livelli di popolarità in termini di numero di visualizzazioni di video, viene segnalato per un'ulteriore revisione. Tale revisione viene effettuata in considerazione dell'ampiezza della diffusione del contenuto e dell'aumento del danno potenziale nel caso in cui il contenuto risulti in violazione delle nostre CG, incluse le nostre politiche I&A.

Inoltre, durante il periodo di riferimento, abbiamo migliorato il rilevamento automatico e l'applicazione della nostra politica "Edited Media and AI-Generated Content (AIGC)", con un conseguente aumento effettivo del numero di video rimossi per violazione della politica. Ciò ha comportato anche una diminuzione del numero di visitatori per video nel di riferimento, a dimostrazione dell'efficacia della strategia di controllo, che ha aumentato la portata dell'applicazione.



Abbiamo inoltre creato team specificamente formati per indagare e rilevare CIO sulla nostra piattaforma. Abbiamo creato team internazionali di fiducia e sicurezza con competenze specialistiche in materia di intelligence sulle minacce, sicurezza, applicazione della legge e scienza dei dati per lavorare a tempo pieno sulle operazioni di influenza. Questi team cercano e analizzano continuamente i segnali di comportamento ingannevole presenti sulla piattaforma, così come gli indizi provenienti da fonti esterne. Collaborano anche con fornitori esterni di intelligence per supportare indagini specifiche caso per caso. Quando indaghiamo e rimuoviamo queste operazioni, ci concentriamo sul comportamento e sulla valutazione dei collegamenti tra account e tecniche per determinare se gli attori sono impegnati in uno sforzo coordinato per ingannare i sistemi di TikTok o la nostra comunità. In ogni caso, riteniamo che le persone dietro queste attività si coordinino tra loro per travisare chi sono e cosa stanno facendo.

Gli account che si impegnano in operazioni di influenza spesso evitano di pubblicare contenuti che di per sé violerebbero le linee guida delle piattaforme. Per questo motivo, quando li analizziamo, ci concentriamo sul comportamento degli account e sui collegamenti tecnici, cercando in particolare le prove che:

- Si coordinano tra loro. Ad esempio, sono gestiti dalla stessa entità, condividono analogie tecniche come l'utilizzo degli stessi dispositivi o collaborano per diffondere la stessa narrazione.
- I soggetti in questione ingannano i nostri sistemi o i nostri utenti. Ad esempio, tentano nascondere la loro posizione reale o utilizzano personaggi falsi per spacciarsi per qualcuno che non sono.
- Cercano di manipolare o corrompere il dibattito pubblico per influenzare il processo decisionale, le convinzioni e le opinioni di una comunità. Ad esempio, cercano di plasmare il discorso su un'elezione o un conflitto.

Questi criteri sono allineati agli standard del settore e alle indicazioni degli esperti che consultiamo regolarmente. Sono particolarmente importanti per aiutarci a distinguere il coordinamento malevolo e non autentico dalle interazioni autentiche che fanno parte di comunità sane e aperte. Ad esempio, non violerebbe le nostre politiche se un gruppo di persone collaborasse autenticamente per sensibilizzare o fare una campagna per una causa sociale o per esprimere un'opinione condivisa (comprese le opinioni politiche). Tuttavia, più account che lavorano insieme in modo ingannevole per diffondere messaggi simili nel tentativo di influenzare le discussioni pubbliche sarebbero vietati e interrotti.



Misura 14.2	
QRE 14.2.1	<p>L'attuazione delle nostre politiche è garantita da diversi mezzi, tra cui strumenti specificamente progettati (come le levette per rivelare i contenuti di marca - cfr. QRE 14.1.1) o indagini umane per individuare comportamenti ingannevoli (per le attività CIO - cfr. QRE 14.1.2).</p> <p>L'attuazione di queste politiche è garantita anche da misure di controllo applicate in tutti gli Stati membri.</p> <p>Le indagini CIO richiedono molte risorse e un'analisi approfondita per garantire un'elevata fiducia nelle azioni proposte. Quando i nostri team hanno il necessario grado di certezza che un account sia coinvolto in un CIO o sia collegato a reti che abbiamo eliminato in passato come parte di un CIO, viene rimosso dalla nostra Piattaforma.</p> <p>Allo stesso modo, quando i nostri team hanno un elevato grado di certezza che un contenuto specifico violi una delle nostre politiche relative ai TTP (cfr. QRE 14.1.1), tale contenuto viene rimosso da TikTok.</p> <p>Infine, potremmo ridurre la scopribilità di alcuni contenuti, anche rendendo i video non idonei alla raccomandazione nella sezione For You della nostra piattaforma. È il caso, ad esempio, dei contenuti che ingannano o manipolano gli utenti aumentare in modo non autentico i follower, i like o le visualizzazioni.</p>



SLI 14.2.1 - SLI 14.2.4								
TTP O AZIONE1	TTP n. 1: creazione di account o botnet non autentici (che possono includere account automatizzati, parzialmente automatizzati o non automatizzati) Metodologia di misurazione dei dati Abbiamo basato il numero di: (i) account falsi rimossi; e (ii) follower degli account falsi (identificati al momento della rimozione dell'account falso), in base al Paese in cui l'account falso è stato attivo per l'ultima volta. Abbiamo aggiornato la nostra metodologia per riportare il rapporto tra la media mensile degli account falsi e gli utenti attivi mensili, sulla base dell'ultima pubblicazione degli utenti attivi mensili, al fine di riflettere meglio i contenuti legati ai TTP rispetto ai contenuti complessivi del servizio.							
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3			SLI 14.2.4		
	N. di azioni intraprese da tipo	Interazione/impegno prima dell'azione				TTP correlati contenuto in relazione a complessivo contenuto su il servizio		



Elenco delle azioni per Stato membro (vedi tabella di esempio)	Numero di account falsi rimossi	Numero di follower degli account falsi individuati al momento della rimozione				Rapporto tra la media mensile degli account Fake e gli utenti attivi mensili		
Stati membri								
Austria	92,511	467,635						
Belgio	176,327	544,073						
Bulgaria	423,060	188,995						
Croazia	74,704	175,230						
Cipro	86,741	124,021						
Repubblica Ceca	194,925	348,626						
Danimarca	155,675	298,306						
Estonia	111,506	239,039						
Finlandia	99,745	195,684						
Francia	2,061,174	20,207,105						
Germania	1,678,822	20,545,728						



Grecia	133,443	1,702,918						
Ungheria	84,057	184,291						
Irlanda	321,237	697,840						
Italia	672,344	5,900,534						
Lettonia	60,145	124,765						
Lituania	79,417	300,241						
Lussemburgo	73,258	611,602						
Malta	60,192	226,073						
Paesi Bassi	886,619	1,575,641						
Polonia	360,959	3,192,516						
Portogallo	190,906	370,719						
Romania	294,195	4,045,608						
Slovacchia	131,567	1,347,301						
Slovenia	298,807	45,359						
Spagna	709,560	5,351,682						
Svezia	239,020	528,326						
Islanda	31,476	253,997						
Liechtenstein	1,369	11,129						
Norvegia	92,800	151,088						



Totale UE	9,750,916	69,539,858				0.010		
Totale SEE	9,876,561	69,956,072						

TTP O AZIONE 2	TTP n. 2: Uso di reazioni false/inautentiche (ad es. like, voti alti, commenti) Metodologia di misurazione dei dati: Abbiamo basato il numero di like falsi rimossi sul Paese di registrazione dell'utente. Abbiamo anche basato il numero di like falsi evitati sul Paese di registrazione dell'utente.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Numero di azioni intraprese per tipo	Interazione/impegno prima dell'azione		
Elenco delle azioni per Stato membro (vedi tabella di esempio)	Numero di like falsi rimossi	Numero di like falsi evitati		
Austria	12,262,551	39,213,306		
Belgio	16,913,076	56,682,105		



Bulgaria	6,468,521	40,004,761		
Croazia	1,821,268	17,901,159		
Cipro	4,176,517	6,960,047		
Repubblica Ceca	3,052,689	31,099,711		
Danimarca	4,183,605	17,585,666		
Estonia	687,649	7,385,026		
Finlandia	3,086,208	19,264,460		
Francia	78,227,394	336,499,329		
Germania	131,158,324	357,582,219		
Grecia	14,621,872	84,211,417		
Ungheria	1,950,636	28,069,699		



Irlanda	4,520,433	31,110,363		
Italia	60,514,367	606,697,045		
Lettonia	1,690,473	11,600,082		
Lituania	1,682,687	11,795,998		
Lussemburgo g	1,920,605	7,987,636		
Malta	1,395,676	3,466,698		
Paesi Bassi	23,557,961	101,316,771		
Polonia	8,833,014	208,518,568		
Portogallo	9,239,486	56,146,620		
Romania	11,254,476	83,405,388		
Slovacchia	1,208,123	18,154,505		

Slovenia	727,133	5,843,233		
Spagna	38,331,442	161,280,031		
Svezia	15,782,957	48,240,073		
Islanda	230,931	1,564,206		
Liechtenstei n	24,827	70,045		
Norvegia	5,457,966	20,708,187		
Totale UE	459,269,143	2,398,021,916		
Totale SEE	464,982,867	2,420,364,354		

TTP O AZIONE 3	<p>TTP n. 3: Uso di falsi follower o abbonati Metodologia di misurazione dei dati:</p> <p>Abbiamo basato il numero di follower falsi rimossi sul Paese di registrazione dell'utente. Abbiamo anche basato il numero di follower falsi evitati sul Paese di registrazione dell'utente.</p>
-------------------	---

	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Numero di azioni intraprese per tipo	Interazione/impegno prima dell'azione		
Elenco delle azioni per Stato membro (vedi tabella esempio)	Numero di follower falsi rimossi	Numero di falsi seguiti evitati		
Stati membri				
Austria	9,980,544	25,000,123		
Belgio	11,916,866	34,550,567		
Bulgaria	4,561,129	26,400,841		
Croazia	1,965,426	18,990,456		
Cipro	1,706,405	18,497,473		



Repubblica Ceca	4,342,681	18,233,387		
Danimarca	3,154,022	23,806,634		
Estonia	482,641	16,887,949		
Finlandia	3,204,999	20,303,735		
Francia	109,481,878	127,136,908		
Germania	125,941,360	138,933,948		
Grecia	7,880,295	38,712,931		
Ungheria	2,589,692	24,773,097		
Irlanda	3,213,842	25,239,860		
Italia	35,511,559	158,916,638		
Lettonia	732,030	17,952,175		



Lituania	2,057,659	18,928,046		
Lussemburgo	1,574,849	21,051,498		
Malta	401,869	15,758,979		
Paesi Bassi	17,070,055	35,162,609		
Polonia	10,128,172	54,501,610		
Portogallo	3,714,261	26,901,973		
Romania	14,021,343	44,172,801		
Slovacchia	4,288,570	21,010,637		
Slovenia	678,185	1,942,793		
Spagna	31,084,803	73,920,335		
Svezia	12,342,226	36,451,604		

Islanda	120,003	2,572,695		
Liechtenstei n	893,407	1,045,728		
Norvegia	3,756,414	7,242,021		
Totale UE	424,027,361	1,084,139,607		
Totale SEE	428,797,185	1,095,000,051		

TTP O AZIONE 4	<p>TTP n. 4: Creazione di pagine, gruppi, gruppi di chat, forum o domini non autentici</p> <p>TikTok non ha pagine, gruppi, gruppi di chat, forum o domini. Questo TTP non è pertinente alla nostra piattaforma.</p>
-------------------	--

TTP O AZIONE 5	<p>TTP n. 5: Dirottamento o impersonificazione dell'account Metodologia di misurazione dei dati:</p> <p>Il numero di account rimossi in base alla nostra politica di impersonificazione si basa sulla posizione approssimativa degli utenti. Abbiamo aggiornato la nostra metodologia per riportare il rapporto tra la media mensile degli account di impersonificazione banditi e gli utenti attivi mensili, sulla base dell'ultima pubblicazione degli utenti attivi mensili, al fine di riflettere meglio i contenuti relativi ai TTP rispetto ai contenuti complessivi del servizio.</p>			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4

	Numero di azioni intraprese per tipo			Contenuto relativo ai TTP in relazione al contenuto complessivo del servizio.
Stati membri	Numero di account banditi in base alla politica di impersonificazione			Conti di impersonificazione su utenti attivi mensili
Elenco delle azioni per Stato membro (vedi tabella esempio)				
Austria	177			
Belgio	300			
Bulgaria	175			
Croazia	77			
Cipro	54			
Repubblica Ceca	134			
Danimarca	115			
Estonia	29			
Finlandia	92			
Francia	2,587			
Germania	2,277			



Grecia	215			
Ungheria	141			
Irlanda	235			
Italia	805			
Lettonia	48			
Lituania	76			
Lussemburgo	43			
Malta	0			
Paesi Bassi	567			
Polonia	1,251			
Portogallo	206			
Romania	1,300			
Slovacchia	63			
Slovenia	43			
Spagna	709			
Svezia	284			
Islanda	15			
Liechtenstein	0			



Norvegia	178			
Totale UE	12,003			0.000013
Totale SEE	12,196			

TTP O AZIONE 6	<p>TTP n. 6. Puntare deliberatamente su destinatari vulnerabili (ad esempio, tramite pubblicità personalizzata, spoofing della posizione o offuscamento)</p> <p>Metodologia di misurazione dei dati:</p> <p>Il numero di nuove reti CIO scoperte che hanno preso di mira i mercati dell'UE si riferisce alle nostre divulgazioni pubbliche per il periodo dal 1° luglio 2024 al 31 dicembre 2024. Abbiamo classificato le reti CIO interrotte in base al Paese che riteniamo abbia preso di mira la rete. Abbiamo incluso tutte le reti che, a nostro avviso, hanno preso di mira uno o più mercati europei o hanno operato da un mercato dell'UE. Pubblichiamo qui tutte le reti CIO che identifichiamo e rimuoviamo nei nostri rapporti di trasparenza.</p> <p>Le reti CIO identificate e rimosse sono descritte in dettaglio qui di seguito, compresa la posizione geografica valutata del funzionamento della rete e il pubblico target valutato della rete, che valutiamo attraverso prove tecniche e comportamentali da fonti proprietarie e aperte. Il numero di follower delle reti CIO è stato calcolato in base al numero di account che seguivano un account all'interno di una rete alla data di rimozione della rete stessa.</p>						
	SLI 14.2.1		SLI 14.2.2			SLI 14.2.3	SLI 14.2.4
	Stati membri (Rete origine)	Numero di istanze di identificato TTP	Numero di azioni intraprese per tipo	Interazione/impegno prima dell'azione	Visualizzazioni/impressioni dopo l'azione	Interazione/impegno dopo l'azione	Tendenze sui pubblici mirati
Luglio-dicembre2024							



Germania	29 conto in il rete k	29 rimosso conti	137,671 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dalla Germania e mirato principalmente a un tedesco pubblico insieme ad altri Mercati europei. Il individui che si celano dietro questo rete creata in modo non autentico conti per amplificare narrazioni favorevoli a La politica estera russa. Il La rete è risultata alternare tra più lingue, indicando un tentativo di indirizzare il pubblico da più mercati.	
Italia	8	8 rimosso conti	3,790,110 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dall'Italia e rivolto a un pubblico globale. Le persone dietro a questo rete creata in modo non autentico conti per promuovere l'amministrazione russa. La rete è risultata visualizzare l'utente anomalo comportamento che valutiamo per essere un tentativo di amplificare in modo inautentico il suo contenuto.	

Germania	42 conto in il rete k	42 rimosso conti	127,451 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	<p>Valutiamo che questa rete operata dalla Germania e rivolto a un pubblico tedesco. Le persone dietro a questo rete sono risultati coordinate al di fuori di TikTok, attraverso un sistema di messaggistica piattaforma, dove hanno condiviso tattiche per amplificare la portata di pro-AFD (alternativa per Deutschland) contenuti politici mirato al 2024 Elezioni statali tedesche. Il rete ha tentato di eludere le azioni intraprese da TikTok contro gli account o contenuti che violavano il nostro politiche.</p>	
----------	--------------------------------------	---------------------	--	-----------------	--------------	---	--



Romania	22 conto in il rete k	22 rimosso conti	299,692 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dalla Romania e ha preso di mira un rumeno pubblico. Gli individui dietro questa rete ha creato account non autentici per per diffondere disinformazione e promuovere narrazioni critiche nei confronti di l'attuale Romania governo. La rete è stata trovato per indirizzare gli utenti lontano da TikTok ai siti web di notizie che valutiamo essere gestiti dalla rete per il perseguimento della sua strategia obiettivo.	
---------	--------------------------------------	---------------------	--	-----------------	--------------	---	--

Italia	22 conto in il rete k	22 rimosso conti	157,913 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dall'Italia e ha preso di mira un moldavo pubblico. Gli individui dietro questa rete ha creato account multipli per creare artificialmente amplificare le narrazioni filorusse critica nei confronti dell'attuale Il governo moldavo, in un tentativo di manipolazione discorso elettorale. Il è stato riscontrato che la rete crea notizie inautentiche in un tentativo di apparire come un informazioni più affidabili fonte.	
--------	--------------------------------------	---------------------	--	-----------------	--------------	---	--

Moldavia	68 conto in il rete k	21 rimosso conti	123 conti seguito un conto all'interno del rete come alla data del rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dalla Moldavia e ha preso di mira la Romania diaspora in Moldavia. Il individui che si celano dietro questo rete creata fittiziamente personaggi per promuovere Lurie Ciocan e il sociale Partito Democratico, tentativo per manipolare il rumeno discorso sulle elezioni. I conti all'interno della rete sono stati trovati per pubblicare un video generato dall'intelligenza artificiale di Stefano il Grande (Prezzo di Moldavia tra il 1457 e il 1504) per promuovere la narrazione della rete.	
----------	--------------------------------------	---------------------	--	-----------------	--------------	--	--



Romania	78 conto in il rete k	78 rimosso conti	1,781 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dalla Romania e ha preso di mira un rumeno pubblico. Gli individui dietro questa rete ha creato account non autentici per per amplificare le narrazioni nel Lingua rumena favorevole al candidato politico Călin Georgescu, nel tentativo di manipolare il rumeno discorso elettorale. Il conti all'interno della rete sono risultati in grado di amplificare la gli stessi commenti ripetutamente.	
Romania	12 conto in il rete k	12 rimosso conti	1,704 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dalla Romania e ha preso di mira un rumeno pubblico. Gli individui dietro questa rete ha creato account non autentici per per amplificare le narrazioni nel Lingua rumena favorevole al candidato politico Mircea Geoană, cercando di manipolare il rumeno discorso elettorale. Il conti in rete sono stati trovato per ripubblicare lo stesso video ripetutamente.	



Romania	21 conto in il rete k	21 rimosso conti	123 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete operata dalla Romania e ha preso di mira un rumeno pubblico. Gli individui dietro questa rete ha creato account non autentici per a Nicolae Ciucă e al PNL partito, cercando di manipolare il rumeno discorso elettorale. Il è stato riscontrato che la rete crea personaggi fittizi.	
Romania	27,217	27.217 rimossi conti	70,892 conti seguito un conto all'interno del rete come alla data di rimozione	Non misurato	Non misurato	Valutiamo che questa rete è stato gestito tramite un falso fornitore di impegno e ha preso di mira un rumeno pubblico. Gli individui dietro questa rete ha usato account non autentici per promuovere la politica dell'AUR e indipendente candidato Călin Georgescu, in un tentativo di manipolazione Elezioni in Romania discorso. Questa campagna si è affidato alla pubblicazione di commenti piuttosto che i video.	

TTP O AZIONE 7	<p>TTP n. 7: impiego di mezzi di comunicazione manipolati e ingannevoli (ad es. "deep fakes", "cheap fakes"...) </p> <p>Abbiamo basato i seguenti numeri sul Paese in cui il video è stato pubblicato: video rimossi a causa di violazioni della politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC). Il numero di visualizzazioni dei video rimossi per violazione di ciascuna di queste policy si basa sulla posizione approssimativa dell'utente.</p>			
Stati membri	Numero di video rimossi a causa della violazione di Edited Media and Politica sui contenuti generati dall'intelligenza artificiale (AIGC)	Numero di visualizzazioni dei video rimosso a causa della politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC).	Numero di video unici etichettati con il tag AIGC "Creatore etichettato come Generato dall'intelligenza artificiale"	Numero di video unici etichettati con il tag AIGC "generato dall'intelligenza artificiale".
Austria	414	216,433	110,859	38,531
Belgio	2,092	1,119,223	166,222	75,316
Bulgaria	227	5,977	75,036	78,668
Croazia	1,361	58,579	27,536	18,595
Cipro	948	19,441	59,263	3,165
Repubblica Ceca	465	8,287,531	51,417	89,409
Danimarca	315	2,742,457	49,328	30,694

Estonia	208	2,063,380	19,687	11,220
Finlandia	716	464,824	60,083	49,106
Francia	8,563	312,078,908	1,399,713	432,739
Germania	11,199	23,904,234	1,380,835	502,916
Grecia	8,742	145,950	206,528	7,936
Ungheria	261	86,870	63,319	74,704
Irlanda	1,063	103,199	32,936	34,736
Italia	3,574	1,892,355	746,928	393,642
Lettonia	129	4,519	99,265	18,852
Lituania	203	25,410	42,778	21,581



Lussemburgo	223	8,729	40,901	3,319
Malta	183	5,811,847	12,100	3,444
Paesi Bassi	1,883	9,080,526	202,203	29,448
Polonia	772	13,404,186	203,835	316,048
Portogallo	1,010	339,124	151,389	64,975
Romania	937	623,525	287,851	37,467
Slovacchia	98	2,014	21,883	28,439
Slovenia	66	605	10,131	6,969
Spagna	4,392	21,882,268	676,935	493,675
Svezia	762	377,862	163,490	105,253



Islanda	85	6,113	3,353	4,720
Liechtenstei n	48	525	357	61
Norvegia	679	139,984	59,556	42,172
Totale UE	50,806	404,749,976	6,362,451	2,970,847
Totale SEE	51,618	404,896,598	6,425,717	3,017,800

TTP O AZIONE 8 Membro	<p>TTP n. 8: utilizzare l'operazione "hack and leak" (che può includere o meno contenuti falsificati)</p> <p>Abbiamo fornito i dati relativi alle reti CIO che abbiamo interrotto nel periodo di riferimento nell'ambito del TTP n. 6. Abbiamo inoltre fornito dati sulle violazioni della nostra politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC) nell'ambito del TTP n. 7. La nostra politica di hacking e leaking è stata lanciata di recente, nel primo semestre del 2024, ma non disponiamo di metriche significative da riferire per il secondo semestre.</p>
-----------------------------	---



TTP O AZIONE 9	TTP n. 9: coordinamento non autentico della creazione o dell'amplificazione di contenuti, compresi i tentativi di ingannare/manipolare gli algoritmi delle piattaforme (ad es. keyword stuffing o post/reposting non autentici progettati per ingannare le persone sulla popolarità dei contenuti, anche da parte degli influencer)			
	Abbiamo fornito i dati relativi alle reti CIO che abbiamo interrotto nel periodo di riferimento nell'ambito del TTP n. 6.			

TTP O AZIONE 10	TTP n. 10: uso di pratiche ingannevoli per ingannare/manipolare gli algoritmi della piattaforma, ad esempio per creare, amplificare o dirottare hashtag, vuoti di dati, bolle di filtraggio o camere dell'eco.			
	Abbiamo fornito i dati relativi alle reti CIO che abbiamo interrotto nel periodo di riferimento nell'ambito del TTP n. 6.			

TTP O AZIONE 11	TTP n. 11. Messaggi o promozioni non trasparenti e compensati da parte degli influencer			
	Metodologia di misurazione dei dati: Non siamo in grado di fornire questa metrica a causa dei dati insufficienti disponibili per il periodo di riferimento.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
	Numero di azioni intraprese per tipo			
Stati membri				
Elenco delle azioni per Stato membro (vedi tabella esempio)				



TTP O AZIONE 12	TTP n. 12: segnalazione coordinata di massa di contenuti o account opposti non violenti			
	Abbiamo fornito i dati relativi alle reti CIO che abbiamo interrotto nel periodo di riferimento nell'ambito del TTP n. 6.			
	SLI 14.2.1	SLI 14.2.2	SLI 14.2.3	SLI 14.2.4
Stati membri				
Elenco delle azioni per Stato membro (vedi tabella esempio)				

Misura 14.3	
QRE 14.3.1	Abbiamo collaborato nell'ambito del gruppo di lavoro sull'integrità dei servizi per creare il primo elenco di TTP.



IV. Integrità dei servizi	
Impegno 15	
I firmatari rilevanti che sviluppano o gestiscono sistemi di IA e che diffondono contenuti generati dall'IA e manipolati attraverso i loro servizi (ad es. deep fake) si impegnano a prendere in considerazione gli obblighi di trasparenza e l'elenco delle pratiche manipolative vietate dalla proposta di legge sull'intelligenza artificiale.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì



<p>Se sì, elencare queste misure di attuazione [breve punti elenco].</p>	<ul style="list-style-type: none"> ● Sulla base della nostra nuova etichetta generata dall'IA, che consente ai creatori di rivelare i contenuti completamente generati dall'IA o modificati in modo significativo dall'IA, abbiamo ampliato i nostri sforzi nello spazio AIGC: <ul style="list-style-type: none"> ○ Implementazione delle credenziali di contenuto della Coalition for Content Provenance and Authenticity (C2PA) che consente ai nostri sistemi di riconoscere istantaneamente ed etichettare automaticamente l'AIGC. ○ Sostenere i gruppi di lavoro della coalizione come membro generale di C2PA. ○ Aderire alla Content Authenticity Initiative (CAI) per promuovere una più ampia adozione dello standard tecnico. ○ Pubblicazione di un nuovo articolo del Centro per la trasparenza Sostegno a responsabili e contenuti generati dall'intelligenza artificiale trasparenti. ○ Sulla base della nostra nuova etichetta per i contenuti generati dall'IA per i creatori e dell'implementazione delle C2PA Content Credentials, abbiamo lanciato una serie di campagne di alfabetizzazione mediatica con la guida di organizzazioni esperte come Mediawise e WITNESS, anche in Brasile, Germania, Francia, Messico e Regno Unito, che insegnano alla nostra comunità come individuare ed etichettare i contenuti generati dall'IA. Questa campagna di trasparenza dell'AIGC, informata da WITNESS, ha raggiunto 80 milioni di utenti a livello globale, di cui oltre 8,5 milioni e 9,5 milioni rispettivamente in Germania e in Francia. ● Ha continuato a unirsi ai partner del settore come parte del "Tech Accord to Combat Deceptive Use of AI in 2024 Elections", un impegno comune per combattere l'uso ingannevole dell'IA nelle elezioni. ● Continuiamo a partecipare a gruppi di lavoro rilevanti, come il gruppo di lavoro sull'IA generativa, che ha preso il via nel settembre 2023.
<p>Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]</p>	<p>No</p>
<p>Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?</p>	<p>Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto COPD.</p>
<p>Misura 15.1</p>	



QRE 15.1.1

La nostra politica sui media modificati e sui contenuti generati dall'IA (AIGC) include un linguaggio comunemente usato e facilmente comprensibile quando ci si riferisce all'AIGC, e delinea i nostri divieti esistenti sull'AIGC che mostra false fonti autorevoli o eventi di crisi, o che mostra falsamente personaggi pubblici in determinati contesti, tra cui il bullismo, l'endorsement o l'essere sostenuti. Con l'evoluzione dell'intelligenza artificiale, continuiamo a investire nella lotta contro l'AIGC dannosa, evolvendo i nostri modelli di rilevamento proattivo, consultando esperti e collaborando con i colleghi per trovare soluzioni condivise.

Sebbene accogliamo con favore la creatività che la nuova IA può liberare, in linea con la nostra politica aggiornata, gli utenti devono rivelare in modo proattivo quando i loro contenuti sono generati dall'IA o manipolati ma mostrano scene realistiche (cioè persone, luoghi o eventi finti che sembrano reali). Nel settembre 2023 abbiamo lanciato un'opzione AI che consente agli utenti di rivelare autonomamente i contenuti generati dall'IA quando pubblicano. Quando questa opzione è attivata, gli utenti visualizzano il tag "Creatore etichettato come generato dall'IA". In alternativa, è possibile utilizzare un adesivo o una didascalia, come "sintetico", "falso", "non reale" o "alterato".

Inoltre, etichettiamo automaticamente i contenuti realizzati con gli effetti di TikTok se utilizzano l'IA. TikTok può applicare automaticamente l'etichetta "generato dall'IA" ai contenuti che identifichiamo come completamente generati o significativamente modificati con l'IA. Ciò può accadere quando un creatore utilizza gli effetti AI di TikTok o carica contenuti generati dall'AI a cui sono allegate le Content Credentials, una tecnologia della Coalition for Content Provenance and Authenticity (C2PA). Le credenziali di contenuto allegano metadati al contenuto che possiamo utilizzare per riconoscere ed etichettare immediatamente l'AIGC. Una volta che il contenuto è etichettato come Generati dall'AI con un'etichetta automatica, gli utenti non sono in grado di rimuovere l'etichetta dal

post. Non consentiamo:

- AIGC che mostra persone dall'aspetto realistico di età inferiore a 18 anni
- AIGC che mostra le sembianze di figure private adulte, se veniamo a conoscenza del fatto che sono state utilizzate senza il loro permesso.
- Media fuorvianti dell'AIGC o modificati che mostrano falsamente:
 - Contenuti che sembrano provenire da una fonte autorevole, come ad esempio un'organizzazione giornalistica rispettabile.
 - Un evento di crisi, come un conflitto o una catastrofe naturale
 - Un personaggio pubblico che è:
 - essere degradati o molestati, o assumere comportamenti criminali o antisociali
 - prendere posizione su una questione politica, su un prodotto commerciale o su una questione di importanza pubblica (come le elezioni)



	■ essere appoggiato o condannato politicamente da un individuo o da un gruppo
Misura 15.2	
QRE 15.2.1	<p>Abbiamo una serie di misure per garantire che i sistemi di IA che sviluppiamo rispettino i principi di equità e siano conformi alle leggi vigenti. A tal fine:</p> <ul style="list-style-type: none">● Abbiamo predisposto linee guida e formazione interne per garantire che la formazione e l'utilizzo dei nostri sistemi di IA siano conformi alle leggi sulla protezione dei dati e ai principi di correttezza.● Abbiamo istituito un processo di verifica della conformità per i nuovi sistemi di intelligenza artificiale che soddisfano determinate soglie e stiamo lavorando per dare priorità alla verifica degli algoritmi sviluppati in precedenza. <p>Siamo inoltre orgogliosi di essere un partner di lancio della Partnership on AI's Responsible Practices for Synthetic Media.</p>

IV. Integrità dei servizi	
Impegno 16	
I firmatari interessati si impegnano a gestire canali di scambio tra i loro team competenti al fine di condividere in modo proattivo le informazioni sulle operazioni di influenza multiplatforma, sulle interferenze straniere nello spazio informativo e sugli incidenti rilevanti che emergono sui rispettivi servizi, con l'obiettivo di prevenire la diffusione e la ricomparsa su altri servizi, nel pieno rispetto della legislazione sulla privacy e con la dovuta considerazione per i rischi per la sicurezza e i diritti umani.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì

Se sì, elencare queste misure di attuazione [brevi punti elenco].	Impegnarsi attivamente con il gruppo di lavoro Crisis Response, condividendo le intuizioni e gli insegnamenti sulle aree rilevanti, compresi i CIO.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto COPD.
Misura 16.1	



QRE 16.1.1		<p>Il fulcro della nostra strategia per l'identificazione e la rimozione dei CIO sulle nostre piattaforme è la collaborazione con le nostre parti interessate, dalla società civile alle segnalazioni degli utenti. Questo approccio facilita noi - e altri - nell'interrompere le operazioni della rete nelle loro iniziali. Oltre a migliorare continuamente le nostre capacità interne, ci impegniamo proattivamente in revisioni complete dei risultati resi pubblici dai nostri colleghi e implementiamo rapidamente le azioni necessarie in linea con le nostre politiche.</p> <p>Per fornire aggiornamenti più regolari e dettagliati sulle CIO che abbiamo interrotto, abbiamo introdotto un nuovo rapporto di trasparenza dedicato alle operazioni di influenza occultadisponibile nel centro di trasparenza di TikTok. In questo rapporto abbiamo anche aggiunto nuove informazioni sulle operazioni che abbiamo precedentemente rimosso e che hanno tentato di tornare sulla nostra piattaforma con nuovi account. Le informazioni e le metriche contenute in questo rapporto hanno lo scopo di informare i colleghi del settore e la comunità di ricerca.</p> <p>Condividiamo gli approfondimenti e le metriche rilevanti all'interno dei nostri report trimestrali sulla trasparenza, l'obiettivo di informare i colleghi del settore e la comunità dei ricercatori. Esaminiamo inoltre gli approfondimenti e le metriche pertinenti di altri colleghi del settore per effettuare confronti incrociati su eventuali comportamenti simili su TikTok.</p> <p>Continuiamo a partecipare ai sottogruppi istituiti per la condivisione delle conoscenze tra i firmatari e la Commissione.</p> <p>Come abbiamo illustrato in altri capitoli di questo rapporto, disponiamo di solide politiche per l'integrità della monetizzazione e abbiamo stabilito procedure operative congiunte tra i team specializzati nelle indagini sulle CIO e i team per l'integrità della monetizzazione per lavorare a indagini congiunte sulle CIO che coinvolgono prodotti monetizzati.</p>		
SLI 16.1.1		N/D		
Numero di azioni come risultato della condivisione delle informazioni				
Dati				
Misura 16.2				



QRE 16.2.1

Pubblichiamo [qui](#) tutte le reti CIO che identifichiamo e rimuoviamo nei nostri rapporti di trasparenza. Non appena emergeranno nuovi comportamenti ingannevoli, continueremo ad evolvere la nostra risposta, a rafforzare le capacità di applicazione e a pubblicare i nostri risultati.



V. Empow ering Users

Impegni 17 - 25



V. Responsabilizzare gli utenti	
Impegno 17	
Alla luce delle iniziative della Commissione europea nel campo dell'alfabetizzazione mediatica, compreso il nuovo Piano d'azione per l'educazione digitale, i firmatari rilevanti si impegnano a proseguire e rafforzare i loro sforzi nel campo dell'alfabetizzazione mediatica e del pensiero critico, anche con l'obiettivo di includere i gruppi vulnerabili.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì



Se sì, elencare queste misure di attuazione [brevi punti elenco].

- Abbiamo lanciato due nuove **campagne generali di alfabetizzazione ai media e di capacità di pensiero critico** nell'UE e due nei Paesi candidati all'UE, in collaborazione con i nostri partner per il fact-checking e l'alfabetizzazione ai media:
 - Francia: Agence France-Presse (AFP)
 - Portogallo: Polígrafo
 - Georgia: Fact Check Georgia
 - Moldavia: StopFals!

Il numero di campagne di alfabetizzazione generale ai media e alle capacità di pensiero critico in Europa sale così a 11 (Danimarca, Finlandia, Francia, Georgia, Irlanda, Italia, Spagna, Svezia, Moldavia, Paesi Bassi e Portogallo).

- Sono stati assunti due nuovi partner per il fact-checking in Europa:
 1. Albania e Kosovo: Internews Kosova
 2. Georgia: Fact Check Georgia
- Abbiamo ampliato la nostra copertura di fact-checking a una serie di Paesi dell'Europa allargata e candidati all'UE:
 - Albania e Kosovo: Internews Kosova
 - Georgia: Fact Check Georgia.
 - Kazakistan: Reuters
 - Moldavia: AFP/Reuters
 - Serbia: Storie di punta
- Abbiamo realizzato 14 **campagne** temporanee di **alfabetizzazione mediatica sull'integrità elettorale** prima delle elezioni regionali, la maggior parte delle quali in collaborazione con i nostri partner per il fact-checking e l'alfabetizzazione mediatica:
 - 8 nell'UE (Austria, Croazia, Francia, 2 x Germania, Irlanda, Lituania e Romania)
 - Austria: Deutsche Presse-Agentur (dpa)
 - Croazia: Faktograf
 - Francia: Agence France-Presse (AFP)
 - Germania (elezioni regionali): Deutsche Presse-Agentur dpa)
 - Germania (elezioni federali): Deutsche Presse-Agentur dpa)
 - Irlanda: Il giornale
 - Lituania: N/A
 - Romania: Cittadini Funky.
 - 1 nel SEE
 - Islanda: N/A
 - 5 in Europa allargata/paesi candidati all'UE (Bosnia, Bulgaria, Cechia, Georgia e Moldavia)
 - Bosnia: N/A

- Bulgaria: N/A
- Cechia: N/A
- Georgia: Fact Check Georgia
- Moldavia: StopFals!

- Durante il periodo di riferimento, abbiamo organizzato 9 sessioni **della Election Speaker Series**, 7 negli Stati membri dell'UE e 2 in Georgia e Moldavia.
 1. Francia: Agence France-Presse (AFP)
 2. Germania: Agenzia di stampa tedesca (dpa)
 3. Austria: Agenzia di stampa tedesca (dpa)
 4. Lituania: Fatti logici
 5. Romania: Cittadini divertenti
 6. Irlanda: Fatti logici
 7. Croazia: Faktograf
 8. Georgia: FactCheck Georgia
 9. Moldavia: Stop a Fals!
- Lanciate quattro nuove **guide** temporanee in-app **per la ricerca di informazioni sulle** catastrofi naturali che rimandano ad agenzie e organizzazioni terze autorevoli:
 - 1) Alluvioni nell'Europa centrale e orientale (Austria, Bosnia, Cechia, Germania, Ungheria, Moldavia, Polonia, Romania e Slovacchia)
 - 2) Incendi in Portogallo
 - 3) Alluvioni in Spagna
 - 4) Ciclone di Mayotte
- Abbiamo continuato i nostri interventi in-app, tra cui video tag, interventi di ricerca e centri di informazione in-app, disponibili in 23 lingue ufficiali dell'UE e in norvegese e islandese per gli utenti del SEE, in merito alle elezioni, al conflitto Israele-Hamas, al cambiamento climatico, all'educazione all'Olocausto, all'Mpox e alla guerra in Ucraina.
- Ha partecipato attivamente **al vertice sui cambiamenti climatici COP29 Nazioni Unite**:
 - Collaborare con la presidenza della COP29 per promuovere i loro contenuti e coinvolgere nuovo pubblico intorno alla conferenza come media partner strategico.
 - Rilancio della campagna globale [#ClimateAction](#) con oltre 7.000 post da tutto il mondo. I contenuti di [#ClimateAction](#) hanno ricevuto oltre 4 miliardi di visualizzazioni video dal lancio nel 2021.
 - Portando al summit 5 creatori, che hanno prodotto collettivamente più di 15 video che hanno ricevuto oltre 60 milioni di visualizzazioni.
 - Lancio di due funzionalità globali (un tag di avviso video e una guida all'intervento di ricerca) per indirizzare gli utenti verso contenuti autorevoli relativi al clima tra il 29 ottobre e il 25 novembre, che sono stati visualizzati 400.000 volte.



- La nostra partnership con [Verified for Climate](#), un'iniziativa congiunta delle Nazioni Unite e dell'agenzia di impatto sociale Purpose, ha continuato a essere la nostra iniziativa di punta per il clima, che ha visto una rete di 35 Campioni Verificati in Brasile, Emirati Arabi Uniti e Spagna, lavorare con selezionati creatori di TikTok per sviluppare contenuti educativi che affrontano la disinformazione e l'informazione sul clima e promuovere l'azione per il clima all'interno della comunità di TikTok.
- [Collaborazione con l'Organizzazione Mondiale della Sanità \(OMS\)](#), con una donazione di 3 milioni di dollari, per sostenere la consapevolezza e l'alfabetizzazione sul benessere mentale creando contenuti affidabili e combattendo la disinformazione attraverso la rete [Fides](#), una comunità eterogenea di professionisti sanitari e creatori di contenuti di fiducia nel Regno Unito, negli Stati Uniti, in Francia, Giappone, Corea, Indonesia, Messico e Brasile.
- Sulla base di questi sforzi, abbiamo anche lanciato la [UK Clinician Creator Network](#), un'iniziativa che riunisce 19 medici qualificati del NHS che condividono attivamente le loro competenze mediche su TikTok, coinvolgendo una comunità di oltre 2,2 milioni di follower.
- rafforzato il nostro approccio ai [media affiliati allo Stato](#):
 - Collaborare con esperti esterni di terze parti per definire la nostra politica sui media affiliati allo Stato, valutare le etichette dei media controllati dallo Stato e continuare a espanderne l'uso.
 - Investimenti continui nelle nostre capacità di rilevamento per gli account dei media affiliati allo Stato (SAM), con particolare attenzione all'automazione e al rilevamento scalare.
- Sulla base della nostra [etichetta di contenuti generati dall'IA](#) per i creatori e dell'implementazione delle C2PA [Content Credentials](#), abbiamo lanciato una serie di [campagne di alfabetizzazione mediatica](#) con la guida di organizzazioni esperte come Mediawise e WITNESS, anche in Brasile, Germania, Francia, Messico e Regno Unito, che insegnano alla nostra comunità come individuare ed etichettare i contenuti generati dall'IA.
 - La nostra campagna di trasparenza dell'AIGC, informata da WITNESS, ha raggiunto 80 milioni di utenti in tutto il mondo, tra cui oltre 8,5M e 9,5M rispettivamente in Germania e Francia.
- Abbiamo portato alla nostra comunità una maggiore trasparenza sui nostri sistemi e sui nostri sforzi di integrità e autenticità, condividendo regolarmente approfondimenti e aggiornamenti. Nel secondo semestre del 2024, abbiamo continuato a espandere il nostro [Centro per la trasparenza](#) con risorse come il nostro primo [Hub per l'integrità delle elezioni negli Stati Uniti](#), l'[Hub per l'integrità delle elezioni in Europa](#), i [rapporti sulle operazioni di influenza occulta](#) dedicati e un nuovo [blog del Centro per la trasparenza](#).
- Abbiamo proseguito la nostra collaborazione con la Amadeu Antonio Stiftung in Germania per il progetto Demo:create, un'iniziativa educativa che aiuta i giovani utenti di TikTok ad affrontare in modo efficace i discorsi di odio online, la disinformazione e la cattiva informazione.
- Continuare a investire nella formazione e nello sviluppo dei nostri team di moderazione umana.
- TikTok continua a co-presiedere il gruppo di lavoro sulle elezioni.



Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quale ulteriore misure di implementazione che pensate di mettere in atto nei prossimi 6 anni. mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto COPD.
Misura 17.1	



QRE 17.1.1

Oltre a rimuovere sistematicamente i contenuti che violano le nostre politiche di I&A, continuiamo a dedicare risorse significative per: espandere le nostre misure in-app che mostrano agli utenti un contesto aggiuntivo su determinati contenuti; reindirizzarli verso informazioni autorevoli; rendere questi strumenti disponibili in 23 lingue ufficiali dell'UE (più, per gli utenti del SEE, in norvegese e islandese).

Collaboriamo con esperti esterni per combattere la disinformazione dannosa. Ad esempio, collaboriamo con l'Organizzazione mondiale della sanità (OMS) per le informazioni mediche e con i nostri partner globali per il fact-checking, tenendo conto del loro feedback e di quello degli utenti, per identificare continuamente nuovi argomenti e valutare quali strumenti possano essere più adatti a sensibilizzare l'opinione pubblica su quell'argomento.

Mettiamo in campo una combinazione di **strumenti di intervento degli utenti** in-app su temi di attualità come le elezioni, il conflitto Israele-Hamas, [l'educazione all'Olocausto](#), Mpox e la guerra in Ucraina...

Tag avviso video.

Un video notice tag è una barra di informazioni in fondo a un video che viene applicata automaticamente a una parola o a un hashtag specifico (o a un insieme di hashtag). La barra informativa è cliccabile e invita gli utenti a "*saperne di più su* [l'argomento]". Gli utenti saranno indirizzati a un sito guida in-app, o una risorsa affidabile di terze parti, a seconda dei casi.



Fatti dell'Olocausto Video Avviso Tag

Intervento di ricerca. Se gli utenti cercano termini associati a un argomento, viene loro presentato un banner che li incoraggia a verificare i fatti e fornisce un link a una fonte di informazioni attendibile. Gli interventi di ricerca non vengono effettuati per i termini di ricerca che violano le nostre Linee guida della comunità, che vengono gestite in base alle nostre politiche.

- Ad esempio, le quattro nuove campagne di alfabetizzazione generale ai media e alle capacità di pensiero critico, lanciate in Francia, Georgia, Moldavia e Portogallo, sono tutte supportate da guide di ricerca per indirizzare gli utenti verso fonti autorevoli.
- Il nostro intervento di ricerca globale sulla COP29, che si è svolto dal 29 ottobre al 25 novembre, ha indirizzato gli utenti verso contenuti autorevoli sul clima ed è stato visualizzato 400.000 volte.



#COP29 for Climate Action

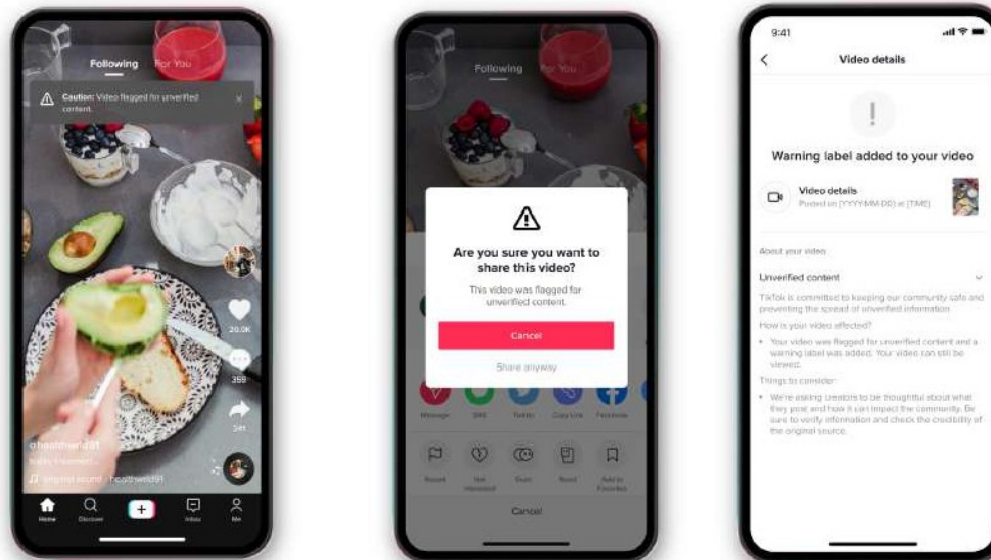
We all have a part to play in protecting our planet's future, and together, we can make a difference. [Learn more](#)

Annuncio di servizio pubblico (PSA). Se gli utenti cercano un hashtag sull'argomento, riceveranno un annuncio di servizio pubblico che ricorderà loro le nostre Linee guida della comunità e presenterà loro dei link a una fonte di informazioni attendibile.

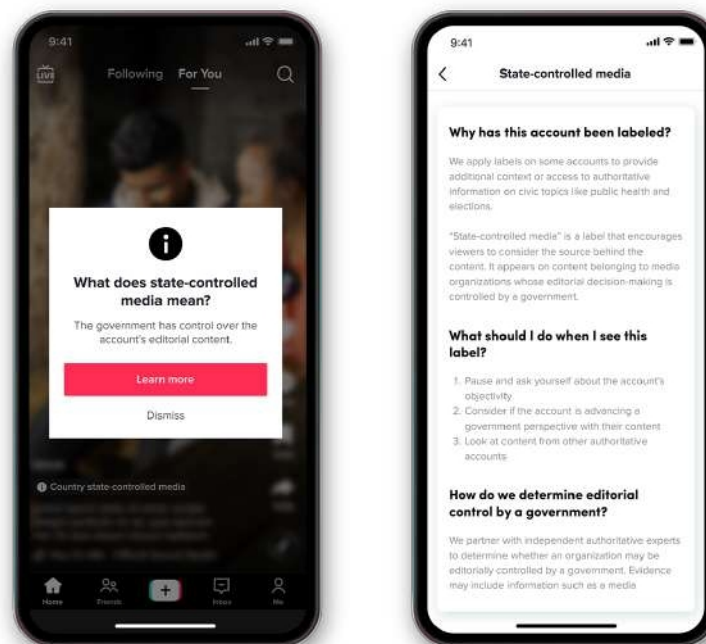
Etichetta dei contenuti non verificati. Oltre agli strumenti sopra menzionati, per incoraggiare gli utenti a considerare l'affidabilità dei contenuti relativi a un'emergenza o a un evento in corso, che sono stati valutati dai nostri partner per il fact-checking ma che non possono essere verificati come accurati, ovvero "contenuti non verificati", applichiamo etichette di avvertimento e invitiamo le persone a [riconsiderare la condivisione di](#) tali contenuti. I dettagli di queste etichette di avvertimento sono inclusi nelle nostre [Linee guida della comunità](#).

Dove gli utenti continuano a postare nonostante l'avviso:

- Per limitare la diffusione di informazioni potenzialmente fuorvianti, il video non potrà essere raccomandato nel feed For You.
- Il creatore del video viene anche informato che il suo video è stato segnalato come contenuto non comprovato e gli vengono fornite ulteriori informazioni sul motivo per cui l'etichetta di avvertimento è stata aggiunta al suo contenuto. Anche in questo caso, si tratta di sensibilizzare il creatore sulla credibilità dei contenuti che ha condiviso.



[Etichetta media controllati dallo Stato](#). La nostra politica sui media affiliati allo Stato consiste nell'etichettare gli account gestiti da entità la cui produzione editoriale o il cui processo decisionale sono soggetti al controllo o all'influenza di un governo. Appliciamo un'etichetta ben visibile a tutti i contenuti e agli account dei media controllati dallo Stato. All'utente viene inoltre mostrata una schermata pop-up che fornisce informazioni sul significato dell'etichetta, lo invita a "saperne di più" e lo reindirizza a una [pagina in-app](#). Questa misura porta trasparenza alla nostra comunità, sensibilizza gli utenti e li incoraggia a considerare l'affidabilità della fonte. Continuiamo a collaborare con gli esperti per informare il nostro approccio ed esplorare il modo in cui possiamo continuare a espanderne l'uso.



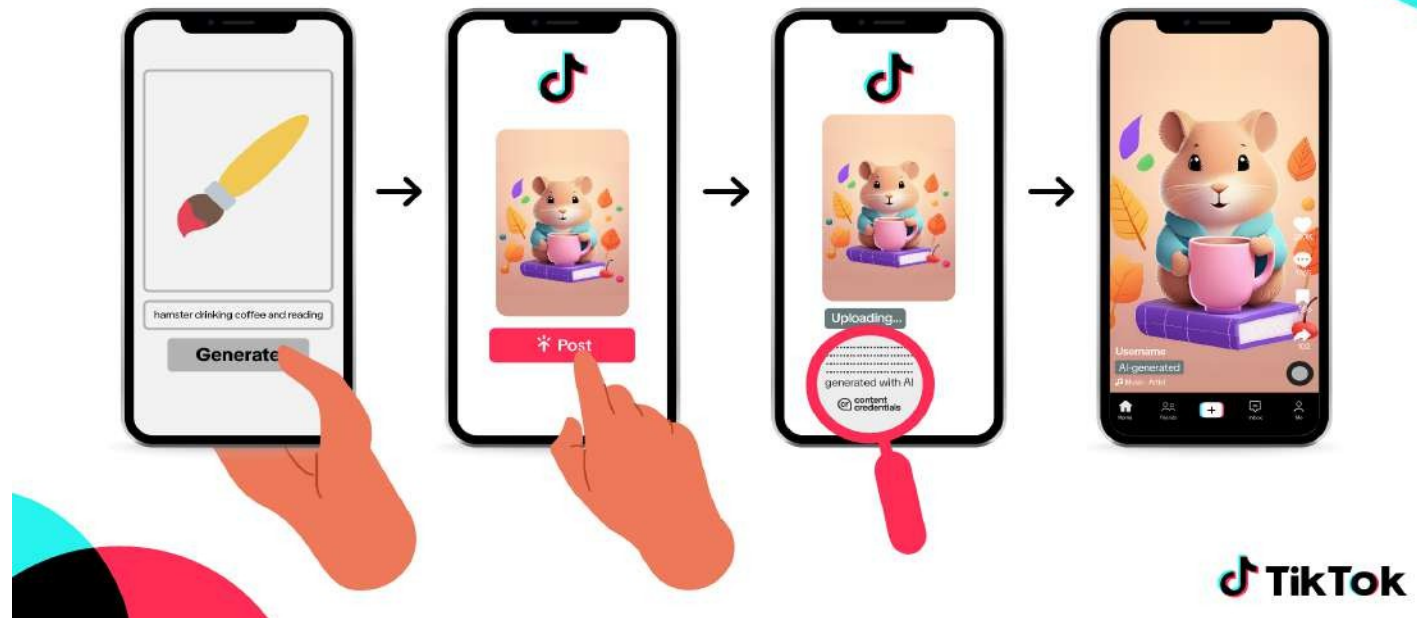
Nell'UE, in Islanda e nel Liechtenstein, abbiamo anche adottato misure per limitare l'accesso ai contenuti delle entità sanzionate dall'UE nel 2024:

- RT- Russia Today UK
- RT - Russia Oggi Germania
- RT - Russia Oggi Francia
- RT- Russia Oggi in spagnolo
- Sputnik
- Rossiya RTR / RTR Planeta
- Rossiya 24 / Russia 24
- Centro TV Internazionale
- NTV/NTV Mir
- Rossiya 1
- REN TV



	<ul style="list-style-type: none"> ● Pervyi Kanal / Canale 1 ● RT Arabo ● Sputnik Arabo ● RT Balcani ● Recensione orientale ● Tsargrad ● Nuova prospettiva orientale ● Katehon ● Voce dell'Europa ● RIA Novosti ● Izvestija ● Rossiiskaja Gazeta
--	--

Etichette per i contenuti generati dall'IA. Poiché un numero sempre maggiore di creatori sfrutta l'Intelligenza Artificiale (IA) per migliorare la propria creatività, sostenere pratiche di creazione di contenuti trasparenti e responsabili. Nel 2023 TikTok ha lanciato un'etichetta generata dall'IA per consentire ai creatori di rivelare i contenuti completamente generati dall'IA o modificati in modo significativo dall'IA. Il lancio di questo nuovo strumento per aiutare i creatori a etichettare i loro contenuti generati dall'IA è stato accompagnato da una [campagna di educazione dei creatori](#), da una [pagina del Centro assistenza](#) e da un [post della Newsroom](#). Nel maggio 2024, abbiamo iniziato a utilizzare le [credenziali di contenuto](#), della Coalition for Content Provenance and Authenticity (C2PA) che consentono ai nostri sistemi di riconoscere immediatamente ed etichettare automaticamente l'AIGC. Nell'interesse della trasparenza, abbiamo anche rinominato gli effetti TikTok AI in modo che includano esplicitamente "AI" nel loro nome e nella corrispondente etichetta degli effetti, e abbiamo aggiornato le nostre linee guida per i creatori di Effect House per fare lo stesso.





SLI 17.1.1	<p>Risorse informative online e in-app dedicate. I suddetti strumenti forniscono agli utenti collegamenti a informazioni accurate e aggiornate provenienti da fonti attendibili. A seconda dell'argomento trattato o del Paese dell'UE di riferimento, gli utenti possono essere indirizzati a un sito fonte autorevole esterna (ad esempio, un sito web del governo nazionale o una commissione elettorale nazionale indipendente), un centro di informazione all'interno dell'app (ad esempio, Guerra in Ucraina) o una pagina dedicata nel Centro per la sicurezza o nel Centro per la trasparenza di TikTok.</p> <p>Utilizziamo il nostro Safety Center per informare la nostra comunità sul nostro approccio alla sicurezza, alla privacy e alla protezione sulla nostra piattaforma. Per quanto riguarda la lotta alla disinformazione dannosa, abbiamo dedicato informazioni su:</p> <ul style="list-style-type: none">• Disinformazione dannosa, sfide online, Covid-19, integrità elettorale, truffe e come condividere in sicurezza contenuti su eventi tragici su TikTok.• La nostra pagina sui partner per la sicurezza fornisce dettagli su alcune delle nostre collaborazioni con esperti globali, organizzazioni non governative e associazioni di settore per contribuire a costruire una piattaforma sicura per la nostra comunità. <p>Gli utenti possono saperne di più sui nostri sforzi di trasparenza nel nostro Transparency Center dedicato, disponibile in diverse lingue dell'UE, che ospita i nostri rapporti di trasparenza, tra cui il rapporto indipendente sulle operazioni di influenza occulta e i rapporti che abbiamo pubblicato nell'ambito del presente Codice, nonché informazioni sui nostri impegni per il mantenimento dell'integrità della piattaforma, ad esempio Protezione dell'integrità delle elezioni, Lotta alla disinformazione, Contrasto alle operazioni di influenza, Sostegno a operazioni responsabili e trasparenti, Contenuti generati dall'intelligenza artificiale e dettagli sulle richieste di rimozione da parte del governo.</p> <p>Utilizziamo anche i post della Newsroom per tenere informata la nostra comunità sugli aggiornamenti e gli sforzi più recenti in materia di <i>notizie, prodotti, comunità, sicurezza e prodotti</i>. Gli utenti possono selezionare il proprio Paese, compresa l'UE, per la lingua preferita, se disponibile, e i post rilevanti a livello regionale. Ad esempio, dopo la pubblicazione del quarto rapporto sul Codice nel settembre 2024, abbiamo fornito agli utenti una panoramica del nostro costante impegno nella lotta alla disinformazione ai sensi del Codice di condotta dell'UE. Abbiamo anche aggiornato gli utenti su come stiamo collaborando con il nostro settore per far progredire la trasparenza e l'alfabetizzazione dell'IA e su come abbiamo protetto l'integrità della piattaforma durante le elezioni presidenziali rumene.</p>		
	<p>Metodologia di misurazione dei dati:</p> <p>Il numero di impressioni, di clic e di click-through rate dei tag di avviso video, degli interventi di ricerca e degli annunci di servizio pubblico si basano sulla posizione approssimativa degli utenti che hanno utilizzato gli strumenti. Il numero di impressioni delle pagine del Safety Center si basa sulla posizione IP degli utenti.</p>		
	Conteggio totale delle impressioni dello strumento	Interazioni/impegno con lo strumento	Altre metriche rilevanti



	Numero di impressioni sull'etichetta dei media controllati dallo Stato	Numero di clic dell'etichetta Media controllati dallo Stato	Tasso di click through dell'etichetta dei media controllati dallo Stato
Stati membri			
Austria	3,705,075	5,771	0.16%
Belgio	3,789,615	6,994	0.18%
Bulgaria	7,727,480	9,390	0.12%
Croazia	1,656,809	2,786	0.17%
Cipro	752,546	1,166	0.15%
Repubblica Ceca	7,602,192	7,762	0.10%
Danimarca	2,074,577	4,350	0.21%
Estonia	1,391,192	2,402	0.17%
Finlandia	3,310,339	9,274	0.28%
Francia	32,521,568	28,995	0.09%
Germania	37,522,365	49,125	0.13%
Grecia	3,107,902	6,491	0.21%
Ungheria	41,012,350	27,450	0.07%
Irlanda	3,250,908	6,757	0.21%
Italia	12,463,432	16,462	0.13%
Lettonia	3,063,840	4,027	0.13%
Lituania	3,025,380	5,056	0.17%

Lussemburgo	439,714	628	0.14%
Malta	417,073	605	0.15%
Paesi Bassi	14,557,284	23,801	0.16%
Polonia	203,836,052	63,752	0.03%
Portogallo	1,518,762	4,985	0.33%
Romania	36,420,337	58,883	0.16%
Slovacchia	1,971,329	3,352	0.17%
Slovenia	724,668	1,403	0.19%
Spagna	6,639,002	11,904	0.18%
Svezia	11,757,565	12,977	0.11%
Islanda	291,908	589	0.20%
Liechtenstein	50,186	48	0.10%
Norvegia	4,367,100	8,605	0.20%
Totale UE	446,259,356	376,548	0.08%
Totale SEE	450,968,550	385,790	0.09%

	Numero di impressioni del video Tag avviso coperto da intervento (disinformazione/negazione dell'Olocausto)	Numero di clic del Tag Avviso video coperti da intervento (disinformazione/negazione dell'Olocausto)	Tasso di clic del Tag Avviso video coperto da intervento (disinformazione/negazione dell'Olocausto)
Stati membri			



Austria	3,987,721	11,081	0.28%
Belgio	3,501,679	10,689	0.31%
Bulgaria	697,482	2,810	0.40%
Croazia	658,928	2,223	0.34%
Cipro	311,308	1,189	0.38%
Repubblica Ceca	2,888,696	13,749	0.48%
Danimarca	1,690,719	6,873	0.41%
Estonia	406,818	1,622	0.40%
Finlandia	3,314,306	12,022	0.36%
Francia	2,293,975	10,994	0.48%
Germania	40,208,515	110,850	0.28%
Grecia	2,559,183	10,007	0.39%
Ungheria	4,785,260	17,185	0.36%
Irlanda	3,352,323	10,490	0.31%
Italia	1,987,326	9,277	0.47%
Lettonia	491,701	2,082	0.42%
Lituania	685,542	2,714	0.40%
Lussemburgo	181,085	658	0.36%
Malta	206,924	592	0.29%



Paesi Bassi	12,745,193	33,329	0.26%
Polonia	27,175,740	70,663	0.26%
Portogallo	1,990,257	6,556	0.33%
Romania	3,636,828	15,035	0.41%
Slovacchia	640,942	2,254	0.35%
Slovenia	462,528	1,551	0.34%
Spagna	8,574,010	30,920	0.36%
Svezia	5,540,266	25,954	0.47%
Islanda	215,411	770	0.36%
Liechtenstein	11,568	47	0.41%
Norvegia	2,909,307	13,198	0.45%
Totale UE	134,975,255	423,369	0.31%
Totale SEE	138,111,541	437,384	0.32%
	Numero di impressioni dell'etichetta di avviso di Video coperte dall'intervento (Mpox)	Numero di clic del Tag Avviso Video coperti dall'intervento (Mpox)	Tasso di click-through del tag di avviso video coperto dall'intervento (Mpox)
Stati membri			
Austria	6,065,332	30,641	0.51%
Belgio	15,383,226	73,644	0.48%
Bulgaria	5,869,376	39,855	0.68%



Croazia	5,206,361	40,720	0.78%
Cipro	1,309,314	7,869	0.60%
Repubblica Ceca	6,134,172	60,989	0.99%
Danimarca	4,604,268	37,820	0.82%
Estonia	2,279,691	18,303	0.80%
Finlandia	8,904,456	66,423	0.75%
Francia	123,453,307	471,892	0.38%
Germania	51,643,857	244,354	0.47%
Grecia	9,476,029	65,533	0.69%
Ungheria	5,483,667	40,088	0.73%
Irlanda	9,413,972	58,759	0.62%
Italia	31,117,509	174,013	0.56%
Lettonia	2,821,714	23,843	0.84%
Lituania	5,065,658	36,987	0.73%
Lussemburgo	823,972	4,245	0.52%
Malta	645,827	3,131	0.48%
Paesi Bassi	15,404,762	115,335	0.75%
Polonia	25,070,807	210,242	0.84%
Portogallo	6,017,068	37,100	0.62%



Romania	12,931,412	100,003	0.77%
Slovacchia	1,798,295	14,348	0.80%
Slovenia	2,037,178	12,289	0.60%
Spagna	47,595,074	178,276	0.37%
Svezia	15,829,378	117,375	0.74%
Islanda	679,537	4,129	0.61%
Liechtenstein	21,397	132	0.62%
Norvegia	6,765,469	64,054	0.95%
Totale UE	422,385,682	2,284,077	0.54%
Totale SEE	429,852,085	2,352,392	0.55%
	Numero di impressioni sull'argomento coperto dal video Intervento (Elezione)	Numero di clic per video Intervento (Elezione)	Tasso di clic per intervento video (Elezione)
Stati membri			
Austria	78,371,511	156,117	0.20%
Belgio	NA	NA	NA
Bulgaria	29,664,185	50,018	0.17%
Croazia	24,640,666	41,715	0.17%
Cipro	NA	NA	NA
Repubblica Ceca	329,546	332	0.10%

Danimarca	NA	NA	NA
Estonia	NA	NA	NA
Finlandia	NA	NA	NA
Francia	1,301,158,781	2,080,600	0.16%
Germania	209,773,848	261,655	0.12%
Grecia	NA	NA	NA
Ungheria	NA	NA	NA
Irlanda	278,245	354	0.13%
Italia	NA	NA	NA
Lettonia	NA	NA	NA
Lituania	9,102,070	15014	0.16%
Lussemburgo	NA	NA	NA
Malta	NA	NA	NA
Paesi Bassi	NA	NA	NA
Polonia	NA	NA	NA
Portogallo	NA	NA	NA
Romania	1,093,883,826	1,531,546	0.14%
Slovacchia	NA	NA	NA
Slovenia	NA	NA	NA

Spagna	NA	NA	NA
Svezia	NA	NA	NAN
Islanda	4,620,010	19,661	0.43%
Liechtenstein	NA	NA	NA
Norvegia	NA	NA	NA
Totale UE	2,747,202,678	4,137,351	0.15%
Totale SEE	2,751,822,688	4,157,012	0.15%

	Numero di impressioni degli interventi di ricerca (disinformazione/negazione dell'Olocausto)	Numero di clic degli interventi di ricerca (disinformazione/negazione dell'Olocausto)	Tasso di clic degli interventi di ricerca (disinformazione/negazione dell'Olocausto)
Stati membri			
Austria	156,298	6,187	3.96%
Belgio	200,324	10,626	5.30%
Bulgaria	62,548	1,701	2.72%
Croazia	100,586	2,631	2.62%
Cipro	24,629	445	1.81%
Repubblica Ceca	88,635	2,476	2.79%
Danimarca	59,881	1,572	2.63%
Estonia	14,970	476	3.18%



Finlandia	118,664	2,024	1.71%
Francia	1,592,000	111,776	7.02%
Germania	1,383,744	66,652	4.82%
Grecia	492,728	2,946	0.60%
Ungheria	118,829	4,853	4.08%
Irlanda	112,337	1,848	1.65%
Italia	877,504	11,749	1.34%
Lettonia	18,212	668	3.67%
Lituania	37,622	820	2.18%
Lussemburgo	11,059	571	5.16%
Malta	7,744	178	2.30%
Paesi Bassi	490,423	6,942	1.42%
Polonia	1,069,545	842	0.08%
Portogallo	221,507	2,507	1.13%
Romania	222,020	5,125	2.31%
Slovacchia	42,499	1,331	3.13%
Slovenia	30,051	1,520	5.06%
Spagna	2,155,115	39,383	1.83%
Svezia	175,333	4,056	2.31%



Islanda	5,203	147	2.83%
Liechtenstein	478	25	5.23%
Norvegia	89,193	2,505	2.81%
Totale UE	9,884,807	291,905	2.95%
Totale SEE	9,979,681	294,582	2.95%
	Numero di impressioni degli interventi di Search (Mpox)	Numero di clic degli interventi di ricerca (Mpox)	Tasso di click-through degli interventi di ricerca (Mpox)
Stati membri			
Austria	467,253	2,111	0.45%
Belgio	669,059	2,501	0.37%
Bulgaria	446,240	2,724	0.61%
Croazia	561,621	3,321	0.59%
Cipro	77,553	452	0.58%
Repubblica Ceca	587,165	4,180	0.71%
Danimarca	435,391	2,571	0.59%
Estonia	147,804	926	0.63%
Finlandia	648,096	4,591	0.71%
Francia	3,031,084	5,826	0.19%
Germania	3,901,089	15,278	0.39%
Grecia	1,145,046	6,796	0.59%



Ungheria	495,768	3,857	0.78%
Irlanda	714,141	2,252	0.32%
Italia	2,604,995	36,148	1.39%
Lettonia	206,307	1,375	0.67%
Lituania	484,805	2,767	0.57%
Lussemburgo	39,807	180	0.45%
Malta	33,713	148	0.44%
Paesi Bassi	1,010,537	4,547	0.45%
Polonia	2,560,968	19,079	0.74%
Portogallo	714,886	3,653	0.51%
Romania	1,339,325	7,857	0.59%
Slovacchia	329,754	2,027	0.61%
Slovenia	164,647	793	0.48%
Spagna	1,775,339	6,112	0.34%
Svezia	1,106,486	6,128	0.55%
Islanda	22,964	245	1.07%
Liechtenstein	1,406	10	0.71%
Norvegia	539,291	3,472	0.64%
Totale UE	25,698,879	148,200	0.58%



Totale SEE	26,262,540	151,927	0.58%
------------	------------	---------	-------

	Numero di impressioni sugli interventi di ricerca (Cambiamento climatico)	Numero di clic degli interventi di ricerca (Cambiamento climatico)	Tasso di click-through degli interventi di ricerca (Cambiamento climatico)
Stati membri			
Austria	228,390	196	0.09%
Belgio	207,808	159	0.08%
Bulgaria	140,769	183	0.13%
Croazia	159,478	128	0.08%
Cipro	19,126	20	0.10%
Repubblica Ceca	163,222	172	0.11%
Danimarca	148,528	134	0.09%
Estonia	29,383	44	0.15%
Finlandia	238,286	213	0.09%
Francia	652,102	446	0.07%
Germania	1,761,399	1,488	0.08%
Grecia	250,015	361	0.14%
Ungheria	270,274	330	0.12%
Irlanda	221,386	118	0.05%
Italia	1,113,346	818	0.07%

Lettonia	37,048	63	0.17%
Lituania	112,397	176	0.16%
Lussemburgo	14,448	17	0.12%
Malta	9,186	5	0.05%
Paesi Bassi	406,345	308	0.08%
Polonia	888,768	1,136	0.13%
Portogallo	198,458	162	0.08%
Romania	375,102	513	0.14%
Slovacchia	93,322	104	0.11%
Slovenia	34,445	26	0.08%
Spagna	842,382	503	0.06%
Svezia	486,125	405	0.08%
Islanda	4,668	7	0.15%
Liechtenstein	548	1	0.18%
Norvegia	223,306	179	0.08%
Totale UE	9,101,538	8,228	0.09%
Totale SEE	9,330,060	8,415	0.09%

	Numero di impressioni degli interventi di Search (Elezione)	Numero di clic degli interventi di ricerca (Elezione)	Tasso di click-through degli interventi di ricerca (elezione)
--	--	--	--

Stati membri			
Austria	708,656	3,263	0.46%
Belgio	NA	NA	NA
Bulgaria	121,672	367	0.30%
Croazia	546,661	1,767	0.32%
Cipro	NA	NA	NA
Repubblica Ceca	17,994	56	0.31%
Danimarca	NA	NA	NA
Estonia	NA	NA	NA
Finlandia	NA	NA	NA
Francia	15,712,577	7,306	0.05%
Germania	7,265,486	13,805	0.19%
Grecia	NA	NA	NA
Ungheria	NA	NA	NA
Irlanda	1,651,434	16,293	0.99%
Italia	NA	NA	NA
Lettonia	NA	NA	NA
Lituania	41,034	127	0.31%
Lussemburgo	NA	NA	NA

Malta	NA	NA	NA
Paesi Bassi	NA	NA	NA
Polonia	NA	NA	NA
Portogallo	NA	NA	NA
Romania	21,733,061	70,746	0.33%
Slovacchia	NA	NA	NA
Slovenia	NA	NA	NA
Spagna	NA	NA	NA
Svezia	NA	NA	NA
Islanda	78,449	1,095	1.40%
Liechtenstein	NA	NA	NA
Norvegia	NA	NA	NA
Totale UE	47,798,575	113,730	0.24%
Totale SEE	47,877,024	114,825	0.24%

	Numero di impressioni di annunci di servizio pubblici (disinformazione/negazione dell'Olocausto)		
Stati membri			
Austria	16		



Belgio	41		
Bulgaria	17		
Croazia	6		
Cipro	4		
Repubblica Ceca	99		
Danimarca	13		
Estonia	60		
Finlandia	27		
Francia	562		
Germania	344		
Grecia	14		
Ungheria	14		
Irlanda	20		
Italia	74		
Lettonia	89		
Lituania	41		
Lussemburgo	2		
Malta	2		
Paesi Bassi	80		



Polonia	154		
Portogallo	11		
Romania	21		
Slovacchia	16		
Slovenia	3		
Spagna	51		
Svezia	87		
Islanda	4		
Liechtenstein	1		
Norvegia	27		
Totale UE	1,868		
Totale SEE	1,900		
	Numero di impressioni di annunci di servizio pubblico (Mpox)		
Stati membri			
Austria	26		
Belgio	26		
Bulgaria	39		
Croazia	13		
Cipro	4		



Repubblica Ceca	76		
Danimarca	17		
Estonia	12		
Finlandia	30		
Francia	473		
Germania	385		
Grecia	28		
Ungheria	33		
Irlanda	38		
Italia	63		
Lettonia	9		
Lituania	11		
Lussemburgo	1		
Malta	1		
Paesi Bassi	147		
Polonia	172		
Portogallo	12		
Romania	40		
Slovacchia	24		

Slovenia	5		
Spagna	82		
Svezia	55		
Islanda	5		
Liechtenstein	0		
Norvegia	18		
Totale UE	1,822		
Totale SEE	1,845		

Misura 17.2	
-------------	--



QRE 17.2.1

Per sensibilizzare i nostri utenti su argomenti specifici e , conduciamo una serie di campagne di alfabetizzazione mediatica su piattaforma e fuori piattaforma. Il nostro approccio può variare a seconda dell'argomento. Alcune campagne sono localizzate (ad esempio, per le elezioni) e ciò significa che collaboriamo con i partner nazionali per sviluppare un approccio che risuoni al meglio con il pubblico locale. Per altre campagne, come quella sulla guerra in Ucraina, ci concentriamo sulla scalabilità e sul collegamento degli utenti a risorse accurate e affidabili.

Di seguito sono riportati alcuni esempi delle campagne che abbiamo condotto più di recente in-app e che hanno sfruttato una serie di strumenti di intervento che abbiamo illustrato nella nostra risposta a QRE.

17.1.1 (ad es. interventi di ricerca e tag di avviso video).

(I) Promuovere l'integrità elettorale. Oltre alle pagine dedicate all'integrità elettorale sul [Centro per la sicurezza](#) e sul [Centro per la trasparenza](#) di TikTok, e al nuovo [Hub](#) dedicato all'[integrità delle elezioni europee](#), che portano consapevolezza e visibilità su come affrontiamo la disinformazione elettorale e le operazioni di influenza occulta sulla nostra piattaforma, abbiamo lanciato campagne di alfabetizzazione mediatica prima di diverse elezioni nell'UE e in Europa.

Elezioni legislative in Francia 2024: Dal 17 giugno 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni legislative francesi del 2024. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che comprendeva video creati in collaborazione con l'organizzazione di fact-checking [Agence France-Presse \(AFP\)](#).



Elezioni regionali in Germania 2024 (Sassonia, Turingia, Brandeburgo): Dall'8 agosto 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni regionali tedesche. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'organizzazione di fact-checking [Deutsche Presse-Agentur \(dpa\)](#).



Elezioni federali in Austria 2024: Dal 13 agosto 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'organizzazione di fact-checking [Deutsche Presse-Agentur \(dpa\)](#).



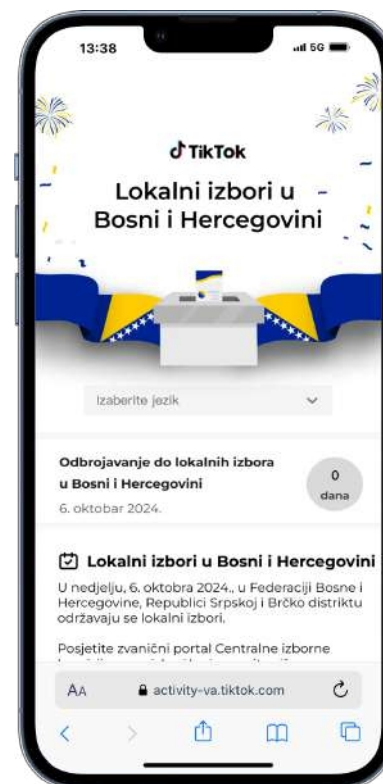
Elezioni presidenziali e referendum UE 2024 in Moldavia: A partire dal 6 settembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni presidenziali in Moldavia del 2024 e sul referendum dell'UE. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'Associazione per la difesa dei diritti umani. organizzazione di fact-checking [StopFals!](#)



Elezioni parlamentari in Georgia 2024: Dal 16 settembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni parlamentari in Georgia del 2024. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'organizzazione di fact-checking [Fact Check Georgia](#).



Elezioni parlamentari in Bosnia 2024: Dal 17 settembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni regionali bosniache del 2024, che conteneva una sezione dedicata all'individuazione della disinformazione.



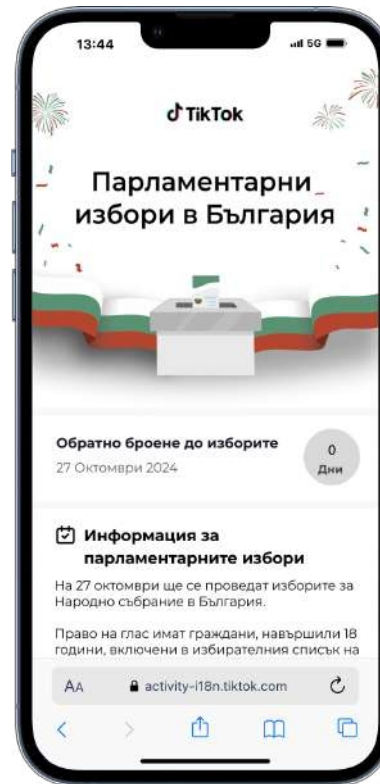
Elezioni parlamentari in Lituania 2024: Dal 17 settembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni parlamentari lituane del 2024, che conteneva una sezione dedicata all'individuazione della disinformazione.



Elezioni regionali in Cechia 2024: Dal 13 settembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni regionali ceche del 2024, che conteneva una sezione dedicata all'individuazione della disinformazione.



Elezioni parlamentari in Bulgaria 2024: Dal 1° ottobre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni parlamentari bulgare del 2024, che conteneva una sezione dedicata all'individuazione della disinformazione.



Elezioni presidenziali e parlamentari in Romania 2024: Dall'11 novembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni rumene del 2024. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'organizzazione di fact-checking [Funky Citizens](#). [Il 6 dicembre 2024, in seguito alla decisione della Corte costituzionale di annullare il primo turno delle elezioni presidenziali, abbiamo aggiornato il nostro Centro elettorale in-app per guidare gli utenti sugli eventi in rapida evoluzione].



Elezioni generali in Irlanda: Dal 7 novembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni generali irlandesi del 2024. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'organizzazione di fact-checking [The Journal](#).



Elezioni parlamentari in Islanda 2024: Dal 7 novembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni parlamentari islandesi del 2024, che conteneva una sezione dedicata all'individuazione della disinformazione.



Elezioni presidenziali in Croazia 2024: Dal 6 dicembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni presidenziali in Croazia del 2024. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'organizzazione di fact-checking [Faktograf](#).



Elezioni federali in Germania 2024: Dal 16 dicembre 2024, abbiamo lanciato un [Centro elettorale](#) in-app per fornire agli utenti informazioni aggiornate sulle elezioni federali tedesche del 2025. Il centro conteneva una sezione dedicata all'individuazione della disinformazione, che comprendeva video creati in collaborazione con l'organizzazione di fact-checking [Deutsche Presse-Agentur \(dpa\)](#).





(II) Serie di relatori sulle elezioni. Per promuovere ulteriormente l'integrità elettorale e informare il nostro approccio alle elezioni, abbiamo invitato esperti esterni locali e regionali adeguatamente qualificati a condividere le loro intuizioni e la loro esperienza di mercato con i nostri team interni. Nel periodo in esame, abbiamo organizzato 9 sessioni di Election Speaker Series, di cui 7 negli Stati membri dell'UE e 2 in Georgia e Moldavia.

1. Francia: Agence France-Presse (AFP)
2. Germania: Agenzia di stampa tedesca (dpa)
3. Austria: Agenzia di stampa tedesca (dpa)
4. Lituania: Fatti logici
5. Romania: Cittadini divertenti
6. Irlanda: Fatti logici
7. Croazia: Faktograf
8. Georgia: FactCheck Georgia
9. Moldavia: Stop a Fals!

(III) Alfabetizzazione ai media (generale). Abbiamo lanciato due nuove campagne generali di alfabetizzazione ai media e di capacità di pensiero critico nell'UE e due nei Paesi candidati all'UE, in collaborazione con i nostri partner per il fact-checking e l'alfabetizzazione ai media:

- Francia: Agence France-Presse (AFP)
- Portogallo: Polígrafo
- Georgia: Fact Check Georgia
- Moldavia: StopFals!

Il numero di campagne di alfabetizzazione generale ai media e alle capacità di pensiero critico in Europa sale così a 11 (Danimarca, Finlandia, Francia, Georgia, Irlanda, Italia, Spagna, Svezia, Moldavia, Paesi Bassi e Portogallo).

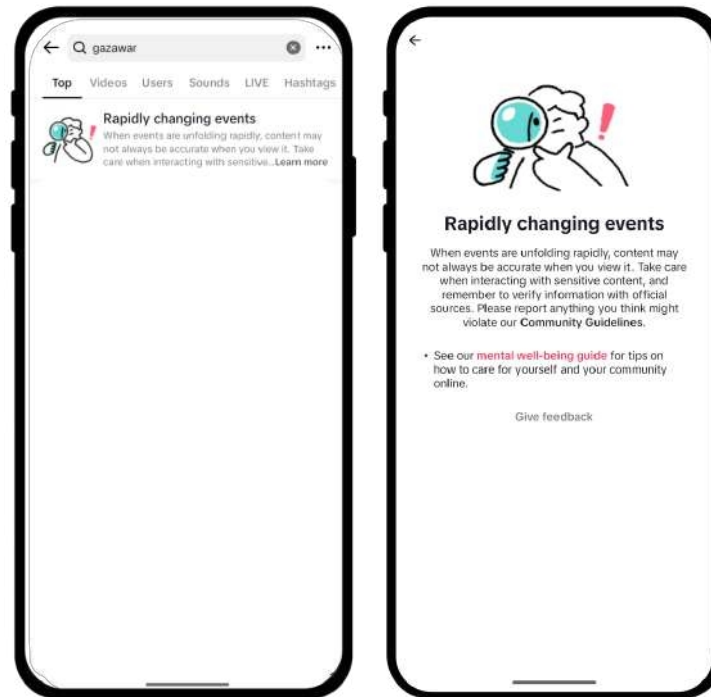


(IV) Alfabetizzazione ai media (guerra in Ucraina). Continuiamo a servire 17 campagne di alfabetizzazione mediatica localizzate specifiche per la guerra in Ucraina in: Ucraina, Romania, Slovacchia, Ungheria, Lettonia, Estonia, Lituania, Cechia, Polonia, Croazia, Slovenia, Bulgaria, Germania, Austria, Bosnia, Montenegro e Serbia.

- Partner di Lead Stories: Ucraina, Romania, Slovacchia, Ungheria, Lettonia, Estonia, Lituania.
- In collaborazione con fakenews.pl: Polonia.
- In collaborazione con Correctiv: Germania, Austria.

Attraverso queste campagne di alfabetizzazione mediatica, gli utenti che cercano parole chiave relative alla guerra in Ucraina su TikTok vengono indirizzati a consigli preparati in collaborazione con enti locali di alfabetizzazione mediatica e con i nostri partner di fiducia per il fact-checking, per aiutarli a identificare la disinformazione e a prevenirla la diffusione sulla piattaforma.

(V) Conflitto Israele-Hamas. Per contribuire alla sensibilizzazione e alla protezione dei nostri utenti, disponiamo di interventi di ricerca che si attivano quando gli utenti cercano termini neutri relativi a questo argomento (ad esempio, Israele, Palestina). Questi interventi di ricerca ricordano agli utenti di fare una pausa e di controllare le loro fonti e li indirizzano anche verso risorse di benessere.



(VI) Alfabetizzazione climatica.

- Il nostro [strumento di ricerca-intervento sui cambiamenti climatici](#) è disponibile in 23 lingue ufficiali dell'UE (più il norvegese e l'islandese per gli utenti del SEE). Lo strumento reindirizza gli utenti alla ricerca di contenuti relativi al cambiamento climatico verso informazioni autorevoli e li incoraggia a segnalare qualsiasi potenziale disinformazione riscontrata.
- Nell'aprile 2024, in collaborazione con [il Mary Robinson Centre](#), TikTok ha lanciato la [TikTok Youth Climate Leaders Alliance](#), un programma rivolto ai giovani tra i 18 e i 30 anni che desiderano apportare cambiamenti significativi di fronte alla crisi climatica.
- Ha partecipato attivamente **al vertice sui cambiamenti climatici COP29 Nazioni Unite**:
 - Collaborare con la presidenza della COP29 per promuovere i loro contenuti e coinvolgere nuovo pubblico intorno alla conferenza come media partner strategico.



- Rilancio della campagna globale [#ClimateAction](#) con oltre 7.000 post da tutto il mondo. I contenuti di [#ClimateAction](#) hanno ricevuto oltre 4 miliardi di visualizzazioni video dal lancio nel 2021.
- Portando al summit 5 creatori, che hanno prodotto collettivamente più di 15 video che hanno ricevuto oltre 60 milioni di visualizzazioni.
- Lancio di due funzionalità globali (un tag di avviso video e una guida all'intervento di ricerca) per indirizzare gli utenti verso contenuti autorevoli relativi al clima tra il 29 ottobre e il 25 novembre, che sono stati visualizzati 400.000 volte.
- Ad agosto 2024, gli hashtag popolari [#ClimateChange](#), [#SustainableLiving](#) e [#ClimateAction](#) hanno più di 800.000 post associati su TikTok.

SLI 17.2.1 - azioni di applicazione delle politiche di cui sopra

Siamo lieti di riferire le metriche relative alle quattro nuove campagne generali di alfabetizzazione ai media e alle capacità di pensiero critico in Francia, Georgia, Moldavia e Portogallo, nonché alle campagne permanenti esistenti che si sono svolte durante il periodo di riferimento in: Danimarca, Finlandia, Irlanda, Italia, Spagna, Svezia e Paesi Bassi.

--	--	--	--

Stati membri

Numero totale di impressioni della pagina H5 (visualizzazioni generate tra il 1° luglio e il 31 dicembre 2024)	Numero di impressioni dell'intervento di ricerca	Numero di clic sull'intervento di ricerca	Tasso di click through dell'intervento di ricerca
72,861	229,676	1,370	0.60%
3,400	107,964	426	0.39%
1,540	10,854	30	0.28%
2,492	64,241	226	0.35%

Irlanda (in collaborazione con The journal.ie)	1,320	14,282	46	0.32%
Finlandia (in collaborazione con Logically Facts)	595	3,725	25	0.67%
Svezia (in collaborazione con Logically Facts)	1,197	13,444	64	0.48%
Spagna (in collaborazione con Maldita)	26,213	1,253,955	3,220	0.26%
Italia (in collaborazione con Facta)	1,948	41,297	181	0.44%
Austria e Germania (in collaborazione con Correctiv)	33,220	15,072,256	45,865	0.3%
Bulgaria	741	309,132	1,095	0.35%
Croazia	811	449,332	1,452	0.32%
Repubblica Ceca	1,025	954,741	1,722	0.18%
Slovenia	286	118,972	407	0.34%

Misura 17.3	
-------------	--



QRE 17.3.1

Come documentato nella pagina dei [partner per la sicurezza](#) la sicurezza del Centro di TikTok e nei [Consigli consultivi di TikTok](#), collaboriamo con una serie di esperti del settore, organizzazioni non governative e associazioni di settore in tutto il mondo nel nostro impegno a costruire una piattaforma sicura per la nostra comunità. Tra questi figurano organismi di alfabetizzazione mediatica, per sviluppare campagne che educano gli utenti e li reindirizzano verso risorse autorevoli, e partner di fact-checking. Esempi specifici di partnership nell'ambito delle campagne e dei progetti definiti nel QRE 17.2.1 sono:

(I) Promuovere l'integrità elettorale. Collaboriamo con diverse organizzazioni mediatiche e fact-checkers per promuovere l'integrità elettorale su TikTok. Per maggiori dettagli sui contributi forniti dai nostri partner per il fact-checking, si rimanda al punto 30.1.3 del QRE.

- Abbiamo condotto 14 **campagne temporanee di alfabetizzazione mediatica sull'integrità elettorale** prima delle elezioni regionali, la maggior parte delle quali in collaborazione con i nostri partner per il fact-checking e l'alfabetizzazione mediatica:
 - 7 nell'UE (Austria, Croazia, Francia, 2 x Germania, Irlanda e Lituania)
 - Austria: Deutsche Presse-Agentur (dpa)
 - Croazia: Faktograf
 - Francia: Agence France-Presse (AFP)
 - Germania (elezioni regionali): Deutsche Presse-Agentur dpa)
 - Germania (elezioni federali): Deutsche Presse-Agentur dpa)
 - Irlanda: Il giornale
 - 1 nel SEE (Islanda)
 - 6 in Europa allargata/paesi candidati all'UE (Bosnia, Bulgaria, Cechia, Georgia, Moldavia e Romania)
 - Georgia: Fact Check Georgia
 - Moldavia: StopFals!
 - Romania: Cittadini Funky.
- **Serie di relatori sulle elezioni.** Per promuovere ulteriormente l'integrità elettorale e informare il nostro approccio alle elezioni, abbiamo invitato esperti esterni locali e regionali adeguatamente qualificati a condividere le loro intuizioni e la loro esperienza di mercato con i nostri team interni. Nel periodo in esame, abbiamo organizzato 9 sessioni di conferenze elettorali, di cui 7 negli Stati membri dell'UE e 2 in Georgia e Moldavia.
 1. Francia: Agence France-Presse (AFP)
 2. Germania: Agenzia di stampa tedesca (dpa)
 3. Austria: Agenzia di stampa tedesca (dpa)
 4. Lituania: Fatti logici



	<ol style="list-style-type: none"> 5. Romania: Cittadini divertenti 6. Irlanda: Fatti logici 7. Croazia: Faktograf 8. Georgia: FactCheck Georgia 9. Moldavia: Stop a Fals! <p>(II) Guerra in Ucraina. Continuiamo a portare avanti le nostre campagne di alfabetizzazione mediatica sulla guerra in Ucraina, sviluppate in collaborazione con i nostri partner Correctiv in Austria e Germania, Fakenews.pl in Polonia e Lead Stories in Ucraina, Romania, Slovacchia, Ungheria, Lettonia, Estonia e Lituania. Abbiamo inoltre esteso questa campagna a Serbia, Bosnia, Montenegro, Cechia, Croazia, Slovenia e Bulgaria.</p>

V. Responsabilizzare gli utenti

Impegno 18

I firmatari si impegnano a ridurre al minimo i rischi di propagazione virale della disinformazione adottando pratiche di progettazione sicure nello sviluppo di sistemi, politiche e funzionalità.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]

Sì

Se sì, elencare queste misure di attuazione [breve elenco].

- Sono stati assunti due nuovi partner per il fact-checking in Europa:
 1. Albania e Kosovo: Internews Kosovo
 2. Georgia: Fact Check Georgia
- Continuare a migliorare l'accuratezza e la copertura complessiva fornita dai nostri modelli di rilevamento di apprendimento automatico.



	<ul style="list-style-type: none"> • Membri del gruppo di lavoro EDMO per la creazione dell'Independent Intermediary Body (IIB) a sostegno della ricerca sulle piattaforme digitali. • Abbiamo perfezionato la nostra procedura operativa standard (SOP) per l'accesso controllato dei ricercatori, al fine di garantire la conformità con le disposizioni della legge delegata sull'accesso ai dati per la ricerca. • Ha partecipato alla tavola rotonda tecnica della CE sull'accesso ai dati nel dicembre 2024. • Abbiamo investito nella formazione e nello sviluppo del nostro team di Fiducia e Sicurezza, includendo sessioni interne regolari dedicate alla condivisione delle conoscenze e alla discussione su temi e tendenze rilevanti e partecipando a eventi esterni per condividere le loro competenze e sostenere l'apprendimento professionale continuo. Ad esempio: <ul style="list-style-type: none"> ○ In vista di alcune elezioni, invitiamo esperti esterni locali/regionali adeguatamente qualificati, nell'ambito della nostra Election Speaker Series. La condivisione della loro esperienza di mercato con i nostri team interni ci fornisce spunti per comprendere meglio le aree che potrebbero potenzialmente costituire una manipolazione elettorale e informa il nostro approccio alle elezioni imminenti. ○ Nel giugno 2024, 12 membri del nostro team Trust & Safety (tra cui i leader del nostro programma di fact-checking) hanno partecipato al GlobalFact11 e hanno preso parte a un'iniziativa di presentazione sul palco per rispondere alle domande sulla nostra strategia di disinformazione e sulle partnership con i verificatori professionisti. • Ha continuato a partecipare e a co-presiedere il gruppo di lavoro sulle elezioni. • In ottobre abbiamo sponsorizzato, partecipato e presentato a Disinfo24, la conferenza annuale del DisinfoLab dell'UE a Riga.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.
Misura 18.1	



QRE 18.1.1

TikTok adotta un approccio multiforme per affrontare la diffusione di disinformazione dannosa, indipendentemente dalle intenzioni. Questo include le nostre politiche, i nostri prodotti, le nostre pratiche e le nostre collaborazioni esterne con fact-checkers, enti di alfabetizzazione mediatica e ricercatori.

(I) Rimozione di contenuti o account in violazione. Per ridurre i potenziali danni, ci proponiamo di rimuovere i contenuti o gli account che violano le nostre CG, comprese le nostre politiche di I&A, prima che vengano visualizzati o condivisi da altre persone. Rileviamo e agiamo su questi contenuti utilizzando una combinazione di automazione e moderazione umana.

- a) **Revisione automatica** Poniamo un'enfasi notevole sul rilevamento proattivo per rimuovere i contenuti violenti. I contenuti caricati sulla piattaforma vengono in genere prima esaminati dalla nostra tecnologia di moderazione automatica, che esamina una serie di segnali attraverso i contenuti, tra cui parole chiave, immagini, didascalie e audio, per identificare i contenuti violenti. Collaboriamo con diversi esperti esterni, come i nostri [partner per il fact-checking](#), per definire i nostri elenchi di parole chiave. Se la nostra tecnologia di moderazione automatica identifica contenuti che costituiscono una potenziale violazione, questi vengono automaticamente rimossi dalla piattaforma o segnalati per un'ulteriore revisione da parte dei nostri team di moderazione umani. In linea con le nostre misure di salvaguardia per garantire decisioni accurate, la rimozione automatica viene applicata quando le violazioni sono più evidenti. Effettuiamo anche controlli mirati su alcuni tipi di contenuti violati, tra cui la disinformazione dannosa, laddove abbiamo identificato rischi specifici o i nostri partner di fact-checking o altri esperti ci hanno segnalato rischi specifici.
- b) **Moderazione umana** Sebbene alcuni tipi di disinformazione possano essere fatti valere solo attraverso la tecnologia - ad esempio, la ripetizione di contenuti precedentemente sfatati - la disinformazione si evolve rapidamente e presenta molte sfumature. Ecco perché abbiamo moderatori della disinformazione con una formazione avanzata e l'accesso a strumenti come il nostro archivio globale di affermazioni precedentemente verificate dai partner di fact-checking accreditati dall'IFCN, che ci aiutano a valutare l'accuratezza dei contenuti. Abbiamo anche team sul campo che collaborano con esperti per dare priorità al contesto e alle sfumature locali. Possiamo anche fornire indicazioni ai nostri team di moderazione per aiutarli a individuare più facilmente e a intervenire rapidamente sui contenuti in violazione. La moderazione umana avverrà anche se un video acquista popolarità o è stato segnalato. I membri della comunità possono segnalare le violazioni nell'app e sul nostro sito web. Il nostro fact-checking



I partner e le altre parti interessate possono anche segnalarci direttamente i contenuti potenzialmente violati.

(II) Sicurezza nelle nostre raccomandazioni. Oltre a rimuovere i contenuti che violano palesemente le nostre CG, abbiamo messo in atto una serie di misure di salvaguardia per garantire che il feed For You (in quanto punto di accesso principale per scoprire contenuti originali e divertenti sulla piattaforma) sia sicuro.

- a. Per i contenuti che non violano le nostre CG ma che possono avere un impatto negativo sull'autenticità della piattaforma, ne riduciamo la visibilità nel feed For You e/o li etichettiamo. I tipi di disinformazione che possiamo rendere inammissibili per il feed For You sono [indicati](#) chiaramente agli utenti: teorie cospirative generiche, informazioni non verificate relative a un'emergenza o a un evento in corso e disinformazione potenzialmente dannosa che è in fase di verifica. Inoltre, etichettiamo gli account e i contenuti delle entità mediatiche affiliate allo Stato per consentire agli utenti di considerare le fonti delle informazioni. I nostri moderatori adottano ulteriori precauzioni per rivedere i video man mano che aumentano di popolarità, al fine di ridurre la probabilità che contenuti non appropriati entrino nel nostro sistema raccomandato.
- b. Fornire accesso a informazioni autorevoli è una parte importante della nostra strategia complessiva per contrastare la disinformazione. A tale scopo, possiamo lanciare centri di informazione con risorse informative di terze parti autorevoli in risposta a eventi globali o locali, aggiungere annunci di servizio pubblico su hashtag o pagine di ricerca, o etichettare i contenuti relativi a un determinato argomento per spingere la nostra comunità a cercare informazioni autorevoli.

(III) La sicurezza nella progettazione. All'interno dei nostri team Trust and Safety Product and Policy, abbiamo esperti in materia dedicati all'integrità e all'autenticità. Quando sviluppiamo una nuova funzionalità o una nuova politica, questi team lavorano a stretto contatto con i partner esterni per garantire che la sicurezza sia integrata in TikTok fin dalla progettazione e che rifletta le migliori pratiche del settore. Ad :

- Collaboriamo con [Irrational Labs](#) per sviluppare e implementare [suggerimenti specifici](#) che aiutino gli utenti a riflettere prima di condividere contenuti non verificati (come indicato in **QRE 21.3.1**),
- [Yad Vashem](#) ha creato un programma di arricchimento sull'Olocausto per il nostro team Trust and Safety. Il programma, della durata di cinque settimane, aveva l'obiettivo di fornire al nostro team un'approfondita

	<p>comprensione dell'Olocausto, delle sue lezioni e della disinformazione legata all'antisemitismo e all'odio.</p> <ul style="list-style-type: none">Abbiamo collaborato con esperti locali/regionali attraverso la nostra Election Speaker Series per garantire che le loro intuizioni e competenze informino i nostri team interni in vista di particolari elezioni nel 2024, tra cui [includere esempi da 17.3.1].
QRE 18.1.2	<p>Il feed For You è l'interfaccia che gli utenti vedono per la prima volta quando aprono TikTok. È il fulcro dell'esperienza di TikTok e il luogo in cui la maggior parte dei nostri utenti trascorre il proprio tempo esplorando la piattaforma. Le interazioni degli utenti agiscono come segnali che aiutano i sistemi di raccomandazione a prevedere i contenuti a cui è più probabile che siano interessati, nonché i contenuti a cui potrebbero essere meno interessati e che potrebbero preferire saltare. Le interazioni degli utenti su TikTok possono influenzare il modo in cui il sistema classifica e serve i contenuti.</p> <p>Questi sono alcuni esempi di informazioni che possono influenzare i contenuti di TikTok nel vostro feed For You:</p> <ul style="list-style-type: none">Interazioni degli utenti: Contenuti che vi piacciono, che condividete, che , che guardate per intero o che saltate, come gli account dei follower che seguite a vostra volta.Informazioni sui contenuti: Suoni, hashtag, numero di visualizzazioni e paese in cui è stato pubblicato il contenuto.Informazioni sull'utente: Impostazioni del dispositivo, preferenza della lingua, posizione, fuso orario e giorno e tipo di dispositivo. <p>Per la maggior parte degli utenti, le interazioni dell'utente, che possono includere il tempo trascorso a guardare un video, sono generalmente più importanti di altre.</p> <p>Oltre ai segnali forniti dagli utenti attraverso il modo in cui interagiscono con i contenuti su TikTok, ci sono altri strumenti che abbiamo costruito per aiutarli a controllare meglio il tipo di contenuti che vengono loro consigliati.</p> <ul style="list-style-type: none">Non sono interessato: Gli utenti possono premere a lungo sul video nel loro feed "Per te" e selezionare "Non sono interessato" dal menu a comparsa. In questo modo ci comunicheranno che non sono interessati a questo tipo di contenuti e limiteremo la quantità di contenuti raccomandati nel loro feed.Filtri per le parole chiave dei video: Possono aggiungere parole chiave - sia parole che hashtag - che filtrare dal loro feed For You.



	<ul style="list-style-type: none"> ● Aggiornamento di For You: Per aiutarvi a scoprire nuovi contenuti, gli utenti possono aggiornare il loro feed For You, consentendo loro di esplorare lati completamente nuovi di TikTok. Condividiamo ulteriori informazioni sui nostri sistemi di raccomandazione nel nostro Centro assistenza e nel Centro per la trasparenza e di seguito nella nostra risposta alla domanda 19.1.1.
QRE 18.1.3	<p>Interveniamo per prevenire e ridurre la diffusione di informazioni errate, fuorvianti o false che possono causare danni significativi a singoli individui o al pubblico in generale. Lo facciamo rimuovendo i contenuti e gli account che violano le nostre regole, investendo nell'alfabetizzazione mediatica e mettendo la nostra comunità in contatto con informazioni autorevoli e collaborando con esperti esterni. Le nostre politiche I&A chiariscono che non consentiamo attività che possano minare l'integrità della nostra piattaforma o l'autenticità dei nostri utenti. Rimuoviamo i contenuti o gli account che contengono informazioni fuorvianti che causano danni significativi o, in determinate circostanze, riduciamo la rilevanza dei contenuti. I tipi di informazioni fuorvianti che possiamo rendere non ammissibili al feed di For You sono indicati nelle nostre Linee guida della community.</p> <ul style="list-style-type: none"> ● Disinformazione <ul style="list-style-type: none"> ○ Teorie del complotto che sono infondate e che sostengono che determinati eventi o situazioni sono portati avanti da gruppi occulti o potenti, come "il governo" o una "società segreta". ○ Disinformazione sulla salute con danni moderati, come ad esempio una raccomandazione non provata su come trattare una malattia minore. ○ Media riproposti, come ad esempio mostrare una folla a un concerto musicale e far credere che si tratti di una protesta politica. ○ travisare fonti autorevoli, come ad esempio fare riferimento in modo selettivo a determinati dati scientifici per sostenere una conclusione contraria ai risultati dello studio. ○ Richieste di risarcimento non verificate relative a un'emergenza o a un evento in corso. ○ Potenziale disinformazione ad alto rischio mentre è in corso una revisione del fact-checking. ● Integrità civica ed elettorale



- Affermazioni non verificate su un'elezione, come l'affermazione prematura che tutte le schede sono state contate o scrutinate.
- Dichiarazioni che travisano in modo significativo informazioni civiche autorevoli, come ad esempio una falsa affermazione sul testo di un disegno di legge parlamentare.

- **Fidanzamento falso**

- Contenuti che ingannano o manipolano gli altri per aumentare i regali o le metriche di coinvolgimento, come promesse di "like-for-like" o altri falsi incentivi per il coinvolgimento nei contenuti.

Per applicare le nostre CG su scala, utilizziamo una combinazione di revisione automatica e moderazione umana. Mentre alcune disinformazioni possono essere applicate solo attraverso la tecnologia - per esempio, la ripetizione di contenuti precedentemente sfatati - la disinformazione si evolve rapidamente ed è molto sfumata. La valutazione della disinformazione dannosa richiede un contesto e una valutazione aggiuntivi da parte dei nostri moderatori della disinformazione, che hanno una formazione, un'esperienza e strumenti migliori per identificare tali contenuti, compreso il nostro archivio globale di affermazioni precedentemente verificate dai fatti. Partner di fact-checking accreditati dall'IFCN e accesso diretto ai nostri partner di fact-checking, ove opportuno.

La nostra rete di partner indipendenti per il fact-checking non modera direttamente i contenuti su TikTok, ma valuta se un'affermazione è vera, falsa o priva di fondamento, in modo che i nostri moderatori possano intervenire in base alle nostre Linee guida della community. Incorporiamo i contributi dei fact-checker nei nostri sforzi di moderazione dei contenuti più ampi attraverso:

- Rapporti di approfondimento proattivi che segnalano le affermazioni nuove e in evoluzione che si vedono su Internet. Questo ci aiuta a individuare la disinformazione dannosa e ad anticipare le tendenze della disinformazione sulla nostra piattaforma.
- Un archivio di affermazioni precedentemente verificate per aiutare i moderatori della disinformazione a prendere decisioni rapide e accurate.

La collaborazione con la nostra rete di organizzazioni indipendenti di fact-checking consente a TikTok di identificare e intervenire sulla disinformazione e di collegare la nostra comunità a informazioni autorevoli su eventi importanti. Si tratta di una parte importante della nostra strategia complessiva per contrastare la disinformazione. Le modalità con cui lo facciamo sono molteplici, tra cui il lancio di centri di informazione con risorse di terze parti autorevoli in risposta a eventi globali o locali,

	<p>l'aggiunta di annunci di servizio pubblico (PSA) su hashtag o pagine di ricerca, o l'etichettatura di contenuti relativi a un determinato argomento per spingere la nostra comunità a cercare informazioni autorevoli.</p> <p>Ci impegniamo anche per l'integrità civica ed elettorale e per mitigare la diffusione di contenuti falsi o fuorvianti su un processo elettorale o civico. Collaboriamo con le commissioni elettorali nazionali, con gli organismi di alfabetizzazione dei media e con le organizzazioni della società civile per garantire alla nostra comunità informazioni accurate e aggiornate sulle elezioni attraverso i nostri centri di informazione elettorale in-app, le guide elettorali, gli interventi di ricerca e le etichette dei contenuti.</p>			
SLI 18.1.1 - azioni che dimostrano l'efficacia delle misure e delle politiche	<p>Metodologia di misurazione dei dati:</p> <p>Il tasso di annullamento delle condivisioni (%) dopo il pop-up di avviso di condivisione dell'etichetta di contenuto non verificato indica la percentuale di utenti che non condividono un video dopo aver visto il pop-up dell'etichetta. Questa metrica si basa sulla posizione approssimativa degli utenti che hanno utilizzato questi strumenti.</p>			
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio)	Tasso di annullamento delle condivisioni (%) dopo il pop-up di avviso di condivisione dell'etichetta di contenuto non verificato (utenti che non condividono il video dopo aver visto il pop-up)			
Stati membri				
Austria	31.81%			



Belgio	33.81%				
Bulgaria	33.97%				
Croazia	33.66%				
Cipro	32.91%				
Repubblica Ceca	29.52%				
Danimarca	30.20%				
Estonia	28.53%				
Finlandia	27.21%				
Francia	37.13%				
Germania	30.09%				
Grecia	32.05%				
Ungheria	31.38%				
Irlanda	29.59%				
Italia	37.65%				
Lettonia	30.90%				
Lituania	30.80%				

Lussemburgo	33.64%				
Malta	35.43%				
Paesi Bassi	27.79%				
Polonia	28.88%				
Portogallo	33.08%				
Romania	30.08%				
Slovacchia	28.89%				
Slovenia	33.33%				
Spagna	34.09%				
Svezia	29.44%				
Islanda	27.86%				
Liechtenstein	19.61%				
Norvegia	25.37%				
Totale UE	32.24%				
Totale SEE	32.13%				
Misura 18.2					

**QRE 18.2.1**

Interveniamo contro la disinformazione che causa danni significativi a singoli individui, alla nostra comunità o al pubblico in generale, indipendentemente dalle intenzioni. Lo facciamo rimuovendo i contenuti e gli account che violano le nostre regole, investendo nell'alfabetizzazione mediatica e collegando la nostra comunità a informazioni autorevoli e collaborando con esperti.

I nostri Termini di servizio e le politiche di I&A previste dalle nostre CG sono la prima linea di difesa per combattere la disinformazione dannosa e (come illustrato più dettagliatamente nel QRE 14.1.1) i comportamenti ingannevoli sulla nostra piattaforma. Queste regole chiariscono ai nostri utenti quali sono i contenuti che rimuoviamo o rendiamo non ammissibili per il feed For You quando rappresentano un rischio di danno per i nostri utenti e la nostra comunità.

In particolare, le nostre politiche non :

- **Disinformazione**

- Informazioni errate che mettono a rischio la sicurezza pubblica o possono indurre il panico su un evento di crisi o di emergenza, tra cui l'utilizzo di filmati storici di un attacco precedente come se fossero attuali, o l'affermazione errata che un bene di prima necessità (come il cibo o l'acqua) non è più disponibile in un determinato luogo. Informazioni errate sulla salute, come affermazioni fuorvianti sui vaccini, consigli medici imprecisi che scoraggiano le persone dal sottoporsi a cure mediche adeguate per una malattia potenzialmente letale, o altre informazioni errate che possono causare effetti negativi sulla salute di un individuo.
- La disinformazione sul cambiamento climatico che mina il consenso scientifico consolidato, come la negazione dell'esistenza del cambiamento climatico o dei fattori che vi contribuiscono.
- Teorie di cospirazione che fanno nomi e attaccano singole persone.
- Teorie di cospirazione violente o che incitano all'odio, come l'invito all'azione violenta, il collegamento a precedenti episodi di violenza, la negazione di eventi violenti ben documentati o il pregiudizio nei confronti di un gruppo con un attributo protetto.

- **Integrità civica ed elettorale**

- La disinformazione elettorale, tra cui:
 - Come, quando e dove votare o registrarsi per votare;
 - Requisiti di eleggibilità degli elettori per partecipare a un'elezione e qualifiche dei candidati per candidarsi a una carica;
 - Leggi, processi e procedure che regolano l'organizzazione e l'attuazione delle elezioni e di altri processi civici, come referendum, proposte di voto o censimenti;



- Risultati finali o esito di un'elezione.

- **Media modificati e contenuti generati dall'intelligenza artificiale (AIGC)**

- Persone dall'aspetto realistico di età inferiore ai 18 anni.
- L'immagine di figure private adulte, se ci rendiamo conto che è stata utilizzata senza il loro permesso.
- Media fuorvianti dell'AIGC o modificati che mostrano falsamente:
 - Contenuto fatto sembrare proveniente da una fonte autorevole, come ad esempio un'organizzazione giornalistica rispettabile;
 - Un evento di crisi, come un conflitto o un disastro naturale.
- Un personaggio pubblico che è:
 - essere degradati o molestati, o assumere comportamenti criminali o antisociali;
 - prendere posizione su una questione politica, su un prodotto commerciale o su una questione di importanza pubblica (come un'elezione);
 - essere appoggiato o condannato politicamente da un individuo o da un gruppo.

- **Fidanzamento falso**

- Facilitare il commercio o la commercializzazione di servizi che aumentano artificialmente il coinvolgimento, come la vendita di follower o like.
- Fornendo istruzioni su come aumentare artificialmente il coinvolgimento su TikTok.

Abbiamo chiarito ancora meglio ai nostri utenti che i seguenti contenuti non sono ammissibili per il feed For You:

- **Disinformazione**

- Teorie del complotto che sono infondate e sostengono che certi eventi o situazioni sono portati avanti da gruppi occulti o potenti, come "il governo" o una "società segreta".
- Disinformazione sanitaria con danni moderati, come ad esempio una raccomandazione non provata su come trattare una malattia minore
- Media riproposti, come ad esempio mostrare una folla a un concerto musicale e far credere che si tratti di una protesta politica.
- travisare fonti autorevoli, come ad esempio fare riferimento in modo selettivo a determinati dati scientifici per sostenere una conclusione contraria ai risultati dello studio
- Richieste di risarcimento non verificate relative a un'emergenza o a un evento in corso di svolgimento
- Potenziale disinformazione ad alto rischio mentre è sottoposta a verifica di fact-checking



- **Integrità civica ed elettorale**

- Affermazioni non verificate su un'elezione, come l'affermazione prematura che tutte le schede sono state contate o scrutinate.
- Dichiarazioni che travisano in modo significativo informazioni civiche autorevoli, come ad una falsa affermazione sul testo di un disegno di legge parlamentare

- **Fidanzamento falso**

- Contenuti che ingannano o manipolano gli altri per aumentare i doni o le metriche di coinvolgimento, come promesse di "like-for-like" o altri falsi incentivi per il coinvolgimento nei contenuti

Come indicato nella QRE 14, rimuoviamo anche gli account che cercano di ingannare le persone o di usare TikTok per influenzare in modo ingannevole l'opinione pubblica. Queste attività vanno dalla creazione di account non autentici o falsi a sforzi più sofisticati per minare la fiducia del pubblico.

All'interno del nostro team Fiducia e sicurezza abbiamo esperti di politiche dedicate al tema dell'integrità e dell'autenticità. Essi tengono costantemente sotto controllo queste politiche e collaborano con partner ed esperti esterni per capire se sono necessari aggiornamenti o nuove politiche e garantire che siano informate da una diversità di prospettive, competenze ed esperienze vissute. In particolare, il nostro Consiglio consultivo sulla sicurezza per l'Europa, che riunisce leader indipendenti del mondo accademico e della società civile, rappresenta un'ampia gamma di background e prospettive ed composto da esperti in materia di libertà di espressione, disinformazione e altri temi legati alla sicurezza, che collaborano con noi per informare e rafforzare le nostre politiche, le caratteristiche dei prodotti e i processi di sicurezza.

Applicazione delle nostre politiche. Rimuoviamo i contenuti - inclusi video, audio, livestream, immagini, commenti, link o altro testo - che violano le nostre politiche I&A. Le persone vengono informate delle nostre decisioni e possono fare ricorso se ritengono che non si sia alcuna violazione. Nelle nostre CG chiariamo anche che bannaremo temporaneamente o permanentemente gli account e/o gli utenti coinvolti in violazioni gravi o ripetute, comprese le violazioni delle nostre politiche I&A.

Applichiamo le nostre politiche di CG, comprese quelle di I&A, attraverso un mix di tecnologia e moderazione umana. Per farlo in modo efficace e su scala, continuiamo a investire nel nostro processo di revisione automatizzato, oltre che nel personale e nella formazione. In TikTok poniamo una notevole enfasi sulla moderazione proattiva dei contenuti. Ciò significa che i nostri team lavorano per individuare e rimuovere il materiale dannoso prima che ci venga segnalato.



	<p>Tuttavia, la disinformazione è diversa da altri problemi di contenuto. Il contesto e il fact-checking sono fondamentali per applicare in modo coerente e accurato le nostre politiche di disinformazione. Per questo motivo, anche se utilizziamo modelli di apprendimento automatico per individuare la potenziale disinformazione, il nostro approccio attuale prevede che il nostro team di moderazione valuti, confermi e rimuova le violazioni della disinformazione. Abbiamo moderatori della disinformazione che hanno una formazione avanzata, competenze e strumenti per intervenire sulla disinformazione dannosa. Questo include un archivio di affermazioni precedentemente verificate per aiutare i moderatori della disinformazione a prendere decisioni rapide e accurate e l'accesso diretto al nostro team di moderazione.</p> <p>partner di fact-checking che aiutano a valutare l'accuratezza dei nuovi contenuti.</p> <p>Cerchiamo di mantenere un equilibrio tra la libertà di espressione e la protezione dei nostri utenti e del pubblico in generale da contenuti dannosi. Il nostro approccio alla lotta contro la disinformazione dannosa, come indicato nelle nostre CG, consiste nel rimuovere i contenuti che sono falsi e che possono causare danni alle persone o al pubblico in generale. Ciò non include le semplici informazioni inesatte che non comportano un rischio di danno. Inoltre, nei casi in cui le verifiche dei fatti siano inconcludenti, in particolare durante le emergenze o gli eventi in corso, i contenuti potrebbero non essere rimossi e potrebbero invece diventare inammissibili per la raccomandazione nel feed For You ed essere etichettati con la dicitura "contenuto non verificato" per limitare la diffusione di informazioni potenzialmente fuorvianti.</p> <p>Siamo lieti di includere in questo rapporto il numero di video resi non ammissibili per il feed For You in base alle politiche I&A pertinenti, come spiegato agli utenti qui.</p> <p>Si noti che, in relazione alle metriche che abbiamo condiviso nella SLI 18.2.1 di seguito, di tutte le visualizzazioni avvenute nel periodo H2 2024, circa meno di 1 su 10.000 visualizzazioni ha riguardato contenuti identificati e rimossi per violazione delle nostre politiche sulla disinformazione dannosa.</p>
SLI 18.2.1	<p>Metodologia di misurazione dei dati:</p> <p>Abbiamo basato i seguenti numeri sul Paese in cui il video è stato pubblicato: video rimossi a causa di violazioni delle nostre politiche di disinformazione, integrità civica ed elettorale, media modificati e AIGC.</p> <p>Il numero di visualizzazioni dei video rimossi a causa della violazione di ciascuna di queste politiche si basa sulla posizione approssimativa dell'utente.</p> <p>Abbiamo anche aggiornato la metodologia sul numero di video resi non ammissibili per il feed For You in base alla nostra politica di disinformazione.</p>

	Numero totale di violazioni	Metrica 1: indicare l'impatto dell'azione intrapresa	Numero totale di violazioni	Metrica 1: indicare l'impatto dell'azione intrapresa
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Numero di video rimossi per violazione della politica di disinformazione	Numero di visualizzazioni di video rimossi per violazione della politica di disinformazione	Numero di video resi non ammissibili per il feed For You in base alla politica di disinformazione.	
Stati membri				
Austria	2,888	1,313,102	1,696	
Belgio	3,902	2,844,929	2,688	
Bulgaria	1,568	5,435,715	1,600	
Croazia	789	973,202	616	
Cipro	511	1,241,327	326	
Repubblica Ceca	2,720	4,705,302	6470	
Danimarca	1,455	2,979,180	1157	
Estonia	319	77,555	453	
Finlandia	984	1,784,968	811	
Francia	44,354	61,693,484	24,035	



Germania	50,335	162,220,869	30,934	
Grecia	4,198	4,431,258	1,735	
Ungheria	2,002	9,947,587	957	
Irlanda	4,676	4,802,257	2,154	
Italia	21,035	39,078,480	19,481	
Lettonia	694	3,745,925	459	
Lituania	520	1,122,197	647	
Lussemburgo	279	162,787	121	
Malta	168	5,599	173	
Paesi Bassi	5,422	28,11,880	6,189	
Polonia	13,028	59,545,691	9,872	
Portogallo	2,629	31,071,224	1,400	
Romania	14,103	64,183,832	11,739	
Slovacchia	1,365	4,714,713	1,472	
Slovenia	574	22,494	346	
Spagna	22,581	37,024,505	54,592	



Svezia	3,489	9,893,681	2,423	
Islanda	122	153,566	77	
Liechtenstein	35	0	33	
Norvegia	1,798	5,158,745	1,200	
Totale UE	206,588	517,833,743	184,546	
Totale SEE	208,543	523,146,054	185,856	
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Numero di video rimossi a causa di violazione di norme civiche ed elettorali Politica di integrità	Numero di visualizzazioni di video rimossi a causa di violazione delle norme civiche e Politica di integrità elettorale	Numero di video rimosso per violazione delle norme sintetiche e i media manipolati	Numero di visualizzazioni di video rimossi per violazione dei media sintetici e manipolati
Stati membri				
Austria	472	843,182	414	216,433
Belgio	1,002	107,828	2,092	1,119,223
Bulgaria	182	110,186	227	5,977
Croazia	64	3,753	1,361	58,579
Cipro	86	1,333	948	19,441
Repubblica Ceca	275	25,952	465	8,287,531
Danimarca	335	14,082	315	2,742,457

Estonia	41	866	208	2,063,380	
Finlandia	199	1,944	716	464,824	
Francia	4,390	8,369,126	8,563	312,078,908	
Germania	12,231	3,510,858	11,199	23,904,234	
Grecia	649	1,726,365	8,742	145,950	
Ungheria	308	273,247	261	86,870	
Irlanda	2,051	568,596	1063	103,199	
Italia	3,910	1,578,217	3,574	1,892,355	
Lettonia	48	9	129	4,519	
Lituania	57	26	203	25,410	
Lussemburgo	66	2,180	223	8,729	
Malta	70	97	183	5,811,847	
Paesi Bassi	1,046	55,695	1,883	9,080,526	
Polonia	768	3,942,081	772	13,404,186	
Portogallo	535	28,529	1,010	339,124	
Romania	4,276	33,123,122	937	623,525	
Slovacchia	41	677	98	2,014	
Slovenia	28	111	66	605	
Spagna	2,126	3,554,918	4,392	21,882,268	

Svezia	633	6,424	762	377,862	
Islanda	26	19	85	6,113	
Liechtenstein	20	0	48	525	
Norvegia	313	1,152,478	679	139,984	
Totale UE	35,889	57,849,404	50,806	404,749,976	
Totale SEE	36,248	59,001,901	51,618	404,896,598	
Misura 18.3					
QRE 18.3.1	<p>Ci consultiamo regolarmente con esperti e ricercatori di terze parti per lo sviluppo di politiche e funzioni volte a ridurre la diffusione della disinformazione. Ad esempio, ci siamo confrontati con esperti di tutto il mondo sulle nostre politiche di disinformazione elettorale, che ci hanno aiutato ad aggiornare le nostre politiche I&A.</p> <p>Siamo orgogliosi della stretta collaborazione con gli psicologi comportamentali Irrational Labs, che ha portato allo sviluppo delle seguenti caratteristiche di avvertimento ed etichettatura (maggiori dettagli in QRE 21.3.1):</p> <ul style="list-style-type: none">• messaggi specializzati per i contenuti non verificati, che segnalano agli spettatori i contenuti non verificati identificati durante un'emergenza o un evento in corso e• la nostra etichetta per i media controllati dallo Stato, che porta trasparenza alla nostra comunità in relazione alle entità mediatiche affiliate allo Stato e sensibilizza gli utenti per a considerare l'affidabilità della fonte. <p>Siamo orgogliosi di essere firmatari del Partnership on AI (PAI) Responsible Practices for Synthetic Media. Abbiamo contribuito allo sviluppo di questo codice di best practice del settore per la trasparenza dell'IA e l'innovazione responsabile, bilanciando l'espressione creativa con i rischi della tecnologia emergente dell'IA. Inoltre, in conformità con gli impegni assunti in qualità di partner di lancio, abbiamo lavorato a un caso di studio che illustra come le Pratiche abbiano informato la nostra politica sui media sintetici.</p>				

V. Responsabilizzare gli utenti	
Impegno 19	
I Firmatari rilevanti che utilizzano sistemi di raccomandazione si impegnano a renderli trasparenti ai destinatari per quanto riguarda i principali criteri e parametri utilizzati per dare priorità o privare di priorità le informazioni, e a fornire agli utenti opzioni sui sistemi di raccomandazione e a rendere disponibili informazioni su tali opzioni.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve elenco].	<ul style="list-style-type: none">● In TikTok ci sforziamo di rendere più trasparente il modo in cui proteggiamo la nostra piattaforma. Continuiamo ad aumentare i rapporti che pubblichiamo volontariamente, la profondità dei dati che divulghiamo e la frequenza con cui li pubblichiamo.● Nel dicembre 2024 abbiamo pubblicato la nostra ultima raccolta di rapporti sulla trasparenza, tra cui: Rapporto sull'applicazione delle linee guida della comunità (luglio-settembre 2024); Rapporto sulle richieste di rimozione da parte del governo; Rapporto sulle richieste di informazioni da parte delle forze dell'ordine, Rapporto sulle richieste di rimozione IP; e i più recenti Rapporti sulle operazioni di influenza segreta, in cui abbiamo condiviso informazioni sulle reti di influenza che abbiamo interrotto nei mesi di ottobre e novembre 2024.● Abbiamo anche lavorato per rendere più facile per le persone studiare in modo indipendente i nostri dati e la nostra piattaforma. Ad esempio attraverso:<ul style="list-style-type: none">○ i nostri strumenti di ricerca, che consentono a oltre 500 team di ricerca studiare in modo indipendente la nostra piattaforma.○ il file di dati scaricabile nel Community Guidelines Enforcement Report che offre l'accesso a dati aggregati, compresi i dati di rimozione per categoria di policy, per i 50 mercati con i maggiori volumi di contenuti rimossi.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No



<p>Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?</p>	
<p>Misura 19.1</p>	
<p>QRE 19.1.1</p>	<p>Il feed For You è l'interfaccia che gli utenti vedono per la prima volta quando aprono TikTok. È il fulcro dell'esperienza di TikTok e il luogo in cui la maggior parte dei nostri utenti trascorre il proprio tempo esplorando la piattaforma.</p> <p>Nei nostri Termini di servizio e nelle CG chiariamo agli utenti (e forniamo anche un contesto più ampio nell'articolo del Centro assistenza e nella pagina del Centro trasparenza) che il feed For You di ciascun titolare di account si basa su un sistema di raccomandazioni personalizzato. Il feed di For You è curato in base a ciascun utente. La sicurezza è integrata nelle nostre raccomandazioni. Oltre a rimuovere i contenuti di disinformazione dannosi che violano le nostre CG, prendiamo provvedimenti per evitare di raccomandare alcune categorie di contenuti che potrebbero non essere adatti a un pubblico ampio, tra cui le teorie cospirative generali e le informazioni non verificate relative a un'emergenza o a un evento in corso. Potremmo anche rendere alcuni di questi contenuti più difficili da trovare nelle ricerche.</p> <p>Parametri principali. Il sistema raccomanda i contenuti classificandoli in base a una combinazione di fattori, tra cui:</p> <ul style="list-style-type: none"> ● le interazioni degli utenti (ad esempio, i contenuti che gli utenti apprezzano, condividono, e guardano per intero o saltano, nonché gli account dei follower che gli utenti seguono a loro volta); ● Informazioni sui contenuti (ad esempio suoni, hashtag, numero di visualizzazioni e paese in cui il contenuto è stato pubblicato); e ● Informazioni sull'utente (ad esempio, impostazioni del dispositivo, preferenze linguistiche, posizione, fuso orario e giorno e tipi di dispositivi). <p>I parametri principali ci aiutano a fare previsioni sui contenuti che probabilmente interessano agli utenti. I diversi fattori possono avere un ruolo più o meno importante nei contenuti consigliati e l'importanza - o la ponderazione - di un fattore può cambiare nel tempo. Per molti utenti, il tempo trascorso a guardare un video specifico è generalmente più importante di altri fattori. Queste previsioni sono anche influenzate dalle interazioni di altre persone su TikTok che sembrano avere interessi simili. Ad esempio, se a un utente piacciono i video 1, 2 e 3 e a un secondo utente piacciono i video 1, 2 e 3.</p>



	<p>video 1, 2, 3, 4 e 5, il sistema di raccomandazione potrebbe prevedere che al primo utente piaceranno anche i video 4 e 5.</p> <p>Gli utenti possono anche accedere alla funzione "Perché questo video", che consente loro di vedere i fattori che hanno influenzato l'apparizione di un particolare video nel loro feed For You. Questa funzione offre una maggiore trasparenza in relazione al funzionamento del nostro sistema di classificazione e consente agli utenti di capire meglio perché un determinato video è stato loro consigliato. La funzione spiega essenzialmente agli utenti come le interazioni passate sulla piattaforma abbiano influito sul video che è stato loro consigliato. Per ulteriori informazioni, consultare il nostro post nella newsroom.</p> <p>Preferenze dell'utente. Oltre alle salvaguardie che abbiamo integrato nella nostra piattaforma, ai nostri utenti la possibilità di personalizzare la loro esperienza in base alle loro preferenze e al loro comfort.</p> <p>Questi includono una serie di funzioni che aiutano a modellare i contenuti che vedono. Ad esempio, feed Per te:</p> <ul style="list-style-type: none"> ● Gli utenti possono cliccare su qualsiasi video e selezionare "non interessato" per indicare che non vogliono vedere contenuti simili. ● Gli utenti possono filtrare automaticamente parole o hashtag specifici dai contenuti consigliati (vedi qui). <p>Gli utenti possono aggiornare il loro feed For You se ritengono che le raccomandazioni non siano più rilevanti per loro o siano troppo simili. Quando il feed For You viene aggiornato, gli utenti visualizzano una serie di nuovi video che includono video popolari (ad esempio, con un alto numero di visualizzazioni o un alto tasso di like). La loro interazione con questi nuovi video informerà le raccomandazioni future.</p> <p>Nell'ambito degli obblighi previsti dal DSA (articolo 38), abbiamo introdotto sulla nostra piattaforma dei feed non personalizzati, che forniscono ai nostri utenti europei un'alternativa ai sistemi di raccomandazione. Gli utenti possono disattivare la personalizzazione in modo che i feed mostrino contenuti non personalizzati. Ad esempio, il feed For You mostrerà invece i video più popolari nelle loro regioni e a livello internazionale. Vedi qui.</p>
Misura 19.2	

SLI 19.2.1 - impostazioni utente	Metodologia di misurazione dei dati: Il numero di utenti che hanno filtrato gli hashtag o una parola chiave per impostare le preferenze per il feed For You, il numero di volte in cui gli utenti hanno cliccato su "non interessato" in relazione al feed For You e il numero di volte in cui gli utenti hanno cliccato sull'aggiornamento del feed For You sono tutti basati sulla posizione approssimativa degli utenti che hanno utilizzato questi strumenti. Il numero di video etichettati con l'etichetta AIGC comprende sia l'etichettatura automatica che quella generata dal creatore.			
	Numero di volte in cui gli utenti si sono impegnati attivamente con queste impostazioni	Numero di volte in cui gli utenti si sono impegnati attivamente con queste impostazioni		
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Numero di utenti che hanno filtrato hashtag o parole	Numero di utenti che hanno cliccato su "non interessato".	Numero di volte in cui gli utenti hanno cliccato sul feed "Per te" Aggiornamenti	Numero di video etichettati con l'etichetta AIGC
Stati membri				
Austria	53,057	886,639	52,559	149,390
Belgio	67,734	1,322,561	83,721	241,538
Bulgaria	34,081	744,333	38,568	153,704
Croazia	20,196	486,259	23,134	46,131
Cipro	7,895	176,600	13,456	62,428
Repubblica Ceca	45,392	753,417	35,791	140,826
Danimarca	35,294	573,821	27,747	80,022



Estonia	11,648	151,267	11,558	30907
Finlandia	45,185	586,897	43,657	109,189
Francia	332,521	7,939,397	486,316	1,832,452
Germania	503,549	7,977,800	648,033	1,883,751
Grecia	52,519	1,344,879	68,577	214,464
Ungheria	46,966	1,020,692	28,543	138,023
Irlanda	54,952	801,523	52,714	67,672
Italia	261,272	6,455,485	295,958	1,140,570
Lettonia	15,527	279,241	24,888	118,117
Lituania	21,247	325,564	23,209	64,359
Lussemburgo	4,519	76,244	5,508	44,220
Malta	3,137	77,760	4,923	15,544
Paesi Bassi	135,944	2,081,920	150,651	231,651
Polonia	196,496	3,383,567	175,988	519,883
Portogallo	57,677	1,152,515	61,327	216,364
Romania	85,551	2,629,162	165,990	325,318
Slovacchia	18,482	347,681	13,822	50,322
Slovenia	9,983	177,990	19,591	17,100
Spagna	275,604	6,889,325	381,588	1,170,610
Svezia	82,868	1,371,265	111,934	268,743

Islanda	4,720	57,250	3,175	8,073
Liechtenstein	129	3,563	291	418
Norvegia	48,188	685,406	63,483	101,728
Totale UE	2,479,296	5,001,3804	3,049,751	9,333,298
Totale SEE	2,532,333	50,760,023	3,116,700	9,443,517

V. Responsabilizzare gli utenti	
Impegno 20	
I firmatari si impegnano a mettere a disposizione degli utenti strumenti per valutare la provenienza e la storia delle modifiche, l'autenticità o l'accuratezza dei contenuti digitali.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve elenco].	TikTok non ha sottoscritto questo impegno. TikTok ritiene che sarebbe imprudente impegnarsi in questa misura in un momento in cui la tecnologia sottostante non è ancora stata provata e gli standard da rispettare non sono ancora stati finalizzati.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No



Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto COPD.
Misura 20.1	
QRE 20.1.1	Non impegnato. TikTok ritiene che sarebbe imprudente impegnarsi in questa misura in un momento in cui la tecnologia sottostante non è ancora stata provata e gli standard da rispettare non sono ancora stati definiti. Una volta che la tecnologia in questione sarà provata e gli standard saranno concordati e identificabili, TikTok valuterà se tale approccio sia vantaggioso, tenendo conto delle misure esistenti.
Misura 20.2	
QRE 20.2.1	Non impegnata. Analogamente alla misura 20.1, TikTok ritiene che sarebbe imprudente impegnarsi in questa misura in questo momento. TikTok è tuttavia disponibile a rivalutare in futuro l'opportunità di un simile approccio.

V. Responsabilizzare gli utenti

Impegno 21

I firmatari rilevanti si impegnano a rafforzare i loro sforzi per fornire agli utenti strumenti migliori per identificare la disinformazione. In particolare, per consentire agli utenti di navigare nei servizi con cognizione di causa, i firmatari rilevanti si impegnano a facilitare, in tutte le lingue degli Stati membri in cui vengono forniti i loro servizi, l'accesso degli utenti agli strumenti di valutazione dell'accuratezza fattuale delle fonti attraverso verifiche dei fatti da parte di organizzazioni di fact-checking che hanno segnalato la potenziale disinformazione, nonché etichette di avvertimento da altre fonti autorevoli.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]

Sì



Se sì, elencare queste misure di attuazione [breve punti elenco].

- Sono stati assunti due nuovi partner per il fact-checking in Europa:
 1. Albania e Kosovo: Internews Kosova
 2. Georgia: Fact Check Georgia
- Abbiamo ampliato la nostra copertura di fact-checking a una serie di Paesi dell'Europa allargata e candidati all'UE:
 - Albania e Kosovo: Internews Kosova
 - Georgia: Fact Check Georgia.
 - Kazakistan: Reuters
 - Moldavia: AFP/Reuters
 - Serbia: Storie di punta
- Abbiamo condotto 14 **campagne** temporanee **di alfabetizzazione mediatica** sull'**integrità elettorale** prima elezioni regionali, la maggior parte delle quali in collaborazione con i nostri partner per il fact-checking e l'alfabetizzazione mediatica:
 - 8 nell'UE (Austria, Croazia, Francia, 2 x Germania, Irlanda, Lituania e Romania)
 - Austria: Deutsche Presse-Agentur (dpa)
 - Croazia: Faktograf
 - Francia: Agence France-Presse (AFP)
 - Germania (elezioni regionali): Deutsche Presse-Agentur dpa)
 - Germania (elezioni federali): Deutsche Presse-Agentur dpa)
 - Irlanda: Il giornale
 - Lituania: N/A
 - Romania: Cittadini divertenti
 - 1 nel SEE
 - Islanda: N/A
 - 5 in Europa allargata/paesi candidati all'UE (Bosnia, Bulgaria, Cechia, Georgia e Moldavia)
 - Bosnia: N/A
 - Bulgaria: N/A
 - Cechia: N/A
 - Georgia: Fact Check Georgia
 - Moldavia: StopFals!
- Lanciate quattro nuove guide temporanee in-app per la ricerca di informazioni sulle catastrofi naturali che rimandano ad agenzie e organizzazioni terze autorevoli:



	<ul style="list-style-type: none"> ○ Alluvioni nell'Europa centrale e orientale (Austria, Bosnia, Cechia, Germania, Ungheria, Moldavia, Polonia, Romania e Slovacchia) ○ Incendi in Portogallo ○ Alluvioni in Spagna ○ Ciclone di Mayotte ● Abbiamo continuato i nostri interventi in-app, tra cui video tag, interventi di ricerca e centri di informazione in-app, disponibili in 23 lingue ufficiali dell'UE e in norvegese e islandese per gli utenti del SEE, in merito alle elezioni, al conflitto Israele-Hamas, al cambiamento climatico, all'educazione all'Olocausto, all'Mpox e alla guerra in Ucraina. ● Collaboriamo con i verificatori dei fatti per valutare l'accuratezza dei contenuti. Talvolta, i nostri partner di fact-checking stabiliscono che i contenuti non possono essere confermati o che le verifiche sono inconcludenti (soprattutto in occasione di eventi in corso). Quando i nostri partner di fact-checking ci forniscono una valutazione che dimostra che l'affermazione non può ancora essere verificata, possiamo utilizzare la nostra etichetta di contenuto non verificato per informare gli spettatori tramite un banner che un video contiene contenuti non verificati, nel tentativo di sensibilizzare gli utenti sulla credibilità dei contenuti. ● Sulla base della nostra nuova etichetta contenuti generati dall'IA per i creatori e dell'implementazione delle C2PA Content Credentials, abbiamo lanciato una serie di campagne di alfabetizzazione mediatica con la guida di organizzazioni esperte come Mediawise e WITNESS, anche in Brasile, Germania, Francia, Messico e Regno Unito, che insegnano alla nostra comunità come individuare ed etichettare i contenuti generati dall'IA. <ul style="list-style-type: none"> ○ La nostra campagna di trasparenza dell'AIGC, informata da WITNESS, ha raggiunto 80 milioni di utenti a livello globale, di cui oltre 8,5 milioni e 9,5 milioni rispettivamente in Germania e in Francia.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.



Misura 21.1	
QRE 21.1.1	<p>Attualmente abbiamo 14 partner di fact-checking accreditati dall'IFCN in tutta l'UE, il SEE e l'Europa:</p> <ol style="list-style-type: none"> 1. Agence France-Presse (AFP) 2. dpa Agenzia di stampa tedesca 3. Demagogo 4. Facta 5. Verifica dei fatti in Georgia 6. Faktograf 7. Internews Kosova 8. Storie di protagonisti 9. Fatti logici 10. Newtral 11. Poligrafo 12. Reuters 13. Feedback scientifico 14. Teyit <p>Questi partner forniscono una copertura di fact-checking in 23 lingue ufficiali dell'AEA, tra cui almeno una lingua ufficiale di ogni Stato membro dell'UE, oltre a georgiano, russo, turco e ucraino.</p> <p>Ci assicuriamo che i nostri utenti beneficino del contesto e degli approfondimenti forniti dalle organizzazioni di fact checking con cui collaboriamo nei seguenti modi:</p> <ul style="list-style-type: none"> ● Applicazione delle politiche di disinformazione. I nostri partner di fact-checking svolgono un ruolo fondamentale nell'aiutarci a far rispettare le nostre politiche di disinformazione, che mirano a promuovere un'esperienza affidabile e autentica per i nostri utenti. Riteniamo che il contesto e il fact-checking siano fondamentali per applicare in modo coerente e accurato queste politiche, quindi, mentre utilizziamo modelli di apprendimento automatico per aiutare a rilevare la potenziale disinformazione, facciamo in modo che i nostri moderatori della disinformazione valutino, confermino e agiscano sulla disinformazione dannosa. Come parte di questo processo, i nostri moderatori possono accedere a un archivio di affermazioni precedentemente verificate e sono in grado di fornire contenuti ai nostri partner esperti di fact checking per un'ulteriore valutazione. Quando i partner di fact-checking segnalano che il contenuto è falso, i nostri moderatori adottano misure per valutarlo e rimuoverlo dal nostro sito.



piattaforma. La nostra risposta alla domanda 31.1.1 fornisce ulteriori informazioni sul modo in cui i partner di fact-checking sono coinvolti in questo processo.

- **Etichettatura di contenuti non verificati.** Come già accennato, collaboriamo con i fact checker per valutare l'accuratezza dei contenuti. Talvolta, i nostri partner di fact-checking stabiliscono che i contenuti non possono essere confermati o che le verifiche sono inconcludenti (soprattutto in occasione di eventi in corso). Quando i nostri partner di fact-checking ci forniscono una valutazione che dimostra che l'affermazione non può ancora essere verificata, possiamo utilizzare la nostra etichetta di contenuto non verificato per informare gli spettatori [tramite un banner](#) che un video contiene contenuti non verificati, nel tentativo di sensibilizzare gli utenti sulla credibilità dei contenuti. In questi casi, il creatore del contenuto viene informato che il suo video è stato contrassegnato come contenuto non comprovato e che il video non potrà essere raccomandato nel feed For You.
- **Strumenti in-app relativi ad argomenti specifici:**
 - **Integrità elettorale.** In vista di diverse elezioni importanti abbiamo lanciato campagne volte a educare il pubblico sul processo di voto, incoraggiando gli utenti a verificare le informazioni con i nostri partner di fact-checking. Ad esempio, la campagna per l'integrità elettorale che abbiamo lanciato in vista delle elezioni legislative francesi del giugno 2024 comprendeva un intervento di ricerca e un [Centro elettorale](#). In-app il centro conteneva una sezione dedicata all'individuazione della disinformazione, che includeva video creati in collaborazione con l'organizzazione di fact-checking [Agence France-Presse \(AFP\)](#). In totale, durante il periodo di riferimento, abbiamo realizzato 14 **campagne temporanee di alfabetizzazione mediatica sull'integrità elettorale** prima delle elezioni regionali.
 - **Cambiamento climatico.** Abbiamo lanciato un intervento di ricerca che reindirizza gli utenti che cercano contenuti relativi al cambiamento climatico verso informazioni autorevoli. Abbiamo collaborato con le Nazioni Unite per fornire le informazioni autorevoli (si veda il nostro post sulla newsroom).
 - **COP29:** tra il 29 ottobre e il 25 novembre abbiamo lanciato due funzionalità globali (un tag di avviso video e una guida alla ricerca di interventi) per indirizzare gli utenti verso contenuti autorevoli relativi al clima, che sono stati visualizzati 400.000 volte.
 - **Disastri naturali:** Lanciate quattro nuove guide temporanee all'interno dell'app per la ricerca di informazioni sulle catastrofi naturali che rimandano ad agenzie e organizzazioni terze autorevoli:
 - 1) Alluvioni nell'Europa centrale e orientale (Austria, Bosnia, Cechia, Germania, Ungheria, Moldavia, Polonia, Romania e Slovacchia)

	<div>2) Incendi in Portogallo</div> <div>3) Alluvioni in Spagna</div> <div>4) Ciclone di Mayotte</div> <div><ul style="list-style-type: none">● Sensibilizzazione degli utenti sulle nostre partnership di fact-checking e sulle etichette. Abbiamo creato delle pagine sul nostro Centro per la sicurezza e il Centro per la trasparenza per sensibilizzare gli utenti sul nostro programma di fact-checking e sulle etichette e per sostenere il lavoro dei nostri partner di fact-checking.</div>				
SLI 21.1.1 - azioni intraprese nell'ambito della misura 21.1	Metodologia di misurazione dei dati: La quota di rimozioni in base alla nostra politica di disinformazione dannosa, la quota di rimozioni proattive, la quota di rimozioni prima di qualsiasi visualizzazione e la quota di rimozioni entro 24 ore sono relative al totale delle rimozioni di ciascuna politica. Il tasso di annullamento delle condivisioni (%) dopo il pop-up di avviso di condivisione dell'etichetta di contenuto non verificato indica la percentuale di utenti che non condividono un video dopo aver visto il pop-up dell'etichetta. Questa metrica si basa sulla posizione approssimativa degli utenti che hanno utilizzato questi strumenti.				
	Raggiungimento di etichette/ fact-checkers e altre fonti autorevoli	Altre metriche pertinenti	Altre metriche pertinenti	Altre metriche pertinenti	Altre metriche pertinenti
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Tasso di annullamento delle condivisioni (%) dopo il pop-up di avviso di condivisione dell'etichetta di contenuto non verificato (utenti che non condividono il video dopo aver visto il pop-up)	Percentuale di allontanamenti in base alla politica di disinformazione	Percentuale di allontanamenti proattivi nell'ambito della politica di disinformazione	Quota di video rimossi prima di qualsiasi visualizzazione in base alla politica di disinformazione	Percentuale di rimozioni di video entro 24 ore per politica di disinformazione e
Stati membri					



Austria	31.81%	20.2%	97.9%	80.9%	82.2%
Belgio	33.81%	14.4%	98.9%	82.5%	89.6%
Bulgaria	33.97%	30.6%	94.4%	59.4%	82.9%
Croazia	33.66%	20.9%	99.0%	70.5%	89.5%
Cipro	32.91%	18.4%	95.7%	71.6%	83.0%
Repubblica Ceca	29.52%	25.2%	91.8%	53.2%	90.9%
Danimarca	30.20%	8.3%	96.9%	73.5%	83.1%
Estonia	28.53%	18.7%	99.4%	75.9%	93.1%
Finlandia	27.21%	15.5%	94.1%	69.8%	89.4%
Francia	37.13%	22.4%	99.2%	86.9%	95.6%
Germania	30.09%	21.8%	97.7%	76.1%	90.9%
Grecia	32.05%	17.3%	96.9%	74.9%	92.3%
Ungheria	31.38%	28.9%	90.5%	63.5%	86.3%
Irlanda	29.59%	22.2%	93.8%	61.2%	88.4%
Italia	37.65%	27.7%	98.3%	72.7%	92.1%
Lettonia	30.90%	27.0%	98.8%	82.4%	94.2%
Lituania	30.80%	23.2%	99.2%	87.5%	94.4%
Lussemburgo	33.64%	9.4%	98.9%	88.5%	86.4%
Malta	35.43%	9.8%	98.2%	89.3%	88.1%

Paesi Bassi	27.79%	16.6%	99.2%	86.3%	89.5%
Polonia	28.88%	30.4%	94.3%	63.9%	89.6%
Portogallo	33.08%	26.7%	97.6%	84.9%	90.6%
Romania	30.08%	41.0%	91.7%	62.5%	82.1%
Slovacchia	28.89%	45.7%	89.2%	56.0%	87.5%
Slovenia	33.33%	22.9%	99.3%	79.1%	95.8%
Spagna	34.09%	28.3%	99.1%	82.6%	90.4%
Svezia	29.44%	10.9%	97.7%	77.8%	90.4%
Islanda	27.86%	4.4%	97.5%	90.2%	92.6%
Liechtenstein	19.61%	3.1%	100.0%	100.0%	91.4%
Norvegia	25.37%	18.8%	96.1%	74.0%	89.9%
Totale UE	32.24%	23.1%	97.4%	76.6%	90.9%
Totale SEE	32.13%	23.0%	97.3%	76.6%	90.9%
Stati membri		Quota di rimozioni di video nell'ambito della politica di integrità civica ed elettorale	Quota di rimozioni video proattive nell'ambito della politica di integrità civica ed elettorale	Quota di rimozioni di video prima di qualsiasi visualizzazione in base alla politica di integrità civica ed elettorale	Quota di rimozioni di video entro 24 ore in base alla politica di integrità civica ed elettorale
Austria		3.3%	96.6%	77.1%	82.8%



Belgio		3.7%	98.6%	89.9%	93.1%
Bulgaria		3.5%	95.1%	90.1%	94.5%
Croazia		1.7%	95.3%	85.9%	87.5%
Cipro		3.1%	98.8%	83.7%	82.6%
Repubblica Ceca		2.5%	98.2%	94.2%	94.9%
Danimarca		1.9%	97.6%	94.6%	96.7%
Estonia		2.4%	97.6%	82.9%	87.8%
Finlandia		3.1%	98.0%	92.5%	97.0%
Francia		2.2%	97.9%	90.0%	96.5%
Germania		5.3%	98.1%	85.1%	96.2%
Grecia		2.7%	98.8%	96.5%	98.2%
Ungheria		4.4%	91.9%	82.5%	95.1%
Irlanda		9.7%	86.0%	24.4%	96.3%
Italia		5.1%	98.6%	81.4%	88.8%
Lettonia		1.9%	97.9%	93.8%	87.5%
Lituania		2.5%	100.0%	93.0%	91.2%
Lussemburgo		2.2%	97.0%	92.4%	98.5%
Malta		4.1%	100.0%	94.3%	95.7%
Paesi Bassi		3.2%	99.4%	91.0%	94.5%

Polonia		1.8%	95.6%	90.9%	93.6%
Portogallo		5.4%	99.4%	97.2%	97.8%
Romania		12.4%	78.0%	27.8%	49.8%
Slovacchia		1.4%	97.6%	92.7%	97.6%
Slovenia		1.1%	100.0%	89.3%	92.9%
Spagna		2.7%	98.5%	69.7%	81.9%
Svezia		2.0%	98.9%	95.1%	98.1%
Islanda		0.9%	100.0%	96.2%	100.0%
Liechtenstein		1.8%	100.0%	100.0%	100.0%
Norvegia		3.3%	96.5%	89.5%	92.7%
Totale UE		4.0%	95.0%	75.3%	88.7%
Totale SEE		4.0%	95.1%	75.4%	88.7%
Stati membri		% rimozioni di video secondo la politica Synthetic Media	% rimozioni video proattive in base alla politica sui media sintetici	% di rimozione dei video prima di qualsiasi visualizzazione in base alla politica dei media sintetici	% di rimozioni di video entro 24 ore secondo la politica di Synthetic Media
Austria		2.9%	99.0%	57.2%	47.3%
Belgio		7.7%	97.6%	62.8%	72.7%
Bulgaria		4.4%	99.1%	46.7%	23.8%

Croazia		36.1%	93.2%	15.4%	11.1%
Cipro		34.2%	93.8%	30.7%	6.9%
Repubblica Ceca		4.3%	97.2%	48.8%	70.8%
Danimarca		1.8%	98.1%	48.6%	59.0%
Estonia		12.2%	96.6%	59.1%	74.5%
Finlandia		11.3%	97.1%	39.9%	55.3%
Francia		4.3%	96.1%	46.5%	47.4%
Germania		4.8%	97.8%	62.1%	56.7%
Grecia		35.9%	89.9%	27.9%	10.2%
Ungheria		3.8%	98.5%	55.6%	57.5%
Irlanda		5.0%	92.8%	52.3%	60.1%
Italia		4.7%	98.8%	47.3%	44.7%
Lettonia		5.0%	99.2%	45.7%	47.3%
Lituania		9.0%	98.0%	47.8%	48.3%
Lussemburgo		7.5%	96.9%	50.7%	41.7%
Malta		10.7%	98.4%	67.2%	79.2%
Paesi Bassi		5.8%	98.7%	60.6%	67.7%
Polonia		1.8%	95.9%	56.3%	51.3%
Portogallo		10.3%	96.0%	37.8%	31.8%

Romania		2.7%	96.8%	37.9%	25.0%
Slovacchia		3.3%	98.0%	38.8%	18.4%
Slovenia		2.6%	100.0%	57.6%	60.6%
Spagna		5.5%	97.7%	33.2%	30.8%
Svezia		2.4%	95.3%	48.7%	53.7%
Islanda		3.1%	98.8%	72.9%	75.3%
Liechtenstein		4.3%	97.9%	68.8%	60.4%
Norvegia		7.1%	94.0%	46.5%	55.7%
Totale UE		5.7%	95.8%	45.9%	41.7%
Totale SEE		5.7%	95.8%	46.0%	42.0%

SLI 21.1.2 - azioni intraprese nell'ambito della misura 21.1

Metodologia di misurazione dei dati:

Il numero di video etichettati con l'etichetta contenuti non verificati si basa sul Paese in cui il video è stato pubblicato.

Il tasso di annullamento delle condivisioni (%) dopo il pop-up di avviso di condivisione dell'etichetta di contenuto non verificato indica la percentuale di utenti che non condividono un video dopo aver visto il dell'etichetta. Questa metrica si basa sulla posizione approssimativa degli utenti che hanno utilizzato questi strumenti.

Numero di etichette applicate ai contenuti, ad esempio sulla base di tali articoli

Metriche significative come l'impatto delle 21.1. misure sulle interazioni degli utenti con i contenuti o sulla loro condivisione.



				verificata come falsa o fuorviante
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)		Numero di video etichettati con l'etichetta "contenuto non verificato".		Tasso di annullamento delle condivisioni (%) dopo il pop-up di avviso di condivisione dell'etichetta di contenuto non verificato (utenti che non condividono il video dopo aver visto il pop-up)
Stati membri				
Austria		1,875		31.8%
Belgio		2,387		33.8%
Bulgaria		2,428		34.0%
Croazia		532		33.7%
Cipro		330		32.9%
Repubblica Ceca		2,431		29.5%
Danimarca		2,438		30.2%
Estonia		190		28.5%
Finlandia		1,768		27.2%
Francia		24,023		37.1%
Germania		28,389		30.1%
Grecia		3,363		32.0%
Ungheria		2,683		31.4%



Irlanda		1,591		29.6%
Italia		23,139		37.6%
Lettonia		415		30.9%
Lituania		389		30.8%
Lussemburgo		135		33.6%
Malta		64		35.4%
Paesi Bassi		4,787		27.8%
Polonia		12,974		28.9%
Portogallo		1,921		33.1%
Romania		6,708		30.1%
Slovacchia		1,229		28.9%
Slovenia		169		33.3%
Spagna		25,829		34.1%
Svezia		3,207		29.4%
Islanda		49		27.9%
Liechtenstein		0		19.6%
Norvegia		1,516		25.4%
Totale UE		155,394		32.2%
Totale SEE		156,959		32.1%



Misura 21.2	
QRE 21.2.1	
Misura 21.3	
QRE 21.3.1	<p>Come indicato nella risposta alla domanda 17.1.1, applichiamo a determinati contenuti le nostre etichette di contenuto non verificato, di media controllati dallo Stato e di contenuti generati dall'intelligenza artificiale, al fine di responsabilizzare la nostra comunità fornendo loro un ulteriore livello di contesto. Ci assicuriamo che queste etichette siano sviluppate e distribuite in linea con le evidenze scientifiche, collaborando con i fact-checker e con esperti esterni, compresi gli scienziati, nei seguenti modi:</p> <ul style="list-style-type: none"> ● Etichetta dei contenuti non verificati. Nel 2021, abbiamo collaborato con gli scienziati comportamentali Irrational Labs per la progettazione e il test dei suggerimenti specializzati che incoraggiano gli utenti a prendere in considerazione i contenuti etichettati come non verificati, prima di , come illustrato nella sezione 17.1.1. Testando i suggerimenti, Irrational Labs ha riscontrato che gli spettatori hanno diminuito del 24% la frequenza di condivisione dei video, mentre i "mi piace" su tali contenuti non comprovati sono diminuiti del 7%. <p>Come già menzionato, collaboriamo con una serie di fact-checkers accreditati dall'IFCN in Europa, che ci aiutano a valutare l'accuratezza di alcuni contenuti sulla nostra piattaforma. Quando i nostri partner di fact-checking stabiliscono che un video non può essere confermato o che i loro fact-checking sono inconcludenti (cosa che talvolta accade, in particolare in occasione di eventi o emergenze), possiamo applicare al video la nostra etichetta di contenuto non verificato.</p> <ul style="list-style-type: none"> ● Etichetta dei media controllati dallo Stato. Da gennaio 2023, applichiamo Le etichette dei media controllati dallo Stato si riferiscono ad account o contenuti in cui è evidente il controllo editoriale e il processo decisionale da parte di membri dello Stato. Per informare il nostro La politica sui media affiliati allo Stato, compresi gli aggiornamenti esposti in questo rapporto, e il nostro approccio per effettuare tali designazioni, ci consultiamo con esperti di media, politologi, accademici e rappresentanti di organizzazioni internazionali e della società civile in Nord e Sud America, Africa, Europa, Medio Oriente, Asia e Australia. Continuiamo a lavorare con questi esperti per informare il nostro approccio globale e l'espansione della politica. <p>Abbiamo lavorato a stretto contatto con Irrational Labs sullo sviluppo della politica dei media affiliati allo Stato e sulle modalità di presentazione dell'etichetta ai nostri utenti. Abbiamo testato diverse opzioni di copia su</p>



	<p>Inglese, spagnolo e arabo attraverso sondaggi quantitativi e panel qualitativi, e hanno scoperto che "[paese] media controllati dallo Stato" è stata l'opzione più preferita dagli utenti, oltre a essere la rappresentazione più accurata del rapporto delle entità mediatiche in questione con i rispettivi governi.</p> <ul style="list-style-type: none">● Etichetta per i contenuti generati dall'IA. Prima di lanciare le nostre nuove etichette generate dall'intelligenza artificiale per i creatori di contenuti che sono completamente generati dall'intelligenza artificiale o modificati in modo significativo dall'intelligenza artificiale, ci siamo consultati con i nostri consigli consultivi sulla sicurezza e con esperti del settore, tra cui il dottor David G. Rand del MIT, che sta studiando come gli spettatori percepiscono i diversi tipi di etichette generate dall'intelligenza artificiale. La ricerca del Dr. Rand ci ha aiutato a progettare le nostre etichette generate dall'IA.

V. Responsabilizzare gli utenti

Impegno 22

I firmatari si impegnano a fornire agli utenti strumenti che li aiutino a prendere decisioni più informate quando si imbattono in informazioni online che possono essere false o fuorvianti e a facilitare l'accesso degli utenti a strumenti e informazioni per valutare l'attendibilità delle fonti di informazione, come gli indicatori di attendibilità per una navigazione online informata, in particolare per quanto riguarda questioni sociali o dibattiti di interesse generale.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve elenco].	TikTok non ha sottoscritto questo impegno.

Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.
Misura 22.1	
QRE 22.1.1	<p>Non impegnato. TikTok ritiene che l'attuazione degli altri impegni previsti Codice (compresi, ma non solo, gli altri impegni relativi alla responsabilizzazione degli utenti e al fact-checking) fornisca un approccio globale alla lotta contro la disinformazione, che comprende l'agevolazione degli utenti nel prendere decisioni più informate quando si imbattono in informazioni online che possono essere false o fuorvianti. Questa posizione si riflette anche negli orientamenti della Commissione. Pertanto, TikTok non ritiene che l'impegno a rispettare questa misura si aggiunga materialmente alle altre misure adottate nell'ambito del Codice.</p> <p>TikTok, tuttavia, mantiene una mentalità aperta. In quanto tale, è disposta a esplorare tali soluzioni con i fornitori interessati a tempo debito e a rivalutare se tale approccio sia vantaggioso, tenendo conto delle misure esistenti.</p>
SLI 22.1.1 - azioni di applicazione delle politiche di cui sopra	N/D
	N/D

Misura 22.2	
-------------	--



QRE 22.2.1	Non impegnato. TikTok non ritiene che questa sia una proposta pratica o attuabile. In ogni caso, questa misura non è necessaria in quanto la combinazione di altri impegni alla base del Codice (compresi, ma non solo, quelli relativi al fact-checking) rappresentano un approccio completo per raggiungere l'obiettivo di fornire agli utenti strumenti per prendere decisioni più informate quando incontrano informazioni online che possono essere false o fuorvianti.
Misura 22.3	
QRE 22.3.1	Non impegnato. Non pertinente, legato alle Misure di cui sopra.
Misura 22.4	
QRE 22.4.1	Non impegnato. Le misure 22.4, 22.5 e 22.6 non sono applicabili in quanto TikTok non è un fornitore di indicatori di affidabilità.
SLI 22.4.1 - azioni di applicazione delle politiche di cui sopra	N/D
	N/D
Dati	Non impegnato. TikTok non ritiene che questa sia una proposta pratica o attuabile. In ogni caso, questa misura non è necessaria in quanto la combinazione di altri impegni alla base del Codice (compresi, ma non solo, quelli relativi al fact-checking) rappresentano un approccio completo per raggiungere l'obiettivo di fornire agli utenti strumenti per prendere decisioni più informate quando incontrano informazioni online che possono essere false o fuorvianti.
Misura 22.5	
QRE 22.5.1	Non impegnato. Non pertinente, legato alle Misure di cui sopra.

SLI 22.5.1 - azioni di applicazione delle politiche di cui sopra	
	Non impegnato. Le misure 22.4, 22.5 e 22.6 non sono applicabili in quanto TikTok non è un fornitore di indicatori di affidabilità.

SLI 22.5.2 - azioni di applicazione delle politiche di cui sopra	N/D
	N/D
Dati	
Misura 22.6	
QRE 22.6.1	Non impegnato. Le misure 22.4, 22.5 e 22.6 non sono applicabili in quanto TikTok non è un fornitore di indicatori di affidabilità.
SLI 22.6.1 - azioni di applicazione delle politiche di cui sopra	N/D
	N/D
Dati	
Misura 22.7	
QRE 22.7.1	Come abbiamo risposto alla domanda 17.1.1, disponiamo di numerosi strumenti (tag di avviso video, interventi di ricerca, annunci di servizio pubblico, centri di informazione in-app e pagine del Safety Center) che conducono gli utenti a fonti autorevoli disponibili in tutti gli Stati membri dell'UE e in 23 lingue ufficiali dell'UE (più, per gli utenti del SEE, norvegese e islandese). Inoltre, gestiamo campagne localizzate su argomenti specifici che impiegano tecniche di coinvolgimento diverse a seconda del paese in cui si trovano.



	materia e/o dello Stato membro coinvolto, ad esempio workshop di persona, campagne radiofoniche e giornalistiche.			
SLI 22.7.1 - azioni di applicazione delle politiche di cui sopra	N/D			

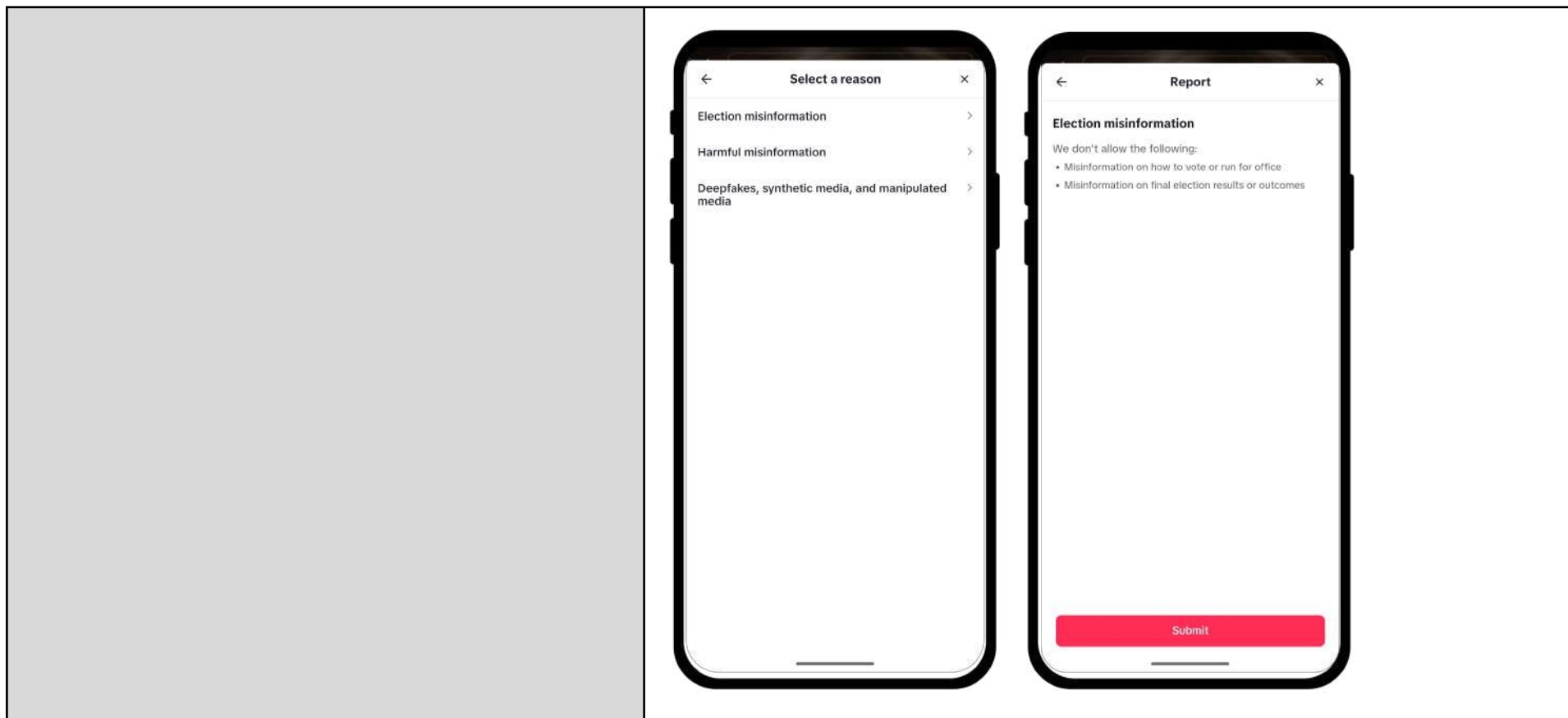
V. Responsabilizzare gli utenti

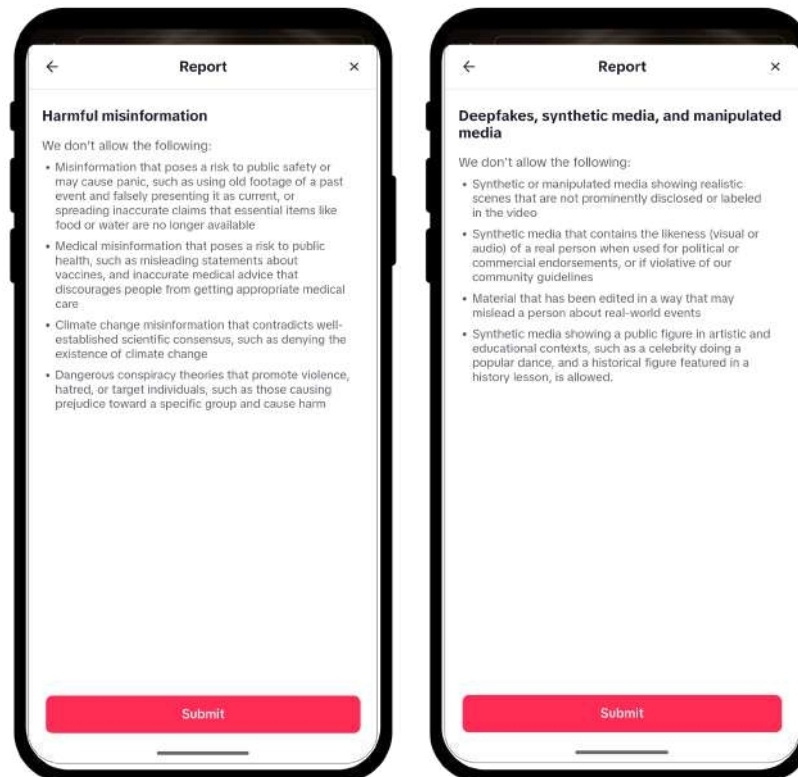
Impegno 23

I Firmatari rilevanti si impegnano a fornire agli utenti la funzionalità di segnalare le informazioni dannose false e/o fuorvianti che violano le politiche o i termini di servizio dei Firmatari.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve punti elenco].	<ul style="list-style-type: none"> In linea con i nostri requisiti DSA, abbiamo continuato a fornire alla nostra comunità nell'Unione Europea un canale di segnalazione dedicato, e un processo di appello per gli utenti che non sono d'accordo con l'esito, per "Segnalare contenuti illegali", consentendo agli utenti di segnalarci i contenuti che ritengono violino la legge.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.

Misura 23.1	
QRE 23.1.1	<p>Forniamo agli utenti modi semplici e intuitivi per segnalare/flaggare contenuti in-app per qualsiasi violazione dei nostri Termini di servizio o CG, compresa la disinformazione dannosa in ogni Stato membro dell'UE e in una lingua ufficiale dell'Unione europea.</p> <ul style="list-style-type: none">● Premendo a lungo (ad esempio, facendo clic per 3) sul contenuto del video e selezionando l'opzione "Segnala".● Selezionando il pulsante "Condividi" disponibile sul lato destro del contenuto del video e poi selezionando l'opzione "Segnala". <p>All'utente vengono quindi mostrate le categorie di motivi di segnalazione tra cui scegliere (che corrispondono ai danni che le nostre CG cercano di risolvere). Nel 2024, abbiamo aggiornato questa funzione per rendere più intuitive le categorie di "disinformazione" e consentire agli utenti di segnalare con una maggiore granularità. Abbiamo inoltre apportato delle modifiche per implementare un'opzione aggiuntiva che consenta agli utenti di segnalare contenuti illegali, in linea con i requisiti previsti dalla DSA.</p>





Gli utenti non hanno bisogno di accedere a un account sulla piattaforma per segnalare i contenuti e possono segnalare i contenuti video anche tramite il sito web di TikTok (facendo clic sul pulsante "Segnala", visualizzato in alto a destra di ogni video quando si passa il mouse su di esso) o tramite il nostro modulo web "Segnala contenuti inappropriati", disponibile nel nostro [Centro assistenza](#).

Siamo consapevoli che la disinformazione dannosa non si limita ai contenuti video e quindi gli utenti possono anche segnalare un commento, una ricerca suggerita, un hashtag, un suono o un account, sempre specificamente per disinformazione dannosa.



Misura 23.2	
<p>QRE 23.2.1 I firmatari interessati riferiranno sulle misure generali adottate per garantire l'integrità dei loro sistemi di segnalazione e di appello, evitando di divulgare informazioni che aiuterebbero gli aspiranti abusatori a trovare e sfruttare le vulnerabilità delle loro difese.</p>	<p>Sistema di reporting</p> <p>Per garantire l'integrità del nostro sistema di segnalazione, utilizziamo una combinazione di revisione automatica e moderazione umana.</p> <p>I video caricati su TikTok vengono inizialmente esaminati dalla nostra tecnologia di moderazione automatica, che mira a identificare i contenuti che violano le nostre Linee guida della comunità. Se viene riscontrata una potenziale violazione delle nostre CG, il sistema di revisione automatica la trasmette ai nostri team di moderazione per un'ulteriore revisione oppure, se c'è un alto grado di certezza che il contenuto violi le nostre CG, la rimuove automaticamente. La rimozione automatica viene applicata solo quando le violazioni sono come nel caso in cui il contenuto contenga nudità o riguardi la sicurezza dei giovani. Lavoriamo costantemente per migliorare la precisione della nostra tecnologia di moderazione automatica, in modo da poter rimuovere più efficacemente i contenuti violati su larga scala, riducendo al contempo il numero di rimozioni errate.</p> <p>Per favorire una revisione equa e coerente dei contenuti potenzialmente violativi, nei casi in cui le violazioni siano meno evidenti, i contenuti verranno passati ai nostri team di moderazione umana per un'ulteriore revisione.</p> <p>I moderatori umani possono prendere in considerazione ulteriori contesti e sfumature, che non sempre possono essere colti dalla tecnologia; nel contesto della disinformazione dannosa, ad esempio, i nostri moderatori hanno accesso a un archivio di affermazioni precedentemente verificate per prendere decisioni rapide e accurate e hanno accesso diretto ai nostri partner di fact-checking che aiutano a valutare l'accuratezza dei nuovi contenuti.</p> <p>Abbiamo cercato di rendere i nostri CG il più chiari e completi possibile e abbiamo messo in atto solidi processi di garanzia della qualità (che comprendono fasi come la revisione dei casi di moderazione, dei flussi, degli appelli e l'esecuzione di analisi delle cause profonde).</p> <p>Come parte dei nostri requisiti ai sensi della DSA, abbiamo introdotto un ulteriore segnalazione canale di per la nostra community nell'Unione Europea per "Segnalare contenuti illegali", che consente agli utenti di segnalarci i contenuti che ritengono violino la legge. TikTok esaminerà il contenuto alla luce delle nostre Linee guida della comunità e, qualora venga rilevata una violazione, il contenuto potrà essere rimosso a livello globale. Se non viene rimosso, il nostro team di moderazione dei contenuti illegali lo esaminerà ulteriormente per valutare se è illegale nella giurisdizione pertinente. In caso affermativo, l'accesso a tali contenuti sarà limitato in quel Paese.</p>



A coloro che segnalano contenuti sospetti di illegalità verrà comunicata la nostra decisione, anche nel caso in cui riteniamo che il contenuto non sia illegale. Gli utenti che non sono d'accordo possono [appellarsi](#) a tali decisioni utilizzando la procedura di appello.

Notiamo inoltre che, sebbene le segnalazioni degli utenti siano importanti, in TikTok poniamo una notevole enfasi sull'individuazione proattiva per rimuovere i contenuti violenti. Siamo orgogliosi del fatto che la stragrande maggioranza dei contenuti rimossi venga identificata in modo proattivo prima che ci venga segnalata.

Sistema di ricorsi.

Siamo trasparenti nei confronti degli utenti per quanto riguarda i ricorsi. Illustriamo [le opzioni](#) disponibili sia per l'utente che ha segnalato il contenuto sia per il creatore del contenuto interessato, qualora non siano d'accordo con la decisione presa.

L'integrità dei nostri sistemi di ricorso è rafforzata dal coinvolgimento dei nostri moderatori umani qualificati, che possono prendere in considerazione il contesto e le sfumature quando decidono se un contenuto è illegale o viola le nostre CG.

I nostri moderatori esaminano tutti i ricorsi sollevati in relazione a video rimossi, commenti rimossi e account bannati e li valutano in base alle nostre politiche. Per garantire la coerenza di questo processo e la sua integrità complessiva, abbiamo cercato di rendere le nostre politiche il più chiare e complete possibile e abbiamo messo in atto solidi processi di garanzia della qualità (che comprendono fasi quali la verifica dei ricorsi e l'esecuzione di analisi delle cause profonde).

Se gli utenti che hanno presentato un ricorso non sono ancora soddisfatti della nostra decisione, possono condividere il loro feedback con noi tramite il [modulo web](#) su TikTok.com. Prendiamo costantemente in considerazione il feedback degli utenti per individuare le aree di miglioramento, anche nell'ambito del processo di ricorso. Gli utenti possono inoltre godere di altri diritti legali in relazione alle decisioni prese da TikTok, come indicato [qui seguito](#) di .



V. Responsabilizzare gli utenti

Impegno 24

I Firmatari rilevanti si impegnano a informare gli utenti i cui contenuti o account sono stati oggetto di azioni di enforcement (contenuti/account etichettati, retrocessi o altrimenti applicati) intraprese sulla base della violazione delle politiche pertinenti a questa sezione (come indicato nella Misura 18.2), e a fornire loro la possibilità di fare ricorso contro l'azione di enforcement in questione e a gestire i reclami in modo tempestivo, diligente, trasparente e obiettivo e a revocare l'azione senza indebiti ritardi se il reclamo è ritenuto fondato.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve elenco].	<ul style="list-style-type: none"> Continuare a inviare notifiche agli utenti in seguito a interventi sull'account o sui contenuti di un utente, che includano una spiegazione chiara dell'azione intrapresa e un modo semplice per appellarsi alla decisione presa. Continuare a fornire ulteriore trasparenza agli utenti sui nostri processi di appello (qui).
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.
Misura 24.1	
QRE 24.1.1	Gli utenti di tutti gli Stati membri dell'UE vengono avvisati con una notifica in-app nella loro lingua locale, quando viene intrapresa la seguente azione:



	<ul style="list-style-type: none"> • la rimozione o comunque la limitazione dell'accesso ai loro contenuti; • un divieto di accesso al conto; • limitazione dell'accesso a una funzione (ad esempio LIVE); oppure • limitazione della loro capacità di monetizzare. <p>Tali notifiche vengono fornite in tempo quasi reale dopo l'esecuzione dell'azione (cioè generalmente entro alcuni secondi o al massimo alcuni minuti).</p> <p>Se abbiamo preso una di queste decisioni, una notifica nella casella di posta elettronica in-app indica la violazione ritenuta, insieme all'opzione per gli utenti di "non essere d'accordo" e presentare un ricorso. Gli utenti possono presentare ricorso entro 180 giorni dalla notifica della decisione che desiderano impugnare. Ulteriori informazioni, tra cui le modalità di ricorso, sono disponibili qui.</p> <p>Tutti i ricorsi sollevati saranno messi in coda per essere esaminati dai nostri moderatori umani specializzati, in da garantire che il contesto sia adeguatamente preso in considerazione nel prendere una decisione. Gli utenti possono monitorare lo stato e visualizzare i risultati del loro appello nella loro casella di posta elettronica in-app.</p> <p>Come già menzionato, i nostri utenti hanno la possibilità di condividere con noi un feedback se non sono d'accordo con il risultato del loro appello. Possono farlo utilizzando la funzione in-app che consente di "segnalare un problema". Prendiamo continuamente in considerazione il feedback degli utenti per individuare le aree di miglioramento del processo di ricorso.</p>			
SLI 24.1.1 - azioni esecutive	Metodologia di misurazione dei dati: <p>Il numero di appelli/ribaltamenti si basa sul Paese in cui è stato pubblicato il video oggetto dell'appello/ribaltamenti. Questi numeri si riferiscono solo alle nostre politiche di disinformazione, integrità civica ed elettorale, media modificati e AIGC.</p>			
	Numero di azioni impugnate	Metriche sui risultati dei ricorsi	Numero di azioni impugnate	
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Numero di appelli di video rimossi per violazione di politica di disinformazione	Numero di annullamenti di ricorsi per violazione di politica di disinformazione	Tasso di successo in appello dei video rimossi per violazione di politica di disinformazione	

Stati membri				
Austria	619	352	56.9%	
Belgio	863	673	78.0%	
Bulgaria	267	107	40.1%	
Croazia	140	84	60.0%	
Cipro	108	56	51.9%	
Repubblica Ceca	902	433	48.0%	
Danimarca	289	215	74.4%	
Estonia	140	113	80.7%	
Finlandia	202	156	77.2%	
Francia	7,461	6,189	83.0%	
Germania	13,540	72,68	53.7%	
Grecia	734	425	57.9%	
Ungheria	481	314	65.3%	
Irlanda	1,091	845	77.5%	
Italia	6,074	4,174	68.7%	

Lettonia	110	83	75.5%	
Lituania	105	87	82.9%	
Lussemburgo	17	16	94.1%	
Malta	38	37	97.4%	
Paesi Bassi	1,207	959	79.5%	
Polonia	4263	1,833	43.0%	
Portogallo	402	274	68.2%	
Romania	2,573	1,598	62.1%	
Slovacchia	401	175	43.6%	
Slovenia	267	153	57.3%	
Spagna	4,920	3,961	80.5%	
Svezia	943	544	57.7%	
Islanda	20	17	85.0%	
Liechtenstein	0	0	0.0%	
Norvegia	437	322	73.7%	
Totale UE	48,157	31,124	64.6%	

Totale SEE	48,614	31,463	64.7%	
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Numero di appelli di video rimossi per violazione della politica di integrità civica ed elettorale	Numero di ribaltamenti di ricorsi per violazione della politica di Integrità Civica ed Elettorale	Tasso di successo in appello dei video rimossi per violazione della politica di integrità civica ed elettorale	
Stati membri				
Austria	79	65	82.3%	
Belgio	149	123	82.6%	
Bulgaria	34	23	67.6%	
Croazia	7	7	100.0%	
Cipro	4	2	50.0%	
Repubblica Ceca	45	33	73.3%	
Danimarca	57	50	87.7%	
Estonia	3	3	100.0%	
Finlandia	12	9	75.0%	
Francia	331	301	90.9%	
Germania	1,302	1,053	80.9%	
Grecia	68	56	82.4%	

Ungheria	45	32	71.1%	
Irlanda	53	48	90.6%	
Italia	553	491	88.8%	
Lettonia	5	5	100.0%	
Lituania	13	11	84.6%	
Lussemburgo	7	4	57.1%	
Malta	3	3	100.0%	
Paesi Bassi	123	103	83.7%	
Polonia	177	125	70.6%	
Portogallo	79	56	70.9%	
Romania	524	403	76.9%	
Slovacchia	11	7	63.6%	
Slovenia	5	4	80.0%	
Spagna	239	202	84.5%	
Svezia	124	100	80.6%	
Islanda	2	0	0.0%	



Liechtenstein	0	0	0.0%	
Norvegia	44	35	79.5%	
Totale UE	4,052	3,319	81.9%	
Totale SEE	4,098	3,354	81.8%	
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio)	Numero di appelli di video rimossi per violazione di Synthetic e i media manipolati	Numero di ribaltamenti di ricorsi per violazione di norme sintetiche e Media manipolati	Tasso di successo in appello dei video rimossi per violazione di Synthetic e i media manipolati	
Stati membri				
Austria	9	8	88.9%	
Belgio	14	12	85.7%	
Bulgaria	5	2	40.0%	
Croazia	12	8	66.7%	
Cipro	4	3	75.0%	
Repubblica Ceca	31	12	38.7%	
Danimarca	18	16	88.9%	
Estonia	18	14	77.8%	
Finlandia	6	5	83.3%	

Francia	110	87	79.1%	
Germania	177	121	68.4%	
Grecia	12	9	75.0%	
Ungheria	22	15	68.2%	
Irlanda	17	15	88.2%	
Italia	57	48	84.2%	
Lettonia	7	3	42.9%	
Lituania	0	0	0.0%	
Lussemburgo	0	0	0.0%	
Malta	0	0	0.0%	
Paesi Bassi	19	14	73.7%	
Polonia	35	25	71.4%	
Portogallo	22	16	72.7%	
Romania	30	24	80.0%	
Slovacchia	5	4	80.0%	
Slovenia	7	2	28.6%	

Spagna	52	40	76.9%	
Svezia	15	7	46.7%	
Islanda	0	0	0.0%	
Liechtenstein	0	0	0.0%	
Norvegia	14	9	64.3%	
Totale UE	704	510	72.4%	
Totale SEE	718	519	72.3%	

V. Responsabilizzare gli utenti	
Impegno 25	
Al fine di aiutare gli utenti dei servizi di messaggistica privata a identificare la possibile disinformazione diffusa attraverso tali servizi, i Firmatari rilevanti che forniscono applicazioni di messaggistica si impegnano a continuare a costruire e implementare funzioni o iniziative che consentano agli utenti di pensare in modo critico alle informazioni che ricevono e li aiutino a determinare se sono accurate, senza alcun indebolimento della crittografia e con il dovuto riguardo alla protezione della privacy.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	Questo impegno non è applicabile in quanto TikTok non è un'app di messaggistica.



Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate mettere in atto nei prossimi 6 mesi?	Questo impegno non è applicabile in quanto TikTok non è un'app di messaggistica.
Misura 25.1	
QRE 25.1.1	Non impegnato. Questo impegno non è applicabile in quanto TikTok non è un'app di messaggistica.
SLI 25.1.1	N/D
	N/D
Dati	
Misura 25.2	
QRE 25.2.1	Non impegnato. Questo impegno non è applicabile in quanto TikTok non è un'app di messaggistica.
SLI 25.2.1 - utilizzo di strumenti selezionati	N/D
	N/D
Dati	



VI. Responsabilizzare la comunità di ricerca

Impegni 26-29

VI. Responsabilizzare la comunità di ricerca

Impegno 26

I firmatari interessati si impegnano a fornire l'accesso, laddove sicuro e praticabile, dati non personali e a dati pubblici anonimizzati, aggregati o resi manifesti, in modo continuo, in tempo reale o quasi reale, con accesso stabile e ricercabile, a fini di ricerca sulla disinformazione, attraverso mezzi automatizzati API o altre soluzioni tecniche aperte e accessibili che consentano l'analisi di tali dati.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]

Sì

Se sì, elencare queste misure di attuazione [breve elenco].

- Continuare a perfezionare il nuovo [Virtual Compute Environment \(VCE\)](#), lanciato nel maggio 2024:
 - Fornire l'accesso ai dati pubblici U18.
 - Aggiunta di nuovi punti dati (ad esempio, Hashtag Info) ed endpoint (ad esempio, Playlist Info). Vedere [Changelog](#).
 - Stabilire un nuovo processo di due diligence con un partner esterno per confermare l'ammissibilità dei richiedenti delle ONG.
- Continuare a sostenere la ricerca indipendente attraverso la Research API e migliorare l'accessibilità:
 - Aggiunta di tre nuovi endpoint per TikTok Shop, lanciato in Spagna e Irlanda nel dicembre 2024.
 - Rendere disponibili i wrapper di [Python e R](#) (linguaggi di programmazione) tramite GitHub.
- Abbiamo continuato a rendere disponibile in Europa l'API per i contenuti commerciali, al fine di rendere trasparente la pubblicità a pagamento, gli inserzionisti e altri contenuti commerciali su TikTok.
- Abbiamo continuato a offrire la nostra Commercial Content Library, un database di annunci UE consultabile pubblicamente con informazioni sugli annunci a pagamento e metadati sugli annunci, come la creatività pubblicitaria, le date cui l'annuncio è stato attivo, i principali parametri utilizzati per il targeting (ad esempio, età, sesso), il numero di persone a cui è stato servito l'annuncio.

Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]

No



Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.
Misura 26.1	
QRE 26.1.1	<p>Abbiamo un Centro per la trasparenza TikTok dedicato, disponibile in diverse lingue dell'UE, che ospita il nostro:</p> <ul style="list-style-type: none"> • Rapporti di trasparenza COPD, come parte dei nostri impegni verso il Codice, pubblichiamo ogni sei mesi un rapporto di trasparenza per fornire dati granulari per i Paesi UE/SEE sui nostri sforzi per combattere la disinformazione online. • I nostri TikTok Community Guidelines Enforcement Reports, che forniscono approfondimenti trimestrali proattivi sul volume e sulla natura dei contenuti e degli account rimossi dalla nostra piattaforma per violazione delle nostre Community Guidelines, dei Termini di servizio o delle Politiche pubblicitarie dal 2019. • Rapporti di trasparenza DSA, sulla base del nostro approccio proattivo alla trasparenza nei nostri rapporti trimestrali sull'applicazione delle linee guida della comunità di TikTok e dei nostri obblighi ai sensi del Digital Services Act ("DSA"), pubblichiamo un rapporto di trasparenza ogni sei mesi per fornire dati granulari per i Paesi dell'UE sulle nostre attività di moderazione dei contenuti. • Nel gennaio 2024, abbiamo iniziato a pubblicare rapporti sulle operazioni di influenza occulta trimestrali, fornendo dettagli più frequenti e dettagliati sulle operazioni di influenza occulta che abbiamo interrotto. <p>Nell'ambito del nostro impegno per la trasparenza normativa e la responsabilità, abbiamo lanciato l'European Online Safety Hub, che funge da "sportello unico" per la nostra comunità per saperne di più su come ci stiamo conformando alla DSA. L'Hub è attualmente disponibile in 22 lingue dell'UE e in almeno una lingua ufficiale di ciascuno degli Stati membri dell'UE. Il nostro sito web dedicato a TikTok per gli sviluppatori ospita le nostre API per gli strumenti di ricerca e per i contenuti commerciali (descritte di seguito).</p>
QRE 26.1.2	In questo rapporto H2 2024, TikTok ha condiviso più di 3.000 punti dati in 30 Paesi UE/SEE, con una leggera diminuzione rispetto ai 3.300 punti dati del nostro rapporto precedente. La riduzione è dovuta al fatto che non stiamo più riportando i dati specifici di COVID-19.



	<p>metriche in questo rapporto. Con la transizione della pandemia da una crisi globale acuta a un problema di salute pubblica più gestito, la rilevanza e l'utilità di queste metriche sono diminuite.</p> <p>Forniamo ai ricercatori l'accesso ai dati che sono pubblicamente disponibili sulla nostra piattaforma attraverso i nostri Strumenti di ricerca e attraverso la nostra API per i contenuti commerciali (dettagliati di seguito).</p> <p>Inoltre, nei nostri rapporti sull'applicazione delle linee guida della trimestrali comunità di TikTok, forniamo informazioni sulle azioni intraprese contro i contenuti e gli account che violano le nostre CG, i Termini di servizio o le Politiche pubblicitarie. Il report include una serie di visualizzazioni dei dati, progettate all'insegna della trasparenza e dell'accessibilità, anche per le persone con problemi di visione a colori.</p> <p>Ci impegniamo a fondo per integrare i dati completi del rapporto e fornire nuovi spunti di riflessione. Per esempio, di recente abbiamo condiviso i dati sull'applicazione dei commenti, compreso il numero di commenti rimossi e la percentuale di commenti pubblicati rimossi.</p> <p>Nell'ambito dei nostri continui sforzi per rendere più semplice lo studio della piattaforma TikTok, il report offre anche l'accesso a dati aggregati, compresi i dati di rimozione per categoria di policy, per i 50 mercati con i maggiori volumi di contenuti rimossi.</p>
SLI 26.1.1	
Dati	
Misura 26.2	
QRE 26.2.1	<p>(I) API di ricerca</p> <p>Per rendere più facile la ricerca indipendente sulla nostra piattaforma e portare trasparenza ai contenuti di TikTok, abbiamo creato un'API di ricerca che fornisce ai ricercatori negli Stati Uniti, nel SEE, nel Regno Unito e in Svizzera l'accesso ai dati pubblici sugli account e sui contenuti, compresi i commenti, le didascalie, i sottotitoli, il numero di commenti, le condivisioni, i "mi piace", i follower e le liste di follower e i preferiti che un video riceve sulla nostra piattaforma. Ulteriori informazioni sono disponibili qui. Consideriamo attentamente</p>



feedback dei ricercatori che hanno utilizzato l'API e continuano ad apportare miglioramenti, come l'aggiunta di ulteriori campi di dati, la semplificazione del processo di richiesta e la possibilità di collaborare attraverso Lab Access, che consente a un massimo di 10 ricercatori di lavorare insieme su un progetto di ricerca condiviso.

(II) Ambiente di calcolo virtuale (VCE)

Il VCE consente ai ricercatori non accademici senza scopo di lucro dell'UE di accedere ai dati pubblici di TikTok e di analizzarli, garantendo al contempo una solida protezione della sicurezza e della privacy. L'accesso e l'analisi dei dati pubblici può avvenire in due fasi:

1. Fase di test: Interrogare i dati utilizzando il kit di sviluppo software (SDK) di TikTok. Il VCE restituirà un campione casuale di dati in base alla query, limitato a 5.000 record al giorno.
2. Fase di esecuzione: Invia uno script da eseguire su tutti i dati pubblici. TikTok offre una potente funzionalità di ricerca che consente di impaginare i dati in incrementi fino a 100.000 record. TikTok esaminerà il file dei risultati per assicurarsi che l'output sia aggregato.

(III) Contenuto commerciale API

Come richiesto dalla DSA e per migliorare la trasparenza degli annunci pubblicitari presentati sulla nostra piattaforma, abbiamo creato un'[API per i contenuti commerciali](#) che include annunci, metadati degli annunci e degli inserzionisti e informazioni sul targeting. I ricercatori e i professionisti devono creare un account TikTok per gli sviluppatori e presentare una domanda per accedere all'API dei contenuti commerciali, che noi controlliamo per evitare che soggetti malintenzionati possano abusare di questi dati.

(IV) Libreria di contenuti commerciali

La Biblioteca dei contenuti commerciali è un database consultabile pubblicamente che contiene informazioni sugli annunci a pagamento e sui metadati degli annunci, come la creatività pubblicitaria, le date di pubblicazione dell'annuncio, i principali parametri utilizzati per il targeting (ad esempio, età, sesso), il numero di persone che hanno ricevuto l'annuncio e altro ancora. Include anche informazioni sui contenuti di natura commerciale etichettati con un'etichetta di partnership a pagamento o promozionale, come i contenuti che promuovono un marchio, un prodotto o un servizio, ma non sono annunci a pagamento.



QRE 26.2.2

(I) Ricerca API

Attraverso la nostra API di ricerca, i ricercatori accademici di istituzioni accademiche senza scopo di lucro negli Stati Uniti e in Europa, o di istituzioni, organizzazioni, associazioni o enti di ricerca senza scopo di lucro nell'UE, possono richiedere di studiare i dati pubblici sui contenuti e sugli account di TikTok. Questi dati pubblici includono commenti, didascalie, sottotitoli, numero di commenti, condivisioni, like, follower e liste di follower e preferiti che un video riceve sulla nostra piattaforma. Maggiori informazioni sono disponibili [qui](#).

(II) Ambiente di calcolo virtuale (VCE)

Attraverso il nostro VCE, i ricercatori non accademici senza scopo di lucro e i ricercatori accademici di istituzioni accademiche senza scopo di lucro dell'UE possono interrogare e analizzare i dati pubblici di TikTok. Per proteggere la sicurezza e la privacy dei nostri utenti, il VCE è progettato per garantire che i dati di TikTok siano elaborati entro parametri limitati. TikTok esamina i risultati solo per garantire che non vengano estratte dalla piattaforma informazioni individuali identificabili. Tutti i risultati aggregati saranno condivisi come link scaricabile all'e-mail del ricercatore primario approvato.

(III) Contenuto commerciale API

Attraverso la nostra API per i contenuti commerciali, i ricercatori e i professionisti qualificati, che possono trovarsi in qualsiasi Paese, possono richiedere dati pubblici sui contenuti commerciali, compresi gli annunci, i metadati degli annunci e degli inserzionisti e le informazioni sul targeting. Ad oggi, l'API per i contenuti commerciali include solo i dati dei Paesi dell'UE.

(IV) Libreria di contenuti commerciali

[La Biblioteca dei contenuti commerciali](#) di TikTok è un archivio di annunci e altri tipi di contenuti commerciali pubblicati per gli utenti solo nello Spazio economico europeo (SEE), in Svizzera e nel Regno Unito, ma è accessibile ai membri del pubblico situati in qualsiasi paese. Ogni annuncio e i relativi dettagli saranno disponibili nella libreria per un anno dall'ultima visualizzazione dell'annuncio da parte di un utente. Attraverso la Commercial Content Library, il pubblico può accedere alle informazioni sugli annunci a pagamento e ai metadati degli annunci, come la creatività pubblicitaria, le date di pubblicazione dell'annuncio, i principali parametri utilizzati per il targeting (ad esempio, età, sesso), il numero di persone a cui è stato servito l'annuncio e altro ancora. Include anche informazioni sui contenuti di natura commerciale etichettati con un'etichetta di partnership a pagamento o con un'etichetta promozionale, come i contenuti che promuovono un marchio, un prodotto o un servizio, ma non sono annunci a pagamento.



QRE 26.2.3	<p>Mettiamo a disposizione dei richiedenti informazioni dettagliate sui nostri strumenti di ricerca (API di ricerca e VCE) e sull'API dei contenuti commerciali, attraverso il nostro sito web dedicato a TikTok per gli sviluppatori, anche per quanto riguarda i dati resi disponibili e le modalità di richiesta di accesso. Nell'agosto 2024, abbiamo istituito un nuovo processo di due diligence con un fornitore esterno per confermare l'ammissibilità dei richiedenti delle ONG.</p> <p>Una volta approvata la domanda di accesso ai nostri strumenti di ricerca, forniamo istruzioni passo-passo per i ricercatori su come accedere ai dati della ricerca, come rispettare le fasi di sicurezza e come eseguire interrogazioni sui dati.</p> <p>Analogamente all'API per i contenuti commerciali, forniamo ai partecipanti informazioni dettagliate su come interrogare i dati degli annunci e recuperare i dati degli inserzionisti pubblici.</p>					
SLI 26.2.1	<p>Strumenti di ricerca, API per i contenuti commerciali e Biblioteca dei contenuti commerciali</p> <p>Durante il periodo di riferimento abbiamo ricevuto:</p> <ul style="list-style-type: none">● 148 domande di accesso agli strumenti di ricerca di TikTok (API di ricerca e VCE) da parte di ricercatori dell'UE e del SEE.● 61 applicazioni per accedere all'API dei contenuti commerciali di TikTok.					
	Numero di domande ricevute per gli strumenti di ricerca	Numero di domande accettate per gli strumenti di ricerca	Numero di domande respinte per gli strumenti di ricerca	Numero di richieste ricevute per l'API dei contenuti commerciali di TikTok	Numero di domande accettate per l'API dei contenuti commerciali di TikTok	Numero di richieste rifiutate per l'API per i contenuti commerciali di TikTok
	Austria	5	3	1	1	0
	Belgio	0	0	0	3	0
	Bulgaria	1	0	0	1	0
	Croazia	2	0	2	0	0
	Cipro	0	0	0	0	0



Repubblica Ceca	2	1	1	0	0	0
Danimarca	4	3	0	0	0	0
Estonia	0	0	0	0	0	0
Finlandia	1	2	0	3	2	1
Francia	16	4	6	11	8	3
Germania	50	12	16	14	11	3
Grecia	5	1	3	0	0	0
Ungheria	1	1	1	2	2	0
Irlanda	3	2	4	1	1	0
Italia	13	5	2	2	2	0
Lettonia	0	0	0	1	1	0
Lituania	0	0	0	2	2	0
Lussemburgo	0	0	0	0	0	0
Malta	0	0	0	0	0	0
Paesi Bassi	17	7	7	3	2	1
Polonia	3	0	1	3	2	1
Portogallo	2	2	0	2	2	0
Romania	6	1	1	0	0	0
Slovacchia	0	0	0	1	1	0

Slovenia	0	0	0	0	0	0
Spagna	11	2	4	6	4	2
Svezia	4	3	1	4	3	1
Islanda	0	0	0	0	0	0
Lichtenstein	0	0	0	0	0	0
Norvegia	2	2	0	1	1	0
Livello UE	146	49	50	60	48	12
Livello SEE	148	51	50	61	49	12
Misura 26.3						
QRE 26.3.1	Accogliamo con favore il feedback dei ricercatori sulle nostre API e disponiamo di un modulo di supporto dedicato in cui i ricercatori possono fornire un feedback sulla loro esperienza. Prima di estendere l'API di ricerca all'Europa, abbiamo agito in base al feedback dei ricercatori statunitensi, semplificando il processo di richiesta e consentendo una maggiore collaborazione attraverso Lab Access.					

VI. Responsabilizzare la comunità di ricerca

Impegno 27

I firmatari interessati si impegnano a fornire ai ricercatori controllati l'accesso ai dati necessari per intraprendere ricerche sulla disinformazione, sviluppando, finanziando e collaborando con un organismo indipendente e terzo che possa controllare i ricercatori e le proposte di ricerca.



In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	
Se sì, elencare queste misure di attuazione [breve elenco].	<ul style="list-style-type: none"> • Siamo membri del gruppo di lavoro EDMO per la creazione dell'Independent Intermediary Body (IIB) a supporto della ricerca sulle piattaforme digitali. • Abbiamo perfezionato la nostra procedura operativa standard (SOP) per l'accesso controllato dei ricercatori, al fine di garantire la conformità con le disposizioni della legge delegata sull'accesso ai dati per la ricerca. • Ha partecipato alla tavola rotonda tecnica della CE sull'accesso ai dati nel dicembre 2024. La tavola rotonda si è concentrata sulle misure tecniche e sulle migliori pratiche che potrebbero essere implementate per facilitare l'introduzione del meccanismo di accesso ai dati per i ricercatori controllati.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.
Misura 27.1	
QRE 27.1.1	Ci siamo impegnati con EDMO e abbiamo partecipato attivamente al gruppo di lavoro istituito per l'implementazione dell'Independent Intermediary Body (IIB). TikTok è stata anche una delle due piattaforme che hanno completato il pilota di accesso ai dati dell'EDMO, sperimentando il processo di condivisione dei dati con i ricercatori selezionati nell'ambito della DSA.
Misura 27.2	
QRE 27.2.1	Continuiamo a partecipare al gruppo di lavoro istituito per l'implementazione dell'Independent Intermediary Body (IIB).

Misura 27.3	
QRE 27.3.1	Abbiamo partecipato al gruppo di lavoro istituito per l'implementazione dell'Independent Intermediary Body (IIB) e siamo pronti a impegnarci per l'accesso dei ricercatori autorizzati. TikTok ha inoltre completato il progetto pilota di accesso ai dati con EDMO, sperimentando il processo di condivisione dei dati con i ricercatori autorizzati designati nell'ambito della DSA.
SLI 27.3.1 - progetti di ricerca vagliati da un ente terzo indipendente	N/D
	N/D
Dati	
Misura 27.4	
QRE 27.4.1	Abbiamo completato il progetto pilota di accesso ai dati con EDMO, sperimentando il processo di condivisione dei dati con i ricercatori selezionati nell'ambito della DSA.

VI. Responsabilizzare la comunità di ricerca	
Impegno 28	
I firmatari si impegnano a sostenere la ricerca in buona fede sulla disinformazione che coinvolge i loro servizi.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve elenco].	<ul style="list-style-type: none">● Continuare a perfezionare il nuovo Virtual Compute Environment (VCE), lanciato nel maggio 2024:<ul style="list-style-type: none">○ Fornire l'accesso ai dati pubblici U18.



	<ul style="list-style-type: none"> ○ Aggiunta di nuovi punti dati (ad esempio, Hashtag Info) ed endpoint (ad esempio, Playlist Info). Vedere Changelog. ○ Stabilire un nuovo processo di due diligence con un partner esterno per confermare la missibilità dei richiedenti delle ONG. ● Continuare a sostenere la ricerca indipendente attraverso la Research API e migliorare l'accessibilità: <ul style="list-style-type: none"> ○ Aggiunta di tre nuovi endpoint per TikTok Shop, lanciato in Spagna e Irlanda nel dicembre 2024. ○ Rendere disponibili i wrapper di Python e R (linguaggi di programmazione) tramite GitHub. ● Abbiamo continuato a rendere disponibile in Europa l'API per i contenuti commerciali, al fine di rendere trasparente la pubblicità a pagamento, gli inserzionisti e altri contenuti commerciali su TikTok. ● Abbiamo continuato a offrire la nostra Commercial Content Library, un database di annunci UE consultabile pubblicamente con informazioni sugli annunci a pagamento e metadati sugli annunci, come la creatività pubblicitaria, le date di diffusione dell'annuncio, i principali parametri utilizzati per il targeting (ad esempio, età, sesso), il numero di persone a cui è stato servito l'annuncio e altro ancora.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.
Misura 28.1	
QRE 28.1.1	<p>TikTok si impegna a facilitare la ricerca e a coinvolgere la comunità dei ricercatori. Come indicato sopra,</p> <p>TikTok si impegna a facilitare la ricerca attraverso i nostri Strumenti di ricerca, API per i contenuti commerciali e Libreria di contenuti commerciali, i cui dettagli completi sono disponibili sui nostri siti web TikTok per gli sviluppatori e Libreria di contenuti commerciali.</p>



Abbiamo molti team e persone che lavorano nei settori dei prodotti, delle politiche, della scienza dei dati, della divulgazione e dell'assistenza legale per facilitare la ricerca. Crediamo che la trasparenza e la responsabilità siano essenziali per promuovere la fiducia nella nostra comunità. Ci impegniamo a garantire la trasparenza nel modo in cui operiamo, moderiamo e raccomandiamo i contenuti, diamo potere agli utenti e proteggiamo la nostra piattaforma. Per questo motivo abbiamo aperto i nostri Transparency and Accountability Centers (TAC) globali per consentire agli ospiti invitati di vedere in prima persona il nostro lavoro per proteggere la sicurezza della piattaforma TikTok.

I nostri TAC sono situati a Dublino, Los Angeles, Singapore e Washington DC. Nell'ottobre 2024 apriremo [la](#) nostra nuova sede di Dublino nella nuova sede di TikTok. Il DUBTAC offre l'opportunità ad accademici, aziende, responsabili politici, legislatori, ricercatori e molti altri esperti provenienti dall'Europa e da tutto il mondo di vedere in prima persona come i team di TikTok svolgono il lavoro importantissimo di garantire la sicurezza, i dati e la privacy della nostra comunità. Durante il periodo di riferimento, il DUBTAC ha ospitato le seguenti visite:

- 22 visite esterne, tra cui 3 ONG/organismi industriali, 6 rappresentanti dei media e 2 creatori.
- Il 22 e 23 ottobre 2024 abbiamo accolto rispettivamente i membri del Consiglio consultivo per la sicurezza dell'Africa subsahariana (SSA) e del Consiglio consultivo per la sicurezza del Medio Oriente, Nord Africa e Turchia (MENAT). A queste visite ha partecipato il personale T&S di TikTok, che ha discusso su una serie di argomenti e scambiato opinioni.
- Nel novembre 2024, abbiamo accolto il Consiglio consultivo per la sicurezza dell'America Latina (LATAM).

Lavoriamo a stretto contatto con i nostri nove [Consigli consultivi](#) regionali, tra cui il Consiglio consultivo europeo per la sicurezza e il Consiglio consultivo statunitense per i contenuti, e con il nostro Consiglio consultivo globale per i giovani, che riunisce una serie di esperti indipendenti provenienti dal mondo accademico e dalla società civile, nonché le prospettive dei giovani. I membri del Consiglio consultivo forniscono competenze e consigli su questioni relative alla sicurezza degli utenti, alla politica dei contenuti e a questioni emergenti che riguardano TikTok e la nostra comunità, tra cui lo sviluppo della nostra [etichetta per i contenuti generati dall'intelligenza artificiale](#) e una recente campagna di sensibilizzazione sull'etichettatura dell'intelligenza artificiale e sull'AIGC potenzialmente fuorviante.

Oltre a questi sforzi, vi è una pletora di modi in cui ci impegniamo con comunità dei ricercatori nel corso del nostro lavoro.



Il nostro **team Outreach & Partnerships Management (OPM)** si dedica alla creazione di partnership e all'impegno regolare con gli stakeholder della società civile e gli esperti esterni, compresa la comunità accademica e di ricerca, per garantire che le loro prospettive influenzino la creazione delle nostre politiche, lo sviluppo delle caratteristiche, la mitigazione dei rischi e le strategie di sicurezza. Per esempio, abbiamo collaborato con esperti globali, tra cui numerosi accademici in Europa, per lo sviluppo del nostro politica sui media affiliati agli Stati, le politiche di disinformazione elettorale e le etichette dei contenuti generati dall'intelligenza artificiale. L'OPM svolge anche un ruolo importante nei nostri sforzi per contrastare la disinformazione, identificando, avviando e gestendo nuovi partner per il nostro programma di fact-checking. Nella seconda metà del 2024, abbiamo esteso la copertura del fact-checking a una serie di Paesi europei e candidati all'UE:

- Moldavia: AFP/Reuters
- Georgia: Fact Check Georgia
- Albania e Kosovo: Internews Kosova
- Serbia: Storie di punta
- Kazakistan: Reuters

Nel periodo che precede alcune elezioni, invitiamo esperti esterni locali/regionali adeguatamente qualificati, nell'ambito della nostra Election Speaker Series. Condividere la loro esperienza di mercato con i nostri team interni ci fornisce spunti per comprendere meglio le aree che potrebbero potenzialmente costituire una manipolazione elettorale e informa il nostro approccio alle elezioni imminenti.

Durante il periodo di riferimento, abbiamo organizzato 9 sessioni della Election Speaker Series, 7 negli Stati membri dell'UE e 2 in Georgia e Moldavia.

1. Francia: Agence France-Presse (AFP)
2. Germania: Agenzia di stampa tedesca (dpa)
3. Austria: Agenzia di stampa tedesca (dpa)
4. Lituania: Fatti logici
5. Romania: Cittadini divertenti
6. Irlanda: Fatti logici
7. Croazia: Faktograf
8. Georgia: FactCheck Georgia
9. Moldavia: Stop a Fals!

I team e il personale di TikTok partecipano regolarmente anche a **eventi incentrati sulla ricerca**. Alla fine di giugno 2024, abbiamo inviato una delegazione di 12 persone al [GlobalFact11](#) a Sarajevo, in Bosnia e



	<p>Erzegovina. TikTok è stato uno dei tre sponsor di alto livello del GlobalFact11, il più grande raduno dell'International Fact-Checking Network per i verificatori professionisti. Oltre alla sponsorizzazione, abbiamo partecipato a una presentazione sul palco principale rispondendo alle domande sulla nostra strategia di disinformazione e sulle partnership con i verificatori professionisti. Abbiamo anche avuto incontri con molti partner esistenti e potenzialmente nuovi, nonché con l'EFCSN. Nel settembre 2024, abbiamo inviato una delegazione di 16 persone alla Trust & Safety Research Conference dell'Università di Stanford. In ottobre abbiamo sponsorizzato, partecipato e presentato a Disinfo24 la conferenza annuale del DisinfoLab dell'UE a Riga. Nel dicembre 2024 abbiamo ospitato un webinar per circa 20 ONG francesi sul Virtual Compute Environment.</p> <p>Oltre all'opportunità di condividere il contesto del nostro approccio, gli interessi di ricerca e le opportunità di collaborazione, questi eventi ci permettono di apprendere l'importante lavoro svolto dalla comunità di ricerca su vari argomenti, tra cui gli aspetti legati alla disinformazione dannosa.</p>
Misura 28.2	
QRE 28.2.1	<p>Abbiamo un sito web dedicato a TikTok per gli sviluppatori che ospita i nostri strumenti di ricerca e le API per i contenuti commerciali.</p> <p>Con l'API di ricerca, i ricercatori possono accedere a:</p> <ul style="list-style-type: none"> • I dati dell'account pubblico, come i profili degli utenti, i follower e gli elenchi di follower, i video che hanno ricevuto un "mi piace", i video inseriti negli appunti e i video ripostati. • Dati sui contenuti pubblici, come commenti, didascalie, sottotitoli e numero di commenti, condivisioni e like ricevuti da un video. <p>Attraverso il VCE, i ricercatori qualificati non accademici e senza scopo di lucro nell'UE possono accedere e analizzare i dati pubblici di TikTok, compresi i dati pubblici U18, in un ambiente sicuro e soggetto a rigorosi controlli di sicurezza.</p> <p>Le nostre API relative ai contenuti commerciali comprendono annunci, metadati di annunci e inserzionisti e informazioni sul targeting. Queste API consentiranno al pubblico e ai ricercatori di eseguire ricerche personalizzate - basate sul nome dell'inserzionista o su parole chiave - sugli annunci e su altri dati di contenuto commerciale archiviati nel repository della Commercial Content Library. La Biblioteca è un database ricercabile con</p>



	informazioni sugli annunci a pagamento e sui metadati degli annunci, come la creatività pubblicitaria, le date di pubblicazione dell'annuncio, i principali parametri utilizzati per il targeting (ad esempio, età, sesso), il numero di persone a cui è stato proposto l'annuncio e altro ancora.
Misura 28.3	
QRE 28.3.1	I dati che mettiamo a disposizione e i criteri di applicazione per i nostri strumenti di ricerca (API di ricerca e VCE) e API di contenuti commerciali sono indipendenti dall'argomento di ricerca e sono chiaramente indicati nel nostro sito web dedicato a TikTok per gli sviluppatori . Nell'agosto 2024 abbiamo istituito un nuovo processo di due diligence con un fornitore esterno per confermare l'ammissibilità dei richiedenti delle ONG.
Misura 28.4	
QRE 28.4.1	Ci impegniamo a mantenere un impegno costante con l'EDMO e con la più ampia comunità di ricerca.

VI. Responsabilizzare la comunità di ricerca	
Impegno 29	
I firmatari si impegnano a condurre ricerche basate su una metodologia trasparente e su standard etici, nonché a condividere i set di dati, i risultati delle ricerche e le metodologie con il pubblico interessato.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No



Se sì, elencare queste misure di attuazione [breve punti elenco].	Questo impegno riguarda gli Organismi di ricerca.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Questo impegno riguarda gli Organismi di ricerca.
Misura 29.1	
QRE 29.1.1	Non impegnato.
QRE 29.1.2	Non impegnato.
QRE 29.1.3	Non impegnato.
SLI 29.1.1 - portata degli stakeholder o dei cittadini informati sui risultati dei progetti di ricerca	N/D
	N/D
Dati	
Misura 29.2	
QRE 29.2.1	Non impegnato.
QRE 29.2.2	Non impegnato.

QRE 29.2.3	N/D
SLI 29.2.1	N/D
	Non impegnato.
Dati	
Misura 29.3	
QRE 29.3.1	Non impegnato.
SLI 29.3.1 - portata degli stakeholder o dei cittadini informati sui risultati dei progetti di ricerca	N/D
	N/D
Dati	



VII. Responsabilizzare la comunità f act-checfiing

Impegni 30 - 33

VII. Potenziamento della comunità di fact-checking

Impegno 30

I firmatari interessati si impegnano a stabilire un quadro per una cooperazione trasparente, strutturata, aperta, finanziariamente sostenibile e non discriminatoria tra loro e la comunità di fact-checking dell'UE per quanto riguarda le risorse e il supporto messi a disposizione dei fact-checkers.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve elenco].	<ul style="list-style-type: none"> • Sono stati assunti due nuovi partner per il fact-checking in Europa: <ol style="list-style-type: none"> 1. Albania e Kosovo: Internews Kosova 2. Georgia: Fact Check Georgia. • In H2 abbiamo anche ampliato la nostra copertura di fact-checking ad altri Paesi europei e candidati all'UE con partner di fact-checking esistenti: <ul style="list-style-type: none"> ○ Moldavia: AFP/Reuters ○ Serbia: Storie di punta • Abbiamo continuato a espandere il nostro archivio di fact-checking per garantire che i nostri team e sistemi sfruttino l'intera portata delle informazioni che i nostri partner di fact-checking hanno inviato a TikTok (indipendentemente dalla lingua originale del contenuto). • Abbiamo continuato a condurre sessioni di feedback con i nostri partner per migliorare ulteriormente l'efficienza del programma di fact-checking. • Continuare a partecipare al gruppo di lavoro nell'ambito del Codice per la creazione di un archivio di fact-checking esterno.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	



Misura 30.1	
QRE 30.1.1	<p>In Europa, collaboriamo con 14 partner di fact-checking che forniscono una copertura di fact-checking in 23 lingue del SEE, tra cui almeno una lingua ufficiale di ogni Stato membro dell'UE, oltre a georgiano, russo, turco e ucraino. I nostri partner dispongono di team di fact-checkers che rivedono e verificano i contenuti riportati. I nostri moderatori utilizzano questo feedback indipendente per prendere provvedimenti e, se del caso, rimuovere o rendere non ammissibili alla raccomandazione i contenuti falsi o fuorvianti o etichettare quelli non verificati.</p> <p>Gli accordi con i nostri partner sono standardizzati, ovvero si basano sui nostri modelli di contratti di servizi standard e sono coerenti con gli standard e le condizioni comuni. Abbiamo rivisto e aggiornato i nostri contratti standard modello nell'ambito del processo di rinnovo annuale dei contratti.</p> <p>I termini degli accordi descrivono:</p> <ul style="list-style-type: none"> • Il servizio che il partner di fact-checking fornirà, ovvero che il suo team di fact checker esamini, valuti e valuti i contenuti video caricati nella coda di fact-checking. • I risultati attesi, ad esempio, sono che i verificatori di fatti consigliano se il contenuto può essere o contenere disinformazione e lo valutano utilizzando le nostre categorie di classificazione. • Un'opzione per accettare che i nostri partner verificatori di fatti forniscano regolarmente rapporti scritti sulle tendenze di disinformazione individuate. • Un'opzione per ricevere in modo proattivo segnalazioni di potenziali disinformazioni dannose da parte dei nostri partner. • Le lingue in cui forniranno i servizi di fact-checking. • La possibilità di richiedere una copertura temporanea per altre lingue o un supporto su progetti aggiuntivi ad hoc. • Tutti gli altri termini chiave, compresi i termini e le commissioni applicabili e le modalità di pagamento.
QRE 30.1.2	<p>Attualmente abbiamo 14 partner di fact-checking accreditati dall'IFCN in tutta l'UE, il SEE e l'Europa:</p> <ol style="list-style-type: none"> 1. Agence France-Presse (AFP) 2. dpa Agenzia di stampa tedesca



3. Demagogo
4. Facta
5. Verifica dei fatti in Georgia
6. Faktograf
7. Internews Kosova
8. Storie di protagonisti
9. Fatti logici
10. Newtral
11. Poligrafo
12. Reuters
13. Feedback scientifico
14. Teyit

Questi partner forniscono una copertura di fact-checking in 23 lingue ufficiali dell'AEA, tra cui almeno una lingua ufficiale di ogni Stato membro dell'UE, oltre a georgiano, russo, turco e ucraino.

Possiamo e abbiamo stipulato accordi temporanei con questi partner di fact-checking per fornire una copertura linguistica aggiuntiva nell'UE durante eventi ad alto rischio come le elezioni o una crisi in corso. Ad esempio, abbiamo temporaneamente esteso la nostra copertura di fact-checking al maltese per le elezioni parlamentari del giugno 2024.

Al di fuori del nostro programma di fact-checking, collaboriamo anche con organizzazioni di fact-checking per sviluppare una serie di campagne di alfabetizzazione mediatica. Ad esempio, durante il periodo in esame, abbiamo collaborato con diverse organizzazioni di fact-checking per **campagne di alfabetizzazione mediatica specifiche per le elezioni**:

- Austria: Deutsche Presse-Agentur (dpa)
- Croazia: Faktograf
- Francia: Agence France-Presse (AFP)
- Georgia: Fact Check Georgia
- Germania (elezioni regionali): Deutsche Presse-Agentur dpa)
- Germania (elezioni federali): Deutsche Presse-Agentur dpa)
- Irlanda: Il giornale
- Moldavia: StopFals!
- Romania: Cittadini divertenti



	<p>Abbiamo inoltre lanciato due nuove campagne generali di alfabetizzazione ai media e di capacità di pensiero critico nell'UE e due nei Paesi candidati all'UE, in collaborazione con i nostri partner per il fact-checking e l'alfabetizzazione ai media:</p> <ul style="list-style-type: none">○ Francia: Agence France-Presse (AFP)○ Portogallo: Polígrafo○ Georgia: Fact Check Georgia○ Moldavia: StopFals! <p>A livello globale, abbiamo 22 partner di fact-checking accreditati dall'IFCN. Lavoriamo continuamente per espandere la nostra rete di fact-checking e teniamo aggiornati gli utenti qui.</p>
QRE 30.1.3	<p>Abbiamo una copertura di fact-checking in 23 lingue ufficiali del SEE: Bulgaro, croato, ceco, danese, olandese, inglese, estone, finlandese, francese, tedesco, greco, ungherese, italiano, lettone, lituano, norvegese, polacco, portoghese, rumeno, slovacco, sloveno, spagnolo e svedese.</p> <p>Abbiamo una copertura per il fact-checking in diverse altre lingue europee o che interessano gli utenti europei, tra cui il georgiano, il russo, il turco e l'ucraino e possiamo richiedere un supporto aggiuntivo in azero, armeno e bielorusso.</p> <p>Per quanto riguarda le iniziative di fact-checking a livello globale, attualmente copriamo più di 50 lingue e valutiamo i contenuti in oltre 100 Paesi, migliorando così l'integrità complessiva del servizio e avvantaggiando gli utenti europei.</p> <p>Al fine di scalare efficacemente il feedback fornito dai nostri fact-checker a livello globale, abbiamo implementato le misure elencate di seguito.</p> <ul style="list-style-type: none">● Archivio di fact-checking. Abbiamo creato un archivio di affermazioni precedentemente verificate per aiutare i moderatori della disinformazione a prendere decisioni rapide e accurate.● Rapporti sulle tendenze. I nostri partner di fact-checking possono fornirci regolarmente rapporti che identificano le tendenze generali della disinformazione osservate sulla nostra piattaforma e nel settore in generale, comprese le nuove tendenze del settore o del mercato, gli eventi o gli argomenti che hanno generato una particolare disinformazione.● Rilevamento proattivo da parte dei nostri partner di fact-checking. I nostri partner di fact-checking sono autorizzati a individuare proattivamente i contenuti che possono costituire disinformazione dannosa su



la nostra piattaforma e suggerire importanti informazioni errate che circolano online e che potrebbero beneficiare di una verifica.

- **Linee guida per il fact-checking.** Creiamo linee guida e promemoria sui trending topic per i nostri moderatori sulla base di precedenti valutazioni di fact-checking. In questo modo i nostri team di moderazione sfruttano le intuizioni dei nostri partner di fact-checking e aiutano i nostri moderatori a prendere decisioni rapide e accurate sui contenuti segnalati, indipendentemente dalla lingua in cui è stata fatta l'affermazione originale.
- **Serie di interventi sulle elezioni.** Per promuovere ulteriormente l'integrità elettorale e informare il nostro approccio alle elezioni UE a livello nazionale, abbiamo invitato esperti esterni locali e regionali adeguatamente qualificati a condividere le loro intuizioni e la loro esperienza di mercato con i nostri team interni. Il nostro recente Election Speaker Series ha visto le presentazioni delle seguenti organizzazioni:
 - Francia: Agence France-Presse (AFP)
 - Germania: Agenzia di stampa tedesca (dpa)
 - Austria: Agenzia di stampa tedesca (dpa)
 - Lituania: Fatti logici
 - Romania: Cittadini divertenti
 - Irlanda: Fatti logici
 - Croazia: Faktograf
 - Georgia: FactCheck Georgia
 - Moldavia: Stop a Fals!

I membri dei team di moderazione ricevono una formazione specializzata sulla disinformazione e hanno accesso diretto a questi strumenti e misure, il che consente loro di intervenire con maggiore precisione sui contenuti violati in tutta Europa e nel mondo.

Stiamo continuando a investire nella costruzione e nel miglioramento di modelli che consentano di utilizzare i risultati di queste misure per aggiornare i modelli di apprendimento automatico che utilizziamo per il rilevamento proattivo, imparando, nel tempo, a cercare contenuti simili che possono essere richiamati in modo proattivo nel nostro sistema di moderazione per la revisione. Utilizziamo una serie di strumenti automatizzati, tra cui:

- Modelli di computer vision, che aiutano a rilevare gli oggetti in modo da poter determinare se il contenuto contiene probabilmente materiale che viola le nostre politiche.
- Gli elenchi di parole chiave e i modelli vengono utilizzati per esaminare i contenuti testuali e audio al fine di individuare il materiale che viola le nostre politiche. Collaboriamo con diversi esperti esterni, tra cui i nostri partner di fact-checking, per informare i nostri elenchi di parole chiave.
- Laddove abbiamo precedentemente individuato contenuti che violano le nostre politiche, utilizziamo tecnologie di de-duplicazione e di hashing che ci permettono di riconoscere copie o quasi copie.

	<p>copie di tali contenuti per impedire un'ulteriore redistribuzione dei contenuti violati sulla nostra piattaforma.</p> <ul style="list-style-type: none">• Abbiamo lanciato la capacità di leggere le Content Credentials che allegano metadati ai contenuti, che possiamo utilizzare per etichettare automaticamente i contenuti generati dall'IA che hanno origine su altre piattaforme principali. <p>Continuare a sfruttare la produzione di fact-checking in questo modo ci permette di aumentare ulteriormente l'impatto positivo del nostro programma di fact checking.</p>
SLI 30.1.1 - Stati membri e lingue oggetto di accordi con le organizzazioni di fact-checking	
Austria	Implementazione della copertura di fact-checking
Belgio	Implementazione della copertura di fact-checking
Bulgaria	Implementazione della copertura di fact-checking
Croazia	Implementazione della copertura di fact-checking
Cipro	Implementazione della copertura di fact-checking
Repubblica Ceca	Implementazione della copertura di fact-checking
Danimarca	Implementazione della copertura di fact-checking
Estonia	Implementazione della copertura di fact-checking
Finlandia	Implementazione della copertura di fact-checking
Francia	Implementazione della copertura di fact-checking



Germania	Implementazione della copertura di fact-checking
Grecia	Implementazione della copertura di fact-checking
Ungheria	Implementazione della copertura di fact-checking
Irlanda	Implementazione della copertura di fact-checking
Italia	Implementazione della copertura di fact-checking
Lettonia	Implementazione della copertura di fact-checking
Lituania	
Lussemburgo	Implementazione della copertura di fact-checking
Malta	Nessuna copertura permanente per il fact-checking. Possiamo e abbiamo stipulato accordi temporanei con partner di fact-checking per fornire una copertura linguistica aggiuntiva nell'UE in occasione di eventi ad alto rischio come elezioni o crisi in corso. Ad esempio, abbiamo temporaneamente esteso la nostra copertura di fact-checking al maltese per le elezioni parlamentari del giugno 2024. Nel frattempo, il nostro repository per il fact-checking e altre iniziative vanno a beneficio di tutti gli utenti europei e garantiscono l'integrità complessiva della nostra piattaforma.
Paesi Bassi	Implementazione della copertura di fact-checking
Polonia	Implementazione della copertura di fact-checking
Portogallo	Implementazione della copertura di fact-checking
Romania	Implementazione della copertura di fact-checking
Slovacchia	Implementazione della copertura di fact-checking



Slovenia	Implementazione della copertura di fact-checking
Spagna	Implementazione della copertura di fact-checking
Svezia	Implementazione della copertura di fact-checking
Islanda	Nessuna copertura permanente per il fact-checking. Possiamo, e abbiamo già stipulato, accordi temporanei con partner di fact-checking per fornire una copertura linguistica aggiuntiva nell'UE durante eventi ad alto rischio come le elezioni o una crisi in atto. Nel frattempo, il nostro repository di fact-checking e altre iniziative vanno a beneficio di tutti gli utenti europei e garantiscono l'integrità complessiva della nostra piattaforma.
Liechtenstein	Implementazione della copertura di fact-checking
Norvegia	Implementazione della copertura di fact-checking
Totale UE	22 lingue
Totale SEE	23 lingue

Misura 30.2	
QRE 30.2.1	<p>Gli accordi con i nostri partner per il fact-checking sono standardizzati, ovvero basano sul nostro modello di master service agreement e sono coerenti con gli standard e le condizioni comuni. Questi accordi, come tutti i nostri contratti, devono rispettare gli standard etici e professionali che stabiliamo internamente, comprese le disposizioni anticorruzione.</p> <p>I nostri partner vengono compensati in modo equo e trasparente in base al lavoro svolto, utilizzando tariffe standardizzate. I nostri partner di fact-checking ci fatturano mensilmente in base al lavoro svolto.</p> <p>Tutti i nostri partner di fact-checking sono organizzazioni indipendenti, certificate dall'organizzazione apartitica IFCN. I nostri accordi con loro stabiliscono esplicitamente che i fact-checkers sono contraenti indipendenti e non esclusivi di TikTok che mantengono l'indipendenza editoriale in relazione a</p>

	<p>il fact-checking, e che i servizi saranno eseguiti in modo professionale e in linea con i più alti standard del settore. I nostri processi sono inoltre impostati in modo da garantire indipendenza dei partner di fact-checking. I nostri partner accedono ai contenuti segnalati attraverso un cruscotto esclusivo a loro uso e forniscono la loro valutazione dell'accuratezza dei contenuti fornendo un rating. I fact-checkers lo fanno in modo indipendente da noi e la loro revisione può includere la chiamata delle fonti, la consultazione di dati pubblici o l'autenticazione di video e immagini.</p> <p>Per favorire la trasparenza e l'apertura nei confronti dei nostri partner di fact-checking, li incontriamo regolarmente e forniamo loro i dati relativi al loro feedback, oltre a condurre sondaggi con loro.</p>
QRE 30.2.2	Ci incontriamo regolarmente con i nostri partner di fact-checking e abbiamo un dialogo continuo con loro su come la nostra partnership sta funzionando e si sta evolvendo. Facciamo sondaggi con i nostri partner di fact-checking per incoraggiare il feedback su ciò che stiamo facendo bene e su come potremmo migliorare.
QRE 30.2.3	Questa disposizione non riguarda TikTok, ma solo le organizzazioni di fact-checking.
Misura 30.3	
QRE 30.3.1	<p>Poiché i nostri partner di fact-checking sono tutti accreditati presso l'IFCN, i nostri partner di fact-checking sono già impegnati in una collaborazione transfrontaliera informale attraverso questa rete.</p> <p>Inoltre, continuiamo a collaborare con i nostri partner per capire come possiamo agevolare un'ulteriore collaborazione attraverso sessioni di feedback individuali con i partner.</p>
Misura 30.4	
QRE 30.4.1	Su queste e altre questioni intratteniamo un dialogo regolare con l'EDMO e l'EFCSN. Continuiamo ad essere aperti a discutere e ad esplorare quali ulteriori progressi possono essere fatti su questi punti.

VII. Potenziamento della comunità di fact-checking

Impegno 31

I firmatari si impegnano a integrare, mettere in mostra o comunque utilizzare in modo coerente il lavoro dei verificatori nei servizi, nei processi e nei contenuti delle loro piattaforme, con una copertura completa di tutti gli Stati membri e di tutte le lingue.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]

Sì

Se sì, elencare queste misure di attuazione [brevi punti elenco].

- Sono stati assunti due nuovi partner per il fact-checking in Europa:
 - 1) Albania e Kosovo: Internews Kosova
 - 2) Georgia: Fact Check Georgia.

, abbiamo esteso la nostra copertura di fact-checking ad altri Paesi dell'Europa allargata e ai Paesi candidati all'UE con partner di fact-checking già esistenti:

- Moldavia: AFP/Reuters
- Serbia: Storie di punta
- Abbiamo continuato a espandere il nostro archivio di fact-checking per garantire che i nostri team e sistemi sfruttino l'intera portata degli approfondimenti che i nostri partner di fact-checking hanno inviato a TikTok (indipendentemente dalla lingua originale dei contenuti).
- Abbiamo continuato a condurre sessioni di feedback con i nostri partner per migliorare ulteriormente l'efficienza del programma di fact-checking.
- Continuare a partecipare al gruppo di lavoro nell'ambito del Codice per la creazione di un archivio di fact-checking esterno.

Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]

No



<p>Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?</p>	<p>Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.</p>
<p>Misura 31.1</p>	
<p>Misura 31.2</p>	
<p>QRE 31.1.1</p>	<p>Per noi la disinformazione dannosa è diversa da altri problemi di contenuto. Il contesto e il fact-checking sono fondamentali per applicare in modo coerente e accurato le nostre politiche di disinformazione dannosa, ed è per questo che collaboriamo con 14 partner di fact-checking in Europa, che coprono 23 lingue del SEE. Sebbene utilizziamo modelli di apprendimento automatico per aiutare a rilevare la potenziale disinformazione, il nostro approccio prevede che i membri del nostro team di moderazione dei contenuti, che ricevono una formazione specializzata sulla disinformazione, valutino, confermino e agiscano sulla disinformazione dannosa. Questo include l'accesso diretto ai nostri partner di fact-checking che ci aiutano a valutare l'accuratezza dei contenuti. Il nostro</p> <p>I partner di fact-checking sono coinvolti nel nostro processo di moderazione in tre modi:</p> <p>(i) un moderatore invia un video ai fact-checkers perché lo esaminino e valutino l'accuratezza del contenuto fornendo una valutazione. I fact-checkers lo faranno in modo indipendente da noi e la loro revisione può includere la chiamata delle fonti, la consultazione di dati pubblici, l'autenticazione di video e immagini e altro ancora.</p> <p>Mentre i contenuti sono sottoposti a fact-checking o quando non possono essere verificati, possiamo ridurre la distribuzione in modo che meno persone li vedano. I fact-checker non intervengono direttamente sui contenuti. Il moderatore prenderà invece in considerazione il feedback dei fact-checkers sull'accuratezza del contenuto quando deciderà se il contenuto viola le nostre CG e quali azioni intraprendere.</p> <p>(ii) contribuendo al nostro database globale di affermazioni precedentemente verificate per aiutare i nostri moderatori della disinformazione a prendere decisioni.</p> <p>(iii) un programma di rilevamento proattivo con i nostri fact-checker che segnalano le affermazioni nuove e in evoluzione che vedono sulla nostra piattaforma. Ciò consente ai nostri moderatori di valutare rapidamente queste affermazioni e di rimuovere le violazioni.</p>



	Inoltre, utilizziamo il feedback del fact-checking per fornire agli utenti un contesto aggiuntivo su determinati contenuti. Come già accennato, quando i nostri partner di fact-checking concludono che il fact-check è inconcludente o che il contenuto non può essere confermato (il che è particolarmente comune durante gli eventi in corso o le crisi), informiamo gli spettatori tramite un banner quando identifichiamo un video con contenuti non verificati, nel tentativo di sensibilizzare gli utenti sulla credibilità del contenuto e di ridurre la condivisione. Il video può anche diventare non idoneo a essere raccomandato nel feed For You di chiunque, per limitare la diffusione di informazioni potenzialmente fuorvianti.			
SLI 31.1.1 - utilizzo di verifiche dei fatti	Metodologia di misurazione dei dati: Il numero di video verificati si basa sul numero di video che sono stati esaminati da uno dei nostri partner di fact-checking nel territorio di riferimento.			
	N. di articoli fact-checked pubblicati			
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Numero di video verificati (attività)			
Stati membri				
Austria	64			
Belgio	141			
Bulgaria	398			
Croazia	137			
Cipro	8			
Repubblica Ceca	200			
Danimarca	175			



Estonia	84			
Finlandia	61			
Francia	1,045			
Germania	837			
Grecia	64			
Ungheria	144			
Irlanda	91			
Italia	202			
Lettonia	40			
Lituania	41			
Lussemburgo	2			
Malta	0			
Paesi Bassi	52			
Polonia	622			
Portogallo	59			
Romania	669			
Slovacchia	138			
Slovenia	22			
Spagna	407			



Svezia	158			
Islanda	1			
Liechtenstein	0			
Norvegia	227			
Totale UE	5,861			
Totale SEE	6,089			

SLI 31.1.2 - impatto delle azioni intraprese	Metodologia di misurazione dei dati: Il numero di video rimossi come risultato di una valutazione di fact-checking e il numero di video rimossi a causa di linee guida politiche, tendenze note di disinformazione e il nostro archivio basato sulla conoscenza si basa sul paese in cui il video è stato pubblicato. Queste metriche corrispondono al numero di rimozioni nell'ambito della politica di disinformazione, poiché tutta la sua applicazione si basa sulle linee guida della politica, sulle tendenze note della disinformazione e sull'archivio basato sulla conoscenza.		
	N/D		
Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Numero di video rimossi a seguito di una valutazione di fact checking	Numero di video rimossi a causa di linee guida, tendenze di disinformazione note e archivio di conoscenze.	
Stati membri			
Austria	8	2,888	
Belgio	26	3,902	



Bulgaria	62	1,568	
Croazia	31	789	
Cipro	0	511	
Repubblica Ceca	42	2,720	
Danimarca	12	1,455	
Estonia	2	319	
Finlandia	4	984	
Francia	166	44,354	
Germania	177	50,335	
Grecia	8	4,198	
Ungheria	21	2,002	
Irlanda	13	4,676	
Italia	40	21,035	
Lettonia	1	694	
Lituania	0	520	
Lussemburgo	0	279	
Malta	0	168	
Paesi Bassi	13	5,422	
Polonia	152	13,028	

Portogallo	10	2,629	
Romania	168	14,103	
Slovacchia	42	1,365	
Slovenia	3	574	
Spagna	55	22,581	
Svezia	15	3,489	
Islanda	1	122	
Liechtenstein	0	35	
Norvegia	14	1,798	
Totale UE	1,071	206,588	
Totale SEE	1,086	208,543	

SLI 31.1.3 - Informazioni quantitative utilizzate per la contestualizzazione degli SLI 31.1.1 / 31.1.2	Metodologia di misurazione dei dati: La metrica che abbiamo fornito mostra la percentuale di video che sono stati rimossi in seguito alla valutazione del fact checking, rispetto al numero totale di video rimossi per violazione della nostra politica di disinformazione dannosa.

Elenco delle azioni per stati membri e lingue (vedi tabella di esempio sopra)	Video rimossi a seguito di una valutazione di fact checking come percentuale del numero totale di video rimossi per violazione della politica di disinformazione dannosa
Austria	0.2%
Belgio	0.5%
Bulgaria	3.6%
Croazia	1.0%
Cipro	0.0%
Repubblica Ceca	1.3%
Danimarca	0.8%
Estonia	0.6%
Finlandia	0.4%
Francia	0.4%
Germania	0.3%
Grecia	0.2%
Ungheria	0.3%
Irlanda	0.0%
Italia	0.2%
Lettonia	0.0%
Lituania	0.0%



Lussemburgo	0.0%
Malta	0.0%
Paesi Bassi	0.1%
Polonia	1.0%
Portogallo	0.3%
Romania	0.9%
Slovacchia	2.8%
Slovenia	0.0%
Spagna	0.2%
Svezia	0.4%
Islanda	0.0%
Liechtenstein	0.0%
Norvegia	0.6%
Totale UE	0.4%
Totale SEE	0.4%

Misura 31.3	
QRE 31.3.1	Partecipiamo al sottogruppo creato a questo scopo. Abbiamo collaborato attivamente con tutti i firmatari per definire i risultati e le tempistiche per la creazione di un archivio esterno per il fact-checking, come previsto da questa misura.

Misura 31.4	
QRE 31.4.1	Ci impegniamo a partecipare attivamente alla discussione sulle soluzioni tecnologiche per facilitare l'uso efficiente dell'archivio comune attraverso le piattaforme e le lingue.

VII. Potenziamento della comunità di fact-checking	
Impegno 32	
I firmatari si impegnano a fornire ai verificatori di fatti un accesso rapido e, ove possibile, automatizzato alle informazioni pertinenti per a massimizzare la qualità e l'impatto del fact-checking, come definito in un quadro da progettare in coordinamento con l'EDMO e un organismo eletto che rappresenti le organizzazioni europee indipendenti di fact-checking.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve punti elenco].	Abbiamo continuato a esplorare modi per migliorare la condivisione dei dati in relazione al nostro progetto pilota di condivisione dei dati di applicazione con i nostri partner di fact-checking sulle affermazioni cui hanno fornito un feedback.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto COPD.

Misura 32.1			
Misura 32.2			
<div>QRE 32.1.1</div> <div><div></div></div>	<div>I nostri partner che si occupano di fact-checking accedono ai contenuti segnalati per la revisione attraverso un cruscotto reso disponibile a loro uso esclusivo. Il cruscotto mostra ai nostri fact-checker alcune informazioni quantitative sui servizi che forniscono, tra cui il numero di video in coda per la valutazione in qualsiasi , nonché il tempo impiegato per la revisione. I fact-checker possono anche utilizzare il dashboard per vedere la valutazione che hanno applicato ai video che hanno precedentemente valutato.</div> <div>In futuro, intendiamo continuare a esplorare modi per aumentare ulteriormente la qualità dei nostri metodi di condivisione dei dati con i partner di fact-checking.</div>		
SLI 32.1.1 - utilizzo delle interfacce e di altri strumenti	<div>Metodologia di misurazione dei dati:</div> <div>N/A. Come indicato nella risposta alla domanda 32.1.1, il cruscotto che attualmente condividiamo con i nostri partner contiene solo informazioni quantitative di alto livello sui servizi che forniscono, tra cui il numero di video in coda per la valutazione in qualsiasi momento e il tempo impiegato per la revisione. Stiamo continuando a lavorare con i nostri partner di fact checking per capire quali altri dati sarebbe utile condividere con loro.</div>		
Dati			
Misura 32.3			
QRE 32.3.1	<div>Continuiamo a partecipare alla task force composta dai rappresentanti dei firmatari interessati che è stata istituita a questo scopo. Nel frattempo, ci stiamo anche impegnando attivamente con EDMO su questo impegno.</div>		

VII. Potenziamento della comunità di fact-checking

Impegno 33

I firmatari rilevanti (cioè le organizzazioni di fact-checking) si impegnano a operare sulla base di rigorose regole etiche e di trasparenza e a tutelare la propria indipendenza.

In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	Questo impegno e questa misura riguardano le organizzazioni di fact checking.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Questo impegno e questa misura riguardano le organizzazioni di fact checking.
Misura 33.1	
QRE 33.1.1	Non impegnato. Questo impegno e questa misura riguardano le organizzazioni di Fact-Checking.
SLI 33.1.1 - numero di fact-checker europei certificati IFCN	N/D



VIII. Transparency Centre Impegni 34 - 36

VIII. Centro per la trasparenza	
<div>Impegno 34</div> <div>Per garantire la trasparenza e la responsabilità nell'attuazione del presente Codice, i firmatari rilevanti si impegnano a creare e mantenere un sito web comune del Centro per la trasparenza, disponibile al pubblico.</div>	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve punti elenco].	Abbiamo partecipato attivamente al gruppo di lavoro che quest'anno ha lanciato con successo il Centro comune per la trasparenza. Da settembre 2023 ricopriamo il ruolo di co-presidente del gruppo di lavoro sulla trasparenza. Da gennaio 2024, abbiamo sostenuto la transizione della manutenzione e dello sviluppo del sito web dal precedente fornitore terzo al firmatario del Codice, Vost.eu.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	No
Misura 34.1	
Misura 34.2	
Misura 34.3	

Misura 34.4	
Misura 34,5	

VIII. Centro per la trasparenza	
Impegno 35	
I firmatari si impegnano a garantire che il Centro per la trasparenza contenga tutte le informazioni rilevanti relative all'attuazione degli Impegni e delle Misure del Codice e che tali informazioni siano presentate in modo facilmente comprensibile, per servizio, e siano facilmente ricercabili.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve punti elenco].	Grazie alla nostra partecipazione al gruppo di lavoro del Centro per la trasparenza, abbiamo fatto in modo che il Centro per la trasparenza permetta al pubblico di accedere alle informazioni generali sul Codice e alle relazioni sottostanti (e che il Centro sia navigabile sia per impegno che per firmatario).
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	no
Misura 35.1	



Misura 35.2	
Misura 35.3	
Misura 35.4	
Misura 35,5	
Misura 35.6	

VIII. Centro per la trasparenza	
Impegno 36	
I firmatari si impegnano ad aggiornare le informazioni pertinenti contenute nel Centro per la trasparenza in tempestivo e completo.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Si/No]	No
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Si/No]	No

Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	
Misura 36.1	
Misura 36.2	
Misura 36.3	
QRE 36.1.1 (per gli impegni 34-36)	Il Centro per la trasparenza è stato lanciato con successo nel febbraio 2023. Continuiamo a caricare il nostro rapporto secondo le scadenze approvate.
QRE 36.1.2 (per gli impegni 34-36)	La gestione del sito web del Centro per la trasparenza è stata trasferita completamente comunità dei firmatari del Codice, con VOST Europe che ha assunto il ruolo di sviluppatore.
SLI 36.1.1	Abbiamo collaborato con il fornitore per sviluppare metriche rilevanti per questa SLI.
Dati	Tra il 1° luglio 2024 e il 31 dicembre 2024, il Centro comune per la trasparenza è stato visitato da 20.255 visitatori unici. I rapporti dei firmatari sono stati scaricati 5.626 volte da 1.275 visitatori unici. In particolare, il precedente rapporto di TikTok sulla BPCO è stato scaricato 302 volte da 135 visitatori.



IX. Impegno permanente della Tasfi-Forza 37

IX. Task-Force permanente	
Impegno 37	
I firmatari si impegnano a partecipare alla Task-force permanente. La Task-force comprende i firmatari del Codice e i rappresentanti di EDMO ed ERGA. È presieduta dalla Commissione europea e comprende rappresentanti del Servizio europeo per l'azione esterna (SEAE). La Task-force può anche invitare esperti di rilievo come osservatori per supportare il suo lavoro. Le decisioni della task force sono prese per consenso.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	Abbiamo partecipato in modo significativo alle Task Force / Plenarie e a tutti i gruppi di lavoro.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D
Misura 37.1	
Misura 37.2	
Misura 37.3	

Misura 37.4	
Misura 37,5	
Misura 37.6	
QRE 37.6.1	<p>Ci siamo impegnati in modo significativo nella Task-force e in tutti i suoi gruppi di lavoro, partecipando alle riunioni e a tutte le discussioni pertinenti, in particolare per quanto riguarda il processo di conversione del Codice e lo sviluppo/attivazione dell'RRS per le elezioni.</p> <p>Continueremo a partecipare alla task force e a tutti i suoi gruppi e sottogruppi di lavoro.</p>



X. Monitoraggio del Codice Impegni 38 - 44



X. Monitoraggio del Codice	
Impegno 38	
I firmatari si impegnano a dedicare adeguate risorse finanziarie e umane e a mettere in atto processi interni appropriati per garantire l'attuazione dei loro impegni ai sensi del Codice.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.
Misura 38.1	

QRE 38.1.1	<p>TikTok ha assegnato al Codice il livello di priorità più alto, il che significa che abbiamo, e continueremo ad avere, risorse adeguate per rispettare i nostri impegni e la nostra conformità.</p> <p>Data l'ampiezza del Codice e degli impegni in esso contenuti, il nostro lavoro si estende a diversi team, tra cui Trust and Safety, Legal, Monetisation Integrity, Product e Public Policy. I team sono dislocati in tutto il mondo per garantire il rispetto degli impegni e della conformità, con un notevole coinvolgimento della nostra Trust and Safety Leadership.</p> <p>In tutta l' Europa, abbiamo migliaia di professionisti della fiducia e della sicurezza che si dedicano a mantenere sicura la nostra piattaforma. Riconosciamo anche l'importanza della conoscenza e dell'esperienza locale quando lavoriamo per garantire la sicurezza online dei nostri utenti. Adottiamo un approccio simile alle nostre partnership con terzi.</p>
------------	--

X. Monitoraggio del Codice	
<p>Impegno 39</p> <p>I firmatari si impegnano a fornire alla Commissione europea, entro un mese dalla fine del periodo di attuazione (6 mesi dopo la firma del presente Codice), i rapporti di riferimento indicati nel preambolo.</p>	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	No
Se sì, elencare queste misure di attuazione [breve punti elenco].	Abbiamo condiviso il nostro rapporto di riferimento con la Commissione nel rispetto dei tempi concordati.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No

Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D

X. Monitoraggio del Codice	
Impegno 40	
I firmatari si impegnano a fornire relazioni periodiche sugli Indicatori del livello di servizio (SLI) e sugli Elementi di rendicontazione qualitativa (QRE). I rapporti e i dati forniti dovrebbero consentire una valutazione approfondita del grado di attuazione degli Impegni e delle Misure del Codice da parte di ciascun Firmatario, a livello di servizio e di Stato membro.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [breve punti elenco].	Nella presente relazione abbiamo riportato gli SLI e i QRE relativi agli impegni sottoscritti.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.



Misura 40.1	
Misura 40.2	
Misura 40.3	
Misura 40.4	
Misura 40,5	
Misura 40.6	

X. Monitoraggio del Codice	
<p>Impegno 41</p> <p>I firmatari si impegnano a lavorare all'interno della task force per sviluppare gli indicatori strutturali e a pubblicarne una prima serie entro 9 mesi dalla firma del presente Codice, nonché a pubblicare una misurazione iniziale insieme al primo rapporto completo. Per raggiungere questo obiettivo, i firmatari si impegnano a sostenerne l'attuazione, compresa la verifica e l'adattamento della serie iniziale di indicatori strutturali concordati nel presente Codice. Ciò al fine di valutare l'efficacia del Codice nel ridurre la diffusione della disinformazione online per ciascuno dei Firmatari interessati e per l'intero ecosistema online nell'UE e a livello di Stati membri. I firmatari collaboreranno con i soggetti interessati a questo proposito, tra cui ERGA e EDMO.</p>	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì



Se sì, elencare queste misure di attuazione [breve punti elenco].	<ul style="list-style-type: none">Abbiamo partecipato attivamente al gruppo di lavoro dedicato allo sviluppo degli indicatori strutturali.Abbiamo sostenuto la pubblicazione della seconda analisi degli indicatori strutturali, ampliando la copertura di 4 mercati e aumentando la dimensione del campione nel settembre 2024.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	N/D
Misura 41.1	
Misura 41.2	
Misura 41.3	

X. Monitoraggio del Codice

Impegno 42

I firmatari interessati si impegnano a fornire, in situazioni particolari come elezioni o crisi, su richiesta della Commissione europea, informazioni e dati proporzionati e appropriati, compresi rapporti specifici ad hoc e capitoli specifici nell'ambito del monitoraggio regolare, in conformità con il sistema di risposta rapida istituito dalla task force.



In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Si/No]	Si
Se sì, elencare queste misure di attuazione [breve punti elenco].	Abbiamo partecipato attivamente al gruppo di lavoro sulla risposta alle crisi, che ha portato all'implementazione del sistema di risposta rapida sviluppato/attivato per le elezioni. Insieme al presente rapporto abbiamo pubblicato anche rapporti di crisi specifici sulla guerra in Ucraina, sul conflitto tra Israele e Hamas e rapporti sulle elezioni lampo in Francia e sulle elezioni presidenziali in Romania.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Si/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.

X. Monitoraggio del Codice	
Impegno 43	
I firmatari si impegnano a produrre rapporti e a fornire dati seguendo i modelli di rapporto armonizzati e la metodologia perfezionata per il rapporto e la divulgazione dei dati, come concordato nella task force.	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Si/No]	Si

Se sì, elencare queste misure di attuazione [brevi punti elenco].	<ul style="list-style-type: none">• Ha partecipato al gruppo di lavoro per il monitoraggio e la rendicontazione.• Relazione di trasparenza pubblicata nel settembre 2024.
Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.

X. Monitoraggio del Codice	
<div>Impegno 44</div> <p>I Firmatari rilevanti che sono fornitori di Piattaforme online di grandi dimensioni si impegnano, nel tentativo di allinearsi con la DSA, ad essere sottoposti ad audit a proprie spese, per verificare il rispetto degli impegni assunti ai sensi del presente Codice. Gli audit devono essere eseguiti da organizzazioni indipendenti e senza conflitti di interesse con il fornitore della piattaforma online di grandi dimensioni in questione. Tali organizzazioni devono avere una comprovata esperienza nel settore della disinformazione, competenze e capacità tecniche adeguate e una comprovata obiettività ed etica professionale, basata in particolare sull'adesione agli standard e alle linee guida di revisione.</p>	
In linea con questo impegno, avete adottato nuove misure di attuazione (ad esempio, modifiche ai vostri termini di servizio, nuovi strumenti, nuove politiche, ecc)? [Sì/No]	Sì
Se sì, elencare queste misure di attuazione [brevi punti elenco].	Attuazione del programma annuale di audit dei DSA.



Prevedete di mettere in atto ulteriori misure di attuazione nei prossimi 6 mesi per migliorare sostanzialmente la maturità dell'attuazione di questo impegno? [Sì/No]	No
Se sì, quali ulteriori misure di implementazione pensate di mettere in atto nei prossimi 6 mesi?	Stiamo continuamente rivedendo e migliorando i nostri strumenti e processi per combattere la disinformazione e l'informazione scorretta e riferiremo di ogni ulteriore sviluppo nel prossimo rapporto sulla BPCO.

Relazioni sulla risposta del servizio durante una crisi

Guerra di aggressione della Russia all'Ucraina

Minacce osservate o previste al momento della segnalazione: [limite di caratteri suggerito 2000 caratteri].

La guerra di aggressione della Russia contro l'Ucraina (di seguito "**guerra in Ucraina**") continua a metterci alla prova con un ambiente incredibilmente complesso e in continua evoluzione. Per TikTok la sicurezza delle persone e della comunità è di fondamentale importanza e lavoriamo costantemente per salvaguardare la nostra piattaforma.

Di seguito riportiamo alcune delle principali minacce che abbiamo osservato sulla nostra piattaforma in relazione alla diffusione di disinformazione dannosa e di operazioni di influenza occulta (**CIO**) relative alla guerra in Ucraina nel periodo di riferimento. Continuiamo a impegnarci per impedire la condivisione di tali contenuti in questo contesto.

(I) Diffusione di disinformazione dannosa

Osserviamo e agiamo laddove appropriato in base alle nostre politiche. Dall'inizio della guerra in Ucraina abbiamo assistito ad affermazioni false o non confermate su attacchi ed eventi specifici, sullo sviluppo o sull'uso di armi, sul coinvolgimento di determinati Paesi nel conflitto e su dichiarazioni relative a specifiche attività militari, come la direzione del movimento delle truppe. Abbiamo anche assistito a casi di riproposizione di filmati in fuorviante, tra cui quelli tratti da videogiochi o filmati non correlati di eventi passati presentati come attuali.

TikTok adotta un approccio dinamico per comprendere e rimuovere le storie fuorvianti. Quando affrontiamo la disinformazione dannosa, applichiamo le nostre [politiche di Autenticità e Integrità e \(politiche I&A\)](#) nelle nostre [Linee guida della community](#) e prendiamo provvedimenti contro i contenuti offensivi sulla nostra piattaforma. Ai nostri team di moderazione vengono fornite indicazioni e linee guida dettagliate per la moderazione della disinformazione legata alle crisi, utilizzando le nostre politiche sulla disinformazione, tra cui fornitura di banche di casi di disinformazione dannosa a supporto del loro lavoro di moderazione.

(II) CIO

Lavoriamo continuamente per individuare e interrompere le operazioni di influenza occulta che tentano di affermarsi su TikTok e di minare l'integrità della nostra piattaforma. Le nostre politiche di I&A vietano i tentativi di influenzare l'opinione pubblica e di ingannare i nostri sistemi o gli utenti sull'identità, l'origine, la posizione approssimativa, la popolarità o lo scopo generale. Abbiamo team specificamente addestrati che sono in allerta per indagare e individuare i CIO sulla nostra piattaforma. Banniamo gli account che tentano di mettere in atto tali comportamenti, interveniamo su altri che valutiamo come parte della rete e li segnaliamo regolarmente nel nostro centro di trasparenza. Quando banniamo questi account, vengono rimossi anche i contenuti da essi pubblicati.

Nel periodo compreso tra luglio e dicembre 2024, siamo intervenuti per rimuovere un totale di 9 reti (per un totale di 20.002 account) che sono state ritenute coinvolte in tentativi coordinati di influenzare l'opinione pubblica sulla guerra in Ucraina e di ingannare i singoli, la nostra comunità o i nostri sistemi. Pubblichiamo tutte le reti CIO che identifichiamo e rimuoviamo nel nostro nuovo rapporto dedicato alla trasparenza CIO.

CIO continuerà a evolversi in risposta al nostro rilevamento e le reti potrebbero tentare di ristabilire una presenza sulla nostra piattaforma.



Per contrastare queste minacce emergenti e rimanere al passo con l'evoluzione delle sfide, disponiamo di team di esperti che si concentrano interamente sull'individuazione, l'investigazione e l'interruzione delle operazioni di influenza occulta.

Mitigazioni in atto al momento della segnalazione: [limite di caratteri suggerito: 2000 caratteri].

Vogliamo garantire che TikTok sia una fonte di informazioni affidabili e sicure e riconosciamo l'aumento del rischio e dell'impatto di informazioni fuorvianti in un periodo di crisi come quello della guerra in Ucraina.

(I) Investimento nel nostro programma di fact-checking

Utilizziamo un approccio stratificato per rilevare la disinformazione dannosa che viola le nostre CG.

La stretta collaborazione con i nostri partner di fact-checking è una parte fondamentale del nostro approccio per contrastare la disinformazione dannosa sulla nostra piattaforma. Il nostro programma di fact-checking prevede una copertura in russo, ucraino e bielorusso. Collaboriamo anche con Reuters, che si dedica al fact-checking dei contenuti in russo e ucraino.

Collaboriamo anche con alcuni dei nostri partner di fact-checking per essere avvisati in anticipo delle narrazioni emergenti di disinformazione, il che ha facilitato le risposte proattive contro le tendenze più dannose e ha assicurato che i nostri team di moderazione abbiano indicazioni aggiornate.

(II) L'interruzione dei CIO

Come indicato in precedenza, l'interruzione delle reti CIO è stata per noi un'attività altamente prioritaria nel contesto della crisi e abbiamo pubblicato un elenco delle reti che abbiamo interrotto nel periodo in questione all'interno del nostro ultimo rapporto di trasparenza pubblicato [qui](#).

Tra luglio e dicembre 2024, siamo intervenuti per rimuovere un totale di 9 reti (per un totale di 20.002 account) che si sono rivelate coinvolte in tentativi coordinati di influenzare l'opinione pubblica sulla guerra in Ucraina e di ingannare individui, la nostra comunità o i nostri sistemi. Pubblichiamo tutte le reti CIO che identifichiamo e rimuoviamo nel nostro rapporto dedicato alla trasparenza CIO.

Contrastare le operazioni di influenza è uno sforzo che coinvolge tutto il settore, in parte perché queste operazioni spesso diffondono la loro attività su più piattaforme. Ci consultiamo regolarmente con esperti terzi, tra cui i nostri [Consigli consultivi per i contenuti e la sicurezza](#) globali, le cui indicazioni ci aiutano a migliorare le nostre politiche e a comprendere il contesto regionale.

(III) Limitazione dell'accesso ai contenuti per i media affiliati allo Stato

Sin dalle prime fasi della guerra, abbiamo limitato l'accesso ai contenuti di una serie di entità mediatiche affiliate allo Stato russo nell'UE, in Islanda e nel Liechtenstein. La nostra politica sui media affiliati allo Stato viene utilizzata per aiutare gli utenti a comprendere il contesto di determinati contenuti e per aiutarli a valutare i contenuti che consumano sulla nostra piattaforma. Da allora sono state applicate etichette ai contenuti pubblicati dagli account affiliati allo Stato di tali entità in Russia, Ucraina e Bielorussia.

Continuiamo a individuare ed etichettare gli account dei media controllati dallo Stato in conformità con la nostra politica di etichettatura dei media controllati dallo Stato a livello globale.



(IV) Mitigare il rischio di monetizzazione della disinformazione dannosa

La pubblicità politica è vietata sulla nostra piattaforma da molti anni, ma come ulteriore misura di mitigazione del rischio di monetizzazione a causa della guerra in Ucraina, vietiamo agli inserzionisti con sede in Russia di rivolgersi ai mercati dell'UE. Abbiamo anche sospeso TikTok nelle regioni di Donetsk e Luhansk, rimuovendo i video Livestream provenienti dall'Ucraina dal feed For You degli utenti situati nell'UE. Inoltre, la possibilità di aggiungere nuovi contenuti video o video Livestream alla piattaforma in Russia rimane sospesa.

(V) Avviare campagne di alfabetizzazione mediatica a livello locale.

Le misure proattive volte a migliorare l'alfabetizzazione digitale dei nostri utenti sono fondamentali e riconosciamo l'importanza di aumentare il rilievo delle informazioni autorevoli. Abbiamo organizzato tredici campagne di alfabetizzazione mediatica a livello locale per affrontare la disinformazione relativa alla guerra in Ucraina in Austria e Bulgaria, Repubblica Ceca, Croazia, Estonia, Germania, Ungheria, Lettonia, Lituania, Polonia, Romania, Slovacchia e Slovenia, in stretta collaborazione con i nostri partner. partner di fact-checking. Gli utenti che cercano parole chiave relative alla guerra in Ucraina vengono indirizzati a suggerimenti, preparati in collaborazione con i nostri partner di fact-checking, per aiutare gli utenti a identificare la disinformazione e a prevenirne la diffusione sulla piattaforma. Abbiamo inoltre stretto una partnership con un'organizzazione locale di fact-checking ucraina, VoxCheck, con l'obiettivo di lanciare una campagna permanente di alfabetizzazione mediatica in Ucraina.

[Nota: i firmatari sono invitati a fornire informazioni pertinenti alla loro particolare risposta alle minacce e alle sfide osservate sui loro servizi.

Essi assicurano che le informazioni riportate di seguito forniscano un resoconto accurato e completo delle loro azioni pertinenti. Poiché le risposte operative alle situazioni di crisi/elezioni possono variare da un servizio all'altro, l'assenza di informazioni non deve essere considerata a priori una carenza nel modo in cui un particolare servizio ha risposto. Le metriche di impatto sono accurate al meglio delle capacità dei firmatari di misurarle].

Politiche e termini e condizioni

Illustrare eventuali modifiche alle vostre politiche

Politica	Modifiche (come nuove politiche introdotte, modifiche, adattamento dell'ambito o dell'implementazione)	Motivazione
Nessun aggiornamento rilevante nel periodo di riferimento.	N/D In caso di crisi, teniamo sotto controllo le nostre politiche e assicuriamo la presenza di team di moderazione.	Le nostre politiche di I&A sono la nostra prima linea di difesa per combattere la disinformazione dannosa e i comportamenti ingannevoli sulla nostra piattaforma. Le nostre linee guida per la comunità chiariscono ai nostri utenti quali contenuti rimuoviamo o rendiamo non ammissibili per feed For You quando rappresentano un rischio di danno per i nostri utenti o per il pubblico in generale. I nostri team di moderazione ricevono indicazioni e linee guida dettagliate per la moderazione di contenuti dannosi per la guerra.



	hanno una guida supplementare.	<p>disinformazione utilizzando le politiche esistenti.</p> <p>All'interno del nostro dipartimento Fiducia e Sicurezza abbiamo team specializzati che si occupano delle politiche di I&A, anche nelle aree dei prodotti e delle politiche. I nostri esperti in materia di I&A tengono costantemente sotto controllo queste politiche e collaborano con partner ed esperti esterni per capire se sono necessari aggiornamenti.</p> <p>Quando si situazioni come la guerra in Ucraina, i nostri team si adoperano per garantire lo sviluppo di una guida appropriata che consenta di applicare in modo efficace le politiche di I&A ai contenuti relativi alla crisi in questione (in questo caso, la guerra). Ciò include l'emanazione di linee guida e indicazioni dettagliate sulle politiche, compresa la fornitura di casi di disinformazione dannosa a supporto dei team di moderazione.</p>
Controllo dei posizionamenti degli annunci		
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.		
Prevenzione dell'uso improprio delle nostre funzioni di monetizzazione <i>(Impegno 1, Misura 1.1)</i>	Descrizione dell'intervento Dall'inizio della guerra in Ucraina, abbiamo sospeso il livestreaming e i nuovi contenuti in Russia e abbiamo assunto una posizione rigorosa per non consentire la monetizzazione in Russia. Dal marzo 2022 agli inserzionisti con sede in Russia è stato vietato il targeting degli annunci in uscita verso i mercati dell'UE. TikTok rimane sospeso nelle regioni di Donetsk e Luhansk. Adottiamo anche misure per rispettare altre sanzioni applicabili, come il geoblocco dei contenuti di persone sanzionate identificate provenienti dall'UE e dal Regno Unito.	
	Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili. N/D	
Moderazione dei contenuti <i>(Impegno 2, Misura 2.2)</i>	Descrizione dell'intervento Utilizziamo una combinazione di moderazione automatica e umana per identificare i contenuti che violano le nostre politiche pubblicitarie. Appliciamo le nostre rigorose politiche sugli annunci e disponiamo di team di esperti che si occupano di indagare e rispondere a qualsiasi tentativo di elusione.	



	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Il nostro impegno nelle pratiche di moderazione degli annunci contribuisce a garantire che annunci che violano le nostre politiche vengano rifiutati o rimossi, sia nel contesto della guerra in Ucraina che, più in generale, sulla nostra piattaforma.</p>
Pubblicità politica	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
<p>Divieto di pubblicità politica (Impegno 4)</p>	<p>Descrizione dell'intervento</p> <p>Nel tentativo di preservare l'integrità della piattaforma e la sicurezza delle persone che la utilizzano, gli account appartenenti a politici o partiti politici non possono fare pubblicità o guadagnare su TikTok.</p> <p>Non consentiamo la promozione politica a pagamento, la pubblicità politica o la raccolta di fondi da parte di politici e partiti politici (per se stessi o per altri). La nostra politica sugli annunci politici include sia gli annunci tradizionali a pagamento che i creatori che ricevono un compenso per sostenere o contrastare un candidato alla carica. Questa è una politica di lunga data di TikTok dal 2019. Non consentiamo contenuti a pagamento o di marca che promuovano o si oppongano a un candidato, a un leader attuale, a un partito o gruppo politico o a una questione a livello federale, statale o locale, compresi gli annunci legati alle elezioni.</p> <p>Siamo lieti che il Regolamento UE 2024/900 sulla trasparenza e l'orientamento della pubblicità politica abbia stabilito una definizione comune di "pubblicità politica". Stiamo rivedendo le nostre politiche per garantire che il nostro divieto di pubblicità politica sia almeno altrettanto ampio del regolamento.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>I nostri team che si occupano di contenuti per l'integrità della monetizzazione hanno osservato un forte aumento dei tentativi di pubblicare annunci relativi a contenuti politici/di guerra durante il periodo iniziale dell'inizio del conflitto. I nostri metodi di controllo del rischio hanno garantito che non vi fosse un corrispondente aumento delle attività che violavano i diritti sulla piattaforma. Dalle prime fasi del conflitto, questi numeri sono diminuiti in modo significativo e non si sono verificati ulteriori picchi.</p>
Integrità dei servizi	



Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.

Identificazione e rimozione delle reti CIO

(Impegno 14, Misura 14.1)

Descrizione dell'intervento

Lottiamo contro le CIO in quanto le nostre politiche di I&A vietano i tentativi di influenzare l'opinione pubblica e di ingannare i nostri sistemi o gli utenti sull'identità, l'origine, la posizione approssimativa, la popolarità o lo scopo generale. Proibiamo e lavoriamo costantemente per interrompere i tentativi di intraprendere operazioni di influenza occulta manipolando la nostra piattaforma e/o fuorviando in modo dannoso la nostra comunità, i nostri team di esperti che si concentrano interamente sull'individuazione, l'investigazione e l'interruzione delle reti CIO hanno rimosso numerose reti che miravano a discutere della guerra in Ucraina.

Contrastare le operazioni di influenza occulta è una sfida particolare, perché gli attori avversari che ne sono alla base evolvono continuamente i modi in cui nascondono i collegamenti tra i loro account. I nostri esperti lavorano per contrastare le operazioni di influenza occulta studiando i numerosi livelli di tecniche, tattiche e procedure che gli attori ingannevoli utilizzano per cercare di manipolare le piattaforme, attingendo da una varietà di discipline tra cui l'intelligence delle minacce e la scienza dei dati.

Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.

Tra luglio e dicembre 2024, abbiamo intrapreso azioni per rimuovere le seguenti [] reti (composte da [] account in totale) che sono risultate coinvolte in tentativi coordinati di influenzare l'opinione pubblica sulla guerra tra Russia e Ucraina e di ingannare individui, la nostra comunità o i nostri sistemi:

Origine della rete: Russia
Descrizione: Riteniamo che questa rete operi dalla Russia e si rivolga a un pubblico ucraino. Gli individui dietro questa rete hanno creato account non autentici per minare il Centro di reclutamento territoriale e di sostegno sociale ucraino. È stato riscontrato un comportamento anomalo da parte degli utenti, che riteniamo sia un tentativo di amplificare in modo non autentico i propri contenuti e di reindirizzare gli utenti da TikTok attraverso la condivisione di link esterni.

Conti rimossi: 19,727
Seguaci: 41,921

Origine della rete: Ucraina
Descrizione: Valutiamo che questa rete operava dall'Ucraina e si rivolgeva a un pubblico sia ucraino che russo. Gli individui dietro questa rete hanno creato account non autentici per amplificare artificialmente le narrazioni in ucraino e russo, critiche nei confronti del governo russo. È stato riscontrato che la rete creava punti di informazione non autentici nel tentativo di apparire come una fonte di informazione più affidabile.



	<p>Conti rimossi: 76 Seguaci: 214.715</p> <p>Origine della rete: Italia Descrizione: Valutiamo che questa rete operava dall'Italia e si rivolgeva a un pubblico globale. Gli individui dietro questa rete hanno creato account non autentici per promuovere l'amministrazione russa. È stato riscontrato che la rete mostrava comportamento anomalo dell'utente che riteniamo essere un tentativo di amplificare in modo non autentico il suo contenuto.</p> <p>Conti rimossi: 8 Seguaci: 3,790,110</p> <p>Origine della rete: Russia Descrizione: Riteniamo che questa rete operi dalla Russia e si rivolga a un pubblico ucraino. Gli individui dietro questa rete hanno creato account non autentici per minare il Centro di reclutamento territoriale e di sostegno sociale ucraino. È stato riscontrato un comportamento anomalo da parte degli utenti, che riteniamo sia un tentativo di amplificare in modo non autentico i propri contenuti e di reindirizzare gli utenti da TikTok attraverso la condivisione di link esterni.</p> <p>Conti rimossi: 19,727 Seguaci: 41,921</p> <p>Origine della rete: Russia Descrizione: Valutiamo che questa rete operava dalla Russia e si rivolgeva a un pubblico ucraino. Gli individui dietro questa rete hanno creato account non autentici e pubblicato contenuti per amplificare artificialmente le narrazioni pro-Russia, nel contesto della guerra in corso tra Russia e Ucraina. È stato riscontrato che la rete riproponeva contenuti duplicati sui suoi account.</p> <p>Conti rimossi: 45 Seguaci: 8,389</p> <p>Origine della rete: Russia (account di media affiliati allo Stato impegnati in operazioni di influenza occulta (Rossiya Segodnya)) Descrizione: Abbiamo rimosso una rete di account che riteniamo affiliati all'organizzazione mediatica russa affiliata allo Stato Rossiya Segodnya (inclusi gli account delle notizie di Sputnik) per violazione della nostra politica contro le operazioni di influenza occulta.</p> <p>Conti rimossi: 99 Seguaci: 9,905,964</p> <p>Origine della rete: Russia (account di media affiliati allo Stato che esercitano un'influenza occulta (TV-Novosti)) Descrizione: Abbiamo rimosso una rete di account che riteniamo affiliati all'organizzazione mediatica russa affiliata allo Stato, TV-Novosti (compresi gli account delle notizie di RT), per violazione della nostra politica contro le operazioni di influenza occulta. Account rimossi: 65</p>
--	---



	<p>Seguaci: 9,830,799</p> <p>Origine della rete: Russia Descrizione: Valutiamo che questa rete operava dalla Russia e si rivolgeva a un pubblico moldavo. Gli individui dietro questa rete hanno creato account non autentici per amplificare artificialmente le narrazioni critiche nei confronti dell'attuale governo moldavo, nel tentativo di manipolare il discorso elettorale. Si è scoperto che la rete utilizzava servizi di offuscamento della posizione per nascondere la sua vera ubicazione. Conti rimossi: 107 Seguaci: 5,026</p> <p>Origine della rete: Russia Descrizione: Valutiamo che questa rete operava dalla Russia e si rivolgeva a un pubblico ucraino. Gli individui dietro questa rete hanno creato account non autentici per amplificare le narrazioni che mettevano in evidenza le sfide affrontate dai soldati ucraini, mettendo in dubbio la credibilità del governo ucraino e suggerendo il declino del sostegno della NATO e degli alleati occidentali. La rete ha utilizzato mezzi tecnici per offuscare la sua vera posizione... Conti rimossi: 51 Seguaci: 1,177,876</p> <p>Abbiamo pubblicato queste informazioni nel nostro ultimo rapporto di trasparenza qui.</p>
<p>Affrontare i media sintetici e manipolati</p> <p><i>(Impegni 14 e 15, Misure 14.1, 15.1 e 15.2).</i></p>	<p>Descrizione dell'intervento</p> <p>L'intelligenza artificiale (IA) offre incredibili opportunità creative, ma può potenzialmente confondere o fuorviare gli utenti se non sanno che i contenuti sono stati generati o modificati con l'IA.</p> <p>La nostra politica "Edited Media and AI-Generated Content (AIGC)" è entrata in vigore nel maggio 2024. In questa politica vietiamo che l'AIGC mostri false fonti autorevoli o eventi di crisi, o che mostri falsamente personaggi pubblici in determinati contesti, tra cui il bullismo, l'approvazione o l'approvazione. TikTok ha anche iniziato a etichettare automaticamente gli AIGC quando vengono caricati da altre piattaforme.</p> <p>Ai fini della nostra politica, AIGC si riferisce a contenuti creati o modificati dalla tecnologia di intelligenza artificiale (AI) o processi di apprendimento automatico, che possono includere immagini di persone reali e mostrare scene altamente realistiche o utilizzare uno stile artistico particolare, come un dipinto, un cartone animato o un anime. Per "contenuti modificati in modo significativo" si intendono contenuti che mostrano persone che fanno o dicono qualcosa che non hanno fatto o detto, o che alterano il loro aspetto in modo tale da renderli difficili da riconoscere o identificare.</p> <p>In conformità con la nostra politica, vietiamo l'AIGC che presenta:</p> <ul style="list-style-type: none">● Persone dall'aspetto realistico di età inferiore ai 18 anni



	<ul style="list-style-type: none"> ● L'immagine di figure private adulte, se ci rendiamo conto che è stata utilizzata senza il loro permesso. ● Media fuorvianti dell'AIGC o modificati che mostrano falsamente: <ul style="list-style-type: none"> ○ Contenuti che sembrano provenire da una fonte autorevole, come ad esempio un'organizzazione giornalistica rispettabile. ○ Un evento di crisi, come un conflitto o una catastrofe naturale ○ Un personaggio pubblico che è: <ul style="list-style-type: none"> ■ essere degradati o molestati, o assumere un comportamento criminale o antisociale ■ prendere posizione su una questione politica, su un prodotto commerciale o su una questione di importanza pubblica (come le elezioni) ■ essere appoggiato o condannato politicamente da un individuo o da un gruppo <p>Con l'evoluzione dell'IA, continuiamo a investire nella lotta contro l'AIGC dannosa, evolvendo i nostri modelli di rilevamento proattivo, consultando esperti e collaborando con i colleghi per soluzioni condivise.</p> <p>Le pratiche vietate sono descritte nelle nostre politiche I&A qui.</p> <p><i>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</i></p> <p>I nostri sforzi sostengono pratiche di creazione di contenuti trasparenti e responsabili, sia nel contesto della guerra in Ucraina che, più in generale, sulla nostra piattaforma.</p>
<p>Eliminare la disinformazione dannosa dalla nostra piattaforma</p> <p><i>(Impegno 14, Misura 14.1)</i></p>	<p><i>Descrizione dell'intervento</i></p> <p>Interveniamo per rimuovere gli account o i contenuti che contengono contenuti inaccurati, fuorvianti o falsi che possono causare danni significativi agli individui o alla società, indipendentemente dalle intenzioni. In ambienti di conflitto, tali informazioni possono includere contenuti ripresi da conflitti passati, contenuti che fanno affermazioni false e dannose su eventi specifici o che incitano al panico. In determinate circostanze, possiamo anche ridurre l'importanza di tali contenuti laddove non ne sia giustificata la rimozione.</p> <p>Impieghiamo un approccio stratificato al rilevamento della disinformazione, sfruttando molteplici strategie sovrapposte per garantire una copertura completa e reattiva. Poniamo una notevole enfasi sulle strategie di moderazione proattiva dei contenuti, al fine di rimuovere la disinformazione dannosa che viola le nostre politiche prima che ci venga segnalata dagli utenti o da .</p> <p>Su TikTok diamo molta importanza alla moderazione proattiva dei contenuti e siamo orgogliosi di rimuovere la maggior parte dei video violenti prima che ci vengano segnalati dagli utenti o da terzi.</p> <p><i>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</i></p> <p>Nel contesto della crisi, siamo orgogliosi di aver rimosso in modo proattivo migliaia di video contenenti disinformazione dannosa relativa alla guerra in Ucraina. Siamo riusciti a farlo grazie a una combinazione di revisioni automatiche, - contenuti di livello umano</p>



	<p>moderazione, effettuando controlli a tappeto mirati su determinati tipi di contenuti (ad esempio hashtag/elenchi di parole chiave sensibili), nonché lavorando a stretto contatto con i nostri partner di fact-checking e rispondendo alle tendenze emergenti da loro identificate.</p> <p><i>Metriche rilevanti:</i></p> <ul style="list-style-type: none"> • Numero di video rimossi a causa della violazione della politica di disinformazione con un proxy relativo alla guerra in Ucraina - 4.429 • Numero di video non raccomandati a causa della violazione della politica di disinformazione con un proxy (solo con riferimento a RU/UA) - 5.903 • Numero di rimozioni proattive di video rimossi per violazione della politica di disinformazione con un proxy relativo alla guerra in Ucraina - 3.889
Responsabilizzare gli utenti	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
<p>Non promuovere in modo proattivo contenuti di tipo giornalistico ai nostri utenti.</p> <p><i>(Impegno 18, Misura 18.1)</i></p>	<p>Descrizione dell'intervento</p> <p>TikTok è principalmente una piattaforma di intrattenimento. Può accadere che il feed "Per te" di un utente mostri nel tempo più contenuti di tipo giornalistico (come ad esempio contenuti giornalistici relativi alla guerra in Ucraina) se si tratta di contenuti che l'utente cerca attivamente e con cui si impegna, ma non promuoviamo attivamente contenuti giornalistici agli utenti su TikTok.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Il nostro approccio ai contenuti di tipo giornalistico sostiene i nostri sforzi per ridurre la diffusione di disinformazione dannosa per gli utenti.</p>
<p>Applicazione dell'etichetta dei media affiliati allo Stato</p> <p><i>(Impegno 17, Misura 17.1)</i></p>	<p>Descrizione dell'intervento</p> <p>Abbiamo limitato l'accesso ad alcune entità mediatiche affiliate allo Stato e rafforzato la nostra politica sui media affiliati allo Stato, al fine di fornire agli utenti un contesto per valutare i contenuti condivisi da tali entità russe, ucraine e bielorusse.</p> <p>Nell'UE, in Islanda e nel Liechtenstein abbiamo adottato misure per limitare l'accesso ai contenuti dei media e degli account soggetti a sanzioni.</p> <p>Abbiamo anche aggiornato la nostra politica sui media affiliati allo Stato per rafforzare il nostro approccio al contrasto dei tentativi di influenza. Questi aggiornamenti comprendono:</p>



	<ul style="list-style-type: none"> - Rendere gli account dei media affiliati allo Stato che tentano di raggiungere le comunità al di fuori del loro Paese su eventi e questioni globali attuali non ammissibili alla raccomandazione, il che significa che i loro contenuti non appariranno nel feed "Per te"; - Vietare agli account dei media affiliati allo Stato in tutti i mercati in cui sono disponibili i nostri marchi di media controllati dallo Stato, anche nell'UE, di fare pubblicità al di fuori del Paese a cui sono principalmente affiliati; - Investire nelle nostre capacità di rilevamento degli account mediatici affiliati allo Stato. <p>Abbiamo anche collaborato con esperti esterni per definire la nostra politica sui media affiliati allo Stato e la valutazione delle etichette dei media controllati dallo Stato.</p> <p>Quando la nostra etichetta di media affiliati allo Stato viene applicata ai contenuti pubblicati dagli account di tali entità in Russia, Ucraina e Bielorussia, agli utenti in tutto il SEE viene automaticamente mostrato un pop-up a schermo intero contenente informazioni sul significato dell'etichetta e che invita l'utente a cliccare su "saperne di più" e a essere reindirizzato a una pagina in-app, che spiega perché il contenuto è stato etichettato come media controllati dallo Stato.</p> <p>Oltre a quanto sopra, continuiamo a investire nell'automazione e nell'individuazione su scala ridotta di account di media affiliati allo Stato. Continuiamo inoltre a collaborare con esperti di terze parti che contribuiscono a definire le nostre politiche sui media affiliati allo Stato e a informare le nostre valutazioni sugli account che sono stati etichettati come controllati dallo Stato. Continuiamo a migliorare i processi esistenti per l'applicazione dell'etichetta di media affiliati allo Stato, cercando ad esempio di automatizzarli laddove possibile e puntando a semplificare tutte le comunicazioni per garantire la massima efficienza. Continuiamo inoltre a sviluppare un ulteriore livello di intervento nei confronti degli account affiliati allo Stato che adottano comportamenti dannosi.</p> <p><i>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</i></p> <p>Continuiamo a individuare ed etichettare gli account dei media controllati dallo Stato in conformità con la nostra politica di etichettatura dei media controllati dallo Stato a livello globale.</p> <p><i>Metriche rilevanti:</i></p> <ul style="list-style-type: none"> ● Numero di video contrassegnati con l'etichetta di media affiliati allo Stato per Russia, Bielorussia e Ucraina: 29.665. ● Numero di impressioni dell'etichetta dei media affiliati allo Stato per Russia, Bielorussia e Ucraina: 158.700.542.
<p>Creare campagne di alfabetizzazione mediatica a livello locale</p> <p><i>(Impegno 17, Misure 17.2 e 17.3)</i></p>	<p><i>Descrizione dell'intervento</i></p> <p>Riconosciamo l'importanza di misure proattive volte a migliorare l'alfabetizzazione digitale dei nostri utenti e ad aumentare rilievo delle informazioni autorevoli.</p> <p>Abbiamo localizzato campagne di alfabetizzazione mediatica relative alla crisi per sensibilizzare i nostri utenti. Abbiamo promosso la campagna attraverso una combinazione dei nostri strumenti di intervento in-app, al fine di garantire che le informazioni autorevoli siano</p>



	<p>promossi ai nostri utenti. Abbiamo inoltre stretto una partnership con un'organizzazione locale di fact-checking ucraina, VoxCheck, con l'obiettivo di lanciare una campagna permanente di alfabetizzazione mediatica in Ucraina.</p> <p>Gli utenti che cercano parole chiave relative alla guerra in Ucraina sono indirizzati a suggerimenti, preparati in collaborazione con i nostri partner di fact checking, per aiutare gli utenti a identificare la disinformazione e a prevenirne la diffusione sulla piattaforma.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>In collaborazione con i nostri partner di fact-checking, abbiamo realizzato tredici campagne di alfabetizzazione mediatica localizzate che affrontano la disinformazione relativa alla guerra in Ucraina in Austria, Bulgaria, Repubblica Ceca, Croazia, Estonia, Germania, Ungheria, Lettonia, Lituania, Polonia, Romania, Slovacchia e Slovenia.</p> <p><i>Metriche rilevanti per le campagne di alfabetizzazione ai media (numeri totali SEE):</i></p> <ul style="list-style-type: none">● Numero totale di impressioni dell'intervento di ricerca - 30.278.338● Numero totale di clic sull'intervento di ricerca - 130.282● Tasso di click through dell'intervento di ricerca: 0,43%.
Responsabilizzare la comunità di ricerca	
<p>Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.</p>	
<p>Misure adottate per sostenere la ricerca sulla disinformazione e la disinformazione legate alle crisi</p> <p><i>(Impegno 27, Misura 26.1 e 26.2)</i></p>	<p>Descrizione dell'intervento</p> <p>Attraverso la nostra API di ricerca, i ricercatori accademici di università no-profit negli Stati Uniti e in Europa possono richiedere di studiare i dati pubblici relativi ai contenuti e agli account di TikTok. Questi dati pubblici includono commenti, didascalie, sottotitoli e numero di commenti, condivisioni, like e preferiti che un video riceve, commenti dalla nostra piattaforma. Ulteriori informazioni sono disponibili qui.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Durante il periodo del presente rapporto COPD, abbiamo approvato 1 domanda attraverso l'API di ricerca, con un focus esplicito guerra in Ucraina.</p>



Potenziare la comunità del Fact-Checking	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Applicare la nostra etichetta di contenuto non verificato e rendere il contenuto non idoneo per la raccomandazione <i>(Impegno 31, Misura 31.2)</i>	Descrizione dell'intervento <p>Quando i nostri moderatori della disinformazione o i nostri partner per il fact-checking stabiliscono che il contenuto non può essere verificato in quel momento (cosa comune durante un evento in corso), applichiamo la nostra etichetta di contenuto non verificato al contenuto per incoraggiare gli utenti a considerare l'affidabilità o la fonte del contenuto. L'applicazione dell'etichetta comporterà anche l'inammissibilità del contenuto alla raccomandazione, al fine di limitare la diffusione di informazioni potenzialmente fuorvianti.</p>
	Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili. <p>La verifica di certe informazioni durante eventi dinamici e in rapido movimento come una guerra può essere impegnativa e i nostri moderatori e verificatori non possono sempre determinare in modo definitivo se i contenuti sono effettivamente disinformazione dannosa, in violazione delle nostre CG.</p> <p>Pertanto, per ridurre al minimo i rischi, quando i nostri fact-checker o i nostri moderatori addestrati non dispongono di informazioni sufficienti per verificare un contenuto potenzialmente fuorviante, applichiamo la nostra etichetta di contenuto non verificato per informare gli utenti che il contenuto è stato esaminato ma non può essere convalidato in modo definitivo. L'obiettivo è quello di sensibilizzare gli utenti sulla credibilità del contenuto e ridurre la condivisione (vedi screenshot qui). La nostra etichetta di contenuto non verificato è disponibile per gli utenti in 23 lingue ufficiali dell'UE (più, per gli utenti del SEE, il norvegese e l'islandese).</p> <p>In caso di applicazione del banner, il contenuto non potrà essere raccomandato nel feed "Per te" di nessuno, per limitare la diffusione di informazioni relative a eventi in corso, i cui dettagli sono ancora in fase di sviluppo e che possono essere potenzialmente fuorvianti.</p>
Garantire una copertura di fact-checking <i>(Impegno 30, Misura 30.1)</i>	Descrizione dell'intervento <p>I nostri sforzi di fact checking coprono il russo, l'ucraino, il bielorusso e tutte le principali lingue europee (comprese le 18 lingue ufficiali europee e una serie di altre lingue che interessano gli utenti europei).</p>
	Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili. <p>Il contesto e la verifica dei fatti sono fondamentali per applicare in modo coerente e accurato le nostre politiche di disinformazione dannosa, ed è questo che abbiamo fatto in modo che, nel contesto della crisi, il nostro programma di verifica dei fatti copra il russo, l'ucraino e il bielorusso.</p> <p>Più in generale, lavoriamo con 14 partner per il fact-checking in Europa, che coprono le lingue parlate di 23 paesi del SEE (oltre a</p>



	<p>e di altre lingue che interessano gli utenti europei). Uno dei nostri partner per il fact-checking, Reuters, è dedicato al fact-checking dei contenuti in russo e ucraino. Per supportare ulteriormente i nostri sforzi di fact-checking in Ucraina, abbiamo anche sfruttato altri reporter di lingua ucraina che sono collegati con alcuni dei nostri partner di fact-checking esistenti.</p> <p><i>Metriche rilevanti:</i></p> <ul style="list-style-type: none"> ● Numero di video verificati con un proxy relativi alla guerra in Ucraina - 577 ● Numero di video rimossi a seguito di una valutazione di fact checking con parole relative alla guerra in Ucraina - 104 ● Numero di video non raccomandati in For Your Feed a seguito di una valutazione di fact checking con parole relative alla guerra in Ucraina - 133
<p>Collaborare con i nostri partner per il fact-checking in relazione alle tendenze emergenti.</p> <p><i>(Impegno 31, Misura 31.1)</i></p>	<p>Descrizione dell'intervento</p> <p>Ci incontriamo mensilmente con i nostri partner di fact checking per discutere delle tendenze della disinformazione e delle narrazioni in corso sul mercato. I nostri partner di fact checking ci forniscono anche indicazioni proattive sui video che hanno trovato su TikTok e che sono considerati disinformazione.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p><i>Metriche rilevanti:</i></p> <ul style="list-style-type: none"> ● Numero di video rimossi a causa della violazione della politica di disinformazione con un proxy relativo alla guerra in Ucraina - 4.429

Relazioni sulla risposta del servizio durante una crisi

Conflitto Israele - Hamas

Minacce osservate o previste al momento della segnalazione: [limite di caratteri suggerito 2000 caratteri].

TikTok riconosce l'importanza e la sensibilità del conflitto tra Israele e Hamas (denominato "Conflitto" in questa sezione). Siamo consapevoli che questo rimane un momento difficile, di paura e di polarizzazione per molte persone in tutto il mondo e su TikTok. TikTok continua a riconoscere la necessità di impegnarsi nella moderazione dei contenuti violenti su larga scala, garantendo al contempo il rispetto e la tutela dei diritti e delle libertà fondamentali dei cittadini europei. Rimaniamo impegnati a sostenere la libera espressione, a sostenere il nostro impegno per i diritti umani e a mantenere la sicurezza della nostra comunità e l'integrità del nostro sito.

In vista dell'anniversario del Conflitto, eravamo consapevoli che ci sarebbe stato un aumento dei contenuti pubblicati in questo periodo e volevamo garantire la sicurezza della nostra comunità e l'integrità della piattaforma in questo momento delicato. In preparazione all'Anniversario del Conflitto, è stato sviluppato un piano completo per affrontare i rischi potenziali e garantire la sicurezza della piattaforma. Ciò ha comportato un coordinamento strategico in diverse regioni, tra cui IL, MENA, APAC, UE, USA/CA e AMS, con l'obiettivo di ridurre i contenuti ad alto rischio e garantire un servizio ininterrotto.

Rimangono impegnati nella trasparenza durante questo periodo e abbiamo tenuto la nostra comunità informata della nostra risposta immediata e continua attraverso il seguente post della Newsroom, aggiornato l'ultima volta in prossimità dell'anniversario del conflitto: nell'ottobre 2024 [Le nostre azioni continue per proteggere la TikTok comunità di durante la guerra tra Israele e Hamas](#).

Di seguito sono riportate alcune delle principali minacce osservate e considerate in relazione al Conflitto e le azioni intraprese per durante il periodo di riferimento.

(I) Diffusione di disinformazione dannosa

La fiducia è alla base della nostra comunità e ci sforziamo di mantenere TikTok uno spazio sicuro e autentico in cui possano prosperare interazioni e contenuti genuini. TikTok adotta un approccio multiforme per affrontare la diffusione di disinformazione dannosa, indipendentemente dalle intenzioni. Questo include le nostre: [politiche di integrità e autenticità](#) (politiche I&A) nelle nostre [linee guida della community](#), prodotti, pratiche e partnership esterne con fact-checkers, enti di alfabetizzazione mediatica e ricercatori. Supportiamo i nostri team di moderazione con una guida dettagliata sulle politiche di disinformazione, una formazione avanzata e l'accesso a strumenti come il nostro database globale di informazioni precedenti. affermazioni verificate dai nostri partner di fact-checking accreditati dall'IFCN, che aiutano a valutare l'accuratezza dei contenuti.

Continuiamo ad agire rapidamente contro la disinformazione, le teorie cospirative, il falso impegno e i falsi account relativi al conflitto.



(II) Operazioni di influenza segreta (CIO)

Le politiche di integrità e autenticità di TikTok non consentono comportamenti ingannevoli che possano causare danni alla nostra comunità o alla società in generale. Ciò include i tentativi coordinati di influenzare o influenzare l'opinione pubblica e di ingannare gli individui, la nostra comunità o i nostri sistemi sull'identità, la posizione approssimativa, le relazioni, la popolarità o lo scopo di un account.

Abbiamo team specificamente addestrati per indagare sulle CIO e l'interruzione delle reti CIO è stata per noi una priorità assoluta nel contesto del Conflitto. Ora forniamo aggiornamenti regolari sulle reti CIO che rileviamo e rimuoviamo dalla nostra piattaforma, comprese quelle identificate in relazione al Conflitto, nel nostro [rapporto di trasparenza CIO](#) . dedicato Tra giugno 2024 e dicembre 2024, abbiamo segnalato 3 nuove interruzioni di reti CIO che risultavano pubblicare contenuti relativi al Conflitto come tema dominante.

Sappiamo che CIO continuerà a evolversi in risposta al nostro rilevamento e che le reti potrebbero tentare di ristabilire una presenza sulla nostra piattaforma; per questo motivo cerchiamo continuamente di rafforzare le nostre politiche e le azioni di applicazione per proteggere la nostra comunità da nuovi tipi di disinformazione dannosa e comportamenti non autentici.

Mitigazioni in atto al momento della segnalazione: [limite di caratteri suggerito: 2000 caratteri].

Ci impegniamo costantemente per garantire che TikTok sia una fonte di informazioni affidabili e sicure e riconosciamo l'aumento del rischio e dell'impatto di informazioni fuorvianti in un momento di crisi. Come parte del nostro processo di gestione delle crisi, abbiamo lanciato un centro di comando che riunisce i membri chiave del nostro team globale di migliaia di professionisti della sicurezza, che rappresentano una gamma di competenze e prospettive regionali, in modo da rimanere agili nel modo in cui agiamo per rispondere a questa crisi in rapida evoluzione. Dall'inizio del conflitto, siamo:

(I) Rispettare le linee guida della comunità di TikTok

Abbiamo aggiornato le [linee guida della comunità](#) e abbiamo iniziato ad applicare politiche più ampie sui discorsi d'odio e sui comportamenti odiosi. Queste politiche mirano ad affrontare meglio i discorsi di odio impliciti o indiretti e a creare un ambiente più sicuro e civile per tutti. Si aggiungono alle nostre politiche di lunga data contro l'antisemitismo e altre ideologie odiose. Abbiamo anche aggiornato la nostra politica sull'incitamento all'odio per riconoscere i contenuti che utilizzano "sionista" come proxy di un attributo protetto quando non è usato per riferirsi a un'ideologia politica e viene invece utilizzato come proxy dell'identità ebraica o israeliana. Questa politica è stata implementata all'inizio del 2024 dopo aver osservato un aumento dell'uso di questa parola in chiave di odio.

Continuare a far rispettare le nostre [politiche](#) contro la [violenza](#), l'[odio](#) e la [disinformazione dannosa](#), intervenendo per rimuovere i contenuti e gli account che violano le regole. Ad esempio, rimuoviamo i contenuti che promuovono Hamas o che sostengono in altro modo gli attacchi o deridono le vittime della violenza. Se viene pubblicato un contenuto che ritrae una persona presa in ostaggio, faremo tutto il possibile per proteggere la sua dignità e rimuoveremo i contenuti che violano le nostre regole. Non tolleriamo tentativi di incitare alla violenza o di diffondere ideologie odiose. Abbiamo una politica di tolleranza zero per i contenuti che inneggiano a organizzazioni e individui violenti e odiosi, e tali organizzazioni e individui non sono ammessi sulla nostra piattaforma. Blocchiamo anche gli hashtag che promuovono la violenza o che violano le nostre regole. Abbiamo rimosso 8.765 video relativi al conflitto che violavano le nostre politiche di disinformazione.



Evolvere i nostri sistemi di rilevamento automatico proattivo in tempo reale, man mano che identifichiamo nuove minacce; questo ci permette di rilevare e rimuovere automaticamente i contenuti grafici e violenti, in modo che né i nostri moderatori né i membri della nostra comunità vi siano esposti.

(II) Sfruttare il nostro programma di verifica dei fatti

Adottiamo un approccio stratificato per individuare la disinformazione dannosa che viola le nostre Linee guida della Comunità e il nostro programma globale di fact-checking ne è una parte fondamentale. L'obiettivo principale del programma di fact-checking è quello di sfruttare l'esperienza di organizzazioni esterne di fact-checking per aiutare a valutare l'accuratezza di affermazioni dannose e difficili da verificare.

Per limitare la diffusione di informazioni potenzialmente fuorvianti, applichiamo [etichette di avvertimento](#) e invitiamo gli utenti a riconsiderare la condivisione di contenuti relativi a eventi in corso o di emergenza, che sono stati valutati dai nostri fact-checkers ma che non possono essere verificati come accurati, ovvero "contenuti non verificati". Consapevoli di come l'evolversi degli eventi possa influenzare la valutazione delle affermazioni sensibili relative ai conflitti giorno per giorno, abbiamo implementato un processo che consente ai nostri partner di fact-checking di aggiornarci rapidamente se le affermazioni precedentemente valutate come "non verificate" vengono verificate con un contesto aggiuntivo e/o in una fase successiva.

(III) Aumentare le nostre capacità di moderazione dei contenuti

TikTok ha moderatori di lingua araba ed ebraica nei team di moderazione dei contenuti che rivedono i contenuti e assistono nelle traduzioni relative ai conflitti. Poiché continuiamo a concentrarci sull'assistenza ai moderatori, in questo periodo abbiamo anche distribuito ulteriori risorse di benessere per i nostri team di moderazione umana.

(IV) L'interruzione dei CIO

Anche l'interruzione delle reti CIO è stata per noi un'attività altamente prioritaria per contrastare comportamenti ingannevoli che possono causare danni alla nostra comunità o alla società in generale. Come già detto in precedenza, tra luglio e dicembre 2024, siamo intervenuti per rimuovere 3 reti (per un totale di 132 account) che sono risultate collegate al Conflitto. Ora pubblichiamo tutte le reti CIO che identifichiamo e rimuoviamo, comprese quelle relative al conflitto, nel nostro rapporto di trasparenza CIO dedicato, [qui](#).

(V) Mitigare il rischio di monetizzazione della disinformazione dannosa

Abbiamo apportato modifiche temporanee alle politiche che regolano le funzioni di TikTok nel tentativo di impedire in modo proattivo che vengano utilizzate per comportamenti di odio o di violenza nella regione. Ad esempio, abbiamo aggiunto ulteriori restrizioni sull'idoneità LIVE come misura temporanea, dato l'aumento del rischio di sicurezza nel contesto dell'attuale situazione degli ostaggi. La nostra [politica sugli annunci politici](#), l'etichettatura GPPA e le [politiche di sicurezza e civiltà](#) contribuiscono a ridurre il rischio di monetizzazione della disinformazione dannosa.

(VI) Interventi di ricerca per aumentare la consapevolezza della potenziale disinformazione.

Per contribuire alla sensibilizzazione e alla protezione dei nostri utenti, abbiamo lanciato interventi di ricerca che si attivano quando gli utenti cercano termini non violenti.



relativi al conflitto (ad esempio, Israele, Palestina). Questi interventi di ricerca ricordano agli utenti di soffermarsi a controllare le fonti e li indirizzano anche verso risorse di benessere. Nell'H2 abbiamo continuato a perfezionare questo processo, concentrandoci in particolare sul miglioramento delle parole chiave per garantirne la pertinenza e l'efficacia.

(VII) Aggiunta di schermate di opt-in su contenuti che potrebbero essere scioccanti o grafici.

Riconosciamo che alcuni contenuti che potrebbero altrimenti infrangere le nostre regole possono essere di interesse pubblico, e permettiamo che questi contenuti rimangano sulla piattaforma per scopi documentaristici, educativi e di controdiscorso. Le schermate di opt-in aiutano a evitare che le persone visualizzino inaspettatamente contenuti scioccanti o grafici, mentre continuiamo a fare [eccezioni di interesse pubblico](#) per alcuni contenuti.

Inoltre, ci impegniamo a collaborare con esperti del settore e della società civile, come [Tech Against Terrorism](#) e i nostri [Consigli consultivi](#), e a collaborare con le forze dell'ordine a livello globale in linea con le nostre [Linee guida per l'applicazione della legge](#), per salvaguardare e proteggere ulteriormente la nostra piattaforma in questi tempi difficili.

[I firmatari sono tenuti a fornire informazioni relative alla loro particolare risposta alle minacce e alle sfide osservate nei loro servizi. Assicurano che le informazioni riportate di seguito forniscano un resoconto accurato e completo delle loro azioni pertinenti. Poiché le risposte operative alle situazioni di crisi/elezioni possono variare da un servizio all'altro, l'assenza di informazioni non deve essere considerata a priori una carenza nel modo in cui un particolare servizio ha risposto. Le metriche di impatto sono accurate al meglio delle capacità di misurazione dei firmatari].

Politiche e termini e condizioni

Illustrare eventuali modifiche alle vostre politiche

Politica	Modifiche (come nuove politiche introdotte, modifiche, adattamento dell'ambito o dell'implementazione)	<p>Motivazione</p> <p>Abbiamo perfezionato e ampliato le nostre eccezioni di notiziabilità per consentire la diffusione di contenuti che documentano una zona di conflitto e di discorsi/critiche politiche legittime, pur rimanendo sensibili al potenziale danno che gli utenti potrebbero subire dall'esposizione a immagini grafiche, comportamenti odiosi o incitamento alla violenza. Nell'ambito di questo sforzo, abbiamo introdotto politiche dedicate ai contenuti relativi al conflitto, in particolare per quanto riguarda la rappresentazione di ostaggi, sofferenze umane e proteste.</p> <p>Inoltre, abbiamo rafforzato le nostre politiche sui contenuti che glorificano Hamas o Hezbollah e sulla promozione o celebrazione di atti violenti commessi da entrambe le parti in conflitto. Per migliorare ulteriormente l'integrità della piattaforma, abbiamo implementato politiche specifiche di integrità e autenticità per i contenuti relativi a Israele-Hamas, con particolare attenzione alle teorie cospirative di varia gravità e alle affermazioni non comprovate.</p>



	<p>Continuiamo a fare affidamento sulle nostre solide politiche di I&A esistenti, che costituiscono una base efficace per affrontare i contenuti relativi al Conflitto. Pertanto, non abbiamo avuto bisogno di introdurre nuove politiche di disinformazione per affrontare la crisi.</p> <p>In caso di crisi, teniamo sotto controllo le nostre politiche e ci assicuriamo che i team di moderazione abbiano una guida supplementare.</p>	<p>Nel contesto del Conflitto, ci affidiamo alle nostre solide politiche di I&A come prima linea di difesa per combattere la disinformazione dannosa e i comportamenti ingannevoli sulla nostra piattaforma.</p> <p>Le nostre Linee guida della comunità indicano chiaramente ai nostri utenti quali contenuti rimuovere o rendere non ammissibili per il feed For You quando rappresentano un rischio di danno per i nostri utenti o per il pubblico in generale. Abbiamo inoltre supportato i nostri team di moderazione con indicazioni e linee guida dettagliate per la moderazione della disinformazione dannosa legata ai conflitti, utilizzando le politiche esistenti.</p> <p>All'interno del nostro dipartimento Fiducia e Sicurezza abbiamo team specializzati che si occupano delle politiche di I&A, anche nelle aree dei prodotti e delle politiche. I nostri esperti in materia di I&A tengono costantemente sotto controllo queste politiche e collaborano con partner ed esperti esterni per capire se sono necessari aggiornamenti.</p> <p>Quando si verificano situazioni come il Conflitto, questi team si adoperano per garantire lo sviluppo di una guida appropriata che consenta di applicare in modo efficace le politiche di I&A ai contenuti relativi alla crisi in questione (in questo caso, il Conflitto). Ciò include l'emanazione di linee guida e indicazioni dettagliate sulle politiche, compresa la fornitura di casi di disinformazione dannosa a supporto dei team di moderazione.</p>
Politiche sulle funzioni di TikTok	<p>Oltre a poter fare affidamento sulle nostre politiche I&A, abbiamo apportato modifiche temporanee alle politiche esistenti che regolano alcune funzionalità di TikTok. Ad esempio, abbiamo aggiunto ulteriori restrizioni sull'ammissibilità dei LIVE come misura temporanea, dato l'aumento del rischio di sicurezza nel contesto dell'attuale situazione degli ostaggi.</p>	<p>Sono stati introdotti aggiustamenti temporanei nel tentativo di prevenire in modo proattivo l'utilizzo di alcune caratteristiche per comportamenti odiosi o violenti nella regione.</p>
Controllo dei posizionamenti degli annunci		



Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.

Prevenzione dell'uso improprio delle nostre funzioni di monetizzazione

(Impegno 1, Misura 1.1 e 1.4)

Descrizione dell'intervento

La nostra [politica sugli annunci politici](#) e le nostre [politiche di sicurezza e civiltà](#) contribuiscono a ridurre la monetizzazione della disinformazione dannosa.

Le ONG che sono state controllate dal nostro team Monetisation Integrity e che collaborano con il nostro team di vendita, sono autorizzate a lanciare campagne pubblicitarie per la raccolta di fondi durante il Conflitto. Questo processo, tuttavia, è soggetto a una rigorosa supervisione per ridurre il rischio di false campagne di raccolta fondi e non consente di sostenere nessuna delle parti coinvolte.

In risposta al Conflitto, abbiamo aggiornato le nostre linee guida sulle funzioni LIVE e quelle sulla monetizzazione per evitare che le persone utilizzino le funzioni di monetizzazione per sfruttare la tragedia in corso a fini personali.

Monitoriamo attentamente il posizionamento dei nostri annunci (soprattutto nel contesto di eventi come il conflitto tra Israele e Hamas) e, nel caso in cui i nostri annunci risultino adiacenti a o su fonti di disinformazione, indagheremo per determinare se il contenuto in questione è stato identificato correttamente e lo verificheremo con Integral Ad Science, Double Verify o Zefr, a seconda dei casi. Provvederemo quindi a modificare eventuali filtri o ad aggiungere la pubblicazione in questione a una blocklist per evitare che si ripeta.

Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.

Il monitoraggio dell'inserimento degli annunci e l'aggiornamento della nostra politica LIVE contribuiscono a evitare che le persone monetizzino la tragedia in corso a scopo di lucro.

Moderazione dei contenuti

(Impegno 2, Misura 2.2)

Descrizione dell'intervento

Utilizziamo una combinazione di moderazione automatica e umana per identificare i contenuti che violano le nostre politiche sugli annunci. Queste politiche vietano, tra l'altro, che i contenuti degli annunci e le pagine di destinazione mostrino contenuti negativi relativi a simboli militari o di polizia, eventi militari sensibili, militarismo, promozione o sbiancamento della guerra, terrorismo, organizzazioni illegali o elementi illegali.

Abbiamo continuato a investire sia nella tecnologia di moderazione automatica - che ora elimina l'80% dei contenuti rimossi da TikTok - sia nei moderatori. Abbiamo continuato ad aggiornare e ampliare i nostri corsi di aggiornamento, formazione e materiale didattico sull'hate speech, compresi quelli sui pregiudizi impliciti che affrontano l'antisemitismo e l'islamofobia. Abbiamo anche ricevuto una formazione aggiuntiva dal



	<p>Anti-Defamation League e American Jewish Committee per approfondire la comprensione delle nuove minacce che incombono sulla comunità ebraica.</p> <p>Il nostro dipartimento Monetisation Integrity dispone di team di moderazione in più sedi che parlano arabo ed ebraico.</p> <p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Data la gamma di potenziali violazioni della politica che potrebbero essere commesse, al momento non siamo in grado di fornire metriche specifiche per questo problema.</p>
<p>Pubblicità politica</p>	
<p>Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.</p>	
<p>Divieto di pubblicità politica</p> <p>(Impegno 5, Misura 5.1)</p>	<p>Descrizione dell'intervento</p> <p>Nel tentativo di preservare l'integrità della piattaforma e la sicurezza delle persone che la utilizzano, gli account appartenenti a politici o partiti politici non possono fare pubblicità o guadagnare su TikTok.</p> <p>Non consentiamo la promozione politica a pagamento, la pubblicità politica o la raccolta di fondi da parte di politici e partiti politici (per se stessi o per altri). La nostra politica sugli annunci politici include sia gli annunci tradizionali a pagamento che i creatori che ricevono un compenso per sostenere o contrastare un candidato alla carica. Questa è una politica di lunga data di TikTok dal 2019. Inoltre, non consentiamo annunci e di destinazione pagine che:</p> <ul style="list-style-type: none"> ● fare riferimento, promuovere o opporsi a candidati o nominati per cariche pubbliche, partiti politici o funzionari governativi eletti o nominati; ● riferimento a un'elezione, tra cui la registrazione degli elettori, l'affluenza alle urne e gli appelli al voto; ● includere il patrocinio a favore o contro referendum passati, attuali o proposti, misure elettorali, risultati o processi legislativi, giudiziari o normativi (compresi quelli che promuovono o attaccano le politiche o i risultati governo); e ● fare riferimento, promuovere o vendere merce con persone, entità o contenuti vietati, compresi slogan, simboli o loghi di campagne elettorali.



	<p>Chiediamo agli utenti di utilizzare la levetta di divulgazione dei contenuti quando pubblicano contenuti di marca e vietiamo i contenuti politici di marca. Durante il riferimento, abbiamo introdotto restrizioni sui contenuti del Feed For You che erano sospettati di essere contenuti politici non divulgati.</p> <p>Siamo lieti che il Regolamento UE 2024/900 sulla trasparenza e l'orientamento della pubblicità politica, entrato in vigore nel periodo di riferimento, abbia ora stabilito una definizione comune di "pubblicità politica". Abbiamo rivisto le nostre politiche per garantire che il nostro divieto di pubblicità politica sia almeno altrettanto ampio quanto il regolamento.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Vietando la pubblicità politica, contribuiamo a garantire alla nostra comunità un'esperienza TikTok creativa e autentica e riduciamo il rischio che la nostra piattaforma venga utilizzata per pubblicizzare e amplificare narrazioni che potrebbero essere divisive o false.</p>
Integrità dei servizi	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
<p>Identificazione e rimozione delle reti CIO</p> <p>(Impegno 14, Misura 14.1)</p>	<p>Descrizione dell'intervento</p> <p>Abbiamo assegnato risorse dedicate all'interno dei nostri team specializzati per monitorare in modo proattivo il CIO in relazione al Conflitto.</p> <p>Lottiamo contro le CIO in quanto le nostre politiche di I&A vietano i tentativi di influenzare l'opinione pubblica e di ingannare i nostri sistemi o utenti sull'identità, l'origine, la posizione approssimativa, la popolarità o lo scopo generale. Abbiamo team specificamente addestrati e dedicati che sono in allerta per indagare e rilevare le reti CIO sulla nostra piattaforma e abbiamo rimosso le reti che mirano al discorso sul Conflitto, in conformità con le nostre politiche di I&A che vietano i comportamenti ingannevoli.</p> <p>Sappiamo che CIO continuerà a evolversi in risposta al nostro rilevamento e che le reti potrebbero tentare di ristabilire una presenza sulla nostra piattaforma; per questo motivo cerchiamo continuamente di rafforzare le nostre politiche e le azioni di applicazione per proteggere la nostra comunità da nuovi tipi di disinformazione dannosa e comportamenti non autentici.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p>



	<p>Tra giugno e dicembre 2024, siamo intervenuti per rimuovere le seguenti 3 reti (per un totale di 132 account) che sono risultate collegate al Conflitto:</p> <p>Origine della rete: Iran Descrizione: Valutiamo che questa rete operava dall'Iran e si rivolgeva a un pubblico globale, creando account per rivolgersi a persone di lingua araba. Gli individui dietro a questa rete hanno creato account non autentici per amplificare artificialmente le narrazioni favorevoli alla politica estera irachena e iraniana sulla guerra tra Israele e Hamas. È stato riscontrato che la rete riproponeva contenuti duplicati sui suoi account. Conti in rete: 26 Seguaci della rete: 66,507</p> <p>Origine della rete: Egitto Descrizione: Valutiamo che questa rete operava dall'Egitto e si rivolgeva a un pubblico israeliano. Gli individui dietro questa rete hanno creato account non autentici per amplificare artificialmente le narrazioni critiche nei confronti delle azioni di Israele a Gaza. Valutiamo che la rete si coordinava online, al di fuori di TikTok, e utilizzava l'intelligenza artificiale per aiutare la generazione di personaggi israeliani fittizi, rivolgendosi a pubblici diversi alternando le lingue araba ed ebraica. Conti in rete: 94 Seguaci della rete: 44,896</p> <p>Descrizione: Valutiamo che questa rete si rivolgeva a un pubblico statunitense. Gli individui dietro questa rete hanno creato una serie di account non autentici che imitano cittadini statunitensi per amplificare le narrazioni critiche nei confronti delle azioni di Israele a Gaza e del sostegno degli Stati Uniti a Israele. La rete ha dimostrato di possedere una sicurezza operativa avanzata. Account in rete: 12 Seguaci della rete: 3,442</p> <p>Ora pubblichiamo tutte le reti CIO che identifichiamo e rimuoviamo, comprese quelle relative al Conflitto, all'interno del nostro rapporto di trasparenza CIO dedicato, qui.</p>
<p>Affrontare i media sintetici e manipolati</p> <p><i>(Impegno 15, Misure 15.1 e 15.2)</i></p>	<p>Descrizione dell'intervento</p> <p>La nostra politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC) chiarisce che non vogliamo che i nostri utenti siano fuorviati da eventi di crisi. Ai fini della nostra politica, AIGC si riferisce a contenuti creati o modificati dalla tecnologia AI o da processi di apprendimento automatico. Include immagini di persone reali e può mostrare scene altamente realistiche.</p> <p>Non permettiamo che l'AIGC sia fuorviante o che i media editati mostrino falsamente:</p> <ul style="list-style-type: none"> • Contenuti che sembrano provenire da una fonte autorevole, come ad esempio un'organizzazione giornalistica rispettabile, • Un evento di crisi, come un conflitto o un disastro naturale,



	<ul style="list-style-type: none"> ● Un personaggio pubblico che è: <ul style="list-style-type: none"> ○ essere degradati o molestati, o assumere un comportamento criminale o antisociale ○ prendere posizione su una questione politica, su un prodotto commerciale o su una questione di importanza pubblica (come le elezioni) ○ diffondere disinformazione su questioni di rilevanza pubblica <p>Inoltre, tutti i media AIGC o modificati, compresi quelli che ritraggono personaggi pubblici, come i politici, devono essere chiaramente etichettati come generati dall'IA e non possono essere utilizzati per sponsorizzazioni.</p> <p>Abbiamo un'etichetta per i contenuti generati dall'IA che consente agli utenti di informare facilmente la comunità quando pubblicano AIGC. L'etichetta può essere applicata a qualsiasi contenuto che sia stato completamente generato o modificato in modo significativo dall'IA, il che rende più facile rispettare l'obbligo di divulgare l'AIGC che mostra scene realistiche. I creatori possono farlo attraverso questa etichetta o attraverso altri tipi di divulgazione, come un adesivo, una filigrana o una didascalia.</p> <p>TikTok è anche orgogliosa di far parte della Content Authenticity Initiative (CAI) e della Coalition for Content Provenance and Authenticity (C2PA) ed è stata la prima piattaforma di condivisione video a mettere in pratica le Content Credentials. TikTok è in grado di leggere le Content Credentials che allegano metadati ai contenuti, che possiamo utilizzare per riconoscere ed etichettare istantaneamente AIGC. Questo aiuta la nostra funzionalità di etichettatura automatica per gli AIGC creati su altre piattaforme.</p>
<p>Eliminare la disinformazione dannosa dalla nostra piattaforma</p> <p><i>(Impegno 14, Misura 14.1)</i></p>	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>I nostri sforzi sostengono pratiche di creazione di contenuti trasparenti e responsabili, che sono rilevanti sia nel contesto del Conflitto che, più in generale, sulla nostra piattaforma.</p> <p>Descrizione dell'intervento</p> <p>Impieghiamo un approccio dinamico al rilevamento della disinformazione, sfruttando strategie multiple e sovrapposte per garantire una copertura completa e reattiva. Poniamo una notevole enfasi sulle strategie di moderazione proattiva dei contenuti, al fine di rimuovere la disinformazione dannosa che viola le nostre politiche prima che ci venga segnalata dagli utenti o da terzi.</p> <p>Interveniamo per rimuovere account o contenuti che contengono informazioni imprecise, fuorvianti o false che possono causare danni significativi agli individui o alla società, indipendentemente dalle intenzioni. In ambienti di conflitto, tali informazioni possono includere contenuti ripresi da conflitti passati, contenuti che fanno affermazioni false e dannose su eventi specifici o che incitano al panico. In determinate circostanze, possiamo ridurre l'importanza di tali contenuti.</p>



	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Nel contesto della crisi, abbiamo rimosso in modo proattivo oltre 8.700 video in H2 contenenti disinformazione dannosa relativa conflitto. Siamo riusciti a farlo grazie a una combinazione di automazione e moderazione umana. Effettuiamo controlli mirati su determinati tipi di contenuti (ad esempio, hashtag/elenchi di parole chiave sensibili) e lavoriamo a stretto contatto con i nostri partner di fact-checking, rispondendo alle tendenze emergenti da loro identificate.</p> <p>Abbiamo una moderazione dei contenuti in lingua araba ed ebraica, poiché riconosciamo l'importanza della lingua e del contesto culturale nel processo di moderazione della disinformazione.</p> <p>Metriche rilevanti:</p> <ul style="list-style-type: none">• Numero di video rimossi per violazione della politica di disinformazione con un proxy (IL/Hamas) - 9.633• Numero di video non raccomandati a causa della violazione della politica di disinformazione con un proxy (IL/Hamas) - 201• Numero di rimozioni proattive di video rimossi per violazione della politica di disinformazione con un proxy (IL/Hamas) 8.765
Responsabilizzare gli utenti	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
<p>Interventi di ricerca per aumentare la consapevolezza della potenziale disinformazione.</p> <p><i>(Impegno 21, Misura 21.1)</i></p>	<p>Descrizione dell'intervento</p> <p>Per ridurre al minimo la scopribilità della disinformazione e contribuire a proteggere i nostri utenti, abbiamo lanciato interventi di ricerca che si attivano quando gli utenti cercano termini neutrali relativi al Conflitto (ad esempio, Israele, Palestina). Valutiamo continuamente l'efficacia delle nostre parole chiave, aggiungendo o rimuovendo termini in base alla loro rilevanza.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Questi interventi di ricerca ricordano agli utenti di soffermarsi a controllare le fonti e li indirizzano anche verso risorse per il benessere.</p>
<p>Non promuovere in modo proattivo contenuti di tipo giornalistico ai nostri utenti.</p>	<p>Descrizione dell'intervento</p>



<i>(Impegno 18, Misura 18.1)</i>	<p>TikTok è principalmente una piattaforma di intrattenimento e non promuove attivamente contenuti di tipo giornalistico agli utenti su TikTok. Tuttavia, se un utente cerca attivamente e si impegna con contenuti di tipo giornalistico, è possibile che il feed "Per te" di un utente mostri nel tempo più contenuti di tipo giornalistico (ad esempio contenuti di tipo giornalistico relativi al Conflitto). Inoltre, il sistema di raccomandazione di TikTok offre un feed personalizzato di contenuti basato sul comportamento di coinvolgimento dell'utente nei confronti dei tipi di contenuti video; di conseguenza, il feed di ogni utente sarà diverso, in base alle sue preferenze. Queste preferenze sono dimostrate dai "mi piace", dalla durata della visione e da altre metriche correlate. Per maggiori informazioni sul funzionamento del nostro sistema di raccomandazione, vedere qui.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Il nostro approccio ai contenuti di tipo giornalistico sostiene i nostri sforzi per ridurre la diffusione di disinformazione dannosa relativa al Conflitto agli utenti.</p>
Responsabilizzare la comunità di ricerca	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
<p>Misure adottate per sostenere la ricerca sulla disinformazione e la disinformazione legate ai conflitti</p> <p><i>(Impegno 26, Misura 26.1 e 26.2)</i></p>	<p>Descrizione dell'intervento</p> <p>Attraverso la nostra API di ricerca, i ricercatori accademici di università no-profit negli Stati Uniti e in Europa possono richiedere di studiare i dati pubblici relativi ai contenuti e agli account di TikTok. Questi dati pubblici includono commenti, didascalie, sottotitoli e numero di commenti, condivisioni, like e preferiti che un video riceve, commenti dalla nostra piattaforma. Ulteriori informazioni sono disponibili qui.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Tra gennaio e giugno 2024 sono state approvate 2 domande API di ricerca relative al conflitto.</p>
Potenziare la comunità del Fact-Checking	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	



<p>Applicazione della nostra etichetta di contenuto non verificato per rendere il contenuto non idoneo alla raccomandazione</p> <p><i>(Impegno 31, Misura 31.2)</i></p>	<p>Descrizione dell'intervento</p> <p>Quando i nostri moderatori della disinformazione o i nostri partner per il fact-checking stabiliscono che il contenuto non può essere verificato in quel (cosa comune durante un'emergenza o un evento in corso), applichiamo la nostra etichetta di contenuto non verificato al contenuto per incoraggiare gli utenti a considerare l'affidabilità o la fonte del contenuto. L'applicazione dell'etichetta comporterà anche l'inammissibilità del contenuto alla raccomandazione, al fine di limitare la diffusione di informazioni potenzialmente fuorvianti.</p> <p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>La verifica di certe informazioni durante eventi dinamici e in rapido movimento come il Conflitto può essere impegnativa e i nostri moderatori e fact-checkers non possono sempre determinare in modo definitivo se i contenuti sono effettivamente disinformazione dannosa. Pertanto, per ridurre al minimo i rischi, quando i nostri fact-checker o i nostri moderatori non dispongono di informazioni sufficienti per verificare un contenuto potenzialmente fuorviante, applichiamo la nostra etichetta di contenuto non verificato per informare gli utenti che il contenuto è stato esaminato ma non può essere convalidato in modo definitivo. L'obiettivo è quello di sensibilizzare gli utenti sulla credibilità del contenuto e di ridurre la condivisione (vedi screenshot qui). La nostra etichetta di contenuto non verificato è disponibile per gli utenti in 23 lingue ufficiali dell'UE (più, per gli utenti del SEE, il norvegese e l'islandese).</p> <p>Quando viene applicata l'etichetta, il contenuto non potrà essere raccomandato nel feed "Per te" di nessuno, per limitare la diffusione di informazioni relative a eventi in corso, i cui dettagli sono ancora in fase di sviluppo e che possono essere potenzialmente fuorvianti.</p>
<p>Garantire una copertura di fact-checking</p> <p><i>(Impegno 30, Misura 30.1)</i></p>	<p>Descrizione dell'intervento</p> <p>Nell'ambito del nostro programma di fact-checking, TikTok collabora con oltre 20 organizzazioni di fact-checking accreditate dall'IFCN che supportano più di 50 lingue, tra cui l'ebraico e l'arabo, per aiutare a valutare l'accuratezza dei contenuti in questo ambiente in rapida evoluzione. Nel contesto del Conflitto, i nostri partner indipendenti di fact-checking seguono la nostra prassi standard, in base alla quale non moderano direttamente i contenuti su TikTok, ma valutano se un'affermazione è vera, falsa o priva di fondamento, in modo che i nostri moderatori possano prendere provvedimenti in base alle nostre Linee guida della comunità. Il contributo dei fact-checker viene poi incorporato nei nostri sforzi di moderazione dei contenuti in una serie di modi diversi, come ulteriormente illustrato nella sezione "indicazione dell'impatto" di seguito.</p> <p>Nel contesto del Conflitto, abbiamo anche modificato il nostro processo di consolidamento delle informazioni per consentirci di tenere traccia e archiviare le affermazioni relative al Conflitto separatamente dal nostro archivio globale di affermazioni precedentemente verificate. Ciò facilita l'accesso rapido ed efficace alle valutazioni pertinenti, che a sua volta aumenta l'efficacia dei nostri sforzi di moderazione. Continuiamo inoltre a migliorare il rilevamento dei discorsi d'odio con una banca di hash audio migliorata che ci aiuta a rilevare i suoni odiosi e con modelli di apprendimento automatico aggiornati per riconoscere i contenuti odiosi emergenti. Inoltre, abbiamo aumentato le risorse per la verifica dei fatti e ampliato il nostro programma di fact-checking collaborando con Fatabyyano per verificare i contenuti in Medio Oriente.</p>



	<p><i>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</i></p> <p>Per noi la disinformazione dannosa è diversa da altri problemi di contenuto. Il contesto e il fact-checking sono fondamentali per applicare in modo coerente e accurato le nostre politiche di disinformazione dannosa, ed è per questo che abbiamo assicurato che, nel contesto della crisi, il nostro programma di fact-checking copra l'arabo e l'ebraico.</p> <p>Come già detto, incorporiamo i contributi dei fact-checker nei nostri sforzi di moderazione dei contenuti più ampi in modi diversi:</p> <ul style="list-style-type: none"> ● Rapporti di approfondimento proattivi che segnalano le affermazioni nuove e in evoluzione che si vedono su Internet. Questo ci aiuta a individuare la disinformazione dannosa e ad anticipare le tendenze della disinformazione sulla nostra piattaforma. ● La collaborazione con i nostri partner di fact-checking per essere avvisati in anticipo delle narrazioni emergenti di disinformazione ha facilitato le risposte proattive contro le tendenze più dannose e ha contribuito a garantire che i nostri team di moderazione abbiano indicazioni aggiornate. ● Un archivio di affermazioni precedentemente verificate per aiutare i moderatori della disinformazione a prendere decisioni rapide e accurate. <p><i>Metriche rilevanti:</i></p> <ul style="list-style-type: none"> ● Numero di compiti di verifica dei fatti relativi a IL/Hamas - 1.061 ● Numero di video rimossi a seguito di una valutazione di fact checking con parole legate a IL/Hamas - 165 ● Numero di video retrocessi (NR) a seguito di una valutazione di fact checking con parole relative a IL/Hamas - 201
<p>Collaborare con i nostri partner per il fact-checking in relazione alle tendenze emergenti.</p> <p><i>(Impegno 31, Misura 31.1)</i></p>	<p><i>Descrizione dell'intervento</i></p> <p>Nel corso del Conflitto, i rappresentanti dei team di TikTok che si occupano delle politiche di disinformazione e dei prodotti si sono collegati regolarmente con i nostri partner esterni che si occupano di fact-checking, per ricevere informazioni anticipate sulle narrazioni emergenti di disinformazione, facilitando le risposte proattive contro le tendenze più dannose.</p> <hr/> <p><i>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</i></p> <p><i>Metriche rilevanti:</i></p> <ul style="list-style-type: none"> ● Numero di video rimossi per violazione della politica di disinformazione con un proxy (IL/Hamas) - 9.633



Segnalazione della risposta del firmatario durante un'elezione

Elezioni francesi 2024

Minacce osservate durante il elettorale: [limite di caratteri suggerito 2000 caratteri].

Abbiamo adottato misure complete per anticipare e affrontare i rischi associati ai processi elettorali, compresi i rischi associati alla disinformazione elettorale nel contesto delle elezioni lampo francesi tenutesi il 30 giugno e il 7 luglio 2024. In risposta all'annuncio delle elezioni lampo, è stato costituito un team elettorale di base e le consultazioni tra i team interfunzionali hanno contribuito a identificare e progettare le strategie di risposta.

TikTok non ha osservato minacce importanti durante le elezioni francesi; alcuni esempi di contenuti violenti che abbiamo interrotto con successo includono:

- Sono stati rilevati 636 tentativi di impersonificazione e sono stati fatti valere contro
- Un totale di 259 brevi messaggi video/fotografici sono stati applicati nei confronti di
- In totale sono stati applicati 19 ID audio contro
- Ci sono stati 46 ripristini di profilo

Mitigazioni in atto durante il elettorale: [limite di caratteri suggerito: 2000 caratteri].

Applicare le nostre politiche

(I) Capacità di moderazione

Abbiamo migliaia di professionisti della fiducia e della sicurezza che si dedicano a mantenere sicura la nostra piattaforma. Come di consueto, i nostri team hanno lavorato a fianco della tecnologia per garantire l'[applicazione delle nostre regole](#) costante per individuare e rimuovere la disinformazione, le operazioni di influenza occulta e altri contenuti e comportamenti che possono aumentare durante un periodo elettorale. Prima delle elezioni abbiamo effettuato un monitoraggio proattivo dei dati, il rilevamento delle tendenze e il monitoraggio regolare delle parole chiave e degli account arricchiti.

(II) Centro di controllo della missione: collaborazione interna interfunzionale

Il 17 giugno, in vista delle elezioni francesi, abbiamo istituito un Centro di Controllo Missione (MCC) dedicato che riunisce i dipendenti di diversi team specializzati del nostro dipartimento di sicurezza. Attraverso l'MCC, i nostri team sono stati in grado di fornire una copertura coerente e dedicata ai potenziali problemi legati alle elezioni nel periodo precedente e durante le elezioni francesi.



(III) Contrastare la disinformazione

I nostri moderatori della disinformazione ricevono una formazione e strumenti migliori per individuare e rimuovere la disinformazione e altri contenuti violenti. Abbiamo anche team sul campo che collaborano con esperti per garantire che il contesto e le sfumature locali si riflettano nel nostro approccio.

Nelle settimane che hanno preceduto e incluso le elezioni lampo, abbiamo rimosso oltre **1.200** video per aver violato le nostre politiche di integrità civica ed elettorale, e oltre **9.000** video per violazione delle nostre politiche di disinformazione. Abbiamo rimosso oltre **il 99%** dei contenuti di disinformazione violati prima che ci venissero segnalati.

(IV) Controllo dei fatti

Il nostro programma globale di fact-checking è una parte fondamentale del nostro approccio stratificato per individuare la disinformazione dannosa nel contesto delle elezioni. L'obiettivo principale del programma di fact-checking è sfruttare l'esperienza di organizzazioni esterne di fact-checking per contribuire a valutare l'accuratezza di affermazioni potenzialmente dannose e difficili da verificare.

TikTok collabora con [14 organizzazioni di fact-checking](#) in tutta Europa per valutare l'accuratezza dei contenuti nella maggior parte delle lingue europee, compreso il francese. [Agence France-Presse](#) (AFP) è il partner di fact-checking per la Francia, che ha fornito copertura alla piattaforma.

(V) Dissuadere le operazioni di influenza occulta

Vietiamo le operazioni di influenza occulta e rimaniamo costantemente vigili contro i tentativi di utilizzare comportamenti ingannevoli e di manipolare la nostra piattaforma. Cerchiamo in modo proattivo e indaghiamo continuamente su indizi di potenziali operazioni di influenza. Collaboriamo anche con le autorità governative e le incoraggiamo a condividere qualsiasi informazione in modo da poter lavorare insieme per garantire l'integrità delle elezioni. Maggiori dettagli sulla nostra politica contro le operazioni di influenza occulta sono pubblicati sul nostro [sito web](#).

(VI) Affrontare i contenuti ingannevoli generati dall'intelligenza artificiale

I creatori sono tenuti a etichettare qualsiasi contenuto realistico generato dall'IA (AIGC) e abbiamo un'[etichetta per i contenuti generati dall'IA](#) per aiutare le persone a farlo. TikTok ha una politica di "Media modificati e contenuti generati dall'intelligenza artificiale (AIGC)", che vieta che gli AIGC mostrino false fonti autorevoli o eventi di crisi, o che mostrino falsamente personaggi pubblici in determinati contesti, tra cui il bullismo, l'endorsement o l'approvazione.

(VII) Conti di governo, politici e partiti politici (GPPPA)

Molti leader politici, ministri e partiti politici sono presenti su TikTok. Questi politici e partiti svolgono un ruolo importante sulla nostra piattaforma: riteniamo che gli account verificati appartenenti a politici e istituzioni forniscano all'elettorato un'altra via di accesso ai propri rappresentanti e ulteriori voci fidate nella lotta comune contro la disinformazione.



Raccomandiamo vivamente alle GPPPA di far [verificare da TikTok](#) i propri account. I badge verificati aiutano gli utenti a fare scelte informate sugli account che scelgono di seguire. È anche un modo semplice per le figure di spicco di far sapere agli utenti stanno vedendo contenuti autentici e contribuisce a creare fiducia tra gli account di alto profilo e i loro follower.

Prima delle elezioni francesi abbiamo incontrato i responsabili della comunicazione dei partiti politici francesi per (i) fornire una panoramica delle politiche di TikTok per gli account politici, (ii) illustrare l'approccio di TikTok all'integrità delle elezioni e alla sicurezza dei dati, (iii) incoraggiare la verifica dell'account e (iv) consentire un contatto diretto per rispondere alle loro richieste specifiche.

Indirizzare le persone verso fonti affidabili

(I) Investire nell'alfabetizzazione mediatica

Investiamo in campagne di alfabetizzazione mediatica come strategia di controinformazione. TikTok ha collaborato con l'AFP in Francia per aiutare la comunità a navigare in sicurezza sulla piattaforma e a proteggersi dalla potenziale disinformazione durante le elezioni. L'AFP ha sviluppato una serie di video educativi che spiegano agli utenti come identificare ed evitare la disinformazione, utilizzare le funzioni di sicurezza di TikTok e valutare criticamente i contenuti relativi al processo elettorale. La comunità francese ha potuto trovare la serie di video con consigli pratici e informazioni utili sul processo elettorale nel relativo Centro elettorale.

Impegno esterno a livello nazionale e comunitario

(I) Sistema di risposta rapida: collaborazione esterna con i firmatari della BPCO

Il sistema di risposta rapida (RRS) del COPD è stato utilizzato per scambiare informazioni tra le organizzazioni della società civile, i verificatori di fatti e le piattaforme online. TikTok ha ricevuto 2 segnalazioni attraverso l'RRS prima delle elezioni francesi, che sono state rapidamente affrontate. Le azioni hanno incluso il divieto di account e la rimozione di contenuti per violazione delle linee guida della comunità.

(II) Coinvolgimento di esperti locali

Per promuovere ulteriormente l'integrità elettorale e informare il nostro approccio alle elezioni francesi, abbiamo organizzato una serie di interventi elettorali con AFP che ha condiviso le proprie intuizioni e competenze di mercato con i nostri team interni.

(III) Impegno con le autorità nazionali e le parti interessate

Per prepararsi alle elezioni francesi, le nostre Relazioni governative hanno rappresentato TikTok a un incontro ufficiale organizzato dalla Commissione UE con ARCOM prima delle elezioni, insieme ai rappresentanti di altre piattaforme online.

Abbiamo inoltre collaborato con il Servizio Informazioni del Governo francese (SIG) per includere le risorse ufficiali pertinenti nella guida elettorale in-app di TikTok.



Come già menzionato, abbiamo anche incontrato i responsabili della comunicazione dei partiti politici francesi per (i) fornire una panoramica delle politiche di TikTok per gli account politici, (ii) delineare l'approccio di TikTok all'integrità elettorale e alla sicurezza dei dati, (iii) incoraggiare la verifica degli account e (iv) consentire un contatto diretto per rispondere alle loro richieste specifiche.		
<p>[Nota: i firmatari sono invitati a fornire informazioni pertinenti alla loro particolare risposta alle minacce e alle sfide osservate sui loro servizi. Essi assicurano che le informazioni riportate di seguito forniscano un resoconto accurato e completo delle loro azioni pertinenti. Poiché le risposte operative alle situazioni di crisi/elezioni possono variare da un servizio all'altro, l'assenza di informazioni non deve essere considerata a priori una carenza nel modo in cui un particolare servizio ha risposto. Le metriche di impatto sono accurate al meglio delle capacità di misurazione dei firmatari].</p>		
Politiche e termini e condizioni		
Illustrare eventuali modifiche alle vostre politiche		
Politica	Modifiche (come nuove politiche introdotte, modifiche, adattamento dell'ambito o dell'implementazione)	Motivazione
N/D	N/D	
Controllo dei posizionamenti degli annunci		
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.		
Controllo delle inserzioni pubblicitarie, compreso il divieto di monetizzazione e di campagne di raccolta fondi per le GPPPA <i>(Impegno 1 e Misura 1.1)</i>	Descrizione dell'intervento Vietiamo la pubblicità politica, che è descritta in modo più dettagliato nella sezione Pubblicità politica di seguito. A tal fine, classifichiamo alcuni account TikTok come account di governo, politici e partiti politici (GPPPA). I GPPPA possono includere entità gestite dal governo, funzionari o candidati eletti, partiti politici, capi di stato o di governo attuali/ex. Quando gli account sono designati come GPPPA, viene loro vietato di inserire annunci su TikTok e di utilizzare le funzioni di monetizzazione. Abbiamo un'eccezione limitata in cui i governi possono essere autorizzati a fare pubblicità (ad esempio per una campagna di salute pubblica), a condizione che lavorino con un rappresentante commerciale di TikTok.	



	<p>Le sollecitazioni per la raccolta di fondi per la campagna elettorale da parte delle GPPPA non sono consentite sulla piattaforma. Ciò include contenuti come un video di un politico che chiede donazioni o un partito politico che indirizza le persone a una pagina di donazione sul proprio sito web. Forniamo ai titolari di account delle GPPPA informazioni sulle nostre politiche e sui nostri sistemi di moderazione e li incoraggiamo attivamente a verificare i loro profili. Per saperne di più, leggete qui.</p> <p>Per far rispettare queste politiche e la corretta etichettatura delle GPPPA, TikTok ha incontrato i responsabili della comunicazione dei partiti politici francesi per (i) fornire una panoramica delle politiche di TikTok per gli account politici, (ii) delineare l'approccio di TikTok all'integrità elettorale e alla sicurezza dei dati, (iii) incoraggiare la verifica degli account e (iv) consentire un contatto diretto per rispondere alle loro richieste specifiche.</p>
	<p style="text-align: center;">Indicazione dell'impatto, comprese le metriche pertinenti, se disponibili.</p> <p>Le nostre politiche specifiche per la GPPPA ci hanno aiutato a riconoscere l'interesse pubblico associato a questi account, pur ponendo dei paletti (ad esempio limitando la pubblicità e le funzioni di monetizzazione).</p>
<p style="text-align: center;">Pubblicità politica</p>	
<p>Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.</p>	
<p>Divieto di pubblicità politica (Impegno 5, Misura 5.1)</p>	<p>TikTok <u>vieta la pubblicità politica</u> sulla sua piattaforma.</p> <p>Riconosciamo che alcuni membri della nostra community potrebbero voler creare o partecipare a contenuti politici su TikTok e la condivisione di convinzioni politiche e la partecipazione a conversazioni politiche sono consentite come contenuti organici, a condizione che non violino le nostre Linee guida della community o la politica sui contenuti di marca. Tuttavia, gli utenti non possono pagare per pubblicizzare o promuovere questi contenuti.</p> <p>Inoltre, nel tentativo di preservare l'integrità della piattaforma e la sicurezza delle persone che la utilizzano, gli account appartenenti a politici o partiti politici non possono fare pubblicità o guadagnare su TikTok.</p> <p>Non consentiamo la promozione politica a pagamento, la pubblicità politica o la raccolta di fondi da parte di politici e partiti politici (per se stessi o per altri). La nostra politica sugli annunci politici vieta sia gli annunci tradizionali a pagamento sia i creatori che vengono pagati per realizzare contenuti politici di marca. Questa è una politica consolidata di TikTok dal 2019. Non consentiamo contenuti a pagamento o di marca che promuovano o si oppongano a un candidato, a un leader attuale, a un partito o gruppo politico o a una questione a livello federale, statale o locale, compresi gli annunci legati alle elezioni, gli annunci di sostegno o gli annunci su questioni. Ciò significa che gli account che identifichiamo come appartenenti a politici e partiti politici (ad esempio, GPPPA) hanno l'accesso alle funzioni pubblicitarie disattivato.</p>



	<p>Gli annunci vengono esaminati prima di essere visualizzati sulla nostra piattaforma. Se si ritiene che un annuncio violi le nostre rigorose politiche sugli annunci, compreso il divieto di annunci politici, non sarà consentito sulla nostra piattaforma. Esaminiamo anche gli annunci che ci vengono segnalati e, una volta esaminati, quelli che violano le norme vengono rimossi. La nostra comunità può anche segnalare, attraverso i nostri strumenti di segnalazione, gli annunci che ritiene violino le nostre regole, che i nostri team esamineranno e rimuoveranno in caso di violazione.</p> <p>Prendiamo estremamente sul serio la nostra responsabilità di garantire l'integrità elettorale. Ci impegniamo a combattere la disinformazione elettorale e a promuovere elezioni corrette. Abbiamo istituito pratiche per mitigare il rischio che la disinformazione dannosa abbia un impatto sull'integrità elettorale, ad esempio investendo in campagne di alfabetizzazione mediatica come strategia di controinformazione. Continuiamo a rivedere e migliorare regolarmente le nostre politiche e i nostri processi per combattere i tentativi sempre più sofisticati di diffondere la disinformazione e per rafforzare ulteriormente i nostri sistemi.</p> <p>Nel periodo in esame abbiamo anche lanciato un aggiornamento della nostra politica sulla pubblicità politica non dichiarata. Questo non ha modificato il nostro divieto di pubblicità politica, in vigore da tempo, ma ha introdotto una soluzione per limitare i contenuti di For you Feed che sono sospetti e non confermati di pubblicità politica.</p> <p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Vietando la pubblicità politica, contribuiamo a garantire alla nostra comunità un'esperienza TikTok creativa e autentica e riduciamo il rischio che la nostra piattaforma venga utilizzata per pubblicizzare e amplificare narrazioni che potrebbero essere divisive o false.</p> <ul style="list-style-type: none"> • Numero di annunci rimossi per le nostre politiche pubblicitarie politiche durante le 4 settimane che precedono e includono i giorni delle elezioni francesi (30 giugno e 7 luglio 2024) - 3.360
Integrità dei servizi	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Identificazione e rimozione delle reti CIO <i>(Impegno 14, Misura 14.1)</i>	Descrizione dell'intervento Durante le elezioni francesi abbiamo continuato a lavorare per individuare e interrompere le operazioni di influenza occulta (CIO) che tentano di insediarsi su TikTok e di minare l'integrità della nostra piattaforma. Per aumentare ulteriormente la trasparenza, la responsabilità e la condivisione intersettoriale, abbiamo introdotto rapporti dedicati alle operazioni di influenza occulta .



	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Durante il periodo di riferimento non abbiamo rilevato alcun CIO focalizzato sulle elezioni francesi. Tuttavia, continuiamo a rimuovere gli account dalle reti CIO precedentemente rivelate quando tentano di ristabilire una presenza sulla piattaforma e i nostri sforzi in tal senso sono resi noti mensilmente sulla nostra pagina di trasparenza CIO.</p>
<p>Affrontare i media fuorvianti dell'AIGC e dei media editati</p> <p><i>(Impegno 15, Misure 15.1 e 15.2)</i></p>	<p>Descrizione dell'intervento</p> <p>La nostra politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC) chiarisce che non vogliamo che i nostri utenti siano fuorviati su questioni politiche. Ai fini della nostra politica, AIGC si riferisce a contenuti creati o modificati dalla tecnologia dell'intelligenza artificiale (AI) o da processi di apprendimento automatico, che possono includere immagini di persone reali e mostrare scene dall'aspetto altamente realistico, o utilizzare un particolare stile artistico, come un dipinto, cartoni animati o anime.</p> <p>Non permettiamo che l'AIGC sia fuorviante o che i media editati mostrino falsamente:</p> <ul style="list-style-type: none"> ● Contenuto fatto sembrare proveniente da una fonte autorevole, come ad esempio un'organizzazione giornalistica rispettabile, ● Un evento di crisi, come un conflitto o un disastro naturale, ● Un personaggio pubblico che è: <ul style="list-style-type: none"> ○ essere degradati o molestati, o assumere un comportamento criminale o antisociale ○ prendere posizione su una questione politica, su un prodotto commerciale o su una questione di importanza pubblica (come le elezioni) ○ essere appoggiato o condannato politicamente da un individuo o da un gruppo. <p>Inoltre, tutti i media AIGC o modificati, compresi quelli che ritraggono personaggi pubblici, come i politici, devono essere chiaramente etichettati come generati dall'IA e non possono essere utilizzati per sponsorizzazioni.</p> <p>Con l'evoluzione dell'IA, continuiamo a investire nella lotta contro l'AIGC dannosa, evolvendo i nostri modelli di rilevamento proattivo, consultando esperti e collaborando con i colleghi per soluzioni condivise.</p> <p>TikTok ha investito in tecnologie e strumenti di etichettatura, tra cui l'implementazione della tecnologia Content Credentials della Coalition for Content Provenance and Authenticity (C2PA), che permette il riconoscimento automatico e l'etichettatura di Contenuti generati dall'intelligenza artificiale. A ciò si aggiunge uno strumento sviluppato da TikTok che consente ai creatori di etichettare facilmente i contenuti generati dall'IA, già utilizzato da 37 milioni di creatori. L'impegno di TikTok per la trasparenza dell'AIGC garantisce un ambiente sicuro per gli utenti, che possono facilmente identificare i contenuti sintetici e comprenderne il contesto.</p> <p>TikTok è membro della Content Authenticity Initiative e della Coalition for Content Provenance and Authenticity ed è stata la prima piattaforma di condivisione video a mettere in pratica le Content Credentials. Siamo in grado di leggere le Content Credentials che allegano metadati ai contenuti, che possiamo utilizzare per riconoscere ed etichettare istantaneamente AIGC. Questo ci ha aiutato a estendere l'etichettatura automatica agli AIGC creati su altre piattaforme.</p>



	<div>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</div> <div>Numero di video rimossi per violazione della nostra politica sui media modificati e dell'AIGC durante le settimane precedenti le elezioni francesi (tenendo conto che le elezioni lampo sono state indette solo il 9 giugno 2024) e compresi i giorni delle elezioni europee francesi (30 giugno e 7 luglio 2024) - 469</div>
Responsabilizzare gli utenti	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Realizzazione di campagne di alfabetizzazione ai media (Impegno 17, Misura 17.2)	<div>Descrizione dell'intervento</div> <div>Tiktok aveva un Centro elettorale in app dedicato alle elezioni francesi. In collaborazione con le commissioni elettorali e le organizzazioni della società civile, i centri elettorali hanno messo in contatto le persone con informazioni affidabili sul voto, tra cui quando, dove e come votare, i requisiti di eleggibilità dei candidati e, infine, i risultati delle elezioni.</div> <div>Il Centro elettorale conteneva una sezione dedicata all'alfabetizzazione mediatica che forniva consigli e risorse su come identificare la disinformazione e migliorare le competenze mediatiche. Questa sezione comprendeva video dei nostri partner di fiducia per il fact-checking e dell'organismo locale di alfabetizzazione mediatica Agence France-Presse (AFP).</div> <div>Abbiamo indirizzato le persone verso i Centri elettorali attraverso suggerimenti su video, LIVE e ricerche relative alle elezioni,</div>
	<div>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</div> <div>Il Centro elettorale lanciato prima delle elezioni francesi è stato visitato 1.578.583 volte e i banner di ricerca sono stati visualizzati 15.712.577 volte.</div>
Coinvolgimento di esperti locali e regionali (Impegno 17, Misura 17.2)	<div>Descrizione dell'intervento</div> <div>Per promuovere ulteriormente l'integrità elettorale e informare il nostro approccio alle elezioni francesi, il 26 giugno 2024 abbiamo organizzato una Election Speaker Series con AFP che ha condiviso le proprie intuizioni e competenze di mercato con i nostri team interni.</div>



	<p>I nostri partner per il fact-checking e gli enti locali per l'alfabetizzazione mediatica hanno anche sostenuto TikTok nel lancio dei Centri elettorali, che presentavano video da loro realizzati. Questo approccio localizzato ha contribuito a garantire che la messaggistica relativa alle elezioni francesi fosse rilevante per la nostra comunità e ha incoraggiato un maggiore coinvolgimento.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Questo impegno con esperti esterni regionali e locali ci ha permesso di informare il nostro approccio a livello nazionale alle elezioni francesi.</p>
Responsabilizzare la comunità di ricerca	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Fornire l'accesso alla nostra API di ricerca (<i>impegno 26 e Misure 26.1 e 26.2</i>)	<p>Descrizione dell'intervento</p> <p>Attraverso la nostra API di ricerca, i ricercatori accademici di università no-profit negli Stati Uniti e in Europa possono richiedere di studiare i dati pubblici relativi ai contenuti e agli account di TikTok. Questi dati pubblici includono commenti, didascalie, sottotitoli, numero di commenti, condivisioni, like e preferiti che un video riceve e commenti dalla nostra piattaforma. Maggiori informazioni sono disponibili qui.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Numero di domande API di ricerca relative alle elezioni francesi approvate da luglio a dicembre 2024: 1</p>
Potenziare la comunità del Fact-Checking	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Garantire la copertura del fact-checking (<i>Impegno 30, Misura 30.1</i>)	<p>Descrizione dell'intervento</p> <p>Agence France-Presse (AFP) è il partner per il fact-checking per la Francia, che ha fornito la copertura per la piattaforma.</p>

	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Numero di video esaminati dai partner di fact-checking nelle settimane precedenti le elezioni francesi: 161</p>
--	--



Segnalazione della risposta del firmatario durante un'elezione

Elezioni presidenziali rumene del 2024

Minacce osservate durante il elettorale: [limite di caratteri suggerito 2000 caratteri].

In qualità di co-presidente del gruppo di lavoro sulle elezioni del Codice di condotta sulla disinformazione, TikTok prende molto seriamente il ruolo di [proteggere l'integrità delle elezioni](#) sulla propria piattaforma. Abbiamo adottato misure complete per anticipare e affrontare i rischi associati ai processi elettorali, compresi i rischi associati alla disinformazione elettorale nel contesto delle elezioni rumene che si sono svolte il 24 novembre 2024.

Di seguito sono riportati alcuni esempi di minacce che TikTok ha osservato in relazione alle elezioni presidenziali rumene:

- TikTok ha riferito di aver rimosso sei reti CIO nel 2024, identificate come specificamente rivolte a un pubblico rumeno. Ulteriori informazioni sulle interruzioni di rete sono pubblicate sulla nostra [pagina alla trasparenza delle operazioni di Influenza Occulta](#) dedicata .
- Oltre a queste reti, vale la pena sottolineare le nostre difese più ampie contro le campagne di influenza occulta in tutta Europa. Nel settembre 2024, abbiamo intrapreso un'azione globale contro una rete segreta collegata a Sputnik Media. Quando eliminiamo tali reti, continuiamo a monitorare eventuali tentativi di riemergere. Nell'ambito della nostra strategia antirecidiva, nel novembre 2024 abbiamo rimosso 11 account ritenuti associati a Sputnik Media e rivolti al pubblico rumeno e moldavo.
- Dalla fine di ottobre abbiamo rimosso in modo proattivo più di 5.500 contenuti legati alle elezioni in Romania per violazione delle nostre politiche di disinformazione, molestie e incitamento all'odio.
- Abbiamo ricevuto 11 notifiche attraverso il sistema di risposta rapida del COPD in relazione alle elezioni presidenziali rumene, che sono state rapidamente affrontate. Le azioni hanno incluso il divieto o il geo-blocco di account e la rimozione di contenuti per violazione delle linee guida della comunità.



Mitigazioni in atto durante il elettorale: [limite di caratteri suggerito: 2000 caratteri].

A. Applicazione delle nostre politiche

(I) Capacità di moderazione

I nostri team hanno lavorato insieme alla tecnologia per garantire l'[applicazione delle nostre regole](#) costante per individuare e rimuovere la disinformazione, le operazioni di influenza occulta e altri contenuti e comportamenti che possono aumentare durante un periodo elettorale. Continuiamo a dare priorità e a migliorare la tecnologia di moderazione automatica di TikTok, in quanto tale tecnologia consente una rimozione più rapida e coerente dei contenuti che violano le nostre regole. Investiamo in tecnologie che migliorano la comprensione dei contenuti e prevedono i rischi potenziali, in modo da poter intervenire sui contenuti violati prima che vengano visualizzati.

Abbiamo migliaia di professionisti della fiducia e della sicurezza che si dedicano a mantenere sicura la nostra piattaforma. Abbiamo 99 moderatori di lingua rumena, il più grande team di questo tipo tra le piattaforme digitali del Paese, sia in termini assoluti che in relazione al numero di utenti. Abbiamo aumentato le risorse della nostra task force per le elezioni rumene, aggiungendo più di 120 esperti in materia in diversi team, tra cui Comportamento ingannevole (che comprende gli analisti di Covert Influence Operations), Sicurezza e Integrità degli annunci.

(II) Centro di controllo della missione: collaborazione interna interfunzionale

Il 23 ottobre 2024, prima del periodo ufficiale di campagna elettorale per le elezioni presidenziali rumene, abbiamo istituito un Centro di Controllo Missione (MCC) dedicato, che comprendeva dipendenti di diversi team specializzati all'interno del nostro dipartimento di sicurezza. Attraverso l'MCC, i nostri team sono stati in grado di fornire una copertura costante e dedicata a potenziali problemi legati alle elezioni nel periodo precedente e durante le elezioni presidenziali rumene.

(III) Contrastare la disinformazione

I nostri moderatori della disinformazione ricevono una formazione e strumenti migliori per individuare e rimuovere la disinformazione e altri contenuti violenti. Abbiamo anche team sul campo che collaborano con esperti per garantire che il contesto locale e le sfumature si riflettano nel nostro approccio. Abbiamo anche integrato le più recenti intuizioni dei nostri partner esperti nelle nostre politiche e linee guida sulla disinformazione e l'impersonificazione. Tra la fine di ottobre e il 17 dicembre 2024 abbiamo rimosso più di 5.500 contenuti legati alle elezioni in Romania per violazione delle nostre politiche di disinformazione, molestie e incitamento all'odio.

(IV) Controllo dei fatti

Il nostro programma globale di fact-checking è una parte fondamentale del nostro approccio stratificato per individuare la disinformazione dannosa nel contesto delle elezioni. L'obiettivo principale del programma di fact-checking è quello di sfruttare l'esperienza di organizzazioni esterne di fact-checking per aiutare a valutare l'accuratezza di affermazioni potenzialmente dannose difficili da verificare. TikTok collabora con [14 organizzazioni di fact-checking](#) in tutta Europa per valutare l'accuratezza dei contenuti nella maggior parte delle lingue europee, compreso il rumeno. **LeadStories**, che è un membro verificato dell'International Fact-Checking Network e dell'European Fact-Checking Network. Fact-Checking Standards Network è il partner di fact-checking per la Romania, che ha fornito copertura alla piattaforma, anche nei fine settimana.



(V) Dissuadere le operazioni di influenza occulta

Vietiamo le operazioni di influenza occulta e rimaniamo costantemente vigili contro i tentativi di utilizzare comportamenti ingannevoli e di manipolare la nostra piattaforma. Cerchiamo in modo proattivo e indaghiamo continuamente su indizi di potenziali operazioni di influenza. Collaboriamo anche con le autorità governative e le incoraggiamo a condividere qualsiasi informazione in modo da poter lavorare insieme per garantire l'integrità delle elezioni. Maggiori dettagli sulla nostra politica contro le operazioni di influenza occulta sono pubblicati sul nostro [sito web](#).

(VI) Affrontare i contenuti ingannevoli generati dall'intelligenza artificiale

I creatori sono tenuti a etichettare qualsiasi contenuto realistico generato dall'IA (AIGC) e abbiamo un'[etichetta per i contenuti generati dall'IA](#) per aiutare le persone a farlo. TikTok ha una politica di "Media modificati e contenuti generati dall'intelligenza artificiale (AIGC)", che vieta che gli AIGC mostrino false fonti autorevoli o eventi di crisi, o che mostrino falsamente personaggi pubblici in determinati contesti, tra cui il bullismo, l'endorsement o l'approvazione.

(VII) Conti di governo, politici e partiti politici (GPPPA)

Classifichiamo gli account dei candidati presidenziali come account di governo, politici e partiti politici ([GPPPA](#)). Applichiamo quindi politiche specifiche ai GPPPA per garantire la giusta esperienza, dato il loro importante ruolo nei processi civici. Ciò include la disabilitazione delle funzioni di monetizzazione.

Raccomandiamo vivamente di [verificare](#) le GPPPA. I badge verificati aiutano gli utenti a fare scelte informate sugli account che scelgono di seguire. È anche un modo semplice per le figure di spicco di far sapere agli utenti stanno vedendo contenuti autentici e contribuisce a creare fiducia tra gli account di alto profilo e i loro follower.

Prima delle elezioni, il team GR di TikTok ha organizzato sessioni dedicate con ogni gruppo politico in Romania per informare sulle nostre politiche ed educare gli attori politici alle misure di sicurezza. TikTok ha inoltre richiesto alle autorità rumene di fornire un elenco di candidati per garantire la corretta applicazione del marchio GPPPA, ove pertinente.

B. Indirizzare le persone verso fonti affidabili

(I) Investire nell'alfabetizzazione mediatica

Investiamo in campagne di alfabetizzazione mediatica come strategia di controinformazione. TikTok ha collaborato con l'ONG locale Funky Citizens in Romania per aiutare la comunità a navigare in sicurezza sulla piattaforma e a proteggersi dalla potenziale disinformazione durante le elezioni. Funky Citizens ha sviluppato una serie di video educativi che spiegano agli utenti come identificare ed evitare la disinformazione, utilizzare le funzioni di sicurezza di TikTok e valutare criticamente i contenuti relativi processo elettorale. La comunità rumena ha potuto trovare la serie di video con consigli pratici e informazioni utili sul processo elettorale sull'account ufficiale TikTok di Citizens Funky e sull'in-app Election Center dedicato alle elezioni rumene. Questi video sono stati visualizzati 47.855.301 volte tra novembre 2024 e dicembre 2024.



C. Impegno esterno a livello nazionale ed europeo

(I) Sistema di risposta rapida: collaborazione esterna con i firmatari della BPCO

Il sistema di risposta rapida (RRS) del COPD è stato utilizzato per scambiare informazioni tra le organizzazioni della società civile, i verificatori di fatti e le piattaforme online. TikTok ha ricevuto 11 notifiche attraverso l'RRS in relazione alle elezioni rumene, che sono state affrontate e gestite; l'applicazione ha incluso il divieto o il geo-blocco di account e la rimozione di contenuti per violazione delle linee guida della comunità.

(II) Coinvolgimento di esperti locali

Per promuovere ulteriormente l'integrità elettorale e informare il nostro approccio alle elezioni presidenziali rumene, abbiamo organizzato una Election Speaker Series con Funky Citizens, che ha condiviso le sue intuizioni e la sua esperienza di mercato con i nostri team interni.

(III) Impegno con le autorità nazionali prima delle elezioni

GR ha organizzato in modo proattivo un incontro dedicato alle elezioni il 22 ottobre 2024 con l'ANCOM, l'Autorità elettorale permanente e il Ministero della Ricerca, dell'Innovazione e della Digitalizzazione per stabilire punti di contatto prima delle elezioni e offrire l'accesso ai nostri strumenti di segnalazione e proporre una cooperazione congiunta per la creazione di un centro elettorale. In occasione di questo incontro, TikTok ha richiesto una lista di candidati per assicurarsi di poter applicare il nostro marchio GPPPA dove necessario.

Il 14 novembre 2024, TikTok, in collaborazione con il Ministero della Ricerca, dell'Innovazione e della Digitalizzazione, ha organizzato una sessione in loco sull'interruzione delle operazioni di influenza occulta. All'incontro hanno partecipato esperti rumeni del Ministero, dell'ANCOM, del DNSC e della Polizia. I rappresentanti di TikTok hanno illustrato l'approccio di TikTok ai rischi posti dalle CIO e hanno condiviso le loro conoscenze professionali.

(III) Impegno con le autorità e le parti interessate nazionali e con le autorità dell'UE dopo le elezioni

Il primo turno delle elezioni presidenziali si è tenuto il 24 novembre 2024. Subito dopo sono emerse preoccupazioni per i risultati delle elezioni e il sospetto di una campagna online non autentica volta a mobilitare gli elettori a favore di un candidato.

Il 29 novembre 2024 TikTok ha partecipato a una tavola rotonda della Commissione europea con il coordinatore rumeno dei servizi digitali ANCOM, le autorità statali competenti, le organizzazioni della società civile e altre piattaforme per discutere della situazione delle elezioni rumene e delle misure adottate dalle piattaforme per contribuire a proteggere l'integrità elettorale.

Il 3 dicembre 2024 abbiamo risposto pubblicamente alle domande dei legislatori della Commissione per il mercato interno e la protezione dei consumatori del Parlamento europeo.

<p>Il 5 dicembre 2024 la Commissione europea ha emesso un "ordine di conservazione" nei confronti di TikTok, imponendogli di conservare i dati relativi ai rischi il suo servizio potrebbe potenzialmente rappresentare per i processi elettorali e il discorso civico nell'UE. L'ordine fa seguito alle informazioni ricevute dalla Commissione nel contesto elezioni rumene.</p> <p>Il 6 dicembre 2024 la Corte costituzionale della Romania ha esercitato il suo potere in base alla Costituzione rumena e ha deciso di annullare l'intero processo elettorale per l'elezione del Presidente della Romania.</p> <p>Il 17 dicembre 2024, la Commissione europea ha avviato un procedimento formale contro TikTok per rischi elettorali ai sensi della DSA nel contesto delle elezioni presidenziali rumene. La decisione di aprire un'indagine ha tenuto conto delle informazioni ricevute autorità rumene attraverso rapporti di intelligence declassificati, nonché di rapporti di terzi. TikTok sta collaborando pienamente con la CE in relazione all'indagine.</p> <p>Più in generale, ci siamo impegnati con le autorità competenti in Romania in relazione alla situazione delle elezioni presidenziali e le abbiamo incoraggiate a condividere qualsiasi informazione in modo da poter lavorare insieme per garantire l'integrità delle elezioni. TikTok ha anche risposto alle richieste di contenuti da parte delle autorità, compresa la CE, rispondendo alle loro domande specifiche sugli account e condividendo i dettagli delle nostre indagini.</p> <p>La Romania ha fissato una data per la ripetizione delle elezioni presidenziali. Il nuovo voto si terrà il 4 maggio, con un ballottaggio previsto due settimane dopo, il 18 maggio.</p>			
<p>[Nota: i firmatari sono invitati a fornire informazioni pertinenti alla loro particolare risposta alle minacce e alle sfide osservate sui loro servizi. Essi assicurano che le informazioni riportate di seguito forniscano un resoconto accurato e completo delle loro azioni pertinenti. Poiché le risposte operative alle situazioni di crisi/elezioni possono variare da un servizio all'altro, l'assenza di informazioni non deve essere considerata a priori una carenza nel modo in cui un particolare servizio ha risposto. Le metriche di impatto sono accurate al meglio delle capacità dei firmatari di misurarle].</p>			
Politiche e termini e condizioni			
Illustrare eventuali modifiche alle vostre politiche			
Politica	Modifiche (come nuove politiche introdotte, modifiche, adattamento dell'ambito o dell'implementazione)		Motivazione

Integrità e Politiche di autenticità (I&A)	N/a		
Controllo dei posizionamenti degli annunci			
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.			
Controllo delle inserzioni pubblicitarie, compreso il divieto di monetizzazione e di campagne di raccolta fondi per le GPPPA (Impegno 1 e Misura 1.1)	Descrizione dell'intervento		
	<p>Vietiamo la pubblicità politica, che è descritta in modo più dettagliato nella sezione Pubblicità politica di seguito. Classifichiamo gli account TikTok politici rilevanti come GPPPA, ad esempio enti governativi, funzionari o candidati eletti, partiti politici, capi di stato o di attuali/ex. Quando gli account sono designati come GPPPA, viene loro vietato di inserire annunci su TikTok e di utilizzare le funzioni di monetizzazione. Abbiamo un'eccezione limitata in cui i governi possono essere autorizzati a fare pubblicità (ad esempio, per un'iniziativa di campagna di salute pubblica), a condizione che lavorino con un rappresentante di TikTok.</p> <p>Anche le sollecitazioni per la raccolta di fondi per la campagna elettorale da parte delle GPPPA non sono consentite sulla piattaforma. Ciò include contenuti come un video di un politico che chiede donazioni o un partito politico che indirizza le persone a una pagina di donazione sul proprio sito web. Forniamo ai titolari di account delle GPPPA informazioni sulle nostre politiche e sui nostri sistemi di moderazione e li incoraggiamo attivamente a verificare i loro profili. Per saperne di più, leggete qui.</p> <p>Per far rispettare queste politiche, i nostri team di relazioni governative locali hanno identificato ed etichettato le GPPPA in Romania prima delle elezioni, assicurandosi anche che ogni singolo account di un candidato presidenziale fosse etichettato come GPPPA.</p>		
	Indicazione dell'impatto, comprese le metriche pertinenti, se disponibili.		
<p>Le nostre politiche specifiche per la GPPPA ci hanno aiutato a riconoscere l'interesse pubblico associato a questi account, ponendo al contempo dei paletti (ad esempio limitando la pubblicità e le funzioni di monetizzazione).</p>			
Pubblicità politica			



Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.

Divieto di pubblicità politica (*impegno 5*), *Misura 5.1*)

TikTok vieta la pubblicità politica sulla sua piattaforma.

Riconosciamo che alcuni membri della nostra community potrebbero voler creare o partecipare a contenuti politici su TikTok e pertanto la condivisione di convinzioni politiche e la partecipazione a conversazioni politiche sono consentite come contenuti organici, a condizione che non violino le nostre [Linee guida della community](#) o la [politica sui contenuti di marca](#). Tuttavia, gli utenti non possono pagare per pubblicizzare o promuovere questi contenuti. Inoltre, nel tentativo di preservare l'integrità della piattaforma e la sicurezza delle persone che la utilizzano, gli account appartenenti a [politici o partiti politici](#) non possono fare pubblicità o guadagnare su TikTok.

Non consentiamo la promozione politica a pagamento, la pubblicità politica o la raccolta di fondi da parte di politici e partiti politici (per se stessi o per altri). La nostra politica sugli annunci politici vieta sia gli annunci tradizionali a pagamento sia i creatori che vengono pagati per realizzare contenuti politici di marca. Questa è una [politica consolidata](#) di TikTok dal 2019. Non consentiamo contenuti a pagamento o di marca che promuovano o si oppongano a un candidato, a un leader attuale, a un partito o a un gruppo politico o a una questione a livello federale, statale o locale, compresi gli annunci legati alle elezioni, gli annunci di sostegno o gli annunci relativi alle questioni. Ciò significa che gli account che identifichiamo come appartenenti a politici e partiti politici (cioè GPPPA) hanno l'accesso alle funzioni pubblicitarie disattivato. Come già detto, abbiamo classificato ogni singolo account di un candidato alla presidenza come GPPPA, il che ci ha permesso di assoggettarlo alle politiche volte a prevenire l'uso improprio di alcune funzioni, tra cui quelle di monetizzazione.

Per far rispettare efficacemente il nostro divieto di pubblicità politica, disponiamo di solidi processi pre e post pubblicazione, attivi 24 ore su 24. In Romania, questi comprendono il rilevamento automatico e la moderazione umana, da parte di moderatori che ricevono una formazione specifica sulle nostre politiche di pubblicità politica. Vietiamo i contenuti politici sia nella [pubblicità a pagamento](#) (cioè quando TikTok riceve un compenso) sia nei [contenuti di marca](#) (ad esempio quando un individuo promuove un candidato o un partito in cambio di un pagamento o di qualsiasi altro incentivo). Rimuoviamo inoltre i contenuti che costituiscono contenuti di marca non divulgati sulla base di richieste basate su prove o informazioni credibili ottenute dalle autorità di regolamentazione competenti.

Gli annunci vengono esaminati prima di essere visualizzati sulla nostra piattaforma. Se si ritiene che un annuncio violi le nostre rigorose politiche sugli annunci, compreso il divieto di annunci politici, non sarà consentito sulla nostra piattaforma. Esaminiamo anche gli annunci che ci vengono segnalati e, una volta esaminati, quelli che violano le norme vengono rimossi. La nostra comunità può anche segnalare, attraverso i nostri strumenti di segnalazione, gli annunci che ritiene violino le nostre regole, che i nostri team esamineranno e rimuoveranno in caso di violazione.

Prendiamo estremamente sul serio la nostra responsabilità di garantire l'integrità elettorale. Ci impegniamo a combattere la disinformazione elettorale e a promuovere elezioni corrette. Abbiamo istituito pratiche per mitigare il rischio che la disinformazione dannosa abbia un impatto sull'integrità elettorale, ad esempio investendo in campagne di alfabetizzazione mediatica come strategia di controinformazione. Continuiamo a rivedere e migliorare regolarmente le nostre



	politiche e processi per combattere i tentativi sempre più sofisticati di diffondere la disinformazione e per ulteriormente i nostri sistemi.
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Vietando la pubblicità politica, contribuiamo a garantire alla nostra comunità un'esperienza TikTok creativa e autentica e riduciamo il rischio che la nostra piattaforma venga utilizzata per pubblicizzare e amplificare narrazioni che potrebbero essere divisive o false.</p> <ul style="list-style-type: none"> Numero di annunci rimossi per violazione delle nostre politiche di pubblicità politica in Romania durante le 4 settimane precedenti e il giorno delle elezioni presidenziali rumene: 2.743.
Integrità dei servizi	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Identificazione e rimozione delle reti CIO <i>(Impegno 14, Misura 14.1)</i>	<p>Descrizione dell'intervento</p> <p>Durante le elezioni presidenziali rumene abbiamo continuato a lavorare per individuare e interrompere le operazioni di influenza occulta (CIO) che tentano di stabilirsi su TikTok e di minare l'integrità della nostra piattaforma.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>TikTok ha potenziato le mitigazioni contro i comportamenti ingannevoli, tra cui lo spam, l'impersonificazione e le attività legate al falso impegno. Un esempio dei nostri sforzi in questo campo:</p> <ul style="list-style-type: none"> Dal 5 al 14 dicembre, abbiamo impedito 4.415.720 falsi like e 1.559.406 false richieste di follow e abbiamo bloccato 33.594 account di spam creati in Romania. Abbiamo anche rimosso: <ul style="list-style-type: none"> 900 account che si spacciano per candidati alle elezioni rumene e funzionari già eletti 92.958 conti falsi 616.548 Mi piace falsi 1.023.652 falsi seguaci Dal 15 al 30 dicembre abbiamo impedito la creazione di oltre 5,3 milioni di falsi like e di oltre 2,6 milioni di false richieste di follow e abbiamo bloccato più di 116.000 account di spam in Romania. Abbiamo anche rimosso: 59 account



	<p>impersonando account di governi, politici o partiti politici rumeni, +59.000 account falsi, +1,5 milioni di like falsi e +1,3 milioni di follower falsi.</p> <p>Come indicato in precedenza, abbiamo segnalato la rimozione di sei reti CIO nel 2024 che sono state identificate come specificamente rivolte a un pubblico rumeno, tra cui:</p> <ul style="list-style-type: none"> • Nel settembre 2024, <ul style="list-style-type: none"> ○ Una rete di 22 account operanti dalla Romania che ha cercato di colpire il pubblico rumeno per diffondere disinformazione e promuovere narrazioni critiche nei confronti del governo rumeno. • Nel novembre 2024, <ul style="list-style-type: none"> ○ Una rete di 78 account operanti dalla Romania che ha cercato di promuovere il candidato Călin Georgescu su TikTok. ○ Una rete di 12 account operanti dalla Romania che ha cercato di amplificare le narrazioni in rumeno favorevoli al candidato politico indipendente Mircea Geoană. • Nel dicembre 2024, <ul style="list-style-type: none"> ○ Una rete di 27.217 account operava attraverso un falso fornitore di engagement, che cercava di promuovere il partito politico AUR e il candidato indipendente Călin Georgescu attraverso la pubblicazione di commenti su larga scala. ○ Una rete di 68 account operava dalla Moldavia e si rivolgeva alla diaspora rumena in Romania cercando di promuovere l'urlo Ciocan e il Partito socialdemocratico. <p>Oltre a queste reti, vale la pena sottolineare le nostre difese più ampie contro le campagne di influenza occulta in Europa. Nel settembre 2024, abbiamo intrapreso un'azione globale contro una rete segreta collegata a Sputnik Media. Quando eliminiamo tali reti, continuiamo a monitorare eventuali tentativi di riemergere. Nell'ambito della nostra strategia antirecidiva, nel novembre 2024 abbiamo rimosso 11 account ritenuti associati a Sputnik Media e rivolti al pubblico rumeno e moldavo.</p> <p>Ulteriori informazioni relative alle interruzioni di rete di cui sopra sono pubblicate sulla nostra pagina alla trasparenza delle dedicate operazioni di influenza occulta.</p>
<p>Affrontare i media fuorvianti dell'AIGC e dei media editati</p> <p><i>(Impegno 15, Misure 15.1 e 15.2)</i></p>	<p style="text-align: center;">Descrizione dell'intervento</p> <p>La nostra politica sui media modificati e sui contenuti generati dall'intelligenza artificiale (AIGC) chiarisce che non vogliamo che i nostri utenti siano fuorviati su questioni politiche. Ai fini della nostra politica, AIGC si riferisce a contenuti creati o modificati dalla tecnologia dell'intelligenza artificiale (AI) o da processi di apprendimento automatico, che possono includere immagini di persone reali e mostrare scene dall'aspetto altamente realistico, o utilizzare un particolare stile artistico, come un dipinto, cartoni animati o anime.</p> <p>Non permettiamo che l'AIGC sia fuorviante o che i media editati mostrino falsamente:</p> <ul style="list-style-type: none"> • Contenuto fatto sembrare proveniente da una fonte autorevole, come ad esempio un'organizzazione giornalistica rispettabile,



	<ul style="list-style-type: none">● Un evento di crisi, come un conflitto o un disastro naturale,● Un personaggio pubblico che è:<ul style="list-style-type: none">○ essere degradati o molestati, o assumere un comportamento criminale o antisociale○ prendere posizione su una questione politica, su un prodotto commerciale o su una questione di importanza pubblica (come un'elezione)○ essere appoggiato o condannato politicamente da un individuo o da un gruppo. <p>Inoltre, tutti i media AIGC o modificati, compresi quelli che ritraggono personaggi pubblici, come i politici, devono essere chiaramente etichettati come generati dall'IA e non possono essere utilizzati per sponsorizzazioni.</p> <p>Con l'evoluzione dell'IA, continuiamo a investire nella lotta contro l'AIGC dannosa, evolvendo i nostri modelli di rilevamento proattivo, consultando esperti e collaborando con i colleghi per soluzioni condivise.</p> <p>TikTok ha investito in tecnologie e strumenti di etichettatura, tra cui l'implementazione della tecnologia Content Credentials della Coalition for Content Provenance and Authenticity (C2PA), che consente il riconoscimento e l'etichettatura automatica dei contenuti generati dall'intelligenza artificiale. A ciò si aggiunge uno strumento sviluppato da TikTok che consente ai creatori di etichettare facilmente i contenuti generati dall'IA, già utilizzato da 37 milioni di creatori. L'impegno di TikTok per la trasparenza dell'AIGC garantisce un ambiente sicuro per gli utenti, che possono facilmente identificare i contenuti sintetici e comprenderne il contesto.</p> <p>TikTok è membro della Content Authenticity Initiative e della Coalition for Content Provenance and Authenticity ed è stata la prima piattaforma di condivisione video a mettere in pratica le Content Credentials. Siamo in grado di leggere le Content Credentials che allegano metadati ai contenuti, che possiamo utilizzare per riconoscere ed etichettare istantaneamente AIGC. Questo ci ha aiutato a estendere l'etichettatura automatica agli AIGC creati su altre piattaforme.</p> <p>Queste misure sono supportate da collaborazioni strategiche con altre aziende tecnologiche leader per combattere la disinformazione generata dall'IA, tra cui la firma del Tech Accord a livello di settore per combattere l'uso ingannevole dell'IA nelle elezioni del 2024 Conferenza sulla sicurezza di Monaco di quest'anno. Inoltre, TikTok sostiene le nuove linee guida della Fondazione internazionale per i sistemi elettorali.</p>
	<p>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</p> <p>Numero di video rimossi per violazione della politica dei media sintetici e manipolati nelle 4 settimane precedenti le elezioni presidenziali rumene e nei giorni delle elezioni: 34</p>
Responsabilizzare gli utenti	

Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Diffusione di campagne di alfabetizzazione mediatica (Impegno 17, Misura 17.2)	<div>Descrizione dell'intervento</div> <p>TikTok aveva un Centro elettorale in-app dedicato alle elezioni presidenziali in Romania. Abbiamo aggiornato il nostro Centro elettorale in-app per collegarlo direttamente al sito web della Commissione elettorale, in modo che sia ancora più facile per le persone accedere a informazioni elettorali autorevoli. In linea con le migliori pratiche di alfabetizzazione mediatica, abbiamo anche aggiunto un promemoria per verificare l'accuratezza delle informazioni elettorali che le persone vedono online e non.</p> <p>TikTok ha inoltre collaborato con la ONG locale Funky Citizens per aiutare la comunità a navigare in sicurezza sulla piattaforma e a da potenziali disinformazioni durante le elezioni.</p> <p>Funky Citizens ha sviluppato una serie di video educativi che spiegano agli utenti come identificare ed evitare la disinformazione, utilizzare le funzioni di sicurezza di TikTok e valutare criticamente i contenuti relativi al processo elettorale. La comunità rumena ha potuto trovare la serie di video con consigli pratici e informazioni utili sul processo elettorale sull'account ufficiale TikTok di Funky Citizens e nel Centro elettorale.</p>
	<div>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</div> <p>Il Centro elettorale lanciato prima delle elezioni presidenziali è stato visitato più di 1.008.537 volte e i banner di ricerca sono stati visualizzati più di 21.733.061 volte.</p> <p>I video di Funky Citizens sono stati visualizzati 47.855.301 volte tra novembre 2024 e dicembre 2024.</p>
Coinvolgimento di esperti locali e regionali (Impegno 17, Misura 17.2)	<div>Descrizione dell'intervento</div> <p>Per promuovere ulteriormente l'integrità elettorale e informare il nostro approccio alle elezioni presidenziali rumene, abbiamo organizzato una Election Speaker Series con Funky Citizens, che ha condiviso le sue intuizioni e la sua esperienza di mercato con i nostri team interni.</p> <p>I nostri partner per il fact-checking e gli enti locali per l'alfabetizzazione mediatica hanno anche sostenuto il nostro lancio dell'Election Center, che includeva i loro video. Questo approccio localizzato ha contribuito a garantire che i messaggi fossero rilevanti per la nostra comunità e ha incoraggiato un maggiore coinvolgimento.</p>
	<div>Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili.</div>

	Questo impegno con esperti esterni regionali e locali ha permesso a TikTok di informare il suo approccio alle elezioni presidenziali rumene.
Responsabilizzare la comunità di ricerca	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Fornire l'accesso alla nostra API di ricerca (impegno 26 e Misure 26.1 e 26.2)	Descrizione dell'intervento Attraverso la nostra API di ricerca, i ricercatori accademici di università no-profit negli Stati Uniti e in Europa possono richiedere di studiare i dati pubblici relativi ai contenuti e agli account di TikTok. Questi dati pubblici includono commenti, didascalie, sottotitoli, numero di commenti, condivisioni, like e preferiti che un video riceve e commenti dalla nostra piattaforma. Maggiori informazioni sono disponibili qui .
	Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili. Numero di applicazioni API di ricerca relative alle elezioni presidenziali rumene che sono state approvate da giugno a dicembre 2024: 4
Potenziare la comunità del Fact-Checking	
Delineare gli approcci pertinenti a questo capitolo, evidenziando le somiglianze/comunità e le differenze con l'applicazione regolare della legge.	
Garantire copertura di fact-checking (Impegno 30, Misura 30.1)	Descrizione dell'intervento LeadStories è il partner di fact-checking per la Romania, che ha fornito copertura alla piattaforma, anche nei fine settimana precedenti alle elezioni presidenziali rumene.
	Indicazione dell'impatto (all'inizio dell'azione: impatto previsto), comprese le metriche pertinenti, se disponibili. Numero di compiti di fact-checking relativi a parole chiave assegnate per le elezioni presidenziali rumene: circa 6.