Consiliul
Uniunii Europene

Bruxelles, 14 septembrie 2018
(OR. en)

12129/18

Dosar interinstituțional:
2018/0331(COD)

CT 144
ENFOPOL 450
COTER 114
JAI 881
CYBER 193
TELECOM 288
FREMP 142
AUDIO 64
DROIPEN 127
COHOM 107
CODEC 1468

PROPUNERE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Data primirii:	12 septembrie 2018
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2018) 640 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind prevenirea diseminării conținutului online cu caracter terorist *O contribuție a Comisiei Europene la reuniunea liderilor de la Salzburg din 19-20 septembrie 2018*

În anexă, se pune la dispoziția delegațiilor documentul COM(2018) 640 final.

Anexă: COM(2018) 640 final

COMISIA
EUROPEANĂ

Bruxelles, 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind prevenirea diseminării conținutului online cu caracter terorist

O contribuție a Comisiei Europene la reuniunea liderilor de la Salzburg din 19-20 septembrie 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

1.1. Motivele și obiectivele propunerii

Omniprezența internetului le permite utilizatorilor să comunice, să lucreze, să socializeze, să creeze, să obțină și să facă schimb de informații și de conținut cu sute de milioane de persoane din întreaga lume. Platformele de internet generează beneficii semnificative pentru bunăstarea economică și socială a utilizatorilor din întreaga Uniune și de dincolo de frontierele acesteia. Pe de altă parte, capacitatea de a ajunge la un public atât de numeros cu costuri minime atrage, de asemenea, infractori care doresc să utilizeze internetul în scopuri ilegale. Atacurile teroriste recente de pe teritoriul UE au arătat modul în care teroriștii utilizează în mod abuziv internetul pentru a ademeni și a recruta susținători, a pregăti și a facilita activitățile teroriste, a glorifica atrocitățile comise, a instiga alte persoane să le urmeze exemplul și a inspira teamă la nivelul societății.

Materialele cu conținut terorist publicate online în aceste scopuri sunt diseminate prin intermediul furnizorilor de servicii de găzduire care permit încărcarea de conținut aparținând unor părți terțe. Mai multe dintre atacurile teroriste recente din Europa au demonstrat că materialele online cu caracter terorist are un rol important în radicalizarea așa-numiților „lupi singuratici”, care sunt astfel încurajați să comită atacuri. Pe lângă impactul său deosebit de grav asupra persoanelor și a societății în general, conținutul cu caracter terorist reduce, de asemenea, încrederea în internet a utilizatorilor și afectează modelele de afaceri și reputația întreprinderilor afectate. Teroriștii au utilizat în mod abuziv nu numai marile platforme de comunicare socială, ci și, din ce în ce mai des, furnizori mai mici care oferă diferite tipuri de servicii de găzduire în întreaga lume. Această utilizare abuzivă a internetului pune în lumină responsabilitatea deosebită față de societate a platformelor de internet, care trebuie să-și protejeze utilizatorii împotriva expunerii la conținutul cu caracter terorist și a riscurilor de securitate grave pe care acest conținut le prezintă pentru publicul larg.

Pentru a răspunde la apelurile din partea autorităților publice, furnizorii de servicii de găzduire au instituit anumite măsuri de combatere a difuzării conținutului cu caracter terorist prin intermediul serviciilor pe care le oferă. S-au făcut progrese prin intermediul cadrelor și al parteneriatelor voluntare, inclusiv al Forumului UE pentru internet, lansat în decembrie 2015 în cadrul Agendei europene privind securitatea. Forumul UE pentru internet a promovat cooperarea voluntară a statelor membre și a furnizorilor de servicii de găzduire, precum și acțiunile de reducere a accesului la conținutul online cu caracter terorist și de responsabilizare a societății civile în ceea ce privește încurajarea discursurilor alternative eficace pe internet. Aceste eforturi au produs mai multe rezultate concrete, precum consolidarea cooperării, îmbunătățirea răspunsurilor formulate de întreprinderi la semnalările trimise de autoritățile naționale, precum și de către Unitatea de semnalare a conținutului online din cadrul Europol, adoptarea de măsuri proactive voluntare pentru a îmbunătăți detectarea automată a conținutului cu caracter terorist, o cooperare mai strânsă în cadrul sectorului, inclusiv în ceea ce privește dezvoltarea „bazei de date a valorilor hash”, pentru a preveni încărcarea unor materiale despre care se știe că au caracter terorist pe platformele conectate, precum și îmbunătățirea transparenței eforturilor realizate. Cooperarea în cadrul Forumului UE pentru internet ar trebui să continue, însă măsurile voluntare și-au arătat limitele. În primul rând, nu toți furnizorii de servicii de găzduire participă la forum, iar, în al doilea rând, stadiul și ritmul progreselor realizate de furnizorii de servicii de găzduire în ansamblu nu sunt suficiente pentru a aborda în mod adecvat această problemă.

Având în vedere aceste limitări, există o nevoie clară de intensificare a acțiunilor la nivelul Uniunii Europene pentru combaterea conținutului online cu caracter terorist. La 1 martie 2018, Comisia a adoptat o recomandare privind măsuri de combatere eficace a conținutului online ilegal, pe baza Comunicării Comisiei din septembrie[1], precum și a eforturilor realizate în cadrul Forumului pentru internet al UE. Recomandarea cuprinde un capitol specific care identifică o serie de măsuri pentru a combate în mod eficient încărcarea și partajarea propagandei teroriste online, cum ar fi îmbunătățiri ale procesului de semnalare, un termen de o oră pentru a răspunde la semnalări, o detectare mai proactivă, eliminarea efectivă și măsuri de salvgardare suficiente pentru a evalua cu precizie conținutul cu caracter terorist.[2]

Nevoia de a consolida măsurile de combatere a conținutului online cu caracter terorist a fost evidențiată, de asemenea, de apelurile lansate de statele membre ale UE; unele state au legiferat deja sau și-au exprimat intenția de a legifera în acest domeniu. În urma seriei de atacuri teroriste din UE și având în vedere faptul că conținutul online cu caracter terorist continuă să fie ușor accesibil, Consiliul European din 22-23 iunie 2017 a solicitat sectorului să „dezvolte tehnologii și instrumente noi care să îmbunătățească detectarea automată și eliminarea conținutului care instigă la acte teroriste. Acest lucru ar trebui completat prin măsuri legislative relevante la nivelul UE, dacă este necesar”. Consiliul European din 28 iunie 2018 a salutat „intenția Comisiei de a prezenta o propunere legislativă pentru îmbunătățirea identificării și a eliminării conținutului care instigă la ură și la comiterea de acte teroriste”. La rândul său, Parlamentul European, în rezoluția sa din 15 iunie 2017 privind platformele online și piața unică digitală, a solicitat platformelor relevante „să adopte măsuri mai stricte pentru a combate conținutul ilegal și dăunător” și a invitat Comisia să prezinte propuneri pentru a aborda aceste aspecte.

Pentru a soluționa aceste probleme și a răspunde solicitărilor statelor membre și ale Parlamentului European, prezenta propunere a Comisiei urmărește să stabilească un cadru juridic clar și armonizat care să prevină utilizarea abuzivă a serviciilor de găzduire pentru diseminarea conținutului online cu caracter terorist, garantând astfel buna funcționare a pieței unice digitale și asigurând încrederea și securitatea. Prezentul regulament urmărește să ofere claritate în ceea ce privește responsabilitatea furnizorilor de servicii de găzduire de a lua toate măsurile adecvate, rezonabile și proporționale necesare pentru a garanta siguranța serviciilor pe care le oferă și pentru a detecta și a elimina în mod rapid și eficace conținutul online cu caracter terorist, fără a aduce atingere importanței fundamentale a libertății de exprimare și de informare într-o societate deschisă și democratică. Regulamentul introduce, de asemenea, o serie de măsuri de salvgardare necesare pentru a asigura respectarea deplină a drepturilor fundamentale precum libertatea de exprimare și de informare într-o societate democratică, în plus față de căile de atac judiciare care sunt garantate de dreptul la o cale de atac eficientă, astfel cum este consacrat la articolul 19 din TUE și la articolul 47 din Carta drepturilor fundamentale a UE.

Propunerea stabilește un set minim de obligații de diligență pentru furnizorii de servicii de găzduire, care include anumite norme și obligații specifice, precum și obligații pentru statele membre, cu obiectivul de a îmbunătăți eficacitatea măsurilor actuale de detectare, identificare și eliminare a conținutului online cu caracter terorist, fără a încălca drepturile fundamentale precum libertatea de exprimare și de informare. Acest cadru juridic armonizat va facilita furnizarea serviciilor online pe piața unică digitală, va asigura condiții de concurență

[1] Comunicarea COM(2017) 555 final privind combaterea conținutului ilegal online.

[2] Recomandarea C(2018)1177 final din 1 martie 2018 privind măsuri de combatere eficace a conținutului ilegal online.

echitabile pentru toți furnizorii de servicii de găzduire care își direcționează serviciile către Uniunea Europeană și va oferi un cadru juridic solid pentru detectarea și eliminarea conținutului cu caracter terorist, însoțite de măsuri de salvgardare adecvate privind protejarea drepturilor fundamentale. În special obligațiile privind transparența vor spori încrederea cetățenilor, mai ales a utilizatorilor de internet, și vor îmbunătăți gradul de responsabilizare a întreprinderilor și transparența acțiunilor acestora, inclusiv față de autoritățile publice. Propunerea stabilește, de asemenea, obligația de a institui măsuri reparatorii și mecanisme de depunere a plângerilor pentru a se asigura că utilizatorii pot contesta eliminarea conținutului care le aparține. Obligațiile impuse statelor membre vor contribui la realizarea acestor obiective, precum și la îmbunătățirea capacității autorităților relevante de a lua măsuri adecvate pentru combaterea conținutului online cu caracter terorist și a criminalității. În cazul în care furnizorii de servicii de găzduire nu respectă regulamentul, statele membre vor putea impune sancțiuni.

1.2. Coerența cu dispozițiile legislative ale UE în domeniul de politică

Prezenta propunere este conformă cu acquis-ul în domeniul pieței unice digitale, în special cu Directiva privind comerțul electronic. Mai precis, eventualele măsuri luate de furnizorul de servicii de găzduire în conformitate cu prezentul regulament, inclusiv măsurile proactive, nu ar trebui să determine, prin ele însele, pierderea de către furnizorul de servicii de găzduire a exonerării de răspundere care se aplică, în anumite condiții, în temeiul articolului 14 din Directiva privind comerțul electronic. Decizia autorităților naționale de a impune măsuri proactive proporționale și specifice nu ar trebui să conducă, în principiu, la impunerea unei obligații generale de supraveghere, astfel cum este definită la articolul 15 alineatul (1) din Directiva 2000/31/CE, pentru statele membre. Cu toate acestea, având în vedere riscurile deosebit de grave asociate diseminării conținutului cu caracter terorist, deciziile adoptate în temeiul prezentului regulament pot deroga, în mod excepțional, de la acest principiu într-un cadru UE. Înainte să adopte astfel de decizii, autoritatea competentă ar trebui să asigure un echilibru just între nevoia de siguranță publică, pe de o parte, și interesele și drepturile fundamentale afectate, pe de altă parte, în special libertatea de exprimare și de informare, libertatea de a desfășura o activitate comercială, protecția datelor cu caracter personal și protecția vieții private. Obligațiile de diligență ale furnizorilor de servicii de găzduire ar trebui să reflecte și să respecte acest echilibru, astfel cum este enunțat în Directiva privind comerțul electronic.

Propunerea este, de asemenea, coerentă și strâns aliniată la dispozițiile Directivei (UE) 2017/541 privind combaterea terorismului, al cărei scop este armonizarea legislației statelor membre care incriminează infracțiunile de terorism. Articolul 21 din Directiva privind combaterea terorismului prevede obligația statelor membre de a lua măsuri care să asigure eliminarea rapidă a conținutului online care se limitează la instigare publică, iar alegerea măsurilor le revine statelor membre. Dat fiind caracterul preventiv al prezentului regulament, acesta abordează, pe lângă materialele care instigă la terorism, și materialele cu scop de recrutare sau de instrucție a teroriștilor, reflectând alte infracțiuni legate de activitățile teroriste, care fac de asemenea obiectul Directivei (UE) 2017/541. Prezentul regulament impune în mod direct obligații pentru furnizorii de servicii de găzduire în ceea ce privește eliminarea conținutului cu caracter terorist și armonizează procedurile privind ordinele de eliminare, cu scopul de a reduce accesul la conținutul online cu caracter terorist.

Regulamentul completează normele stabilite de viitoarea Directivă a serviciilor mass-media audiovizuale, în măsura în care domeniul de aplicare personal și material al acesteia este mai larg. Regulamentul acoperă nu numai platformele de partajare a materialelor video, ci toate categoriile de furnizori de servicii de găzduire. De asemenea, acesta reglementează nu numai

materialele video, ci și imaginile și materialele scrise. În plus, prezentul regulament depășește sfera de aplicare a directivei în ceea ce privește dispozițiile de fond, prin armonizarea normelor privind cererile de eliminare a conținutului cu caracter terorist, precum și a măsurilor proactive.

Regulamentul propus se bazează pe Recomandarea[3] Comisiei din martie 2018 privind conținutul ilegal. Recomandarea rămâne în vigoare, iar toți cei care au un rol în reducerea accesibilității conținutului ilegal, inclusiv a conținutului cu caracter terorist, ar trebui să continue să își alinieze eforturile la măsurile identificate în recomandare.

1.3. Rezumatul regulamentului propus

Domeniul de aplicare personal al propunerii include furnizorii de servicii de găzduire care își oferă serviciile în Uniune, indiferent de locul în care sunt stabiliți sau de dimensiune. Legislația propusă introduce o serie de măsuri menite să prevină utilizarea abuzivă a serviciilor de găzduire pentru diseminarea conținutului online cu caracter terorist și să garanteze buna funcționare a pieței unice digitale, asigurând în același timp încrederea și securitatea. Conținutul ilegal cu caracter terorist este definit, în conformitate cu definiția infracțiunilor de terorism prevăzută în Directiva (UE) 2017/541, drept informații care sunt utilizate pentru instigarea la săvârșirea de infracțiuni de terorism, promovarea săvârșirii unor astfel de infracțiuni și glorificarea lor, încurajând contribuirea la infracțiuni de terorism și furnizând instrucțiuni pentru comiterea acestora, precum și promovând participarea la grupurile teroriste.

Pentru a asigura eliminarea conținutului ilegal cu caracter terorist, regulamentul instituie un ordin de eliminare, care poate fi emis ca decizie administrativă sau judiciară de către o autoritate competentă a unui stat membru. În aceste cazuri, furnizorul de servicii de găzduire este obligat să elimine conținutul sau să blocheze accesul la acesta în termen de o oră. În plus, regulamentul armonizează cerințele minime pentru semnalările trimise de autoritățile competente ale statelor membre și de organismele Uniunii (precum Europol) furnizorilor de servicii de găzduire, în vederea examinării în raport cu clauzele și condițiile acestora. În fine, conform regulamentului, furnizorii de servicii de găzduire trebuie să ia, atunci când este necesar, măsuri proactive, proporționale cu nivelul de risc și să elimine materialele cu caracter terorist din serviciile oferite, inclusiv prin utilizarea unor instrumente de detectare automată.

Măsurile care urmăresc reducerea conținutului online cu caracter terorist sunt însoțite de o serie de măsuri de salvgardare esențiale pentru a asigura protecția deplină a drepturilor fundamentale. Printre măsurile de protecție împotriva eliminării eronate a conținutului fără caracter terorist, propunerea stabilește obligația de a institui măsuri reparatorii și mecanisme de depunere a plângerilor, astfel încât utilizatorii să poată contesta eliminarea conținutului lor. Regulamentul introduce și obligații privind transparența măsurilor luate de furnizorii de servicii de găzduire împotriva conținutului cu caracter terorist, asigurând astfel responsabilitatea față de utilizatori, cetățeni și autoritățile publice.

De asemenea, regulamentul le impune statelor membre să se asigure că autoritățile lor competente dispun de capacitatea necesară pentru a interveni împotriva conținutului online cu caracter terorist. În plus, statele membre au obligația de a se informa reciproc și de a coopera între ele; în acest scop, pot utiliza canalele create de Europol pentru a asigura coordonarea cu privire la ordinele de eliminare și la semnalări. De asemenea, regulamentul prevede obligația furnizorilor de servicii de găzduire de a prezenta mai detaliat măsurile luate și de a informa

[3] Recomandarea C(2018)1177 final din 1 martie 2018 privind măsuri de combatere eficace a conținutului ilegal online.

autoritățile de aplicare a legii atunci când detectează conținut care reprezintă o amenințare la adresa vieții sau a siguranței. În fine, furnizorii de servicii de găzduire au obligația de a păstra conținutul pe care îl elimină, ca măsură de salvgardare împotriva eliminării eronate și pentru a asigura faptul că probele potențiale vor putea fi utilizate în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

2.1. Temei juridic

Temeiul juridic este articolul 114 din Tratatul privind funcționarea Uniunii Europene, care prevede instituirea de măsuri menite să asigure funcționarea pieței interne.

Articolul 114 este temeiul juridic adecvat pentru armonizarea condițiilor aplicabile furnizorilor de servicii de găzduire care oferă servicii transfrontaliere în cadrul pieței unice digitale și pentru abordarea acelor diferențe dintre dispozițiile statelor membre care ar putea împiedica funcționarea pieței interne. Astfel se previne și apariția unor obstacole viitoare în calea activității economice ca urmare a evoluțiilor diferite ale legislațiilor naționale.

Articolul 114 din TFUE poate fi, de asemenea, utilizat pentru a impune obligații furnizorilor de servicii stabiliți în afara granițelor UE în cazurile în care furnizarea de servicii afectează piața internă, în măsura în care acest lucru este necesar pentru îndeplinirea obiectivului pieței interne care este urmărit.

2.2. Alegerea instrumentului

Articolul 114 din TFUE oferă legiuitorului Uniunii posibilitatea de a adopta regulamente și directive.

Întrucât propunerea stabilește obligații pentru furnizorii care oferă de obicei servicii în mai multe state membre, aplicarea divergentă a acestor norme ar afecta furnizarea de servicii de către furnizorii care își desfășoară activitatea în mai multe state membre. Un regulament permite ca aceeași obligație să fie impusă în mod uniform în întreaga Uniune, este direct aplicabil, oferă claritate, asigură o mai mare securitate juridică și previne transpunerea divergentă în statele membre. Din aceste motive, se consideră că forma cea mai potrivită pentru acest instrument este un regulament.

2.3. Subsidiaritate

Având în vedere dimensiunea transfrontalieră a problemelor abordate, măsurile incluse în propunere trebuie să fie adoptate la nivelul Uniunii pentru realizarea obiectivelor vizate. Prin natura sa, internetul este transfrontalier, iar conținutul găzduit într-un stat membru poate fi accesat, în mod normal, din oricare alt stat membru.

În momentul de față a început să apară o rețea fragmentată de norme naționale de combatere a conținutului online cu caracter terorist, iar această fragmentare riscă să devină tot mai evidentă. Această situație ar obliga întreprinderile să se conformeze unor reglementări divergente și ar crea astfel condiții inegale pentru întreprinderi, precum și lacune în materie de securitate.

Prin urmare, acțiunea UE va oferi mai multă securitate juridică și va spori eficacitatea măsurilor luate de furnizorii de servicii de găzduire pentru combaterea conținutului online cu caracter terorist. Astfel, mai multe întreprinderi vor avea posibilitatea să ia măsuri, inclusiv cele stabilite în afara Uniunii Europene, fapt ce va contribui la consolidarea integrității pieței unice digitale.

Acest obiectiv justifică necesitatea unei acțiuni a UE, astfel cum se reflectă în Concluziile Consiliului European din iunie 2018, prin care Comisia a fost invitată să prezinte o propunere legislativă în acest domeniu.

2.4. Proporționalitate

Propunerea le impune furnizorilor de servicii de găzduire să aplice măsuri pentru a elimina în mod rapid conținutul cu caracter terorist din serviciile pe care le oferă. O serie de caracteristici importante limitează propunerea la ceea ce este necesar pentru atingerea obiectivelor de politică.

Propunerea ține seama de sarcina impusă furnizorilor de servicii de găzduire și de măsurile de salvgardare necesare, inclusiv de protecția libertății de exprimare și de informare, precum și de alte drepturi fundamentale. Termenul de o oră pentru eliminarea conținutului se aplică numai ordinelor de eliminare, în cazul cărora autoritățile competente au stabilit caracterul ilegal printr-o decizie supusă controlului judiciar. În ceea ce privește semnalările, se prevede obligația de a institui măsuri pentru a facilita evaluarea rapidă a conținutului cu caracter terorist, fără a impune însă obligația de eliminare și nici termene absolute. Decizia finală rămâne o decizie voluntară a furnizorului de servicii de găzduire. Sarcina impusă întreprinderilor în ceea ce privește evaluarea conținutului este atenuată de faptul că autoritățile competente din statele membre și organismele Uniunii oferă explicații cu privire la motivul pentru care conținutul poate fi considerat conținut cu caracter terorist. Furnizorii de servicii de găzduire iau măsuri proactive, atunci când acestea se impun, pentru a-și proteja serviciile împotriva diseminării conținutului cu caracter terorist. Obligațiile specifice legate de măsurile proactive se limitează la furnizorii de servicii de găzduire care sunt expuși la conținutul cu caracter terorist, fapt demonstrat de primirea unui ordin de eliminare care a devenit definitiv, și ar trebui să fie proporționale cu nivelul de risc, precum și cu resursele societății în cauză. Păstrarea conținutului eliminat și a datelor conexe este limitată la o perioadă proporțională cu obiectivele de a permite desfășurarea procedurilor de reexaminare administrativă sau control judiciar și de a preveni, depista, investiga și urmări penal infracțiunile de terorism.

3. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

3.1. Consultări cu părțile interesate

În pregătirea prezentei propuneri legislative, Comisia a consultat toate părțile interesate relevante pentru a le înțelege punctele de vedere și a identifica o posibilă cale de urmat. Comisia a desfășurat o consultare publică deschisă privind măsurile menite să asigure o combatere mai eficace a conținutului ilegal și a primit 8 961 de răspunsuri, dintre care 8 749 din partea unor persoane fizice, 172 din partea unor organizații, 10 din partea unor administrații publice și 30 din partea altor categorii de respondenți. În paralel, a fost realizat un sondaj Eurobarometru privind conținutul online ilegal, cu un eșantion aleatoriu de 33 500 de rezidenți în UE. De asemenea, în mai și iunie 2018 Comisia a consultat autoritățile din statele membre și furnizorii de servicii de găzduire cu privire la măsurile specifice de combatere a conținutului online cu caracter terorist.

Pe ansamblu, majoritatea părților interesate au considerat conținutul online cu caracter terorist ca fiind o problemă societală gravă care afectează atât utilizatorii de internet, cât și modelele de afaceri ale furnizorilor de servicii de găzduire. La un nivel mai general, 65 % dintre

respondenții la sondajul Eurobarometru[4] au considerat că internetul nu este sigur pentru utilizatori, iar 90 % dintre respondenți au considerat că este important să se combată diseminarea conținutului online ilegal. Din consultările cu statele membre a reieșit că, deși măsurile voluntare au dat rezultate, multe state membre simt necesitatea unor norme obligatorii privind conținutul terorist, așa cum reiese și din concluziile Consiliului European din iunie 2018. În timp ce, în general, furnizorii de servicii de găzduire s-au declarat în favoarea continuării măsurilor voluntare, aceștia au atras atenția asupra efectelor negative potențiale ale fragmentării juridice la nivelul Uniunii.

Numeroase părți interesate au subliniat, de asemenea, necesitatea asigurării unui echilibru între eventualele reglementări privind eliminarea conținutului, în special măsurile proactive și termenele stricte, și măsurile de salvgardare privind drepturile fundamentale, mai ales libertatea de exprimare. Părțile interesate au menționat o serie de măsuri necesare legate de transparență, de responsabilitate, precum și de necesitatea evaluărilor efectuate de o persoană atunci când se utilizează instrumente automatizate.

3.2. Evaluarea impactului

Comitetul de analiză a reglementării a emis un aviz pozitiv cu rezerve în ceea ce privește evaluarea impactului și a făcut o serie de sugestii de îmbunătățire[5]. În urma acestui aviz, raportul de evaluare a impactului a fost modificat pentru a se ține seama de principalele observații ale Comitetului, punându-se accentul în mod specific pe conținutul cu caracter terorist și, în același timp, subliniind implicațiile asupra funcționării pieței unice digitale și oferind o analiză mai aprofundată a impactului asupra drepturilor fundamentale și a funcționării măsurilor de salvgardare propuse în cadrul opțiunilor.

Dacă nu se vor lua măsuri suplimentare, se preconizează că acțiunile voluntare din cadrul scenariului de referință vor continua și vor avea un anumit impact asupra reducerii conținutului online cu caracter terorist. Cu toate acestea, este puțin probabil ca măsurile voluntare să fie luate de către toți furnizorii de servicii de găzduire expuși la un astfel de conținut și se estimează că agravarea fragmentării juridice va crea obstacole suplimentare în calea furnizării de servicii la nivel transfrontalier. Pe lângă scenariul de referință, au fost analizate trei opțiuni de politică principale, cărora le corespund niveluri din ce în ce mai mari de eficacitate în ceea ce privește atingerea obiectivelor stabilite în evaluarea impactului și a obiectivului general de politică referitor la reducerea conținutului online cu caracter terorist.

Pentru toate cele trei opțiuni, obligațiile îi vizează pe toți furnizorii de servicii de găzduire (domeniu de aplicare personal) stabiliți în UE și în țări terțe, în măsura în care aceștia își oferă serviciile în Uniune (domeniu de aplicare geografic). Având în vedere natura problemei și necesitatea de a evita utilizarea abuzivă a platformelor mai mici, niciuna dintre opțiuni nu prevede derogări pentru IMM-uri. Toate opțiunile ar impune stabilirea unui reprezentant legal în UE, inclusiv pentru societățile stabilite în afara UE, pentru a asigura punerea în aplicare a normelor UE. Conform tuturor opțiunilor, statele membre vor trebui să elaboreze mecanisme de sancționare.

Toate opțiunile prevăd crearea unui nou sistem armonizat de ordine de eliminare a conținutului online cu caracter terorist, emise de autoritățile naționale și având ca destinatari furnizorii de servicii de găzduire, precum și cerința de a elimina acest conținut în termen de o

[4] Sondajul Eurobarometru nr. 469, Conținutul online ilegal, iunie 2018.
[5] Link către avizul CAR cu privire la regulament.

oră. Aceste ordine nu ar necesita neapărat o evaluare din partea furnizorilor de servicii de găzduire și ar putea fi atacate în justiție.

Toate cele trei opțiuni prevăd măsuri de salvgardare, în special proceduri de depunere a plângerilor și căi de atac eficiente, inclusiv judiciare, precum și alte dispoziții pentru a preveni eliminarea eronată a conținutului fără caracter terorist, asigurându-se, în același timp, respectarea drepturilor fundamentale. De asemenea, toate opțiunile includ obligații de raportare, sub forma unor rapoarte publice privind transparența și a comunicării informațiilor către statele membre și Comisie, precum și către autorități, pentru presupuse infracțiuni. În plus, sunt prevăzute obligații de cooperare între autoritățile naționale, furnizorii de servicii de găzduire și, atunci când este relevant, Europol.

Principalele diferențe dintre cele trei opțiuni se referă la domeniul de aplicare a definiției conținutului cu caracter terorist, la nivelul de armonizare a semnalărilor, la domeniul de aplicare al măsurilor proactive, la obligațiile de coordonare ale statelor membre, precum și la cerințele în materie de conservare a datelor. Opțiunea 1 ar limita domeniul de aplicare material la conținutul diseminat pentru a instiga în mod direct la comiterea unui act terorist, conform unei definiții restrânse, în timp ce opțiunile 2 și 3 au o abordare mai generală, acoperind, de asemenea, materialele cu scopuri de recrutare și instrucție. În ceea ce privește măsurile proactive, conform opțiunii 1, furnizorii de servicii de găzduire expuși la conținuturi teroriste ar trebui să efectueze o evaluare a riscurilor, însă măsurile proactive de abordare a riscurilor și-ar păstra caracterul voluntar. Opțiunea 2 le-ar impune furnizorilor de servicii de găzduire să elaboreze un plan de acțiune, care ar putea include utilizarea de instrumente automatizate care să prevină reîncărcarea conținutului deja eliminat. Opțiunea 3 include măsuri proactive mai cuprinzătoare, impunând ca furnizorii de servicii expuși la conținut cu caracter terorist să identifice, de asemenea, materialele noi. Conform tuturor opțiunilor, cerințele legate de măsurile proactive ar fi proporționale cu nivelul de expunere la materialele teroriste, precum și cu capacitatea economică a furnizorului de servicii. În ceea ce privește semnalările, opțiunea 1 nu prevede o abordare armonizată, în timp ce opțiunea 2 prevede o astfel de abordare pentru Europol, iar opțiunea 3 include, de asemenea, semnalările emise de statele membre. Conform opțiunilor 2 și 3, statele membre ar fi obligate să se informeze reciproc, să se coordoneze și să coopereze între ele, iar conform opțiunii 3 acestea ar trebui să se asigure, de asemenea, că autoritățile lor competente au capacitatea de a detecta și de a notifica conținutul cu caracter terorist. În fine, opțiunea 3 include și cerința de a păstra datele ca măsură de salvgardare în cazurile de eliminare eronată și pentru a facilita anchetele penale.

În plus față de dispozițiile legale, în cazul tuturor opțiunilor legislative s-a preconizat că acestea vor fi însoțite de o serie de măsuri de sprijin, în special pentru a facilita cooperarea dintre autoritățile naționale și Europol și colaborarea cu furnizorii de servicii de găzduire, precum și sprijinul pentru cercetare, dezvoltare și inovare în vederea elaborării și a adoptării de soluții tehnologice. De asemenea, după adoptarea instrumentului juridic ar putea fi utilizate instrumente suplimentare de sensibilizare și de sprijin pentru IMM-uri.

Evaluarea impactului a concluzionat că pentru atingerea obiectivului de politică sunt necesare o serie de măsuri. O definiție extinsă a conținutului cu caracter terorist care să includă cele mai dăunătoare materiale este preferabilă unei definiții restrânse a conținutului (opțiunea 1). Obligațiile proactive limitate la prevenirea reîncărcării conținutului cu caracter terorist (opțiunea 2) ar avea un impact mai mic comparativ cu obligațiile legate de detectarea noilor conținuturi cu caracter terorist (opțiunea 3). Dispozițiile privind semnalările ar trebui să se refere atât la semnalările emise de Europol, cât și la cele emise de statele membre (opțiunea 3), deci să nu să se limiteze la semnalările Europol (opțiunea 2), deoarece semnalările din partea statelor membre reprezintă o contribuție importantă la efortul global de

reducere a accesibilității la conținutul online cu caracter terorist. Astfel de măsuri ar trebui să fie puse în aplicare în plus față de măsurile comune tuturor opțiunilor, inclusiv măsurile de salvgardare solide împotriva eliminării eronate a conținutului.

3.3. Drepturile fundamentale

Propaganda teroristă online urmărește să instige persoanele să comită atacuri teroriste, inclusiv prin instrucțiuni detaliate cu privire la modul în care pot fi provocate cele mai grave daune. După comiterea unor astfel de atrocități, în general se publică alte materiale, care glorifică actele respective și instigă alte persoane să le urmeze exemplul. Prezentul regulament contribuie la protejarea securității publice, prin reducerea accesibilității conținuturilor cu caracter terorist care promovează și încurajează încălcarea drepturilor fundamentale.

Propunerea ar putea aduce atingere mai multor drepturi fundamentale:

(a) drepturile furnizorului de conținut: dreptul la libertatea de exprimare; dreptul la protecția datelor cu caracter personal; dreptul la respectarea vieții private și de familie, principiul nediscriminării și dreptul la o cale de atac eficientă;

(b) drepturile furnizorului de servicii: dreptul de a desfășura în mod liber o activitate comercială; dreptul la o cale de atac eficientă;

(c) drepturile tuturor cetățenilor: dreptul la libertatea de exprimare și de informare.

Ținând seama de acquis-ul relevant, în propunerea de regulament sunt incluse măsuri de salvgardare adecvate și solide pentru a asigura protecția drepturilor acestor părți.

Un prim element în acest context este că regulamentul stabilește o definiție a conținutului online cu caracter terorist în conformitate cu definiția infracțiunilor de terorism prevăzută de Directiva (UE) 2017/541. Această definiție se aplică ordinelor de eliminare și semnalărilor, precum și măsurilor proactive. Definiția garantează faptul că va trebui eliminat numai conținutul ilegal care corespunde unei definiții la nivelul întregii Uniuni a infracțiunilor penale conexe. În plus, regulamentul include obligații generale aplicabile furnizorilor de servicii de găzduire de a acționa în mod diligent, proporțional și nediscriminatoriu în ceea ce privește conținutul pe care îl stochează, în special atunci când pun în aplicare clauzele și condițiile proprii, în scopul de a preveni eliminarea conținutului fără caracter terorist.

În mod mai specific, regulamentul a fost conceput astfel încât să asigure proporționalitatea măsurilor adoptate în raport cu drepturile fundamentale. În ceea ce privește ordinele de eliminare, evaluarea conținutului (inclusiv verificările juridice, atunci când este necesar) de către o autoritate competentă justifică termenul de o oră pentru eliminarea conținutului. De asemenea, dispozițiile prezentului regulament referitoare la semnalări se limitează la semnalările transmise de autoritățile competente și de organismele Uniunii în care se oferă explicații privind motivele pentru care conținutul poate fi considerat conținut cu caracter terorist. Deși responsabilitatea pentru eliminarea conținutului identificat într-o semnalare îi revine în continuare furnizorului de servicii de găzduire, decizia acestuia este facilitată de evaluarea menționată anterior.

În ceea ce privește măsurile proactive, responsabilitatea pentru identificarea, evaluarea și eliminarea conținutului le revine în continuare furnizorilor de servicii de găzduire, cărora li se cere să instituie măsuri de salvgardare pentru a preveni eliminarea eronată a conținutului, inclusiv prin evaluări efectuate de o persoană, în special atunci când este necesară o analiză suplimentară a contextului. În plus, spre deosebire de scenariul de referință, conform căruia

societățile cele mai afectate instituie instrumente automatizate fără o supraveghere publică, autoritățile competente din statele membre trebuie informate în legătură cu elaborarea și cu punerea în aplicare a măsurilor. Această obligație reduce riscurile de eliminare eronată, atât pentru societățile care instituie instrumente noi, cât și pentru cele care utilizează deja astfel de instrumente. În plus, furnizorii de servicii de găzduire sunt obligați să pună la dispoziția furnizorilor de conținut mecanisme de depunere a plângerilor ușor de utilizat pentru contestarea deciziei de a elimina conținutul care le aparține, precum și să publice rapoarte privind transparența pentru publicul larg.

În fine, în cazul eliminării eronate a conținutului și a datelor conexe în pofida acestor măsuri de salvgardare, furnizorii de servicii de găzduire trebuie să le păstreze timp de șase luni, astfel încât să fie posibilă recuperarea acestora și să se asigure eficacitatea procedurilor de depunere a plângerilor și de reexaminare, în vederea protejării libertății de exprimare și de informare. În același timp, păstrarea conținutului eliminat contribuie și la asigurarea aplicării legii. Furnizorii de servicii de găzduire trebuie să instituie măsuri de salvgardare tehnice și organizaționale pentru a se asigura că datele nu sunt utilizate în alte scopuri.

Măsurile propuse, în special cele referitoare la ordinele de eliminare, semnalări, măsurile proactive și păstrarea datelor, ar trebui nu numai să îi protejeze pe utilizatorii de internet împotriva conținutului cu caracter terorist, ci și să contribuie la protejarea dreptului la viață al cetățenilor, prin reducerea accesibilității conținutului online cu caracter terorist.

4. IMPLICAȚII BUGETARE

Propunerea legislativă de regulament nu are un impact asupra bugetului Uniunii.

5. ALTE ELEMENTE

5.1. Planuri de punere în aplicare și măsuri de monitorizare, evaluare și raportare

Până cel târziu la [un an de la data aplicării prezentului regulament], Comisia va stabili un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament. Programul de monitorizare va stabili indicatorii și mijloacele care trebuie să fie utilizate și intervalele care trebuie să fie aplicate pentru colectarea de date și de alte dovezi necesare. Programul va specifica acțiunile care urmează să fie întreprinse de către Comisie și de către statele membre în ceea ce privește colectarea și analizarea datelor și a altor dovezi pentru a monitoriza progresele înregistrate și a evalua prezentul regulament.

Conform programului de monitorizare stabilit, în termen de doi ani de la intrarea în vigoare a prezentului regulament, Comisia va prezenta un raport privind punerea în aplicare, pe baza rapoartelor privind transparența publicate de întreprinderi și a informațiilor transmise de statele membre. Comisia va efectua o evaluare la cel puțin patru ani de la intrarea în vigoare a regulamentului.

Pe baza constatărilor evaluării, inclusiv cu privire la eventualele lacune sau vulnerabilități rămase, și ținând seama de evoluțiile tehnologice, Comisia va analiza necesitatea extinderii domeniului de aplicare al regulamentului. Dacă este necesar, Comisia va prezenta propuneri în vederea adaptării prezentului regulament.

Comisia va sprijini punerea în aplicare, monitorizarea și evaluarea regulamentului prin intermediul unui grup de experți al Comisiei. Acest grup va facilita cooperarea dintre furnizorii de servicii de găzduire, autoritățile de aplicare a legii și Europol, va încuraja

schimburile de informații și practicile pentru detectarea și eliminarea conținutului cu caracter terorist, va oferi cunoștințe de specialitate cu privire la evoluția modului de operare al teroriștilor în mediul online și va oferi consiliere și orientări, dacă este cazul, în sprijinul punerii în aplicare a dispozițiilor.

Punerea în aplicare a regulamentului propus ar putea fi facilitată printr-o serie de măsuri de sprijin. Printre acestea se numără posibilitatea de a dezvolta o platformă în cadrul Europol care să faciliteze coordonarea semnalărilor și a ordinelor de eliminare. Cercetările finanțate de UE care vizează evoluția modului de operare al teroriștilor contribuie la îmbunătățirea înțelegerii și la sensibilizarea tuturor părților interesate relevante. În plus, Orizont 2020 sprijină cercetarea în vederea dezvoltării de noi tehnologii, inclusiv pentru prevenirea automatizată a încărcării conținutului cu caracter terorist. De asemenea, Comisia va continua să analizeze posibilitățile de utilizare a instrumentelor financiare ale UE pentru a sprijini autoritățile competente și furnizorii de servicii de găzduire în vederea punerii în aplicare a prezentului regulament.

5.2. Explicarea detaliată a dispozițiilor specifice ale propunerii

Articolul 1 prezintă obiectul regulamentului, indicând că acesta prevede norme menite să prevină utilizarea abuzivă a serviciilor de găzduire pentru diseminarea de conținut online cu caracter terorist, inclusiv obligații de diligență pentru furnizorii de servicii de găzduire și măsuri pe care trebuie să le adopte de statele membre. De asemenea, în acest articol se stabilește domeniul de aplicare geografic, regulamentul aplicându-se furnizorilor de servicii de găzduire care oferă servicii în Uniune, indiferent de locul unde își au sediul.

Articolul 2 cuprinde definițiile termenilor utilizați în propunere. Articolul stabilește, printre altele, o definiție a conținutului cu caracter terorist în scop preventiv, pe baza Directivei privind combaterea terorismului, incluzând materialele și informațiile care instigă, încurajează sau promovează săvârșirea de infracțiuni teroriste sau contribuirea la aceste infracțiuni, oferă instrucțiuni în acest sens sau promovează participarea la activitățile unui grup terorist.

Articolul 3 prevede obligații de diligență care trebuie respectate de furnizorii de servicii de găzduire atunci când iau măsuri în conformitate cu prezentul regulament, în special în ceea ce privește drepturile fundamentale relevante. Articolul dispune ca furnizorii de servicii de găzduire să includă în clauzele și condițiile lor dispoziții corespunzătoare care să prevină difuzarea conținutului cu caracter terorist și să se asigure că acestea sunt aplicate.

Articolul 4 le cere statelor membre să împuternicească autoritățile competente să emită ordine de eliminare și instituie obligația ca furnizorii de servicii de găzduire să elimine conținutul în termen de o oră de la primirea unui ordin de eliminare. Articolul stabilește și setul minim de elemente pe care trebuie să le cuprindă ordinele de eliminare, precum și procedurile pe care trebuie să le aplice furnizorii de servicii de găzduire pentru a da feedback autorității emitente și a o informa în cazul în care îi este imposibil să respecte ordinul sau dacă sunt necesare clarificări suplimentare. Se prevede, de asemenea, că autoritatea emitentă trebuie să informeze autoritatea care supraveghează măsurile proactive din statul membru competent pentru furnizorul de servicii de găzduire.

Articolul 5 prevede obligația ca furnizorii de servicii de găzduire să instituie măsuri pentru evaluarea rapidă a conținutului care face obiectul unei semnalări emise de o autoritate competentă dintr-un stat membru sau de un organism al Uniunii, fără a impune însă cerința de

a elimina conținutul menționat și fără a stabili termene specifice pentru luarea de măsuri. Articolul stabilește și setul minim de elemente pe care trebuie să le cuprindă semnalările, precum și procedurile pe care trebuie să le aplice furnizorii de servicii de găzduire pentru a-i da feedback și a-i cere clarificări autorității care a semnalat conținutul.

Articolul 6 prevede că, atunci când este necesar, furnizorii de servicii de găzduire trebuie să ia măsuri proactive care să fie eficace și proporționale. Acesta stabilește o procedură prin care să se asigure că anumiți furnizori de servicii de găzduire (și anume cei care au primit un ordin de eliminare devenit definitiv) adoptă măsuri proactive suplimentare, atunci când acest lucru este necesar pentru a atenua riscurile și în funcție de nivelul de expunere al serviciilor pe care le oferă la conținutul cu caracter terorist. Furnizorul de servicii de găzduire ar trebui să coopereze cu autoritatea competentă în ceea ce privește măsurile pe care i se cere să le adopte, iar în cazul în care nu se poate ajunge la un acord, autoritatea îi poate impune furnizorului de servicii să ia măsuri. Articolul stabilește, de asemenea, o procedură de reexaminare a deciziei autorității.

Conform articolului 7, furnizorii de servicii de găzduire trebuie să păstreze conținutul eliminat și datele conexe timp de șase luni, în scopul desfășurării procedurilor de reexaminare și în scopuri de anchetare. Această perioadă poate fi prelungită pentru a permite finalizarea reexaminării. Articolul impune, de asemenea, furnizorilor de servicii obligația de a institui măsuri de salvgardare pentru a preveni accesarea sau prelucrarea în alte scopuri a conținutului păstrat și a datelor conexe.

Conform articolului 8, furnizorii de servicii de găzduire trebuie să ofere explicații privind politicile lor de combatere a conținutului cu caracter terorist și să publice rapoarte anuale privind transparența care să prezinte măsurile luate în acest sens.

Articolul 9 cuprinde măsuri de salvgardare specifice referitoare la instituirea și punerea în aplicare a măsurilor proactive atunci când se utilizează instrumente automatizate, pentru a se asigura că deciziile sunt corecte și întemeiate.

Conform articolului 10, furnizorii de servicii de găzduire trebuie să instituie mecanisme de depunere a plângerilor în cazul eliminării conținutului, al semnalărilor și al măsurilor proactive și să examineze cu promptitudine toate plângerile.

Articolul 11 prevede obligația ca furnizorii de servicii de găzduire să-i ofere furnizorului de conținut informații cu privire la eliminarea conținutului, cu excepția cazului în care autoritatea competentă solicită nedivulgarea din motive de siguranță publică.

Articolul 12 le cere statelor membre să se asigure că autoritățile competente dispun de capacitatea necesară și de resurse suficiente pentru a-și îndeplini responsabilitățile care le revin în temeiul prezentului regulament.

Articolul 13 prevede că statele membre trebuie să coopereze între ele și, după caz, cu Europol, pentru a evita suprapunerile și interferențele cu investigațiile. Articolul include și posibilitatea ca statele membre și furnizorii de servicii de găzduire să utilizeze instrumente specifice, inclusiv instrumentele Europol, pentru prelucrarea și feedback-ul privind ordinele de eliminare și semnalările, precum și să coopereze în ceea ce privește măsurile proactive. De asemenea, statele membre trebuie să dispună de canale de comunicare adecvate care să permită un schimb rapid de informații în vederea punerii în aplicare și a asigurării respectării

dispozițiilor prezentului regulament. Articolul prevede că furnizorii de servicii de găzduire trebuie să informeze autoritățile relevante în cazul în care iau cunoștință de orice fel de dovadă referitoare la infracțiuni de terorism, în sensul articolului 3 din Directiva (UE) 2017/541 privind combaterea terorismului.

Articolul 14 prevede instituirea de puncte de contact atât de către furnizorii de servicii de găzduire, cât și de către statele membre, în scopul de a facilita comunicarea, în special în ceea ce privește semnalările și ordinele de eliminare.

Articolul 15 stabilește care stat membru este competent în ceea ce privește supravegherea măsurilor proactive, stabilirea sancțiunilor și monitorizarea eforturilor.

Articolul 16 prevede că furnizorii de servicii de găzduire care nu au niciun sediu pe teritoriul unui stat membru, dar care oferă servicii în cadrul Uniunii, trebuie să desemneze un reprezentant legal în Uniune.

Conform articolului 17, statele membre trebuie să desemneze autorități competente în ceea ce privește emiterea ordinelor de eliminare, semnalarea conținutului cu caracter terorist, supravegherea punerii în aplicare a măsurilor proactive și asigurarea respectării regulamentului.

Articolul 18 prevede că statele membre trebuie să stabilească norme privind sancțiunile în cazul nerespectării obligațiilor și cuprinde criterii pe care statele membre trebuie să le ia în considerare atunci când stabilesc tipul și nivelul sancțiunilor. Având în vedere că eliminarea rapidă a conținutului cu caracter terorist identificat într-un ordin de eliminare este deosebit de importantă, ar trebui instituite norme specifice privind sancțiunile financiare aplicabile în cazul încălcărilor sistematice ale acestei cerințe.

Articolul 19 stabilește o procedură mai rapidă și mai flexibilă pentru modificarea prin acte delegate a formularelor pentru ordinele de eliminare și a canalelor autentificate de transmitere.

Articolul 20 stabilește condițiile în care Comisia are competența de a adopta acte delegate pentru a aduce modificările necesare formularelor și cerințelor tehnice pentru ordinele de eliminare.

Articolul 21 le impune statelor membre obligația de a colecta și de a comunica informațiile specifice legate de aplicarea regulamentului cu scopul de a sprijini Comisia în exercitarea atribuțiilor sale în temeiul articolului 23. Comisia trebuie să instituie un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament.

Articolul 22 prevede obligația Comisiei de a prezenta un raport privind aplicarea prezentului regulament la doi ani de la intrarea sa în vigoare.

Articolul 23 prevede obligația Comisiei de a prezenta un raport privind evaluarea prezentului regulament la cel puțin trei ani de la intrarea sa în vigoare.

Articolul 24 prevede că regulamentul propus intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial și devine aplicabil la șase luni de la data intrării sale în vigoare. Acest termen este propus având în vedere necesitatea de a adopta măsuri de punere în aplicare și, în același timp, recunoscând nevoia urgentă ca normele prevăzute de regulament să fie

aplicate pe deplin. Termenul de șase luni a fost stabilit pe baza ipotezei că negocierile se vor desfășura cu rapiditate.

2018/0331 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind prevenirea diseminării conținutului online cu caracter terorist

O contribuție a Comisiei Europene la reuniunea liderilor de la Salzburg din 19-20 septembrie 2018

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[6],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Prezentul regulament are scopul de a asigura buna funcționare a pieței unice digitale în cadrul unei societăți deschise și democratice, prin prevenirea utilizării abuzive a serviciilor de găzduire în scopuri teroriste. Funcționarea pieței unice digitale ar trebui să fie îmbunătățită prin sporirea securității juridice pentru furnizorii de servicii de găzduire, îmbunătățirea încrederii utilizatorilor în mediul online și consolidarea măsurilor de salvgardare privind libertatea de exprimare și de informare.

(2) Furnizorii de servicii de găzduire care activează pe internet joacă un rol esențial în economia digitală, prin crearea de legături între întreprinderi și cetățeni și prin facilitarea dezbaterii publice, a difuzării și primirii de informații, de idei și opinii, contribuind astfel în mod semnificativ la inovare, la creșterea economică și la crearea de locuri de muncă în Uniune. Serviciile acestora pot fi însă utilizate abuziv de părți terțe pentru a desfășura activități ilegale online. Un motiv de preocupare deosebită îl reprezintă utilizarea abuzivă a serviciilor de găzduire de către grupurile teroriste și susținătorii acestora pentru a disemina online conținut cu caracter terorist cu scopul de a-și răspândi mesajele, a radicaliza și a recruta noi persoane, precum și de a facilita și direcționa activitățile teroriste.

(3) Prezența conținutului online cu caracter terorist are consecințe negative grave pentru utilizatori, pentru cetățeni și pentru societate în general, precum și pentru furnizorii de servicii online care găzduiesc un astfel de conținut, deoarece subminează încrederea utilizatorilor și afectează modelele de afaceri ale acestora. Având în vedere rolul lor

[6] JO C , , p. .

central și mijloacele și capacitățile tehnologice asociate serviciilor pe care le oferă, furnizorii de servicii online au responsabilități societale specifice de a-și proteja serviciile împotriva utilizării abuzive de către teroriști și de a contribui la combaterea conținutului cu caracter terorist diseminat prin intermediul serviciilor pe care le oferă.

(4) Eforturile de combatere a conținutului online cu caracter terorist inițiate la nivelul Uniunii în 2015 prin intermediul unui cadru de cooperare voluntară între statele membre și furnizorii de servicii de găzduire trebuie să fie completate de un cadru legislativ clar, pentru a reduce și mai mult accesibilitatea conținutului online cu caracter terorist și pentru a aborda în mod adecvat o problemă care evoluează rapid. Acest cadru legislativ își propune să valorifice eforturile voluntare, care au fost consolidate prin Recomandarea (UE) 2018/334 a Comisiei[7], și răspunde solicitărilor formulate de Parlamentul European în vederea consolidării măsurilor de combatere a conținuturilor ilegale și dăunătoare, precum și de Consiliul European în vederea îmbunătățirii detectării și eliminării automate a conținutului care instigă la acte teroriste.

(5) Aplicarea prezentului regulament nu ar trebui să aducă atingere aplicării articolului 14 din Directiva 2000/31/CE[8]. În special, eventualele măsuri luate de furnizorul de servicii de găzduire în conformitate cu prezentul regulament, inclusiv eventualele măsuri proactive, nu ar trebui să determine, prin ele însele, pierderea de către furnizorul de servicii de găzduire a beneficiului scutirii de răspundere care se aplică, în anumite condiții, în temeiul articolului respectiv. Prezentul regulament nu aduce atingere competențelor autorităților și instanțelor naționale de a stabili răspunderea furnizorilor de servicii de găzduire în cazurile specifice în care nu sunt îndeplinite condițiile prevăzute la articolul 14 din Directiva 2000/31/CE pentru scutirea de răspundere.

(6) Prezentul regulament stabilește norme menite să prevină utilizarea abuzivă a serviciilor de găzduire pentru diseminarea conținutului online cu caracter terorist, astfel încât să se asigure buna funcționare a pieței interne, cu respectarea deplină a drepturilor fundamentale protejate în ordinea juridică a Uniunii, în special a celor garantate prin Carta drepturilor fundamentale a Uniunii Europene.

(7) Prezentul regulament contribuie la protecția securității publice, instituind totodată măsuri de salvgardare adecvate și solide în vederea protejării drepturilor fundamentale care ar putea fi afectate. Printre acestea se numără dreptul la respectarea vieții private și la protecția datelor cu caracter personal, dreptul la o protecție jurisdicțională efectivă, dreptul la liberă exprimare, inclusiv libertatea de a primi și de a transmite informații, libertatea de a desfășura o activitate comercială și principiul nediscriminării. Autoritățile competente și furnizorii de servicii de găzduire ar trebui să adopte măsuri numai atunci când acestea sunt necesare, adecvate și proporționale în cadrul unei societăți democratice, luând în considerare importanța deosebită acordată libertății de exprimare și de informare, care constituie un fundament esențial al unei societăți pluraliste și democratice și una dintre valorile pe care este întemeiată Uniunea. Măsurile care interferează cu libertatea de exprimare și de informare ar trebui să fie strict direcționate, în sensul că acestea trebuie să servească la prevenirea

[7] Recomandarea (UE) 2018/334 a Comisiei din 1 martie 2018 privind măsuri de combatere eficace a conținutului ilegal online (JO L 63, 6.3.2018, p. 50).

[8] Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (Directiva privind comerțul electronic) (JO L 178, 17.7.2000, p. 1).

diseminării conținutului cu caracter terorist, fără a afecta însă dreptul de a primi și de a transmite informații în mod legal, având în vedere rolul central al furnizorilor de servicii de găzduire în facilitarea dezbaterii publice și a difuzării și primirii de informații, opinii și idei în conformitate cu legea.

(8) Dreptul la o cale de atac eficientă este consacrat la articolul 19 din TUE și la articolul 47 din Carta drepturilor fundamentale a Uniunii Europene. Orice persoană fizică sau juridică are dreptul la o cale de atac judiciară eficientă în fața instanței naționale competente împotriva unei măsuri luate în temeiul prezentului regulament, care ar putea aduce atingere drepturilor persoanei respective. Acest drept include în special posibilitatea ca furnizorii de servicii de găzduire și furnizorii de conținut să conteste efectiv un ordin de eliminare în fața instanței din statul membru ale cărui autorități au emis ordinul respectiv.

(9) Pentru a oferi claritate cu privire la acțiunile care trebuie luate de furnizorii de servicii de găzduire și de autoritățile competente pentru a preveni diseminarea conținutului online cu caracter terorist, prezentul regulament ar trebui să stabilească o definiție cu caracter preventiv a conținutului cu caracter terorist, pe baza definiției infracțiunilor de terorism stabilite de Directiva (UE) 2017/541 a Parlamentului European și a Consiliului[9]. Având în vedere nevoia de a combate cele mai dăunătoare forme de propagandă teroristă online, definiția ar trebui să includă materialele și informațiile care instigă, încurajează sau promovează săvârșirea de infracțiuni teroriste sau contribuirea la acestea, oferă instrucțiuni în acest sens sau promovează participarea la activitățile unui grup terorist. Aceste informații includ în special texte, imagini, înregistrări audio și înregistrări video. Atunci când evaluează dacă un anumit conținut reprezintă conținut cu caracter terorist în sensul prezentului regulament, autoritățile competente și furnizorii de servicii de găzduire ar trebui să ia în considerare factori precum natura și modul de formulare a declarațiilor, contextul în care au fost făcute și potențialul acestora de a conduce la consecințe dăunătoare, afectând securitatea și siguranța persoanelor. Faptul că materialul a fost produs, poate fi atribuit sau este diseminat în numele unei organizații teroriste sau al unei persoane care figurează pe listele UE constituie un factor important pentru evaluare. Conținutul diseminat în scopuri educative, jurnalistice sau de cercetare ar trebui să fie protejat în mod adecvat. În plus, exprimarea unor puncte de vedere radicale, polemice sau controversate în cadrul dezbaterii publice privind chestiuni politice sensibile nu ar trebui să fie considerată conținut cu caracter terorist.

(10) Pentru a include în domeniul său de aplicare serviciile de găzduire online în cadrul cărora este diseminat conținutul cu caracter terorist, prezentul regulament ar trebui să se aplice serviciilor societății informaționale care stochează informații furnizate de un destinatar al serviciului la cererea acestuia și care pun informațiile stocate la dispoziția părților terțe, indiferent dacă această activitate are un caracter pur tehnic, automat și pasiv. De exemplu, astfel de furnizori de servicii ale societății informaționale includ platformele de comunicare socială, serviciile de streaming video, serviciile de partajare de materiale video, imagini și materiale audio, partajarea de fișiere și alte servicii de tip cloud, în măsura în care acești furnizori pun informațiile la dispoziția părților terțe, precum și site-uri pe care utilizatorii pot face comentarii sau posta recenzii. Regulamentul ar trebui să se aplice, de asemenea, furnizorilor de servicii de

[9] Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

găzduire stabiliți în afara Uniunii, dar care oferă servicii în Uniune, întrucât, proporțional, o mare parte a furnizorilor de servicii de găzduire expuși la conținutul cu caracter terorist în cadrul serviciilor oferite sunt stabiliți în țări terțe. Astfel s-ar asigura faptul că toate societățile care desfășoară activități pe piața unică digitală respectă aceleași cerințe, indiferent de țara în care sunt stabilite. Pentru a stabili dacă un furnizor de servicii oferă sau nu servicii în Uniune, este necesară o evaluare din care să reiasă dacă furnizorul de servicii le permite persoanelor juridice sau fizice din unul sau mai multe state membre să îi utilizeze serviciile. Cu toate acestea, simpla accesibilitate, din unul sau mai multe state membre, a site-ului unui furnizor de servicii sau a unei adrese de e-mail și a altor date de contact, luată separat, nu ar trebui să fie o condiție suficientă pentru aplicarea prezentului regulament.

(11) Existența unei legături substanțiale cu Uniunea ar trebui să fie relevantă pentru a stabili domeniul de aplicare al prezentului regulament. Ar trebui să se considere că există o astfel de legătură substanțială cu Uniunea atunci când furnizorul de servicii are un sediu în Uniune sau, în absența acestuia, pe baza existenței unui număr semnificativ de utilizatori în unul sau mai multe state membre sau a direcționării activităților către unul sau mai multe state membre. Direcționarea activităților către unul sau mai multe state membre poate fi determinată examinând toate circumstanțele relevante, cum ar fi utilizarea unei limbi sau a unei monede utilizate în general în statul membru respectiv sau posibilitatea de a comanda bunuri sau servicii. Direcționarea activităților către un stat membru ar putea, de asemenea, să fie stabilită pe baza unor elemente precum existența unei aplicații în magazinul de aplicații național relevant, difuzarea de materiale publicitare locale sau în limba utilizată în statul membru respectiv sau modul de gestionare a relațiilor cu clienții, de exemplu oferirea de servicii de relații cu clienții în limba utilizată în mod obișnuit în statul membru respectiv. Ar trebui să se considere că există o legătură substanțială și în cazul în care un furnizor de servicii își direcționează activitățile către unul sau mai multe state membre astfel cum se prevede la articolul 17 alineatul (1) litera (c) din Regulamentul (CE) nr. 1215/2012 al Parlamentului European și al Consiliului[10]. Pe de altă parte, furnizarea serviciului în vederea simplei respectări a interdicției de discriminare prevăzute în Regulamentul (UE) 2018/302 al Parlamentului European și al Consiliului[11] nu poate fi considerată, exclusiv pe baza acestui motiv, drept direcționare a activităților către un anumit teritoriu din Uniune.

(12) Furnizorii de servicii de găzduire ar trebui să aplice anumite obligații de diligență pentru a preveni diseminarea conținutului cu caracter terorist în cadrul serviciilor lor. Aceste obligații de diligență nu ar trebui să constituie o obligație generală de supraveghere. Obligațiile de diligență ar trebui să includă obligația ca, atunci când aplică prezentul regulament, furnizorii de servicii de găzduire să acționeze în mod diligent, proporțional și nediscriminatoriu în ceea ce privește conținutul pe care îl stochează, în special atunci când pun în aplicare clauzele și condițiile proprii, în scopul de a preveni eliminarea conținutului fără caracter terorist. Eliminarea conținutului sau

---

10 Regulamentul (UE) nr. 1215/2012 al Parlamentului European și al Consiliului din 12 decembrie 2012 privind competența judiciară, recunoașterea și executarea hotărârilor în materie civilă și comercială (JO L 351, 20.12.2012, p. 1).

11 Regulamentul (UE) 2018/302 al Parlamentului European și al Consiliului din 28 februarie 2018 privind prevenirea geoblocării nejustificate și a altor forme de discriminare bazate pe cetățenia sau naționalitatea, domiciliul sau sediul clienților pe piața internă și de modificare a Regulamentelor (CE) nr. 2006/2004 și (UE) 2017/2394, precum și a Directivei 2009/22/CE (JO L 601, 2.3.2018, p. 1).

blocarea accesului la acesta trebuie să se realizeze cu respectarea libertății de exprimare și de informare.

(13) Este necesară armonizarea procedurilor și a obligațiilor care rezultă din ordinele juridice care îi obligă pe furnizorii de servicii de găzduire să elimine conținut cu caracter terorist sau să blocheze accesul la acesta, în urma unei evaluări efectuate de autoritățile competente. Statele membre ar trebui să fie în continuare libere să aleagă autoritățile competente desemnate pentru a îndeplini aceste sarcini, care pot fi autorități administrative, autorități de aplicare a legii sau autorități judiciare. Având în vedere viteza răspândirii conținutului cu caracter terorist în cadrul serviciilor online, se prevede obligația furnizorilor de servicii de găzduire de a se asigura că un conținut cu caracter terorist identificat în ordinul de eliminare este eliminat sau accesul la acesta este blocat în termen de o oră de la primirea ordinului respectiv. Furnizorilor de servicii de găzduire le revine decizia de a elimina sau de a bloca accesul utilizatorilor din Uniune la conținutul în cauză.

(14) Autoritatea competentă ar trebui să transmită ordinul de eliminare direct destinatarului și punctului de contact prin orice mijloace electronice care permit o înregistrare scrisă, în condiții care îi permit furnizorului de servicii să stabilească autenticitatea, inclusiv exactitatea datei și orei de trimitere și de primire a ordinului, de exemplu prin e-mail și platforme securizate sau alte canale securizate, inclusiv cele puse la dispoziție de către furnizorul de servicii, în conformitate cu normele de protecție a datelor cu caracter personal. Această cerință poate fi îndeplinită în special prin utilizarea serviciilor de distribuție electronică înregistrată calificate, astfel cum se prevede în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului[12].

(15) Semnalările emise de autoritățile competente sau de Europol constituie un mijloc eficace și rapid de a informa furnizorii de servicii de găzduire cu privire la un anumit conținut din cadrul serviciilor lor. Acest mecanism de alertare a furnizorilor de servicii de găzduire cu privire la informații care pot fi considerate cu caracter terorist, care îi permite furnizorului să evalueze, în mod voluntar, compatibilitatea cu propriile clauze și condiții, ar trebui să rămână disponibil pe lângă ordinele de eliminare. Este important ca furnizorii de servicii de găzduire să evalueze în mod prioritar aceste semnalări și să ofere un feedback rapid cu privire la măsurile luate. Furnizorul de servicii de găzduire este cel care ia decizia finală de a elimina sau nu conținutul, după ce stabilește dacă acesta este compatibil sau nu cu clauzele și condițiile sale. La punerea în aplicare a prezentului regulament în ceea ce privește semnalările, mandatul Europol, astfel cum este prevăzut în Regulamentul (UE) 2016/794[13], nu este afectat.

(16) Având în vedere raza de acțiune și viteza necesare pentru identificarea și înlăturarea în mod eficace a conținutului cu caracter terorist, adoptarea unor măsuri proactive proporționale, inclusiv prin utilizarea de mijloace automatizate în anumite cazuri, constituie un element esențial pentru abordarea conținutului online cu caracter terorist. În vederea reducerii accesibilității conținutului cu caracter terorist în cadrul serviciilor lor, furnizorii de servicii de găzduire ar trebui să evalueze dacă este adecvat să ia

---

12 Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).

13 Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).

măsuri proactive, în funcție de riscuri și de nivelul de expunere la conținutul cu caracter terorist, precum și de efectele asupra drepturilor terților și de interesul public al informațiilor. În consecință, furnizorii de servicii de găzduire ar trebui să stabilească măsurile proactive adecvate, eficace și proporționale care ar trebui aplicate. Această cerință nu ar trebui să implice o obligație generală de supraveghere. În contextul acestei evaluări, absența ordinelor de eliminare și a semnalărilor adresate unui furnizor de servicii de găzduire indică un nivel scăzut de expunere la conținutul cu caracter terorist.

(17) Atunci când pun în aplicare măsuri proactive, furnizorii de servicii de găzduire ar trebui să se asigure că utilizatorii își mențin dreptul la libertatea de exprimare și de informare, inclusiv dreptul de a primi și a transmite informații. Pe lângă respectarea cerințelor prevăzute în legislație, inclusiv în legislația privind protecția datelor cu caracter personal, furnizorii de servicii de găzduire ar trebui să acționeze cu diligența necesară și să instituie măsuri de salvgardare, inclusiv, după caz, în ceea ce privește supravegherea și verificările efectuate de persoane, pentru a evita luarea unor decizii neintenționate și eronate care să determine eliminarea conținutului fără caracter terorist. Acest lucru este deosebit de important atunci când furnizorii de servicii de găzduire utilizează mijloace automatizate de detectare a conținutului cu caracter terorist. Orice decizie de utilizare a unor mijloace automatizate, indiferent dacă este luată la inițiativa furnizorului de servicii de găzduire sau la cererea autorității competente, ar trebui evaluată pentru a stabili fiabilitatea suportului tehnologic și impactul asupra drepturilor fundamentale.

(18) Pentru a se asigura că furnizorii de servicii de găzduire expuși la conținut terorist iau măsurile adecvate pentru a preveni utilizarea abuzivă a serviciilor lor, autoritățile competente ar trebui să le solicite furnizorilor de servicii de găzduire care au primit un ordin de eliminare devenit definitiv să prezinte măsurile proactive luate. Acestea ar putea consta în măsuri de prevenire a reîncărcării conținutului cu caracter terorist care a fost eliminat sau la care accesul a fost blocat ca urmare a unui ordin de eliminare sau a semnalărilor primite, cu ajutorul unor instrumente publice sau private de comparare cu conținutul despre care se știe că are un caracter terorist. Se pot utiliza, de asemenea, instrumente tehnice fiabile pentru a identifica noi conținuturi cu caracter terorist, fie instrumente disponibile pe piață, fie instrumente elaborate de furnizorul de servicii de găzduire. Furnizorul de servicii ar trebui să transmită informații cu privire la măsurile proactive specifice instituite, pentru a-i permite autorității competente să evalueze dacă măsurile sunt eficace și proporționale și dacă, în cazul în care sunt utilizate mijloace automatizate, furnizorul de servicii de găzduire deține capacitățile necesare pentru supravegherea și verificarea de către persoane. Pentru a evalua eficacitatea și proporționalitatea măsurilor, autoritățile competente ar trebui să ia în considerare parametrii relevanți, inclusiv numărul de ordine de retragere și semnalări adresate furnizorului, capacitatea economică a acestuia și impactul serviciului oferit în ceea ce privește diseminarea de conținut cu caracter terorist (de exemplu, numărul de utilizatori din Uniune).

(19) Ca urmare a solicitării, autoritatea competentă ar trebui să inițieze un dialog cu furnizorul de servicii de găzduire cu privire la măsurile proactive care trebuie instituite. Dacă este necesar, autoritatea competentă ar trebui să impună adoptarea unor măsuri adecvate, eficace și proporționale, în cazul în care consideră că măsurile luate sunt insuficiente pentru acoperirea riscurilor. O decizie de impunere a unor astfel de măsuri proactive specifice nu ar trebui să conducă, în principiu, la impunerea unei obligații generale de supraveghere, astfel cum se prevede la articolul 15 alineatul (1)

din Directiva 2000/31/CE. Având în vedere riscurile deosebit de grave asociate diseminării conținutului cu caracter terorist, deciziile adoptate de autoritățile competente pe baza prezentului regulament ar putea deroga de la abordarea stabilită la articolul 15 alineatul (1) din Directiva 2000/31/CE în ceea ce privește anumite măsuri specifice și direcționate, a căror adoptare este necesară din motive imperative de siguranță publică. Înainte de adoptarea unor astfel de decizii, autoritatea competentă ar trebui să asigure un echilibru just între obiectivele de interes public și drepturile fundamentale implicate, în special libertatea de exprimare și de informare și libertatea de a desfășura o activitate comercială, și să furnizeze o justificare corespunzătoare.

(20) Obligația impusă furnizorilor de servicii de găzduire de a păstra conținutul eliminat și datele conexe ar trebui să fie stabilită pentru scopuri specifice și să fie limitată în timp la ceea ce este necesar. Este necesar ca cerința de păstrare să se extindă la datele conexe în măsura în care aceste date ar fi altfel pierdute ca urmare a eliminării conținutului în cauză. Datele conexe pot include date precum „datele privind abonații”, inclusiv, în special, date referitoare la identitatea furnizorului de conținut, precum și „date privind accesul”, inclusiv, de exemplu, date privind data și ora utilizării de către furnizorul de conținut sau ale conectării la serviciu și ale deconectării de la acesta, împreună cu adresa IP alocată furnizorului de conținut de către furnizorul de servicii de acces la internet.

(21) Obligația de păstrare a conținutului pentru proceduri de reexaminare administrativă sau de control judiciar este necesară și justificată în vederea asigurării unor măsuri de reparare eficace pentru furnizorul de conținut al cărui conținut a fost eliminat sau la conținutul căruia s-a blocat accesul, precum și în vederea republicării acestui conținut în forma anterioară eliminării sale, în funcție de rezultatul procedurii de reexaminare. Obligația de a păstra conținutul în scopuri de anchetare și de urmărire penală este justificată și necesară având în vedere valoarea pe care acest material ar putea să o aibă în contracararea sau prevenirea activității teroriste. În cazul în care întreprinderile elimină materialul sau blochează accesul la acesta, în special prin măsuri proactive proprii, și nu informează autoritatea competentă deoarece apreciază că acest lucru nu intră în sfera de aplicare a articolului 13 alineatul (4) din prezentul regulament, este posibil ca autoritățile de aplicare a legii să nu afle de existența conținutului. Prin urmare, păstrarea conținutului în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism este, de asemenea, justificată. În aceste scopuri, păstrarea obligatorie a datelor este limitată la datele care ar putea avea legătură cu infracțiunile de terorism și, prin urmare, ar putea contribui la urmărirea penală a acestor infracțiuni sau la prevenirea riscurilor majore la adresa siguranței publice.

(22) În vederea asigurării proporționalității, perioada de păstrare ar trebui să fie limitată la șase luni pentru ca furnizorii de conținut să aibă suficient timp ca să inițieze procedura de reexaminare și pentru ca autoritățile de aplicare a legii să aibă acces la datele relevante pentru investigarea și urmărirea penală a infracțiunilor de terorism. Totuși, la cererea autorității care efectuează reexaminarea, această perioadă poate fi prelungită atât cât este necesar în cazul în care procedura de reexaminare este inițiată, dar nu este finalizată în perioada de șase luni. Această durată ar trebui să fie suficientă pentru a permite autorităților de aplicare a legii să păstreze dovezile necesare în ceea ce privește investigațiile, asigurând în același timp un echilibru cu drepturile fundamentale vizate.

(23) Prezentul regulament nu aduce atingere garanțiilor procedurale și măsurilor procedurale de investigare legate de accesul la conținutul și la datele conexe păstrate în

scopul investigării și urmăririi penale a infracțiunilor de terorism, astfel cum sunt reglementate de dreptul intern al statelor membre și de dreptul Uniunii.

(24) Transparența politicilor furnizorilor de servicii de găzduire în ceea ce privește conținutul cu caracter terorist este esențială pentru o creștere a gradului de răspundere față de propriii utilizatori și a încrederii cetățenilor în piața digitală. Furnizorii de servicii de găzduire ar trebui să publice rapoarte anuale privind transparența care să conțină informații relevante privind măsurile întreprinse în legătură cu detectarea, identificarea și eliminarea conținutului cu caracter terorist.

(25) Procedurile de depunere a plângerilor constituie o măsură de salvgardare necesară împotriva eliminării eronate a conținutului protejat în temeiul libertății de exprimare și de informare. Furnizorii de servicii de găzduire ar trebui, așadar, să instituie mecanisme de depunere a plângerilor ușor de utilizat și să se asigure că plângerile sunt tratate cu promptitudine și în deplină transparență față de furnizorul de conținut. Cerința ca furnizorul de servicii de găzduire să republice conținutul în cazul în care acesta a fost eliminat dintr-o eroare nu aduce atingere posibilității furnizorilor de servicii de găzduire de a pune în aplicare propriile clauze și condiții din alte motive.

(26) În conformitate cu dreptul la protecție jurisdicțională, prevăzut la articolul 19 din TUE și la articolul 47 din Carta drepturilor fundamentale a Uniunii Europene, persoanele trebuie să afle motivele care au dus la eliminarea conținutului pe care l-au încărcat sau la blocarea accesului la conținutul respectiv. În acest scop, furnizorul de servicii de găzduire ar trebui să pună la dispoziția furnizorului de conținut informații relevante care să îi permită acestuia din urmă să conteste decizia. Totuși, acest lucru nu necesită neapărat transmiterea unei notificări către furnizorul de conținut. În funcție de circumstanțe, furnizorii de servicii de găzduire pot înlocui conținutul care este considerat ca fiind conținut cu caracter terorist cu un mesaj care să indice că acesta a fost eliminat sau că accesul la acest conținut a fost blocat în conformitate cu prezentul regulament. La cerere, ar trebui să se ofere informații suplimentare privind motivele în cauză și posibilitățile furnizorului de conținut de a contesta decizia. În cazul în care autoritățile competente decid că, din motive de siguranță publică, inclusiv în contextul unei investigații, este inoportun sau neproductiv ca furnizorului de conținut să i se notifice direct eliminarea conținutului sau blocarea accesului la acesta, autoritățile respective ar trebui să informeze furnizorul de servicii de găzduire.

(27) Pentru a evita duplicarea și eventualele interferențe cu investigațiile, autoritățile competente ar trebui să se informeze, să se coordoneze și să coopereze unele cu altele și, după caz, cu Europol atunci când emit ordine de eliminare sau trimit semnalări furnizorilor de servicii de găzduire. În vederea punerii în aplicare a dispozițiilor prezentului regulament, Europol ar putea oferi sprijin în conformitate cu mandatul său actual și cu cadrul juridic existent.

(28) Pentru a asigura punerea în aplicare eficace și suficient de coerentă a măsurilor proactive, autoritățile competente din statele membre ar trebui să se pună de acord cu privire la discuțiile pe care le au cu furnizorii de servicii de găzduire referitoare la identificarea, punerea în aplicare și evaluarea măsurilor proactive specifice. O astfel de cooperare este necesară și în ceea ce privește adoptarea de norme privind sancțiunile, precum și aplicarea și asigurarea respectării acestora.

(29) Este esențial ca autoritatea competentă din statul membru responsabil de impunerea de sancțiuni să fie pe deplin informată cu privire la emiterea de ordine de eliminare și semnalări, precum și cu privire la schimburile ulterioare dintre furnizorul de servicii de găzduire și autoritatea competentă relevantă. În acest scop, statele membre ar trebui să

se asigure că dispun de canale și mecanisme de comunicare adecvate care să permită schimbul de informații relevante în timp util.

(30) Pentru a facilita schimburile rapide între autoritățile competente, precum și cu furnizorii de servicii de găzduire, și pentru a evita duplicarea eforturilor, statele membre pot utiliza instrumentele elaborate de Europol, cum ar fi actuala aplicație de gestionare a semnalărilor conținutului online (IRMa) sau instrumentele care îi vor succeda.

(31) Având în vedere consecințele deosebit de grave ale anumitor conținuturi cu caracter terorist, furnizorii de servicii de găzduire ar trebui să informeze cu promptitudine autoritățile din statul membru în cauză sau autoritățile competente din statul membru în care sunt stabiliți sau în care au un reprezentant legal cu privire la existența oricăror dovezi referitoare la infracțiuni de terorism de care iau cunoștință. Pentru a asigura proporționalitatea, această obligație se limitează la infracțiunile de terorism care corespund definiției de la articolul 3 alineatul (1) din Directiva (UE) 2017/541. Obligația de informare nu implică obligația furnizorilor de servicii de găzduire de a căuta în mod activ astfel de dovezi. Statul membru în cauză este statul membru competent pentru investigarea și urmărirea penală a infracțiunilor de terorism în temeiul Directivei (UE) 2017/541 pe baza cetățeniei infractorului sau a victimei potențiale a infracțiunii sau a locației vizate de actul de terorism. În caz de îndoială, furnizorii de servicii de găzduire pot transmite informațiile către Europol, care ar trebui să ia măsuri în conformitate cu mandatul său, inclusiv să le transmită autorităților naționale competente.

(32) Autoritățile competente ale statelor membre ar trebui să aibă posibilitatea de a utiliza astfel de informații pentru a lua măsurile de investigare prevăzute în dreptul lor intern sau în dreptul Uniunii, inclusiv emiterea unui ordin european de divulgare în temeiul Regulamentului privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală[14].

(33) Atât furnizorii de servicii de găzduire, cât și statele membre ar trebui să stabilească puncte de contact pentru a facilita tratarea rapidă a ordinelor de eliminare și a semnalărilor. Spre deosebire de reprezentantul legal, punctul de contact are scopuri operaționale. Punctul de contact al furnizorului de servicii de găzduire ar trebui să constea din orice mijloace specifice care permit depunerea electronică a ordinelor de eliminare și a semnalărilor, precum și din resurse tehnice și umane care permit tratarea rapidă a acestora. Nu este obligatoriu ca punctul de contact pentru furnizorul de servicii de găzduire să fie situat în Uniune, iar furnizorul de servicii de găzduire este liber să desemneze un punct de contact existent, cu condiția ca acest punct de contact să poată îndeplini funcțiile prevăzute în prezentul regulament. Pentru a garanta eliminarea conținutului cu caracter terorist sau blocarea accesului la acesta în termen de o oră de la primirea ordinului de eliminare, furnizorii de servicii de găzduire ar trebui să se asigure că punctul de contact este accesibil 24 de ore din 24, 7 zile din 7. Informațiile privind punctul de contact ar trebui să indice și limba în care se poate desfășura comunicarea cu punctul de contact. Pentru a facilita comunicarea dintre furnizorii de servicii de găzduire și autoritățile competente, furnizorii de servicii de găzduire sunt încurajați să asigure comunicarea într-una dintre limbile oficiale ale Uniunii în care sunt disponibile clauzele și condițiile lor.

[14] COM(2018) 225 final.

(34) Având în vedere faptul că nu există o obligație generală ca furnizorii de servicii să asigure o prezență fizică pe teritoriul Uniunii, ar trebui stabilit clar care este statul membru competent în cazul furnizorului de servicii de găzduire care oferă servicii pe teritoriul Uniunii. Ca regulă generală, furnizorul de servicii de găzduire este de competența statului membru în care își are sediul principal sau în care și-a desemnat un reprezentant legal. Cu toate acestea, în cazul în care un alt stat membru emite un ordin de eliminare, autoritățile sale ar trebui să fie în măsură să asigure executarea ordinelor respective prin aplicarea unor măsuri coercitive de natură nepunitivă, cum ar fi penalitățile cu titlu cominatoriu. Totuși, în cazul unui furnizor de servicii de găzduire care nu are niciun sediu în Uniune și care nu desemnează un reprezentant legal, orice stat membru ar trebui să poată aplica sancțiuni, cu condiția respectării principiului *ne bis in idem*.

(35) Furnizorii de servicii de găzduire care nu au niciun sediu în Uniune ar trebui să desemneze în scris un reprezentant legal pentru a asigura îndeplinirea și asigurarea respectării obligațiilor care le revin în temeiul prezentului regulament.

(36) Reprezentantul legal ar trebui să fie abilitat din punct de vedere juridic să acționeze în numele furnizorului de servicii de găzduire.

(37) În sensul prezentului regulament, statele membre ar trebui să desemneze autorități competente. Cerința de desemnare a unor autorități competente nu presupune neapărat instituirea de noi autorități, funcțiile stabilite în prezentul regulament putând fi încredințate unor organisme existente. Prezentul regulament impune desemnarea de autorități competente pentru emiterea ordinelor de eliminare și a semnalărilor, pentru supravegherea măsurilor proactive și pentru impunerea de sancțiuni. Este la latitudinea statelor membre să decidă numărul de autorități pe care doresc să le desemneze pentru îndeplinirea acestor sarcini.

(38) Pentru a asigura îndeplinirea efectivă de către furnizorii de servicii de găzduire a obligațiilor care le revin în temeiul prezentului regulament, este necesar să se stabilească o serie de sancțiuni. Statele membre ar trebui să adopte norme privind sancțiunile, inclusiv, după caz, orientări privind amenzile. Este necesar să se stabilească sancțiuni deosebit de aspre pentru cazurile în care furnizorul de servicii de găzduire omite în mod sistematic să elimine conținutul cu caracter terorist sau să blocheze accesul la acesta în termen de o oră de la primirea ordinului de eliminare. Nerespectarea normelor în anumite cazuri ar putea fi sancționată respectându-se principiile *ne bis in idem* și proporționalității și asigurându-se faptul că sancțiunile țin cont de neîndeplinirea sistematică a obligațiilor. Pentru a garanta securitatea juridică, regulamentul ar trebui să stabilească în ce măsură obligațiile relevante pot face obiectul unor sancțiuni. În cazul nerespectării articolului 6, ar trebui să se adopte sancțiuni numai în ceea ce privește obligațiile care decurg dintr-o solicitare de raportare efectuată în temeiul articolului 6 alineatul (2) sau dintr-o decizie de impunere a unor măsuri proactive suplimentare în temeiul articolului 6 alineatul (4). Atunci când se stabilește dacă ar trebui impuse sau nu sancțiuni financiare, ar trebui să se țină seama în mod corespunzător de resursele financiare ale furnizorului. Statele membre ar trebui să se asigure că sancțiunile nu încurajează eliminarea conținutului care nu este conținut cu caracter terorist.

(39) Utilizarea unor formulare standardizate facilitează cooperarea și schimbul de informații între autoritățile competente și furnizorii de servicii, permițându-le să comunice într-un mod mai rapid și mai eficace. Este deosebit de important ca ordinelor de eliminare să li se dea curs rapid. Formularele reduc costurile de traducere

și contribuie la asigurarea unui nivel ridicat de calitate. De asemenea, formularele de răspuns ar trebui să permită un schimb standardizat de informații, iar acest lucru va fi deosebit de important în cazul în care furnizorii de servicii nu își vor putea respecta obligațiile. Canalele de transmitere autentificate pot garanta autenticitatea ordinului de eliminare, inclusiv exactitatea datei și a orei la care s-a trimis și la care s-a primit ordinul.

(40) Pentru a permite o modificare rapidă, atunci când este necesar, a conținutului formularelor care trebuie utilizate în sensul prezentului regulament, Comisiei ar trebui să i se delege competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene în vederea modificării anexelor I, II și III la prezentul regulament. Pentru a se putea ține seama de evoluția tehnologiei și a cadrului juridic aferent, Comisia ar trebui, de asemenea, să fie împuternicită să adopte acte delegate pentru a completa prezentul regulament cu cerințe tehnice privind mijloacele electronice care trebuie utilizate de către autoritățile competente pentru transmiterea ordinelor de eliminare. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, iar respectivele consultări să se efectueze în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare[15]. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces în mod sistematic la reuniunile grupurilor de experți ale Comisiei care se ocupă de pregătirea actelor delegate.

(41) Statele membre ar trebui să colecteze informații privind punerea în aplicare a legislației. Este necesar să se stabilească un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament, pentru a contribui la evaluarea legislației.

(42) Pe baza constatărilor și a concluziilor raportului privind punerea în aplicare și a rezultatelor exercițiului de monitorizare, Comisia ar trebui să efectueze o evaluare a prezentului regulament cel mai devreme la trei ani după intrarea sa în vigoare. Evaluarea ar trebui să se bazeze pe următoarele cinci criterii: eficiență, eficacitate, relevanță, coerență și valoare adăugată europeană. Aceasta va viza funcționarea diferitelor măsuri operaționale și tehnice prevăzute în regulament, inclusiv eficacitatea măsurilor de îmbunătățire a detectării, a identificării și a eliminării conținutului cu caracter terorist, eficacitatea mecanismelor de salvgardare, precum și impactul asupra drepturilor și intereselor părților terțe care ar putea fi afectate, și va include o reexaminare a cerinței de informare a furnizorilor de conținut.

(43) Deoarece obiectivul prezentului regulament, și anume asigurarea unei bune funcționări a pieței unice digitale prin prevenirea diseminării conținutului online cu caracter terorist, nu poate fi realizat în mod satisfăcător de către statele membre și, prin urmare, având în vedere amploarea și efectele limitării, poate fi realizat mai bine la nivelul Uniunii, Uniunea poate adopta măsuri, în conformitate cu principiul subsidiarității prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, prevăzut la același articol, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivului menționat,

[15] JO L 123, 12.5.2016, p. 1.

ADOPTĂ PREZENTUL REGULAMENT:

SECȚIUNEA I
DISPOZIȚII GENERALE

Articolul 1
Obiect și domeniu de aplicare

(1) Prezentul regulament stabilește norme uniforme pentru a preveni utilizarea abuzivă a serviciilor de găzduire pentru diseminarea conținutului online cu caracter terorist. Acesta prevede în special:

(a) norme privind obligațiile de diligență pe care trebuie să le aplice furnizorii de servicii de găzduire pentru a preveni diseminarea conținutului cu caracter terorist prin intermediul serviciilor lor și pentru a asigura, atunci când este necesar, eliminarea rapidă a acestuia;

(b) un set de măsuri care urmează să fie instituite de statele membre pentru identificarea conținutului cu caracter terorist, pentru eliminarea rapidă a acestuia de către furnizorii de servicii de găzduire și pentru facilitarea cooperării cu autoritățile competente din alte state membre, cu furnizorii de servicii de găzduire și, după caz, cu organismele relevante ale Uniunii.

(2) Prezentul regulament se aplică furnizorilor de servicii de găzduire care oferă servicii în Uniune, indiferent de locul unde se află sediul lor principal.

Articolul 2
Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „furnizor de servicii de găzduire” înseamnă un furnizor de servicii ale societății informaționale care constau în stocarea informațiilor furnizate de furnizorul conținutului la cererea acestuia și în punerea informațiilor respective la dispoziția terților;

(2) „furnizor de conținut” înseamnă un utilizator care a furnizat informații care sunt stocate sau care au fost stocate la cererea sa de către un furnizor de servicii de găzduire;

(3) „oferirea de servicii în Uniune” înseamnă: oferirea posibilității ca persoanele juridice sau fizice din unul sau mai multe state membre să utilizeze serviciile furnizorului de servicii de găzduire care are o legătură substanțială cu statul membru sau cu statele membre în cauză, cum ar fi:

(a) existența unui sediu al furnizorului de servicii de găzduire în Uniune;

(b) existența unui număr semnificativ de utilizatori în unul sau mai multe state membre;

(c) direcționarea activităților către unul sau mai multe state membre.

(4) „infracțiuni de terorism” înseamnă infracțiunile care corespund definiției de la articolul 3 alineatul (1) din Directiva (UE) 2017/541;

(5) „conținut cu caracter terorist” înseamnă una sau mai multe dintre următoarele informații care:

(a) instigă la săvârșirea de infracțiuni de terorism sau promovează săvârșirea unor astfel de infracțiuni, inclusiv prin glorificarea lor, generând astfel un pericol de săvârșire a unor astfel de infracțiuni;

(b) încurajează contribuirea la infracțiuni de terorism;

(c) promovează activitățile unui grup terorist, în special prin încurajarea participării la un grup terorist sau a sprijinirii unui grup terorist în sensul articolului 2 punctul 3 din Directiva (UE) 2017/541;

(d) oferă instrucțiuni referitoare la metode sau tehnici cu scopul săvârșirii unor infracțiuni de terorism;

(6) „diseminarea conținutului cu caracter terorist” înseamnă punerea conținutului cu caracter terorist la dispoziția unor părți terțe prin intermediul serviciilor furnizorilor de servicii de găzduire;

(7) „clauze și condiții” înseamnă toate condițiile și clauzele, indiferent de denumirea sau forma acestora, care reglementează relația contractuală dintre furnizorul de servicii de găzduire și utilizatorii acestora;

(8) „semnalare” înseamnă o notificare adresată de către o autoritate competentă sau, după caz, de către un organism relevant al Uniunii, unui furnizor de servicii de găzduire, referitoare la informații care pot fi considerate conținut cu caracter terorist, a căror compatibilitate cu propriile clauze și condiții trebuie să fie examinată voluntar de către furnizor, cu scopul de a preveni diseminarea conținutului cu caracter terorist;

(9) „sediu principal” înseamnă sediul central sau sediul social în cadrul căruia se exercită principalele funcții financiare și controlul operațional.

SECȚIUNEA II
Măsuri de prevenire a diseminării conținutului online cu caracter terorist

Articolul 3
Obligații de diligență

(1) Furnizorii de servicii de găzduire iau măsuri adecvate, rezonabile și proporționale, în conformitate cu prezentul regulament, pentru a combate diseminarea conținutului cu caracter terorist și pentru a-i proteja pe utilizatori împotriva conținutului cu caracter terorist. În acest sens, aceștia acționează în mod diligent, proporțional și nediscriminatoriu, luând în considerare în mod corespunzător drepturile fundamentale ale utilizatorilor, și țin cont de importanța fundamentală a libertății de exprimare și de informare într-o societate deschisă și democratică.

(2) Furnizorii de servicii de găzduire includ în clauzele și condițiile lor dispoziții menite să prevină diseminarea conținutului cu caracter terorist și le aplică.

Articolul 4
Ordine de eliminare

(1) Autoritatea competentă are competența de a emite o decizie prin care să îi impună furnizorului de servicii de găzduire să elimine conținutul cu caracter terorist sau să blocheze accesul la acesta.

(2) Furnizorii de servicii de găzduire elimină conținutul cu caracter terorist sau blochează accesul la acesta în termen de o oră de la primirea ordinului de eliminare.

(3) Ordinele de eliminare conțin următoarele elemente, în conformitate cu formularul prevăzut în anexa I:

(a) identificarea autorității competente care emite ordinul de eliminare și autentificarea ordinului de eliminare de către autoritatea competentă;

(b) o expunere a motivelor care să explice de ce conținutul este considerat conținut cu caracter terorist, cel puțin prin referire la categoriile de conținuturi cu caracter terorist enumerate la articolul 2 punctul 5;

(c) o adresă URL (*Uniform Resource Locator*) și, dacă este necesar, informații suplimentare care să permită identificarea conținutului menționat;

(d) o trimitere la prezentul regulament ca temei juridic al ordinului de eliminare;

(e) marca temporală a emiterii ordinului;

(f) informații privind căile de atac de care dispun furnizorul de servicii de găzduire și furnizorul de conținut;

(g) dacă este relevant, decizia de a nu comunica informațiile cu privire la eliminarea conținutului cu caracter terorist sau blocarea accesului la acesta, astfel cum se menționează la articolul 11.

(4) La cererea furnizorului de servicii de găzduire sau a furnizorului de conținut, autoritatea competentă furnizează o expunere detaliată a motivelor, fără a aduce atingere obligației furnizorului de servicii de găzduire de a respecta ordinul de eliminare în termenul stabilit la alineatul (2).

(5) Autoritățile competente adresează ordinele de eliminare sediului principal al furnizorului de servicii de găzduire sau reprezentantului legal desemnat de furnizorul de servicii de găzduire în temeiul articolului 16 și le transmit punctului de contact menționat la articolul 14 alineatul (1). Aceste ordine se trimit prin mijloace electronice capabile să producă o înregistrare scrisă și în condiții care permit stabilirea autenticității expeditorului, inclusiv exactitatea datei și a orei la care s-a trimis și la care s-a primit ordinul.

(6) Furnizorii de servicii de găzduire confirmă primirea ordinului și, fără întârzieri nejustificate, informează autoritatea competentă cu privire la eliminarea conținutului cu caracter terorist sau la blocarea accesului la acesta, indicând, în special, data și ora la care au întreprins acțiunea respectivă, utilizând formularul prevăzut în anexa II.

(7) În cazul în care furnizorul de servicii de găzduire nu poate respecta ordinul de eliminare din cauza unei situații de forță majoră sau a unei imposibilități *de facto* care nu îi poate fi imputată, acesta informează autoritatea competentă fără întârzieri nejustificate, explicând motivele și utilizând formularul prevăzut în anexa III. Termenul prevăzut la alineatul (2) se aplică de îndată ce motivele invocate nu mai sunt valabile.

(8) În cazul în care furnizorul de servicii de găzduire nu poate respecta ordinul de eliminare deoarece ordinul conține erori evidente sau nu conține informații suficiente pentru a permite executarea sa, acesta informează autoritatea competentă fără întârzieri nejustificate, solicitând clarificările necesare și utilizând formularul prevăzut în anexa III. Termenul prevăzut la alineatul (2) se aplică de îndată ce îi sunt transmise clarificările solicitate.

(9) Autoritatea competentă care a emis ordinul de eliminare informează autoritatea competentă care supraveghează punerea în aplicare a măsurilor proactive, menționată la articolul 17 alineatul (1) litera (c), atunci când ordinul de eliminare devine definitiv. Un ordin de eliminare devine definitiv dacă nu a fost contestat în termenul prevăzut de dreptul intern aplicabil sau dacă, în urma unei căi de atac, a fost confirmat.

Articolul 5
Semnalări

(1) Autoritatea competentă sau organismul relevant al Uniunii poate trimite o semnalare unui furnizor de servicii de găzduire.

(2) Furnizorii de servicii de găzduire instituie măsuri operaționale și tehnice care facilitează evaluarea rapidă a conținutului care a fost trimis de autoritățile competente și, după caz, de organismele relevante ale Uniunii, pentru a fi examinat în mod voluntar de către aceștia.

(3) Semnalarea se adresează sediului principal al furnizorului de servicii de găzduire sau reprezentantului legal desemnat de furnizorul de servicii în temeiul articolului 16 și se transmite punctului de contact menționat la articolul 14 alineatul (1). Semnalările se trimit prin mijloace electronice.

(4) Semnalarea conține informații suficient de detaliate, inclusiv motivele pentru care conținutul este considerat conținut cu caracter terorist, o adresă URL și, dacă este necesar, informații suplimentare care să permită identificarea conținutului cu caracter terorist semnalat.

(5) Furnizorul de servicii de găzduire evaluează cu prioritate conținutul identificat în semnalare în conformitate cu clauzele și condițiile proprii și decide dacă să elimine conținutul sau să blocheze accesul la acesta.

(6) Furnizorul de servicii de găzduire informează prompt autoritatea competentă sau organismul relevant al Uniunii cu privire la rezultatul evaluării și la data și ora la care a întreprins o eventuală acțiune ca urmare a semnalării.

(7) În cazul în care furnizorul de servicii de găzduire consideră că semnalarea nu conține informații suficiente pentru a evalua conținutul semnalat, acesta informează fără întârziere autoritățile competente sau organismul relevant al Uniunii, solicitând informațiile sau clarificările suplimentare necesare.

Articolul 6
Măsuri proactive

(1) Furnizorii de servicii de găzduire iau măsuri proactive, atunci când acestea se impun, pentru a-și proteja serviciile împotriva diseminării de conținut cu caracter terorist. Măsurile trebuie să fie eficace și proporționale, ținând seama de riscul și nivelul de expunere la conținutul cu caracter terorist, de drepturile fundamentale ale utilizatorilor și de importanța fundamentală a libertății de exprimare și de informare într-o societate deschisă și democratică.

(2) Atunci când este informată în conformitate cu articolul 4 alineatul (9), autoritatea competentă menționată la articolul 17 alineatul (1) litera (c) solicită furnizorului de servicii de găzduire să prezinte un raport, în termen de trei luni de la primirea

solicitării și, ulterior, cel puțin o dată pe an, cu privire la măsurile proactive specifice pe care le-a adoptat, inclusiv prin utilizarea de instrumente automatizate, pentru:

(a) a preveni reîncărcarea conținutului care a fost eliminat sau la care s-a blocat accesul deoarece se consideră că este un conținut cu caracter terorist;

(b) a detecta, a identifica și a elimina rapid conținutul cu caracter terorist sau a bloca rapid accesul la acesta.

Această solicitare se trimite la sediul principal al furnizorului de servicii de găzduire sau reprezentantului legal desemnat de furnizorul de servicii.

În rapoarte se includ toate informațiile relevante care să permită autorității competente menționate la articolul 17 alineatul (1) litera (c) să evalueze dacă măsurile proactive sunt eficace și proporționale, inclusiv dacă eventualele instrumente automatizate utilizate și mecanismele de supraveghere și de verificare de către oameni funcționează.

(3) În cazul în care autoritatea competentă menționată la articolul 17 alineatul (1) litera (c) consideră că măsurile proactive luate și raportate în temeiul alineatului (2) sunt insuficiente pentru a atenua și a gestiona riscul și nivelul de expunere, aceasta poate solicita furnizorului de servicii de găzduire să adopte măsuri proactive specifice suplimentare. În acest scop, furnizorul de servicii de găzduire cooperează cu autoritatea competentă menționată la articolul 17 alineatul (1) litera (c) pentru a identifica măsurile specifice pe care ar trebui să le instituie furnizorul de servicii de găzduire, pentru a stabili principalele obiective și jaloane, precum și termenele de realizare a acestora.

(4) În cazul în care nu se poate ajunge la niciun acord în termen de trei luni de la adresarea solicitării în temeiul alineatului (3), autoritatea competentă menționată la articolul 17 alineatul (1) litera (c) poate emite o decizie prin care să impună măsuri proactive specifice suplimentare, necesare și proporționale. Atunci când adoptă această decizie, autoritatea competentă ține cont în special de capacitatea economică a furnizorului de servicii de găzduire, de efectul acestor măsuri asupra drepturilor fundamentale ale utilizatorilor și de importanța fundamentală a libertății de exprimare și de informare. Decizia se trimite la sediul principal al furnizorului de servicii de găzduire sau reprezentantului legal desemnat de furnizorul de servicii. Furnizorul de servicii de găzduire raportează periodic cu privire la punerea în aplicare a măsurilor, conform indicațiilor autorității competente menționate la articolul 17 alineatul (1) litera (c).

(5) Un furnizor de servicii de găzduire poate, în orice moment, să solicite autorității competente menționate la articolul 17 alineatul (1) litera (c) reexaminarea și, după caz, revocarea unei solicitări sau a unei decizii emise în temeiul alineatelor (2), (3) și, respectiv, (4). Autoritatea competentă emite o decizie motivată într-un termen rezonabil de la primirea solicitării din partea furnizorului de servicii de găzduire.

Articolul 7
Păstrarea conținutului și a datelor conexe

(1) Furnizorii de servicii de găzduire păstrează conținutul cu caracter terorist care a fost eliminat sau la care accesul a fost blocat ca urmare a unui ordin de eliminare, a unei semnalări sau a unor măsuri proactive în temeiul articolelor 4, 5 și 6 și a datelor conexe eliminate ca urmare a eliminării conținutului cu caracter terorist și care sunt necesare pentru:

(a) proceduri de reexaminare administrativă sau de control judiciar;

(b) prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism.

(2) Conținutul cu caracter terorist și datele conexe menționate la alineatul (1) se păstrează timp de șase luni. La cererea autorității sau a instanței competente, conținutul cu caracter terorist se păstrează o perioadă mai lungă, în cazul în care și atât timp cât acest lucru este necesar pentru desfășurarea procedurilor de reexaminare administrativă sau de control judiciar menționate la alineatul (1) litera (a).

(3) Furnizorii de servicii de găzduire se asigură că atât conținutul cu caracter terorist, cât și datele conexe păstrate în temeiul alineatelor (1) și (2) fac obiectul unor măsuri de salvgardare tehnice și organizatorice adecvate.

Respectivele măsuri de salvgardare tehnice și organizatorice asigură accesul la conținutul cu caracter terorist și la datele conexe și prelucrarea acestora exclusiv în scopurile menționate la alineatul (1) și asigură un nivel ridicat de securitate a datelor cu caracter personal în cauză. Furnizorii de servicii de găzduire revizuiesc și actualizează respectivele măsuri de salvgardare atunci când este necesar.

SECȚIUNEA III
MĂSURILE DE SALVGARDARE ȘI RĂSPUNDEREA

Articolul 8
Obligații în materie de transparență

(1) Furnizorii de servicii de găzduire prezintă, în clauzele și condițiile lor, politica pe care o aplică pentru prevenirea diseminării conținutului cu caracter terorist, inclusiv, după caz, o explicație pertinentă privind funcționarea măsurilor proactive și utilizarea instrumentelor automatizate.

(2) Furnizorii de servicii de găzduire publică anual un raport privind transparența referitor la măsurile întreprinse pentru combaterea diseminării conținutului cu caracter terorist.

(3) Rapoartele privind transparența conțin cel puțin următoarele informații:

(a) informații referitoare la măsurile luate de furnizorul de servicii de găzduire în ceea ce privește detectarea, identificarea și eliminarea conținutului cu caracter terorist;

(b) informații referitoare la măsurile luate de furnizorul de servicii de găzduire pentru a preveni reîncărcarea conținutului care a fost eliminat sau la care s-a blocat accesul deoarece se consideră că este un conținut cu caracter terorist;

(c) numărul de conținuturi cu caracter terorist care au fost eliminate sau la care accesul a fost blocat ca urmare a unor ordine de eliminare, a unor semnalări sau, respectiv, a unor măsuri proactive;

(d) o prezentare generală și rezultatele procedurilor de depunere a plângerilor.

Articolul 9

Măsuri de salvgardare privind utilizarea și punerea în aplicare a măsurilor proactive

(1) În cazul în care furnizorii de servicii de găzduire utilizează instrumente automatizate în temeiul prezentului regulament cu privire la conținutul pe care îl stochează, aceștia prevăd măsuri de salvgardare eficace și adecvate, astfel încât deciziile luate privind conținutul în cauză, în special deciziile de a elimina sau a bloca accesul la conținutul considerat conținut cu caracter terorist, să fie corecte și întemeiate.

(2) Măsurile de salvgardare respective constau în special în supravegherea și efectuarea de verificări de către o persoană, dacă este nevoie, și, în orice caz, atunci când este necesară o evaluare detaliată a contextului relevant pentru a se stabili dacă respectivul conținut trebuie considerat conținut cu caracter terorist.

Articolul 10

Mecanisme de depunere a plângerilor

(1) Furnizorii de servicii de găzduire instituie mecanisme eficace și accesibile care să permită furnizorilor de conținut al căror conținut a fost eliminat sau la care s-a blocat accesul ca urmare a unei semnalări efectuate în temeiul articolului 5 sau a unor măsuri proactive luate în temeiul articolului 6 să depună o plângere împotriva acțiunii furnizorului de servicii de găzduire prin care să solicite republicarea conținutului.

(2) Furnizorii de servicii de găzduire analizează prompt fiecare plângere primită și republică conținutul, fără întârzieri nejustificate, în cazul în care eliminarea sa sau blocarea accesului a fost nejustificată. Aceștia informează autorul plângerii cu privire la rezultatul examinării.

Articolul 11

Informarea furnizorilor de conținut

(1) În cazul în care furnizorii de servicii de găzduire elimină un conținut cu caracter terorist sau au blocat accesul la acest conținut, aceștia informează furnizorul de conținut cu privire la eliminarea conținutului cu caracter terorist sau la blocarea accesului la acesta.

(2) La cererea furnizorului de conținut, furnizorul de servicii de găzduire îi comunică acestuia motivele eliminării sau ale blocării accesului și posibilitățile de contestare a deciziei.

(3) Obligația prevăzută la alineatele (1) și (2) nu se aplică în cazul în care autoritatea competentă decide că nu ar trebui să se efectueze nicio informare din motive de siguranță publică, cum ar fi prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor de terorism, atât timp cât este necesar, dar nu mai mult de [patru] săptămâni de la adoptarea deciziei. În acest caz, furnizorul de servicii de găzduire nu comunică nicio informație privind eliminarea conținutului cu caracter terorist sau blocarea accesului la acesta.

SECȚIUNEA IV
Cooperarea dintre autoritățile competente, organismele Uniunii și furnizorii de servicii de găzduire

Articolul 12
Capacitățile autorităților competente

Statele membre se asigură că autoritățile lor competente dispun de capacitatea necesară și de resurse suficiente pentru a-și atinge obiectivele și pentru a-și îndeplini obligațiile care le revin în temeiul prezentului regulament.

Articolul 13
Cooperarea dintre furnizorii de servicii de găzduire, autoritățile competente și, după caz, organismele relevante ale Uniunii

(1) Autoritățile competente din statele membre se informează, se coordonează și cooperează unele cu altele și, după caz, cu organismele relevante ale Uniunii, cum ar fi Europol, în ceea ce privește ordinele de eliminare și semnalările, în scopul de a evita suprapunerile, de a spori coordonarea și de a evita interferențele cu investigațiile din diferitele state membre.

(2) Autoritățile competente din statele membre informează, se coordonează și cooperează cu autoritatea competentă menționată la articolul 17 alineatul (1) literele (c) și (d) în ceea ce privește măsurile luate în temeiul articolului 6 și măsurile de executare luate în temeiul articolului 18. Statele membre se asigură că autoritatea competentă menționată la articolul 17 alineatul (1) literele (c) și (d) deține toate informațiile relevante. În acest scop, statele membre instituie canale sau mecanisme de comunicare adecvate care să asigure schimbul de informații relevante în timp util.

(3) Statele membre și furnizorii de servicii de găzduire pot alege să utilizeze instrumente specifice, inclusiv, dacă este cazul, cele stabilite de organisme relevante ale Uniunii, cum ar fi Europol, pentru a facilita în special:

   (a) prelucrarea și feedback-ul privind ordinele de eliminare prevăzute la articolul 4;

   (b) prelucrarea și feedback-ul privind semnalările prevăzute la articolul 5;

   (c) cooperarea în vederea identificării și punerii în aplicare a măsurilor proactive prevăzute la articolul 6.

(4) În cazul în care furnizorii de servicii de găzduire iau cunoștință de vreo dovadă referitoare la infracțiuni de terorism, aceștia informează prompt autoritățile competente pentru investigarea și urmărirea penală a infracțiunilor din statul membru în cauză sau punctul de contact din statul membru în care au sediul principal sau un reprezentant legal, în conformitate cu articolul 14 alineatul (2). În caz de îndoială, furnizorii de servicii de găzduire pot transmite aceste informații către Europol, care urmează să ia măsuri corespunzătoare.

Articolul 14
Puncte de contact

(1) Furnizorii de servicii de găzduire stabilesc un punct de contact care să primească ordinele de eliminare și semnalările prin mijloace electronice și să asigure

prelucrarea rapidă a acestora în conformitate cu articolele 4 și 5. Aceștia se asigură că informațiile privind punctul de contact sunt făcute publice.

(2) În informațiile menționate la alineatul (1) se precizează limba sau limbile oficiale ale Uniunii, astfel cum sunt menționate în Regulamentul 1/58, în care se poate desfășura comunicarea cu punctul de contact și în care trebuie să aibă loc corespondența ulterioară privind ordinele de eliminare și semnalările prevăzute la articolele 4 și 5. Printre acestea se numără cel puțin una dintre limbile oficiale ale statului membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal, în conformitate cu articolul 16.

(3) Statele membre stabilesc un punct de contact care să trateze solicitările de clarificare și feedback cu privire la ordinele de eliminare și semnalările pe care le emit. Informațiile referitoare la punctul de contact se fac publice.

SECȚIUNEA V
PUNERE ÎN APLICARE ȘI EXECUTARE

Articolul 15
Competență

(1) Statul membru în care se află sediul principal al furnizorului de servicii de găzduire este competent în sensul articolelor 6, 18 și 21. Se consideră că un furnizor de servicii de găzduire al cărui sediu principal nu se află în unul dintre statele membre este de competența statului membru în care își are reședința sau sediul reprezentantul legal menționat la articolul 16.

(2) În cazul în care un furnizor de servicii de găzduire nu desemnează un reprezentant legal, sunt competente toate statele membre.

(3) În cazul în care o autoritate a unui alt stat membru emite un ordin de eliminare în conformitate cu articolul 4 alineatul (1), statul membru respectiv are competența de a adopta măsuri coercitive în conformitate cu dreptul său intern în vederea executării ordinului de eliminare.

Articolul 16
Reprezentantul legal

(1) Un furnizor de servicii de găzduire care nu are un sediu în Uniune, dar oferă servicii în Uniune desemnează, în scris, o persoană fizică sau juridică în calitate de reprezentant legal al său în Uniune pentru primirea, asigurarea respectării și executarea ordinelor de eliminare, a semnalărilor, a solicitărilor și a deciziilor emise de autoritățile competente în temeiul prezentului regulament. Reprezentantul legal trebuie să își aibă reședința sau sediul în unul dintre statele membre în care furnizorul de servicii de găzduire își oferă serviciile.

(2) Furnizorul de servicii de găzduire încredințează reprezentantului legal sarcina de a primi, a asigura respectarea și a executa ordinele de eliminare, semnalările, solicitările și deciziile menționate la alineatul (1) în numele furnizorului de servicii de găzduire în cauză. Furnizorii de servicii de găzduire îi conferă reprezentantului lor legal competențele și resursele necesare pentru a coopera cu autoritățile competente și pentru a respecta deciziile și ordinele în cauză.

(3) Reprezentantul legal desemnat poate fi considerat răspunzător pentru nerespectarea obligațiilor prevăzute în prezentul regulament, fără a se aduce atingere răspunderii furnizorului de servicii de găzduire și acțiunilor în justiție care ar putea fi inițiate împotriva acestuia.

(4) Furnizorul de servicii de găzduire notifică desemnarea autorității competente menționate la articolul 17 alineatul (1) litera (d) din statul membru în care își are reședința sau sediul reprezentantul legal. Informațiile referitoare la reprezentantul legal se fac publice.

SECȚIUNEA VI
DISPOZIȚII FINALE

Articolul 17
Desemnarea autorităților competente

(1) Fiecare stat membru desemnează autoritatea sau autoritățile competente pentru:

(a) a emite ordine de eliminare în temeiul articolului 4;

(b) a detecta, a identifica și a semnala conținuturile cu caracter terorist furnizorilor de servicii de găzduire în temeiul articolului 5;

(c) a supraveghea punerea în aplicare a măsurilor proactive în temeiul articolului 6;

(d) a asigura respectarea obligațiilor prevăzute în prezentul regulament prin aplicarea de sancțiuni în temeiul articolului 18.

(2) Până cel târziu la [*șase luni de la intrarea în vigoare a prezentului regulament*], statele membre îi notifică Comisiei autoritățile competente menționate la alineatul (1). Comisia publică această notificare și eventualele modificări ale acesteia în *Jurnalul Oficial al Uniunii Europene*.

Articolul 18
Sancțiuni

(1) Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării obligațiilor care le revin furnizorilor de servicii de găzduire în temeiul prezentului regulament și iau toate măsurile necesare pentru a asigura punerea în aplicare a sancțiunilor respective. Aceste sancțiuni se limitează la încălcarea obligațiilor prevăzute la:

(a) articolul 3 alineatul (2) (clauzele și condițiile furnizorilor de servicii de găzduire);

(b) articolul 4 alineatele (2) și (6) (executarea ordinelor de eliminare și feedback-ul referitor la acestea);

(c) articolul 5 alineatele (5) și (6) (evaluarea semnalărilor și feedback-ul referitor la acestea);

(d) articolul 6 alineatele (2) și (4) (rapoartele privind măsurile proactive și adoptarea de măsuri în urma unei decizii de impunere a unor măsuri proactive specifice);

(e) articolul 7 (păstrarea datelor);

(f) articolul 8 (transparență);

(g) articolul 9 (măsurile de salvgardare legate de măsurile proactive);

(h) articolul 10 (procedurile de depunere a plângerilor);

(i) articolul 11 (informarea furnizorilor de conținut);

(j) articolul 13 alineatul (4) (informarea privind dovezile referitoare la infracțiuni de terorism);

(k) articolul 14 alineatul (1) (punctele de contact);

(l) articolul 16 (desemnarea unui reprezentant legal).

(2) Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive. Până cel târziu la … [*șase luni după data intrării în vigoare a prezentului regulament*], statele membre notifică Comisiei normele și măsurile respective, precum și orice modificare ulterioară a acestora.

(3) Statele membre se asigură că, atunci când stabilesc tipul și nivelul sancțiunilor, autoritățile competente țin cont de toate circumstanțele relevante, inclusiv de:

(a) natura, gravitatea și durata încălcării;

(b) caracterul încălcării (intenționat sau din neglijență);

(c) încălcările anterioare comise de persoana juridică considerată responsabilă;

(d) capacitatea financiară a persoanei juridice considerate răspunzătoare;

(e) nivelul de cooperare al furnizorului de servicii de găzduire cu autoritățile competente.

(4) Statele membre se asigură că nerespectarea sistematică a obligațiilor prevăzute la articolul 4 alineatul (2) face obiectul unor sancțiuni financiare de până la 4 % din cifra de afaceri globală a furnizorului de servicii de găzduire corespunzătoare ultimului exercițiu financiar.

Articolul 19

Cerințe tehnice și modificări ale formularelor pentru ordinele de eliminare

(1) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 20 pentru a completa prezentul regulament cu cerințe tehnice privind mijloacele electronice pe care autoritățile competente trebuie să le utilizeze pentru transmiterea ordinelor de eliminare.

(2) Comisia este împuternicită să adopte astfel de acte delegate pentru a modifica anexele I, II și III, cu scopul de a răspunde cu eficacitate unei eventuale necesități de îmbunătățire a conținutului formularelor aferente ordinelor de eliminare și al formularelor care trebuie utilizate pentru a furniza informații privind imposibilitatea de a executa ordinul de eliminare.

Articolul 20

Exercitarea delegării

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

(2) Se conferă Comisiei, pentru o perioadă de timp nedeterminată de la [*data aplicării prezentului regulament*], competența de a adopta actele delegate menționate la articolul 19.

(3) Delegarea de competențe menționată la articolul 19 poate fi revocată în orice moment de către Parlamentul European sau de către Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere valabilității actelor delegate care sunt deja în vigoare.

(4) Înainte de a adopta un act delegat, Comisia îi consultă pe experții desemnați de fiecare stat membru, în conformitate cu principiile prevăzute în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 19 intră în vigoare numai dacă nici Parlamentul European, nici Consiliul nu a formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau dacă, înaintea expirării termenului respectiv, atât Parlamentul European, cât și Consiliul au informat Comisia că nu vor formula obiecții. Acest termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 21
Monitorizare

(1) Statele membre colectează de la autoritățile lor competente și de la furnizorii de servicii de găzduire care sunt de competența lor informații privind măsurile pe care le-au luat în conformitate cu prezentul regulament și le trimit Comisiei până la data de [31 martie] a fiecărui an. Aceste informații cuprind:

(a) informații privind numărul de ordine de eliminare și de semnalări emise, numărul de conținuturi cu caracter terorist care au fost eliminate sau la care s-a blocat accesul, inclusiv termenele aferente, în conformitate cu articolele 4 și 5;

(b) informații privind măsurile proactive specifice luate în temeiul articolului 6, inclusiv informații privind volumul conținutului cu caracter terorist care a fost eliminat sau la care s-a blocat accesul, și termenele aferente;

(c) informații privind numărul de plângeri depuse și măsurile luate de furnizorii de servicii de găzduire în temeiul articolului 10;

(d) informații privind numărul căilor de atac inițiate și deciziile luate de autoritatea competentă în conformitate cu dreptul intern.

(2) Până cel târziu la [*un an de la data aplicării prezentului regulament*], Comisia stabilește un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament. Programul de monitorizare stabilește indicatorii și mijloacele care trebuie să fie utilizate și intervalele care trebuie să fie aplicate pentru colectarea de date și de alte dovezi necesare. Programul specifică acțiunile care urmează să fie întreprinse de către Comisie și de către statele membre în ceea ce privește colectarea și analizarea datelor și a altor dovezi pentru a monitoriza progresele și a evalua prezentul regulament în temeiul articolului 23.

Articolul 22
Raport privind punerea în aplicare

Până cel târziu la ... [*doi ani după intrarea în vigoare a prezentului regulament*], Comisia prezintă Parlamentului European și Consiliului un raport privind aplicarea prezentului regulament. În raportul Comisiei se iau în considerare informațiile privind monitorizarea prevăzute la articolul 21 și informațiile care rezultă din obligațiile în materie de transparență prevăzute la articolul 8. Statele membre furnizează Comisiei informațiile necesare pentru elaborarea raportului respectiv.

Articolul 23
Evaluare

Nu mai devreme de [*trei ani de la data aplicării prezentului regulament*], Comisia efectuează o evaluare a prezentului regulament și prezintă Parlamentului European și Consiliului un raport referitor la aplicarea prezentului regulament, care vizează inclusiv funcționarea și eficacitatea mecanismelor de salvgardare. Dacă este cazul, raportul este însoțit de propuneri legislative. Statele membre furnizează Comisiei informațiile necesare pentru elaborarea raportului respectiv.

Articolul 24
Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la [6 luni de la intrarea sa în vigoare].

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*