Consiliul
Uniunii Europene

Bruxelles, 7 decembrie 2018
(OR. en)

15336/18

Dosar interinstituțional:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	6 decembrie 2018
Destinatar:	Delegațiile
Nr. doc. ant.:	14978/18 + COR 1
Nr. doc. Csie:	12129/18 + ADD 1-3
Subiect:	Propunere de regulament al Parlamentului European și al Consiliului privind prevenirea diseminării conținutului online cu caracter terorist - abordare generală

În cadrul reuniunii sale din 6 decembrie 2018, Consiliul a convenit asupra unei abordări generale, astfel cum figurează în anexă.

Modificările față de propunerea Comisiei sunt marcate prin ***caractere cursive aldine*** pentru textul adăugat și prin […] pentru textul eliminat.

ANEXĂ

[…]

[…] ***Proiect de***

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind prevenirea diseminării conținutului online cu caracter terorist

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[1],

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.

[1] JO C , , p. .

(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 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[2], 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.

[2] 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).

(5) Aplicarea prezentului regulament nu ar trebui să aducă atingere aplicării articolului 14 din Directiva 2000/31/CE[3]. 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. ***Prezentul regulament nu se aplică activităților legate de securitatea națională, deoarece aceasta rămâne responsabilitatea exclusivă a fiecărui stat membru.***

(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.

---

[3] 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).

(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***, precum și libertatea presei și pluralismul mass-mediei,*** care constituie [...] fundamentul 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 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 ***și posibilitatea ca furnizorii de servicii de găzduire să conteste o decizie de impunere a unor măsuri proactive sau a unor sancțiuni în fața instanței din statul membru în care își au sediul sau un reprezentant legal.***

(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[4]. Având în vedere nevoia de a combate cele mai dăunătoare forme de propagandă teroristă online, definiția ar trebui să includă materialele care [...] instigă, încurajează sau promovează săvârșirea de infracțiuni teroriste sau contribuirea la acestea [...] ori promovează participarea la activitățile unui grup terorist. [...] ***Definiția include conținutul care oferă indicații pentru fabricarea și folosirea explozibililor, a armelor de foc ori a altor arme sau substanțe nocive ori periculoase, precum și a substanțelor CBRN, sau cu privire la alte metode ori tehnici, inclusiv selecționarea țintelor, cu scopul de a comite infracțiuni de terorism.*** Aceste ***materiale*** [...] 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, [...], **de contradiscurs** sau de cercetare ar trebui protejat în mod adecvat, ***asigurându-se un just echilibru între drepturile fundamentale, inclusiv și în special libertatea de exprimare și de informare și necesitățile în materie de siguranță publică. În cazul în care materialul diseminat este publicat sub responsabilitatea editorială a furnizorului de conținut, orice hotărâre privind eliminarea unui astfel de conținut ar trebui să țină seama de standardele jurnalistice care au fost stabilite de reglementările din domeniul presei sau mass-mediei și care sunt în conformitate cu dreptul Uniunii, precum și cu dreptul la libertatea de exprimare și cu dreptul mass-mediei la libertate și la pluralism, astfel cum sunt consacrate la articolul 11 din Carta drepturilor fundamentale.*** 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.

---

[4] 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).

(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 ***și materiale*** furnizate de un destinatar al serviciului la cererea acestuia și care pun informațiile ***și materialele*** stocate la dispoziția părților terțe, indiferent dacă această activitate are un caracter pur tehnic, automat și pasiv. [...] ***Stocarea conținutului constă în păstrarea de date în memoria unui server fizic sau virtual; aceasta exclude din domeniul de aplicare simpla transmitere și alte servicii de comunicații electronice în sensul [Codului european al comunicațiilor electronice] sau furnizorii de servicii de memorare în cache ori alte servicii furnizate la alte niveluri ale infrastructurii de internet, cum ar fi registrele de domeniu sau birourile de înregistrare, DNS (sistem de nume de domenii) sau serviciile adiacente, precum serviciile de plată sau serviciile de protecție DDoS (distributed denial of service). În plus, informațiile trebuie stocate la solicitarea furnizorului conținutului; numai acele servicii pentru care furnizorul conținutului este destinatarul direct intră în domeniul de aplicare. În cele din urmă, informațiile stocate se pun la dispoziția părților terțe, prin care se înțelege orice utilizator terț care nu este furnizorul conținutului. Nu intră în domeniul de aplicare serviciile de comunicare interpersonală care permit schimbul de informații direct interpersonal și interactiv între un număr finit de persoane, în care persoanele care inițiază comunicarea sau participă la aceasta își stabilesc destinatarul/destinatarii.*** Ca exemplu, printre furnizorii de ***servicii de găzduire*** [...] se numără 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 și servicii ***de stocare*** [...]. ***Prezentul regulament se aplică activității de furnizare de servicii de găzduire, mai degrabă decât unui furnizor specific sau activității sale principale, care ar putea combina serviciile de găzduire cu alte servicii care nu intră în domeniul de aplicare al prezentului regulament.***

(10a) Regulamentul ar trebui să se aplice, de asemenea, furnizorilor de servicii de 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[5]. 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[6] nu poate fi considerată, exclusiv pe baza acestui motiv, drept direcționare a activităților către un anumit teritoriu din Uniune.

---

[5] 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).

[6] 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).

(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 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. ***Fără a aduce atingere cerinței de păstrare a datelor în temeiul articolului 7 din prezentul regulament sau în temeiul [proiectului legislativ privind probele electronice], f***urnizorilor de servicii de găzduire le revine decizia de a elimina sau de a bloca accesul utilizatorilor din Uniune la conținutul în cauză. ***Acest lucru ar trebui să aibă drept consecință prevenirea accesului sau cel puțin îngreunarea acestuia și descurajarea în mod serios a utilizatorilor de internet care le folosesc serviciile de la a accesa conținutul la care accesul a fost blocat.***

(13a) Ordinul de eliminare ar trebui să includă o clasificare a conținutului relevant drept conținut cu caracter terorist și să conțină suficiente informații, astfel încât conținutul să fie localizat prin furnizarea unui URL și a oricăror alte informații suplimentare, cum ar fi o captură de ecran a conținutului în cauză. Dacă i se solicită, autoritatea competentă ar trebui să furnizeze o expunere de motive suplimentară, privind motivele pentru care conținutul este considerat a fi conținut cu caracter terorist. Nu este necesar ca motivele prezentate să conțină informații sensibile care ar putea periclita anchetele. Cu toate acestea, expunerea de motive ar trebui să permită furnizorului de servicii de găzduire și, în ultimă instanță, furnizorului de conținut să își exercite eficient dreptul lor la o cale de atac.

(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[7].

[7] 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).

(15) [...] Mecanismul de [...] ***semnalare*** constând în alertarea furnizorilor de servicii de găzduire cu privire la informații și materiale care pot fi considerate cu caracter terorist, care îi permite furnizorului să evalueze, în mod voluntar, compatibilitatea ***cu*** propriile clauze și condiții, ***constituie un [...] mijloc extrem de eficace, rapid și proporțional de a informa furnizorii de servicii de găzduire cu privire la un anumit conținut din cadrul serviciilor lor [...].*** 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[8], 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 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 risc sau*** un nivel scăzut de expunere la conținutul cu caracter terorist.

---

8 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).

(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, ***„date privind operațiile” 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 ***expuși la conținutul cu caracter terorist*** 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***, în cazul în care acest lucru nu este contrar obiectivului măsurilor întreprinse.***

(25) Procedurile de depunere a plângerilor constituie o măsură de salvgardare necesară împotriva eliminării eronate***, ca urmare a măsurilor luate în conformitate cu clauzele și condițiile furnizorilor de servicii de găzduire,*** 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. ***De asemenea, furnizorii de conținut al căror conținut a fost eliminat în urma unui ordin de eliminare ar trebui să aibă dreptul la o cale de atac eficientă în conformitate cu articolul 19 din TUE și cu articolul 47 din Carta drepturilor fundamentale a Uniunii Europene.***

(26) ***De manieră mai generală,*** pentru o protecție jurisdicțională efectivă ***î***[...]n 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 [...] ***înainte de a*** emite ordine de eliminare sau ***atunci când*** trimit semnalări furnizorilor de servicii de găzduire. Atunci când decide emiterea ordinului de eliminare, autoritatea competentă ar trebui să țină seama în mod corespunzător de orice notificare a unei interferențe cu interesele investigației („deconflictualizare”). […] ***Atunci când decide emiterea unui ordin de eliminare, autoritatea competentă ar trebui să țină seama în mod corespunzător de orice notificare a unei interferențe cu interesele investigației („deconflictualizare”). În cazul în care o autoritate competentă este informată de către o autoritate competentă din alt stat membru cu privire la un ordin de eliminare existent, nu ar trebui emis un ordin dublu.*** 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. ***Comisia ar trebui să faciliteze o astfel de coordonare și cooperare.***

(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 [...] ***sunt încurajate*** să utilizeze instrumentele ***dedicate*** 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[9].

(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 în orice mijloace specifice***, elaborate intern sau prin externalizare,*** care permit depunerea electronică a ordinelor de eliminare și a semnalărilor, precum și din resurse tehnice [...] ***sau*** 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 expuși conținutului cu caracter terorist, demonstrat prin primirea unui ordin de eliminare,*** 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.

(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, din motive de punere în aplicare eficace, rapiditate și politică publică, orice stat membru ar trebui să dețină competența în ceea ce privește ordinele de eliminare și semnalările.***

---

9 COM(2018)225 final.

(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. ***Furnizorii de servicii de găzduire pot apela la un reprezentant legal existent, cu condiția ca respectivul reprezentant legal să fie în măsură să își exercite funcțiile prevăzute în prezentul 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, ***care pot fi de natură administrativă sau penală,*** 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 evaluează natura încălcării și se decide în privința aplicării de sancțiuni, ar trebui respectate pe deplin drepturile fundamentale, precum libertatea de exprimare.*** 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[10]. 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 sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(41) Statele membre ar trebui să colecteze informații privind punerea în aplicare a legislației. ***Statele membre pot utiliza rapoartele privind transparența ale furnizorilor de servicii de găzduire și le pot completa, după caz, cu informații mai detaliate.*** 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.

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

(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,

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.

(3) ***Prezentul regulament nu are drept efect modificarea obligației de respectare a drepturilor fundamentale și a principiilor juridice fundamentale, astfel cum sunt consfințite la articolul 6 din Tratatul privind Uniunea Europeană.***

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 stabilirea sediului furnizorului de servicii de găzduire în Uniune;

În cazul în care nu există un sediu stabilit în Uniune, evaluarea legăturii substanțiale se face pe baza unor criterii factuale specifice, precum

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

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

(4) „infracțiuni de terorism” înseamnă ***unul dintre actele săvârșite cu intenție enumerate*** [...] la articolul 3 alineatul (1) din Directiva (UE) 2017/541;

(5) „conținut cu caracter terorist” înseamnă [...] ***materiale care ar putea contribui la săvârșirea cu intenție a unor acte, astfel cum sunt enumerate la articolul 3 alineatul (1) literele (a)-(i) din Directiva 2017/541, astfel:***

(aa) amenință că vor săvârși o infracțiune de terorism;

(a) instigă la săvârșirea de infracțiuni de terorism sau promovează săvârșirea unor astfel de infracțiuni, [...] ***de exemplu*** [...] ***prin glorificarea actelor teroriste,*** generând astfel un pericol de săvârșire a unor astfel de infracțiuni;

(b) ***solicită unor persoane sau unui grup de persoane să săvârșească sau*** [...] ***să*** contribuie[...] la săvârșirea de infracțiuni de terorism;

(c) promovează activitățile unui grup terorist, în special prin solicitarea unor persoane sau a unui grup de persoane să [...] participe [...] la **activitățile infracționale ale** unui grup terorist sau să sprijine [...] aceste activități în sensul articolului 2 punctul 3 din Directiva (UE) 2017/541;

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] ***în Uniune***.

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 ***că nu vor stoca conținut cu caracter terorist*** și aplică dispoziții menite să prevină diseminarea conținutului cu caracter terorist.

Articolul 4

Ordine de eliminare

(1) Autoritatea competentă are competența de a emite [...] ***un ordin de eliminare*** 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; […] ***o evaluare a conținutului,*** cel puțin prin referire la categoriile ***relevante*** de conținuturi cu caracter terorist enumerate la articolul 2 punctul 5;

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

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

(d) marca temporală a emiterii ordinului;

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

(f) 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 [...] ***suplimentară*** a motivelor, ***explicând de ce conținutul este considerat a fi conținut cu caracter terorist*** 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) ***Fără întârzieri nejustificate, f***[...]urnizorii de servicii de găzduire confirmă primirea ordinului și [...] 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 4a

Procedura de consultare pentru ordinele de eliminare

(1) Autoritatea emitentă transmite o copie a ordinului de eliminare autorității competente menționate la articolul 17 alineatul (1) litera (a) din statul membru în care se află sediul principal al furnizorului de servicii de găzduire concomitent cu transmiterea acesteia către furnizorul de servicii de găzduire în conformitate cu articolul 4 alineatul (5).

(2) În cazul în care autoritatea competentă a statului membru în care se află sediul principal al furnizorului de servicii de găzduire are motive întemeiate să considere că ordinul de eliminare ar putea afecta interesele fundamentale ale statului membru respectiv, aceasta informează autoritatea emitentă competentă.

(3) Autoritatea emitentă ia în considerare aceste circumstanțe și, după caz, retrage sau adaptează ordinul de eliminare.

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 suficiente [...] [...] ***privind*** motivele pentru care conținutul este considerat conținut cu caracter terorist ***și furnizează*** 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 ***fără întârzieri nejustificate*** [...] 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, [...] ***în funcție de risc și de nivelul de expunere la conținutul cu caracter terorist,*** 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 aborda în mod eficace reapariția*** [...] 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. ***Autoritatea competentă menționată la articolul 17 alineatul (1) litera (c) este cea care decide cu privire la caracterul și domeniul de aplicare ale măsurilor proactive, în conformitate cu obiectivul prezentului regulament.*** 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**,** [...] 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 [...] ***expuși la conținut cu caracter terorist*** 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 ***aborda în mod eficace*** [...] re[...]***apariția*** 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 [...] ***șase*** săptămâni de la adoptarea deciziei. ***Această perioadă poate fi prelungită o dată, cu încă șase săptămâni, în cazul în care acest lucru este justificat.*** 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 [...] ***competente*** *ale Uniunii*

(1) Autoritățile competente din statele membre se informează, se coordonează și cooperează unele cu altele și, după caz, cu organismele [...] ***competente*** 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) ***Pentru o punere în aplicare eficace a prezentului regulament, precum și pentru a se evita suprapunerile,*** statele membre și furnizorii de servicii de găzduire pot alege să utilizeze instrumente specifice, inclusiv [...] cele stabilite de organisme [...] ***competente*** 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 (***statele***) membru (***membre***) în cauză [...]. ***În cazul în care este imposibil să se identifice statul (statele) membru (membre) vizat(e), f***[...]urnizorii de servicii de găzduire [...] n***otifică punctul de contact din statul membru în care au sediul principal sau un reprezentant legal, în conformitate cu articolul 14 alineatul (3), și, de asemenea,*** transmit 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. ***Orice stat membru este competent în sensul articolelor 4 și 5, indiferent de locul în care furnizorul de servicii de găzduire are sediul principal sau în care și-a desemnat un reprezentant legal.***

(2) În cazul în care un furnizor de servicii de găzduire nu desemnează un reprezentant legal, sunt competente toate statele membre. ***În cazul în care un stat membru decide să își exercite competența, acesta informează toate celelalte state membre în acest sens.***

[…] […]

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 [***douăsprezece*** [...] *luni de la intrarea în vigoare a prezentului regulament*], statele membre îi notifică Comisiei ***autoritatea sau*** 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) Aceste sancțiuni trebuie să fie eficace, proporționale și cu efect de descurajare. Până cel târziu la [*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 ***sau fizică*** considerată responsabilă;

(d) capacitatea financiară a persoanei juridice ***sau fizice*** 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 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 [***12*** [...] 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*