Martedì 20 ottobre 2020

P9_TA(2020)0274

Atto sui servizi digitali e questioni sollevate in materia di diritti fondamentali

Risoluzione del Parlamento europeo del 20 ottobre 2020 sull'atto sui servizi digitali e le questioni sollevate in materia di diritti fondamentali (2020/2022(INI))

(2021/C 404/03)

Il Parlamento europeo,

— visto il trattato sull'Unione europea (TUE), in particolare l'articolo 2,

— visto il trattato sul funzionamento dell'Unione europea (TFUE), in particolare gli articoli 16 e 114,

— vista la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 6, 7, 8, 11, 13, 21, 22, 23, 24, 26, 38 e 47,

— vista la direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico») ([1]),

— visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE («regolamento generale sulla protezione dei dati», GDPR) ([2]),

— vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche («direttiva relativa alla vita privata e alle comunicazioni elettroniche») ([3]),

— vista la direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi («direttiva sui servizi di media audiovisivi»), in considerazione dell'evoluzione delle realtà del mercato ([4]),

— vista la direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE ([5]) («direttiva sul diritto d'autore»),

— vista la raccomandazione (UE) 2018/334 della Commissione del 1º marzo 2018 sulle misure per contrastare efficacemente i contenuti illegali online ([6]),

— vista la valutazione della minaccia della criminalità organizzata su Internet (IOCTA), pubblicata da Europol il 18 settembre 2018,

— vista la pertinente giurisprudenza della Corte di giustizia dell'Unione europea,

— visto l'articolo 54 del suo regolamento,

— visti i pareri della commissione per il mercato interno e la protezione dei consumatori e della commissione per la cultura e l'istruzione,

— vista la relazione della commissione per le libertà civili, la giustizia e gli affari interni (A9-0172/2020),

([1]) GU L 178 del 17.7.2000, pag. 1.
([2]) GU L 119 del 4.5.2016, pag. 1.
([3]) GU L 201 del 31.7.2002, pag. 37.
([4]) GU L 303 del 28.11.2018, pag. 69.
([5]) GU L 130 del 17.5.2019, pag. 92.
([6]) GU L 63 del 6.3.2018, pag. 50.

Martedì 20 ottobre 2020

A. considerando che i diritti fondamentali, ad esempio la protezione della vita privata e dei dati personali, il principio di non discriminazione, nonché la libertà di espressione e di informazione, devono essere ancorati al centro di una politica dell'UE efficace e duratura in materia di servizi digitali; che tali diritti devono essere evidenti sia nella lettera della legge sia nello spirito della loro attuazione;

B. considerando che i tipi di servizi digitali e i ruoli dei fornitori di servizi digitali sono radicalmente cambiati da quando, 20 anni fa, è stata adottata la direttiva sul commercio elettronico;

C. considerando che solo i servizi digitali che rispettano i diritti fondamentali degli utenti possono conquistare la fiducia di questi ultimi, assicurando così sia la diffusione dei servizi sia un vantaggio competitivo e un modello aziendale stabile per le imprese;

D. considerando che le norme sulla protezione dei dati applicabili a tutti i fornitori che offrono servizi digitali nel territorio dell'UE sono state recentemente aggiornate e armonizzate in tutta l'UE con il regolamento generale sulla protezione dei dati; che le norme in materia di tutela della vita privata nell'ambito delle comunicazioni elettroniche, che costituiscono un sottoinsieme dei servizi digitali, rientrano nella direttiva relativa alla vita privata e alle comunicazioni elettroniche e sono attualmente oggetto di revisione;

E. considerando che la quantità di tutti i tipi di contenuti generati dagli utenti e condivisi e dei servizi forniti attraverso le piattaforme online, compresi i servizi cloud, è aumentata in modo esponenziale e a un ritmo senza precedenti, con l'aiuto delle tecnologie avanzate; che ciò include contenuti illegali, quali immagini di materiale pedopornografico online, nonché contenuti che, pur essendo legali, sono potenzialmente dannosi per la società e la democrazia, come la disinformazione sui rimedi contro la COVID-19;

F. considerando che la disinformazione e l'incitamento all'odio online si sono sempre più diffusi negli ultimi anni a causa di persone e soggetti perturbatori che utilizzano le piattaforme online per aumentare la polarizzazione, che a sua volta è sfruttata a fini politici; che le donne, le persone di colore, le persone appartenenti o percepite come appartenenti a minoranze etniche o linguistiche e le persone LGBTIQ sono spesso prese di mira da incitamenti all'odio discriminatorio, bullismo, minacce e ricerca di capri espiatori online;

G. considerando che tale tendenza è stata favorita da piattaforme online il cui modello commerciale si basa sulla raccolta e l'analisi dei dati degli utenti finalizzate a generare più traffico e visualizzazioni nonché, di conseguenza, più dati di profilazione e quindi più profitto; che ciò porta all'amplificazione dei contenuti sensazionalistici; che l'incitamento all'odio e la disinformazione danneggiano l'interesse pubblico compromettendo il dibattito pubblico rispettoso e onesto e pongono minacce alla sicurezza pubblica dal momento che possono suscitare violenza nel mondo reale; che contrastare tali contenuti è fondamentale per garantire il rispetto dei diritti fondamentali e difendere lo Stato di diritto e la democrazia nell'UE;

H. considerando che i social media e altre piattaforme di distribuzione dei contenuti utilizzano tecniche di profilazione per indirizzare in maniera mirata e distribuire i loro contenuti, nonché la pubblicità; che i dati raccolti dalle tracce digitali lasciate dalle persone possono essere estratti in modo tale da consentire un'inferenza altamente accurata di informazioni personali molto intime, specialmente quando tali dati sono combinati con altri insiemi di dati; che gli scandali di Cambridge Analytica e Facebook hanno mostrato i rischi associati a operazioni opache di trattamento dei dati da parte delle piattaforme online, rivelando che determinati elettori erano stati esposti a una propaganda politica micromirata e, talvolta, anche a una disinformazione mirata;

I. considerando che gli algoritmi automatizzati che decidono come trattare, rendere più o meno prioritari, distribuire e cancellare contenuti di terzi sulle piattaforme online, anche durante le campagne politiche ed elettorali, spesso riproducono modelli discriminatori esistenti nella società, determinando pertanto un rischio elevato di discriminazione per le persone già colpite; che l'utilizzo diffuso degli algoritmi per l'eliminazione o il blocco dei contenuti solleva altresì preoccupazioni in merito allo Stato di diritto nonché questioni di legalità, legittimità e proporzionalità;

J. considerando che un esiguo numero di fornitori di servizi principalmente non europei detiene un potere significativo sul mercato ed esercita un'influenza sui diritti e le libertà delle persone, sulle nostre società e le nostre democrazie controllando il modo in cui sono presentati informazioni, servizi e prodotti, il che ha notevoli ripercussioni sul

funzionamento degli Stati membri e sui loro cittadini; che le decisioni di tali piattaforme possono avere conseguenze di ampia portata per la libertà di espressione e di informazione e per la libertà e il pluralismo dei media;

K. considerando che finora l'approccio politico volto a contrastare i contenuti illegali online nell'UE si è concentrato principalmente sulla cooperazione volontaria e su rimozioni autorizzate da provvedimenti giudiziari, ma che un numero crescente di Stati membri sta adottando ulteriori normative a livello nazionale che affrontano i contenuti illegali in maniera non armonizzata; che disposizioni volte a far fronte a taluni tipi di contenuti illegali sono state inserite nella recente normativa settoriale a livello dell'UE;

L. considerando che un semplice approccio di autoregolamentazione delle piattaforme non garantisce un adeguato livello di trasparenza, responsabilità e sorveglianza; che un tale approccio non fornisce informazioni adeguate alle autorità pubbliche, alla società civile e agli utenti sul modo in cui le piattaforme affrontano i contenuti illegali e i contenuti che violano i loro termini e condizioni, né sul modo in cui curano i contenuti in generale;

M. considerando che un tale approccio può non garantire il rispetto dei diritti fondamentali e genera una situazione in cui le responsabilità in materia giudiziaria sono in parte affidate a privati, il che crea un rischio di interferenza con il diritto alla libertà di espressione;

N. considerando che la sorveglianza e la supervisione a livello normativo sono settoriali nell'UE; che sarebbe utile un ulteriore coordinamento più globale tra i diversi organismi di sorveglianza in tutta l'UE;

O. considerando che la carenza di dati pubblici solidi e comparabili sulla prevalenza dei contenuti illegali e dannosi online, sulle segnalazioni e la rimozione di tali contenuti autorizzata dal giudice e quella basata sull'autoregolamentazione, nonché sul seguito dato dalle autorità competenti crea una deficit di trasparenza e responsabilità, sia nel settore privato che in quello pubblico; che mancano informazioni sugli algoritmi utilizzati dalle piattaforme e dai siti web e sul modo in cui le piattaforme trattano la rimozione erronea dei contenuti;

P. considerando che lo sfruttamento sessuale dei minori online rappresenta una delle forme di contenuti illegali agevolate dagli sviluppi tecnologici; che la grande quantità di materiale pedopornografico che circola comporta gravi sfide nell'ambito degli sforzi di individuazione, indagine e, soprattutto, l'identificazione delle vittime; che secondo Europol, le segnalazioni ricevute dal Centro nazionale per i minori scomparsi e vittime di sfruttamento, negli Stati Uniti, concernenti condivisioni online di materiale pedopornografico sono aumentate del 106 % nell'ultimo anno;

Q. considerando che secondo la giurisprudenza della Corte di giustizia dell'Unione europea (CGUE) i contenuti dovrebbero essere rimosso a seguito di un provvedimento giudiziario emesso da uno Stato membro; che i prestatori di servizi di hosting possono ricorrere a strumenti e tecnologie di ricerca automatizzati per rilevare ed eliminare contenuti equivalenti ad altri che siano stati precedentemente dichiarati illeciti, ma non dovrebbero avere un obbligo generale di sorvegliare sulle informazioni che memorizzano né di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite, come previsto all'articolo 15, paragrafo 1, della direttiva 2000/31/CE;

R. considerando che un'identificazione elettronica affidabile è essenziale per garantire un accesso sicuro ai servizi digitali e per effettuare transazioni elettroniche in maniera più sicura; che attualmente solo 15 Stati membri hanno notificato alla Commissione il loro regime di identificazione per il riconoscimento transfrontaliero nel quadro del regolamento (UE) n. 910/2014 ([7]) («regolamento eIDAS»);

S. considerando che Internet e le sue piattaforme rappresentano tuttora una sede fondamentale per le attività dei gruppi terroristici e sono utilizzati come strumento per alimentare propaganda, reclutare proseliti e promuovere le attività di tali gruppi;

([7]) Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

Martedì 20 ottobre 2020

1. crede nei chiari vantaggi sociali ed economici di un mercato unico digitale funzionante per l'UE e i suoi Stati membri; accoglie con favore tali vantaggi, in particolare il migliore accesso alle informazioni e il rafforzamento della libertà di espressione; sottolinea l'importante obbligo di garantire un ecosistema digitale equo in cui siano rispettati i diritti fondamentali quali sanciti dai trattati e dalla Carta dei diritti fondamentali dell'Unione europea, specialmente la libertà di espressione e di informazione, la non discriminazione, la libertà e il pluralismo dei media, la vita privata e la protezione dei dati, e in cui sia garantita la sicurezza degli utenti online; evidenzia che gli interventi legislativi e gli altri interventi normativi nel mercato unico digitale volti a garantire il rispetto di tale obbligo dovrebbero limitarsi allo stretto necessario; ricorda che l'impiego di meccanismi di rimozione dei contenuti al di fuori delle garanzie previste per il giusto processo contravviene all'articolo 10 della Convenzione europea dei diritti dell'uomo;

2. esorta la Commissione ad adottare un approccio normativo su misura per affrontare le differenze tuttora esistenti tra il mondo online e quello offline nonché le sfide poste dalla diversità degli attori e dei servizi offerti online; ritiene essenziale, a tale proposito, applicare approcci normativi differenti ai contenuti illeciti e leciti; sottolinea che i contenuti illegali e i reati favoriti dall'informatica dovrebbero essere contrastati con lo stesso rigore e sulla base degli stessi principi giuridici applicati ai contenuti illegali e ai comportamenti criminali offline, e con le stesse garanzie per i cittadini; ricorda che la direttiva sul commercio elettronico è il quadro giuridico per i servizi online nel mercato interno che disciplina la gestione dei contenuti;

3. reputa necessario che i contenuti illegali siano rimossi rapidamente e costantemente per affrontare i reati e le violazioni dei diritti fondamentali; ritiene che i codici di condotta volontari affrontino solo in parte la questione;

4. invita i fornitori di servizi digitali a ritirare i contenuti dalla rete in modo diligente, proporzionato e non discriminatorio e tenendo conto, in ogni circostanza, dei diritti fondamentali degli utenti e dell'importanza fondamentale della libertà di espressione e di informazione in una società aperta e democratica, al fine di evitare la rimozione di contenuti che non sono illeciti; chiede ai fornitori di servizi digitali che di loro iniziativa intendono limitare alcuni contenuti leciti dei loro utenti di valutare la possibilità di etichettare tali contenuti, invece di ritirarli dalla rete, fornendo agli utenti la possibilità di scegliere, sotto la propria responsabilità, se accedervi o meno;

5. ritiene che qualsiasi misura di rimozione dei contenuti autorizzata giuridicamente nell'atto sui servizi digitali dovrebbe riguardare solo i contenuti illegali, quali definiti dal diritto dell'UE e nazionale, e che l'atto legislativo non dovrebbe includere concetti e termini indefiniti in quanto ciò creerebbe incertezza giuridica per le piattaforme online e metterebbe a rischio i diritti e la libertà di espressione;

6. riconosce, tuttavia, che l'attuale ecosistema digitale incoraggia anche comportamenti problematici, come il «micro-targeting» basato su caratteristiche che espongono vulnerabilità fisiche o psicologiche, la diffusione dell'incitamento all'odio, i contenuti razzisti e la disinformazione, i problemi emergenti quali l'abuso organizzato di molteplici piattaforme nonché la creazione di account o la manipolazione di contenuti online da parte di algoritmi; osserva con preoccupazione che alcuni modelli commerciali si basano sulla presentazione di contenuti sensazionalistici e polarizzanti agli utenti al fine di aumentare il tempo di visualizzazione e, pertanto, i profitti delle piattaforme online; sottolinea gli effetti negativi di tali modelli commerciali sui diritti fondamentali degli individui e per la società nel suo insieme; chiede trasparenza sulle politiche di monetizzazione delle piattaforme online;

7. evidenzia pertanto che la diffusione di tali contenuti dannosi dovrebbe essere contenuta; è fermamente convinto che, a tal fine, siano fondamentali l'alfabetizzazione mediatica, il controllo degli utenti sui contenuti loro proposti e l'accesso del pubblico a contenuti e a un'istruzione di elevata qualità; accoglie pertanto con favore l'iniziativa della Commissione di creare un Osservatorio europeo dei media digitali per sostenere servizi indipendenti di verifica dei fatti, aumentare la conoscenza del pubblico in merito alla disinformazione online e sostenere le autorità pubbliche incaricate di monitorare i media digitali;

8. invita la Commissione e gli Stati membri a sostenere i media indipendenti e di servizio pubblico nonché le campagne educative sull'alfabetizzazione mediatica e le campagne di sensibilizzazione mirate nell'ambito della società civile; rileva che è opportuno prestare particolare attenzione ai contenuti dannosi nel contesto dell'utilizzo di Internet da parte dei minori, in particolare in merito alla loro esposizione al cyberbullismo, alle molestie sessuali, alla pornografia, alla violenza o all'autolesionismo;

9. rileva che, dato che le attività online di un individuo forniscono informazioni approfondite sulla sua personalità e consentono di manipolarla, la raccolta generalizzata e indiscriminata di dati personali riguardo a ogni utilizzo di un servizio digitale interferisce in modo sproporzionato con il diritto alla tutela della vita privata e alla protezione dei dati personali; evidenzia, in particolare, il potenziale impatto negativo della pubblicità micro-mirata e comportamentale e della valutazione delle persone, in particolare dei minori e di gruppi vulnerabili, in quanto interferiscono nella vita privata degli individui, il che solleva questioni in merito alla raccolta e all'uso dei dati utilizzati per personalizzare la pubblicità, offrire prodotti o servizi o fissare prezzi; conferma che il diritto degli utenti a non essere oggetto di un tracciamento diffuso nell'utilizzo dei servizi digitali è stato incluso nel regolamento generale sulla protezione dei dati (GDPR) e dovrebbe essere adeguatamente applicato in tutta l'UE; osserva che la Commissione, nella sua proposta di un nuovo regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche (2017/0003(COD)), ha proposto di subordinare la cura mirata dei contenuti a un esplicito consenso;

10. ritiene che la pubblicità politica oscura o ingannevole sia una classe particolare di minaccia online poiché influenza i meccanismi essenziali che consentono il funzionamento della nostra società democratica, in particolare qualora tali contenuti siano sponsorizzati da terzi, compresi attori stranieri; sottolinea che, quando la profilazione è impiegata su ampia scala per il micro-targeting politico in modo da manipolare il comportamento di voto, può seriamente compromettere le basi della democrazia; invita pertanto i fornitori di servizi digitali ad adottare le misure necessarie a identificare ed etichettare i contenuti caricati da social bot e si attende che la Commissione fornisca orientamenti sull'uso di tali tecnologie digitali persuasive nelle campagne elettorali e nelle strategie di pubblicità politica; chiede, a tale riguardo, l'istituzione di rigorosi requisiti di trasparenza per la visualizzazione di pubblicità politica a pagamento;

11. ritiene necessario che i contenuti illegali siano rimossi in modo coerente e senza indebiti ritardi al fine di affrontare le violazioni, in particolare quelle relative ai minori e ai contenuti terroristici, e le violazioni dei diritti fondamentali con le garanzie necessarie, quali la trasparenza della procedura, il diritto di ricorso e l'accesso a un ricorso effettivo in sede giudiziaria; ritiene che i codici di condotta volontari e le condizioni di fornitura contrattuali standard non siano adeguatamente applicati e abbiano dimostrato di far fronte solo parzialmente alla questione; sottolinea che la responsabilità ultima di applicare la legge, decidere in merito alla legalità delle attività online e ordinare ai fornitori di servizi di hosting di rimuovere i contenuti illegali o di disabilitarne l'accesso spetta alle autorità indipendenti competenti;

12. riconosce il fatto che, sebbene possa essere facilmente stabilita la natura illegale di alcuni tipi di contenuti, la decisione è più difficile per altri tipi di contenuti in quanto richiedono una contestualizzazione; segnala che gli attuali strumenti automatizzati non sono in grado di effettuare analisi critiche e di comprendere adeguatamente l'importanza del contesto per specifici elementi del contenuto, il che potrebbe condurre a inutili rimozioni e danneggiare la libertà di espressione e l'accesso a informazioni diverse, anche sulle opinioni politiche, sfociando così nella censura; sottolinea che un controllo umano delle relazioni automatizzate da parte dei fornitori di servizi o dei loro contraenti non risolve pienamente il problema, specialmente se è esternalizzato a personale privato che non ha l'indipendenza, le qualifiche e la responsabilità sufficienti;

13. osserva con preoccupazione che i contenuti illegali online possono essere moltiplicati con facilità e rapidità e che, pertanto, il loro effetto negativo può essere amplificato in tempi molto brevi; ritiene tuttavia che la legge sui servizi digitali non dovrebbe imporre ai prestatori di servizi di hosting o altri intermediari tecnici l'obbligo di utilizzare strumenti automatizzati per la moderazione dei contenuti;

14. ricorda che i contenuti illegali online non dovrebbero essere soltanto rimossi dalle piattaforme online, ma dovrebbero essere altresì oggetto di un seguito da parte dalle autorità di contrasto e della magistratura qualora si tratti di atti criminali; invita la Commissione a valutare se obbligare le piattaforme online a segnalare i reati gravi alle autorità competenti, quando vengono a conoscenza di un tale reato; ritiene, a tale proposito, che un problema fondamentale in alcuni Stati membri sia il fatto di non avere soltanto casi irrisolti, ma anche casi non aperti; chiede la rimozione degli ostacoli alla presentazione di denunce presso le autorità competenti; è convinto che, data la natura transfrontaliera di Internet e la rapida diffusione dei contenuti illegali online, occorra migliorare e fondare sui principi di necessità e proporzionalità la cooperazione tra i fornitori di servizi e le autorità nazionali competenti, nonché la cooperazione transfrontaliera tra le autorità nazionali competenti; sottolinea, a tale riguardo, la necessità di rispettare l'ordinamento giuridico dell'UE e i principi consolidati della cooperazione transfrontaliera e della reciproca fiducia; invita gli Stati membri

a fornire alle rispettive autorità di contrasto e giudiziarie le competenze, le risorse e gli strumenti necessari per consentire loro di trattare in maniera efficace il crescente numero di casi che interessano i contenuti illegali online e la risoluzione delle controversie riguardanti il ritiro di contenuti dalla rete, nonché a migliorare l'accesso alla giustizia nel settore dei servizi digitali;

15. sottolinea che un contenuto specifico può essere considerato illegale in uno Stato membro ma rientrare nel diritto alla libertà di espressione in un altro; evidenzia che, per tutelare la libertà di parola, evitare conflitti tra leggi, scongiurare blocchi geografici ingiustificati e inefficaci e promuovere un mercato unico digitale armonizzato, ai fornitori di servizi di hosting non dovrebbe essere imposto di rimuovere o disabilitare l'accesso alle informazioni che sono lecite nello Stato membro in cui sono ubicati, o in cui risiede o è ubicato il loro rappresentante legale designato; ricorda che le autorità nazionali possono soltanto eseguire gli ordini di rimozione emanati dalle autorità competenti indipendenti indirizzati a prestatori di servizi stabiliti nel loro territorio; ritiene necessario rafforzare i meccanismi di cooperazione tra gli Stati membri con il sostegno della Commissione e delle pertinenti agenzie dell'Unione; chiede un dialogo strutturato tra gli Stati membri al fine di determinare il rischio di tipi specifici di contenuti e individuare potenziali differenze nella valutazione di tali rischi tra gli Stati membri;

16. sottolinea che i contenuti illeciti dovrebbero essere rimossi dal luogo in cui sono ospitati e che gli intermediari di semplice trasporto non dovrebbero essere tenuti a bloccare l'accesso ai contenuti;

17. è fermamente convinto che l'attuale quadro giuridico dell'UE che disciplina i servizi digitali dovrebbe essere aggiornato per affrontare le sfide poste dalla frammentazione tra gli Stati membri e dalle nuove tecnologie, come la prevalenza della profilazione e del processo decisionale algoritmico che permeano tutti gli ambiti della vita, nonché garantire la chiarezza giuridica e il rispetto dei diritti fondamentali, in particolare la libertà di espressione e il diritto alla vita privata in maniera adeguata alle esigenze future in considerazione del rapido sviluppo della tecnologia;

18. accoglie con favore l'impegno della Commissione volto a introdurre un approccio armonizzato in materia di obblighi per i fornitori di servizi digitali, compresi gli intermediari online, al fine di evitare la frammentazione del mercato interno e l'applicazione incoerente delle normative; invita la Commissione a proporre le soluzioni più efficienti ed efficaci per il mercato interno nel suo complesso, adoperandosi al contempo per evitare nuovi inutili oneri amministrativi e far sì che il mercato unico digitale rimanga aperto, equo, sicuro e competitivo per tutti i suoi partecipanti; sottolinea che il regime di responsabilità per i fornitori di servizi digitali deve essere proporzionato, non deve sfavorire i fornitori piccoli e medi e non deve limitare irragionevolmente l'innovazione e l'accesso alle informazioni;

19. ritiene che la riforma dovrebbe basarsi sulle solide fondamenta e il pieno rispetto del diritto vigente dell'UE, in particolare del regolamento generale sulla protezione dei dati e della direttiva relativa alla vita privata e alle comunicazioni elettroniche, attualmente in fase di revisione, e rispettare il primato di altri strumenti settoriali come la direttiva sui servizi di media audiovisivi; sottolinea che la modernizzazione delle norme sul commercio elettronico può incidere sui diritti fondamentali; esorta pertanto la Commissione a essere estremamente vigile nel suo approccio nonché a integrare nella sua revisione le norme internazionali in materia di diritti umani;

20. sottolinea che la capacità pratica dei singoli utenti di comprendere la complessità degli ecosistemi di dati e di orientarsi al loro interno è estremamente limitata, analogamente alla loro capacità di stabilire se le informazioni che ricevono e i servizi che utilizzano siano resi loro disponibili alle stesse condizioni di altri utenti; invita pertanto la Commissione a porre la trasparenza e la non discriminazione al centro della legge sui servizi digitali;

21. insiste affinché la legge sui servizi digitali debba mirare ad assicurare un elevato livello di trasparenza in merito al funzionamento dei servizi online e un ambiente digitale privo di discriminazione; sottolinea che, oltre al solido quadro normativo esistente che tutela la vita privata e i dati personali, è necessario prevedere un obbligo per le piattaforme online al fine di garantire l'uso legittimo degli algoritmi; invita pertanto la Commissione a sviluppare un regime basato sulla direttiva relativa al commercio elettronico che definisca chiaramente la responsabilità dei fornitori di servizi per affrontare i rischi cui sono esposti i loro utenti e tutelare i loro diritti prevedendo un obbligo di trasparenza e spiegabilità degli algoritmi, sanzioni per far rispettare tali obblighi, la possibilità di un intervento umano e altre misure quali audit annuali indipendenti e prove di stress specifiche per favorire e garantire la conformità;

22. sottolinea che alcuni fornitori di servizi digitali devono essere in grado di identificare inequivocabilmente gli utenti in modo equivalente ai servizi offline; prende atto di una raccolta non necessaria di dati personali, come i numeri di cellulare, da parte delle piattaforme online al momento della registrazione per un servizio, spesso indotta dal ricorso alle possibilità di autenticazione unica; sottolinea che il RGPD descrive chiaramente il principio di minimizzazione dei dati, limitando in tal modo i dati raccolti a quelli strettamente necessari allo scopo; raccomanda che le piattaforme online che utilizzano i servizi ad autenticazione unica che detengono una quota di mercato dominante siano tenuti anche a supportare almeno un sistema d'identificazione aperto basato su un quadro non proprietario, decentrato e interoperabile;

23. sottolinea che, qualora sia necessario un determinato tipo di identificazione ufficiale offline, occorre creare un sistema di identificazione elettronica online equivalente e sicuro; ritiene che l'identificazione online possa essere migliorata applicando l'interoperabilità transfrontaliera delle identificazioni elettroniche di cui al regolamento eIDAS in tutta l'Unione europea; chiede alla Commissione di valutare la possibilità di creare un sistema unico europeo di autenticazione come alternativa ai singoli sistemi privati di autenticazione e di introdurre l'obbligo per i servizi digitali di offrire sempre anche un'opzione di autenticazione manuale, stabilita per impostazione predefinita; sottolinea che tale servizio dovrebbe essere sviluppato in modo tale che la raccolta di dati di autenticazione identificabili da parte del fornitore di servizi di autenticazione sia tecnicamente impossibile e che i dati raccolti siano limitati al minimo indispensabile; raccomanda pertanto alla Commissione di valutare anche la possibilità di creare un sistema di verifica per gli utenti dei servizi digitali, al fine di garantire la protezione dei dati personali e la verifica dell'età, in particolare per i minori, che non dovrebbe essere utilizzato per motivi commerciali o per tracciare gli utenti tra i siti; sottolinea che tali sistemi di autenticazione e di verifica dovrebbero applicarsi solo ai servizi digitali che richiedono l'identificazione personale, l'autenticazione o la verifica dell'età; ricorda che gli Stati membri e le istituzioni dell'Unione devono garantire che le identificazioni elettroniche siano sicure e trasparenti, trattino solo i dati necessari per l'identificazione dell'utente e siano utilizzate esclusivamente per scopi legittimi e non siano utilizzate a fini commerciali né per limitare l'accesso generale a Internet o per tracciare gli utenti tra i siti;

24. ritiene indispensabile disporre della piena armonizzazione e chiarezza a livello dell'UE per quanto concerne le norme in materia di responsabilità per garantire il rispetto dei diritti fondamentali e delle libertà degli utenti in tutta l'UE; ritiene che tali norme debbano mantenere le esenzioni di responsabilità per gli intermediari che non siano effettivamente a conoscenza dell'attività o delle informazioni illecite presenti sulle loro piattaforme; esprime preoccupazione per il fatto che le recenti leggi nazionali per contrastare l'incitamento all'odio e la disinformazione conducano a una crescente frammentazione delle norme e a un minore livello di tutela dei diritti fondamentali nell'UE;

25. chiede, a tal fine, proposte legislative che mantengano aperto e competitivo il mercato unico digitale prevedendo requisiti armonizzati per i fornitori di servizi digitali affinché applichino procedure e garanzie procedurali efficaci, coerenti, trasparenti ed eque per affrontare i contenuti illegali in linea con il diritto nazionale ed europeo, anche attraverso procedure armonizzate di notifica e intervento;

26. ritiene, a tale proposito, che sia essenziale per le piattaforme online avvalersi di norme, requisiti e garanzie chiari riguardo alla responsabilità per i contenuti di terzi; propone che sia posto in essere un quadro normativo comune per individuare e rimuovere in modo efficiente i contenuti illegali;

27. sottolinea che le norme relative ai meccanismi di notifica e intervento dovrebbero essere integrate dagli obblighi per le piattaforme di adottare misure specifiche che sono proporzionate alla loro portata e alle loro capacità tecniche e operative onde affrontare in modo efficace la comparsa di contenuti illegali all'interno dei loro servizi; riconosce pertanto che, ove sia fattibile sul piano tecnologico, sulla base di ordini sufficientemente motivati di autorità pubbliche indipendenti competenti, e tenendo pienamente conto del contesto specifico dei contenuti, ai fornitori di servizi digitali possa essere richiesto di eseguire ricerche periodiche di parti distinte di contenuti che un tribunale abbia già dichiarato illecite, purché la sorveglianza e la ricerca delle informazioni oggetto di tale ingiunzione siano limitate a informazioni che veicolano un messaggio il cui contenuto rimane sostanzialmente invariato rispetto a quello che ha dato luogo all'accertamento d'illeceità e che contiene gli elementi specificati nell'ingiunzione, i quali, conformemente alla sentenza della Corte di giustizia del 3 ottobre 2019 nella causa C-18/18 ([8]), sono identici o equivalenti in maniera tale da non costringere il fornitore di servizi di hosting ad effettuare una valutazione autonoma di tale contenuto;

([8]) Sentenza della Corte di giustizia del 3 ottobre 2019, Eva Glawischnig-Piesczek contro Facebook Ireland Limited, causa C-18/18, ECLI:EU:C:2019:821.

28. sostiene che la scelta delle misure concrete dovrebbe essere lasciata alle piattaforme; è favorevole a un approccio equilibrato basato su un dialogo con le parti interessate e su una valutazione dei rischi cui sono esposte le piattaforme, nonché su una chiara catena di responsabilità per evitare oneri normativi superflui per le piattaforme e restrizioni inutili e sproporzionate dei diritti fondamentali, in particolare la libertà di espressione, l'accesso alle informazioni, anche riguardo alle idee politiche, e il diritto alla vita privata; sottolinea che alcuni obblighi possono essere ulteriormente specificati dalla legislazione settoriale; evidenzia che qualsiasi misura messa in atto a tal fine non può costituire, de jure o de facto, un requisito generale in materia di monitoraggio;

29. sottolinea la necessità di adeguate garanzie e obblighi in materia di giusto processo, tra cui un requisito per l'attività di sorveglianza e verifica umane, oltre a procedure di contronotifica, onde consentire ai titolari dei contenuti e a coloro che caricano i contenuti di difendere adeguatamente i loro diritti in maniera tempestiva e garantire che le decisioni di rimozione o di blocco siano legali, accurate, fondate, tutelino gli utenti e rispettino i diritti fondamentali; evidenzia che le persone che presentano sistematicamente e in maniera ripetuta notifiche errate o abusive dovrebbero essere sanzionate; ricorda che, oltre alle procedure di contronotifica e alle risoluzioni extragiudiziali delle controversie da parte delle piattaforme a norma del sistema interno di reclamo, dovrebbe rimanere disponibile la possibilità di un ricorso giurisdizionale effettivo per soddisfare il diritto a un ricorso effettivo;

30. sostiene il mantenimento dell'attuale quadro relativo alla responsabilità limitata per i contenuti e al principio del paese di origine, ma ritiene essenziale un migliore coordinamento delle richieste di rimozione tra le autorità nazionali competenti; sottolinea che i contenuti illeciti online dovrebbero essere rimossi dal luogo in cui sono ospitati; evidenzia che tali richieste dovrebbero essere soggette alle garanzie giuridiche al fine di impedire gli abusi e garantire il pieno rispetto dei diritti fondamentali; sottolinea che le richieste di rimozione delle autorità competenti dovrebbero essere specifiche e indicare chiaramente la base giuridica per la rimozione; evidenzia che ai prestatori di servizi che non ottemperano agli ordini legittimi dovrebbe applicarsi un meccanismo efficace di controllo e di applicazione, comprese sanzioni proporzionate che tengano conto delle loro capacità tecniche e operative;

31. ricorda che i fornitori di servizi digitali non devono essere giuridicamente tenuti a conservare i dati personali dei loro utenti o abbonati a fini di contrasto, a meno che la conservazione mirata non sia ordinata da un'autorità competente indipendente nel pieno rispetto del diritto dell'Unione e della giurisprudenza della CGUE; ricorda inoltre che tale conservazione dei dati dovrebbe essere limitata a quanto strettamente necessario rispetto alle categorie di dati da conservare, ai mezzi di comunicazione interessati, alle persone interessate e il periodo di conservazione adottato;

32. ritiene che, al fine di tutelare i diritti fondamentali, la legge sui servizi digitali dovrebbe introdurre norme volte ad assicurare che le condizioni di servizio dei prestatori di servizi digitali siano chiare, trasparenti, eque e rese disponibili agli utenti in modo facile e accessibile; deplora il fatto che le condizioni di servizio di alcune piattaforme di contenuti costringano i funzionari delle autorità di contrasto a utilizzare account personali per indagare su determinate denunce, il che costituisce una minaccia sia per tali indagini che per la sicurezza personale e chiede un coordinamento più efficiente tra gli Stati membri riguardo al seguito dato dalle autorità di contrasto ai contenuti illegali segnalati; ricorda che eventuali ingiunzioni di rimozione da parte di autorità competenti indipendenti devono sempre basarsi sul diritto e non sulle condizioni di servizio dei prestatori di servizi;

33. invita la Commissione a garantire che gli utenti abbiano accesso a contenuti online diversificati e di qualità quale mezzo per garantire che i cittadini siano adeguatamente informati; auspica che la legge sui servizi digitali garantisca che i contenuti mediatici di qualità siano facilmente accessibili e reperibili sulle piattaforme di terzi e che le rimozioni dei contenuti siano in linea con le norme in materia di diritti umani e limitate ai contenuti che siano palesemente illegali o di cui un'autorità competente indipendente ne abbia riscontrato l'illegalità; sottolinea che i contenuti legali non dovrebbero essere soggetti ad alcun obbligo giuridico di rimozione o blocco;

34. sostiene un dialogo maggiore tra gli Stati membri, le autorità competenti e le parti interessate pertinenti al fine di sviluppare, valutare e migliorare gli approcci normativi non vincolanti, tra cui il codice di buone pratiche dell'UE sulla disinformazione, onde affrontare ulteriormente le categorie relative ai contenuti legali, compresa la disinformazione; auspica che la Commissione elabori orientamenti che includano norme rafforzate in materia di trasparenza sulla moderazione dei contenuti e sulla strategia pubblicitaria all'interno di uno strumento specifico che accompagna la legge sui servizi digitali, al fine di garantire che la rimozione e il blocco dei contenuti legali sulla base di termini e condizioni siano

limitati al minimo indispensabile; invita inoltre la Commissione a istituire un quadro che vieti alle piattaforme di esercitare un secondo livello di controllo sui contenuti forniti sotto la responsabilità di un fornitore di servizi di media e soggetti a una sorveglianza e a norme specifiche;

35. sottolinea, inoltre, che agli utenti dovrebbe essere offerta una maggiore scelta e un maggiore controllo riguardo ai contenuti che vedono, comprese più opzioni sul modo in cui i contenuti sono loro presentati e la possibilità di non partecipare a eventuali selezioni di contenuti; è fortemente convinto che la concezione e le prestazioni dei sistemi di raccomandazione dovrebbero essere di facile utilizzo e pienamente trasparenti;

36. ritiene che la definizione di politiche basate sulla responsabilità, sia nel settore privato che nel settore pubblico, e su elementi concreti richieda dati solidi sull'incidenza e il contrasto per quanto concerne l'attività illecita e la rimozione di contenuti illegali online, nonché dati solidi relativi agli algoritmi di trattamento dei contenuti delle piattaforme online;

37. chiede, a tale proposito, un obbligo di rendicontazione pubblica annuale, globale e costante per le piattaforme, il quale sia proporzionato alla loro portata e alle loro capacità operative, più in particolare nell'ambito delle loro procedure di moderazione dei contenuti, tra cui informazioni sulle misure adottate contro le attività illecite online e dati standardizzati in merito alla quantità di contenuti rimossi e alle motivazioni e basi giuridiche sottostanti, al tipo e alla motivazione delle richieste di rimozione ricevute, al numero di richieste di cui è stata rifiutata l'esecuzione e ai motivi al riguardo; sottolinea che tali relazioni, che contemplano le azioni intraprese in un dato anno, dovrebbero essere presentate entro la fine del primo trimestre dell'anno successivo;

38. chiede altresì un obbligo di rendicontazione pubblica annuale per le autorità nazionali, tra cui dati standardizzati sul numero di richieste di rimozione e le relative basi giuridiche, sul numero di richieste di rimozione che sono state oggetto di ricorsi amministrativi o giurisdizionali, sull'esito di tali procedimenti, citando i casi in cui i contenuti o le attività sono erroneamente identificati come illegali, e sul numero totale di decisioni che prevedono l'imposizione di sanzioni, ivi compresa una descrizione del tipo di sanzione imposta;

39. esprime preoccupazione per la frammentazione e la mancanza documentata di risorse finanziarie e umane per quanto concerne gli organi di supervisione e sorveglianza; chiede una maggiore cooperazione tra gli Stati membri in materia di sorveglianza regolamentare dei servizi digitali;

40. ritiene che, al fine di garantire la corretta applicazione della legge sui servizi digitali, sia necessario armonizzare all'interno del mercato unico digitale la vigilanza sul rispetto delle procedure, delle garanzie procedurali e degli obblighi di trasparenza previsti da tale legge; sostiene, a tale proposito, un'applicazione solida e rigorosa da parte di una struttura di vigilanza indipendente dell'UE che abbia la competenza di imporre ammende sulla base di una valutazione di una serie di fattori chiaramente definiti, quali la proporzionalità, le misure tecniche e organizzative e la negligenza; ritiene che ciò dovrebbe includere la possibilità di prevedere ammende basate su una percentuale del fatturato complessivo annuo di una società;

41. sottolinea che gli audit delle politiche e degli algoritmi interni dei fornitori di servizi digitali dovrebbero essere effettuati nel debito rispetto del diritto dell'Unione, in particolare dei diritti fondamentali degli utenti dei servizi, tenendo conto dell'importanza della non discriminazione e della libertà di espressione e di informazione in una società aperta e democratica, e senza pubblicare dati sensibili sotto il profilo commerciale; insiste sulla necessità di valutare, in seguito a denunce o su iniziativa degli organi di vigilanza, se e in che modo i fornitori di servizi digitali amplificano i contenuti, ad esempio mediante motori di raccomandazione e funzioni di ottimizzazione quali l'autocompletamento e l'analisi delle tendenze;

42. ritiene che le relazioni sulla trasparenza elaborate dalle piattaforme e dalle autorità competenti nazionali dovrebbero essere messe a disposizione del pubblico e analizzate ai fini delle tendenze strutturali in materia di rimozione, individuazione e blocco a livello dell'UE;

43. sottolinea l'importanza di consentire agli utenti di far valere i propri diritti fondamentali online, anche mediante procedure di reclamo facilmente accessibili, imparziali, trasparenti, efficienti e gratuite, meccanismi di segnalazione relativi ai contenuti illeciti e a comportamenti criminosi per i singoli individui e le imprese, mezzi di ricorso, misure educative e di sensibilizzazione in materia di protezione dei dati e sicurezza dei minori online;

44. ritiene che le esperienze passate abbiano dimostrato l'efficacia di consentire lo sviluppo di modelli commerciali innovativi e di rafforzare il mercato unico digitale eliminando gli ostacoli alla libera circolazione dei servizi digitali e impedendo l'introduzione di nuovi ostacoli ingiustificati a livello nazionale, e che il mantenimento di questo approccio ridurrebbe la frammentazione del mercato interno; ritiene inoltre che la legge sui servizi digitali possa offrire opportunità per lo sviluppo delle conoscenze e delle competenze dei cittadini nel settore della digitalizzazione, garantendo al contempo un elevato livello di protezione dei consumatori, anche mediante la tutela della sicurezza online;

45. sottolinea il carattere indispensabile delle norme convenute riguardo alla sicurezza essenziale nel ciberspazio affinché i servizi digitali offrano ai cittadini i loro pieni benefici; prende atto pertanto dell'urgente necessità per gli Stati membri di adottare un'azione coordinata al fine di assicurare l'igiene informatica di base e prevenire pericoli evitabili nel ciberspazio, anche mediante misure legislative;

46. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione.