Parlamentul European
2014-2019

TEXTE ADOPTATE

P8_TA(2019)0421

Prevenirea diseminării conținutului online cu caracter terorist ***I

Rezoluția legislativă a Parlamentului European din 17 aprilie 2019 referitoare la propunerea de regulament al Parlamentului European și al Consiliului privind prevenirea diseminării conținutului online cu caracter terorist (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD))

(Procedura legislativă ordinară: prima lectură)

Parlamentul European,

– având în vedere propunerea Comisiei prezentată Parlamentului European și Consiliului (COM(2018)0640),

– având în vedere articolul 294 alineatul (2) și articolul 114 din Tratatul privind funcționarea Uniunii Europene, în temeiul cărora propunerea a fost prezentată de către Comisie Parlamentului (C8-0405/2018),

– având în vedere articolul 294 alineatul (3) din Tratatul privind funcționarea Uniunii Europene,

– având în vedere avizul motivat prezentat de către Camera Deputaților din Cehia în cadrul Protocolului nr. 2 privind aplicarea principiilor subsidiarității și proporționalității, în care se susține că proiectul de act legislativ nu respectă principiul subsidiarității,

– având în vedere avizul Comitetului Economic și Social European din 12 decembrie 2018[1],

– având în vedere articolul 59 din Regulamentul său de procedură,

– având în vedere raportul Comisiei pentru libertăți civile, justiție și piața internă, precum și avizul Comisiei pentru cultură și educație și al Comisiei piața internă și protecția consumatorilor (A8-0193/2019),

1. adoptă poziția în primă lectură prezentată în continuare;

2. solicită Comisiei să îl sesizeze din nou în cazul în care își înlocuiește, își modifică în mod substanțial sau intenționează să-și modifice în mod substanțial propunerea;

3. încredințează Președintelui sarcina de a transmite Consiliului și Comisiei, precum și

[1] JO C 110, 22.3.2019, p. 67.

parlamentelor naționale poziția Parlamentului.

P8_TC1-COD(2018)0331

Poziția Parlamentului European adoptată în primă lectură la 17 aprilie 2019 în vederea adoptării Directivei (UE) .../... a Parlamentului European și a Consiliului privind ~~prevenirea~~ *combaterea* diseminării conținutului online cu caracter terorist [AM 1]

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[2],

---

1 JO C 110, 22.3.2019, p. 67.

2 Poziția Parlamentului European din 17 aprilie 2019.

întrucât:

(1) Prezentul regulament are scopul de a asigura buna funcționare a pieței unice digitale în cadrul unei societăți deschise și democratice, prin ***combaterea*** ~~prevenirea~~ utilizării abuzive a serviciilor de găzduire în scopuri teroriste ***și prin aducerea unei contribuții la securitatea publică în societățile europene***. Funcționarea pieței unice digitale ar trebui să fie îmbunătățită prin ***întărirea*** ~~sporirea~~ securității juridice pentru furnizorii de servicii de găzduire, îmbunătățirea încrederii utilizatorilor în mediul online și consolidarea măsurilor de ***protecție a libertății*** ~~salvgardare privind libertatea~~ de exprimare***, a libertății*** de ***a primi și a transmite informații și idei într-o societate deschisă și democratică, precum și a libertății și a pluralismului mass-mediei***. ~~și de informare~~. **[AM 2]**

(1a) Regulamentul privind furnizorii de servicii de găzduire poate numai să completeze strategiile statelor membre de combatere a terorismului, care trebuie să pună accentul pe măsurile offline, cum ar fi investițiile în activitatea socială, inițiativele de deradicalizare și contactele cu comunitățile afectate pentru a asigura o prevenire sustenabilă a radicalizării în societate. **[AM 3]**

(1b) ***Conținutul cu caracter terorist face parte din problema mai amplă a conținutului online ilegal, care include și alte forme de conținut, cum ar fi exploatarea sexuală a copiilor, practicile comerciale ilegale și încălcările drepturilor de proprietate intelectuală. Traficul cu conținut ilegal este adesea realizat de către organizații teroriste și de alte organizații criminale pentru a spăla bani și a strânge fonduri de pornire pentru finanțarea operațiunilor. Această problemă necesită o combinație de măsuri legislative, fără caracter legislativ și voluntare, bazate pe colaborarea dintre autorități și furnizori, cu deplina respectare a drepturilor fundamentale. Deși amenințarea pe care conținutul ilegal o presupune a fost atenuată de inițiative de succes precum Codul de conduită elaborat în domeniu privind contracararea discursului de incitare la ură în mediul online și alianța mondială WePROTECT pentru eliminarea abuzurilor sexuale online asupra copiilor, este necesar să se edifice un cadru legislativ pentru cooperarea transfrontalieră între autoritățile naționale de reglementare în vederea eliminării conținutului ilegal.*** **[AM 4]**

(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 ***oferirea oportunităților de învățare și*** facilitarea dezbaterii publice, a difuzării și primirii de informații, de idei și opinii, contribuind astfel în mod semnificativ la inovare, la creşterea 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.
[AM 5]

(3) ~~Prezența~~ ***Deși nu constituie singurul factor, prezența*** conținutului online cu caracter terorist ***s-a dovedit a fi decisivă în favorizarea radicalizării persoanelor care au comis acte teroriste și, prin urmare,*** 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 ***dăunează modelelor*** ~~afectează modelele~~ de afaceri ale acestora. Având în vedere rolul lor central și ***proporțional cu*** mijloacele și capacitățile tehnologice asociate serviciilor pe care le oferă, furnizorii de servicii online au responsabilități societale ***speciale*** ~~specifice~~ de a-și proteja serviciile împotriva utilizării abuzive de către teroriști și de a ***ajuta autoritățile competente să combată conținuturile*** ~~contribui la combaterea conținutului~~ cu caracter terorist ***difuzate*** ~~diseminat~~ prin intermediul serviciilor pe care le oferă***, ținând seama totodată de importanța fundamentală a libertății de exprimare și a libertății de a primi și transmite informații și idei într-o societate deschisă și democratică***. **[AM 6]**

(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[3], și răspunde solicitărilor formulate de Parlamentul European în vederea consolidării măsurilor de combatere a conținuturilor ilegale și dăunătoare, ***în concordanță cu cadrul orizontal instituit prin Directiva 2000/31/CE,*** precum și de Consiliul European în vederea îmbunătățirii detectării și eliminării ~~automate a~~ conținutului care instigă la acte teroriste. **[AM 7]**

[3] 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[4]. ~~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~~ ***în*** Directiva 2000/31/CE pentru scutirea de răspundere. **[AM 8]**

(6) Prezentul regulament stabileşte norme menite să ~~prevină~~ ***combată*** utilizarea abuzivă a serviciilor de găzduire pentru diseminarea conținutului online cu caracter terorist, astfel încât să se asigure buna funcționare a pieței interne, ***iar aceste norme ar trebui să respecte pe deplin drepturile*** ~~cu respectarea deplină a drepturilor~~ fundamentale protejate în ordinea juridică a Uniunii, în special ***pe cele*** ~~a celor~~ garantate prin Carta drepturilor fundamentale a Uniunii Europene. **[AM 9]**

---

[4] 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 ***urmărește să*** contribuie la protecția securității publice ***și ar trebui să institui***~~e, 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 ***măsuri care*** ~~atunci când acestea~~ sunt necesare, adecvate și proporționale ***într-o societate democratică***, ~~în cadrul unei societăți democratice~~ luând în considerare importanța deosebită acordată libertății de exprimare***, libertății de a primi și a transmite informații și idei, drepturilor la respectarea vieții private*** și de ***familie, precum și protecției datelor cu caracter personal***, și ~~de informare,~~ care constituie ***fundamentele esențiale ale*** ~~un fundament esențial al~~ unei societăți pluraliste și democratice și ~~una dintre~~ ***constituie*** valorile pe care este întemeiată Uniunea. ***Orice măsuri ar trebui să evite imixtiunea în*** ~~Măsurile care interferează cu~~ libertatea de exprimare și de informare ~~ar trebui să fie strict direcționate~~, în ***măsura posibilului ar trebui*** ~~sensul că acestea trebuie~~ să servească la ***combaterea*** ~~prevenirea~~ diseminării conținutului cu caracter terorist***, prin intermediul unei abordări strict specifice***, 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. ***Măsurile online eficiente împotriva terorismului și protecția libertății de exprimare nu sunt obiective contradictorii, ci obiective care se completează și se consolidează reciproc.***
[AM 10]

(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***, precum și posibilitățile ca furnizorii de conținut să conteste măsurile specifice luate de furnizorul de servicii de găzduire***. **[AM 11]**

(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~~ ***combate*** 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[5]. Având în vedere nevoia de a combate ***cel*** ~~cele~~ mai ***dăunător conținut terorist*** ~~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***, cauzând, astfel, pericolul ca una sau mai multe astfel de infracțiuni să fie comise intenționat. Definiția ar trebui să cuprindă, de asemenea, 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 chimice, biologice, radiologice și nucleare (CBRN), sau indicații cu privire la alte metode ori tehnici, inclusiv selectarea țintelor, cu scopul de a comite infracțiuni de terorism.*** 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 ***sau în scopul sensibilizării opiniei publice împotriva activității teroriste***ar trebui să fie protejat în mod adecvat. ***În special în cazurile în care furnizorul de conținut deține o responsabilitate editorială, orice decizie privind eliminarea materialului diseminat ar trebui să țină seama de standardele jurnalistice stabilite de reglementările aplicabile presei sau mass-mediei în conformitate cu dreptul Uniunii și Carta drepturilor fundamentale***. În plus, exprimarea unor puncte de vedere radicale, polemice sau controversate în

---

5 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).

cadrul dezbaterii publice privind chestiuni politice sensibile nu ar trebui să fie considerată conținut cu caracter terorist. **[AM 12]**

(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 ***publicului*** ~~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 ***publicului*** ~~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 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. ***Prezentul regulament nu ar trebui să se aplice serviciilor de tip cloud, inclusiv serviciilor de tip cloud între întreprinderi, în cadrul cărora furnizorul de servicii nu are drepturi contractuale asupra conținutului stocat sau a modului în care acesta este prelucrat sau făcut public de clienții săi sau de utilizatorii finali ai respectivilor clienți, și în cazul cărora furnizorul de servicii nu are nicio posibilitate tehnică de a elimina un anumit conținut stocat de clienții săi sau de utilizatorii finali ai serviciilor sale.*** **[AM 13]**

(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 (UE) nr. 1215/2012 al Parlamentului European și al Consiliului[6]. 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[7] nu poate fi considerată, exclusiv pe baza acestui motiv, drept direcționare a activităților către un anumit teritoriu din Uniune. **[AM 14]**

---

6 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).

7 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 ***combate*** ~~preveni~~ diseminarea ***către public a*** conținutului cu caracter terorist în cadrul serviciilor lor. Aceste obligații de diligență nu ar trebui să constituie o obligație generală ***a furnizorilor*** de ***servicii de găzduire de a monitoriza informațiile pe care le stochează, și nici o obligație generală de a căuta în mod activ fapte sau circumstanțe care să indice o activitate ilegală*** ~~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 ***transparent,*** 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 ***evita*** ~~preveni~~ eliminarea conținutului fără caracter terorist. Eliminarea conținutului sau blocarea accesului la acesta trebuie să se realizeze cu respectarea libertății de exprimare***, a libertății*** de ***a primi și a transmite informații și idei într-o societate deschisă și democratică, precum și a libertății și pluralismului mass-mediei***. ~~și de informare~~. **[AM 15]**

(13) Este necesară armonizarea procedurilor și a obligațiilor care rezultă din ordinele ***de eliminare***~~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 ***care să le permită să desemneze o autoritate judiciară sau o autoritate administrativă sau*** ~~desemnate pentru a îndeplini aceste sarcini, care pot fi autorități administrative, autorități~~ de aplicare a legii ***funcțională și independentă pentru a îndeplini această sarcină*** ~~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.~~ **[AM 16]**

(14) Autoritatea competentă ar trebui să transmită ordinul de eliminare direct ***punctului de contact al furnizorului de servicii de găzduire, iar în cazul în care sediul principal al furnizorului de servicii*** de ***găzduire se află într-un alt stat membru, autorității competente a statului membru respectiv*** ~~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[8].
[AM 17]

[8] 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) 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[9], nu este afectat. **[AM 18]**

[9] 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).

(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 ***specifice*** ~~inclusiv prin utilizarea de mijloace automatizate în anumite cazuri~~, constituie un element esențial pentru ~~abordarea~~ ***combaterea*** 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 ***specifice*** ~~proactive~~, în funcție de riscuri și de nivelul de expunere la ***conținuturi*** ~~conținutul~~ cu caracter terorist, precum și de efectele asupra drepturilor terților și de interesul public ***de a primi și transmite informații, îndeosebi în cazurile în care există un grad ridicat de expunere la conținut cu caracter terorist și de primire de ordine de eliminare*** ~~al informațiilor~~. În consecință, furnizorii de servicii de găzduire ar trebui să stabilească măsurile ***adecvate, specifice***, ~~proactive adecvate~~, eficace și proporționale care ar trebui aplicate. Această cerință nu ar trebui să implice o obligație generală de supraveghere. ***Aceste măsuri specifice pot include informarea periodică a autorităților competente, creșterea resurselor umane care se ocupă de măsurile de protecție a serviciilor împotriva diseminării de conținut cu caracter terorist și schimbul de bune practici.*** 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. **[AM 19]**

(17) Atunci când pun în aplicare măsuri ***specifice*** ~~proactive~~, furnizorii de servicii de găzduire ar trebui să se asigure că ***este menținut*** ~~utilizatorii își mențin~~ dreptul ***utilizatorilor*** la libertatea de exprimare și ~~de informare, inclusiv dreptul~~ ***la libertatea*** de a primi și a transmite informații ***și idei într-o societate deschisă și democratică***. 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~~.
[AM 20]

(18) Pentru a se asigura că furnizorii de servicii de găzduire expuși la conținut ***cu caracter*** terorist iau măsurile adecvate pentru a preveni utilizarea abuzivă a serviciilor lor, ***autoritatea competentă*** ~~autoritățile competente~~ ar trebui să le solicite furnizorilor de servicii de găzduire care au primit un ***număr ridicat de ordine*** ~~ordin~~ de eliminare ***finală*** ~~devenit definitiv~~ să prezinte măsurile ***specifice*** ~~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 ***necesare,*** 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 ***necesitatea,*** eficacitatea și proporționalitatea măsurilor, autoritățile competente ar trebui să ia în considerare parametrii relevanți, inclusiv numărul de ordine de ***eliminare*** ~~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)***, precum și garanțiile instituite pentru a proteja libertatea de exprimare și de informare și numărul de incidente legate de restricționarea unui conținut legal***. **[AM 21]**

(19) Ca urmare a solicitării, autoritatea competentă ar trebui să inițieze un dialog cu furnizorul de servicii de găzduire cu privire la măsurile ***specifice necesare*** ~~proactive~~ care trebuie instituite. Dacă este necesar, autoritatea competentă ar trebui să ***îi solicite furnizorului de servicii de găzduire să reevalueze măsurile necesare sau să solicite*** ~~impună~~ adoptarea unor măsuri adecvate, eficace și proporționale ***specifice***, 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 c~~onducă, 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.~~ ***nu respectă principiile necesității și proporționalității sau sunt insuficiente pentru a face față riscurilor. Autoritatea competentă ar trebui să impună doar măsuri proactive pe care furnizorul de servicii de găzduire le poate aplica în mod rezonabil, luând în considerare, printre alți factori, resursele financiare și de altă natură ale furnizorului de servicii de găzduire. O decizie de punere în aplicare a unor astfel de măsuri specifice nu ar trebui să conducă la impunerea unei obligații generale de supraveghere***, ***astfel cum se prevede la articolul 15 alineatul (1) din Directiva 2000/31/CE***. **[AM 22]**

(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. **[AM 23]**

(21) Obligația de păstrare a conținutului pentru proceduri de reexaminare administrativă sau ***judiciară, sau pentru căi de atac,*** ~~de control judiciar~~ este necesară și justificată în vederea asigurării unor măsuri ***reparatorii*** ~~de reparare~~ eficace pentru furnizorul de conținut al cărui conținut a fost eliminat ***al cărui conținut*** ~~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 ***materiale*** ~~materialul~~ sau blochează accesul la acesta ***prin intermediul propriilor măsuri specifice***, ***ele ar trebui să informeze de îndată autoritățile competente de asigurare a aplicării legii. Păstrarea conținutului în scopul prevenirii, depistării***, ***anchetării*** și ***urmăririi penale a infracțiunilor de terorism este, de asemenea, justificată. În acest scop, conținutul cu caracter terorist și datele aferente ar trebui stocate numai pentru o perioadă specifică***, ***care să permită autorităților***, ~~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 ***verifice conținutul și să decidă dacă acest lucru ar fi necesar*** în ***scopurile specifice respective. Această perioadă nu trebuie să depășească șase luni. Pentru prevenirea***, ***detectarea***, ***anchetarea și urmărirea penală a infracțiunilor cu caracter terorist***,~~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. **[AM 24]**

(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 ***sau*** ~~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 ***procedurile*** ~~procedura~~ de reexaminare ***sau de căi de atac sunt inițiate***, ~~este inițiată~~, dar nu ***sunt finalizate*** ~~este finalizată~~ în perioada de șase luni. Această durată ar trebui***, de asemenea,*** să fie suficientă pentru a permite autorităților de aplicare a legii să păstreze ***materialele*** ~~dovezile~~ necesare în ceea ce privește investigațiile ***și urmăririle penale***, asigurând în același timp un echilibru cu drepturile fundamentale vizate. **[AM 25]**

(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. ***Numai*** furnizorii de servicii de găzduire ***care fac obiectul unor ordine de eliminare pentru anul respectiv*** ar trebui ***obligați*** să publice rapoarte anuale privind transparența care să ***cuprindă*** ~~conțină~~ informații ***pertinente*** ~~relevante~~ privind măsurile întreprinse în legătură cu detectarea, identificarea și eliminarea conținutului cu caracter terorist. **[AM 26]**

(24a) Autoritățile competente pentru emiterea de ordine de eliminare ar trebui să publice, de asemenea, rapoarte privind transparența care să cuprindă informații privind numărul de ordine de eliminare, numărul de refuzuri, numărul de conținuturi teroriste identificate care au dus la anchetarea și urmărirea penală a infracțiunilor de terorism, precum și numărul de cazuri de conținuturi identificate în mod eronat ca fiind teroriste. **[AM 27]**

(25) Procedurile de depunere a plângerilor constituie o măsură de salvgardare necesară împotriva eliminării eronate a conținutului protejat în temeiul libertății de exprimare ***al libertății*** de ***a primi și de a transmite informații și idei într-o societate deschisă și democratică***. ~~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. **[AM 28]**

(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~~ ***pertinente, cum ar fi motivele pentru eliminare sau pentru blocarea accesului***, ***temeiul juridic pentru acțiune,*** 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. **[AM 29]**

(27) Pentru a evita duplicarea și eventualele ***imixtiuni în anchete și pentru a minimiza cheltuielile suportate de către furnizorii de servicii afectați***, ~~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. **[AM 30]**

(27a) Semnalările emise 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 coopereze cu Europol și 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, mandatul Europol, astfel cum este prevăzut în Regulamentul (UE) 2016/794[10], nu este afectat. **[AM 31]**

10 *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).*

(28) Pentru a asigura punerea în aplicare eficace și suficient de coerentă a măsurilor ***de către furnizorii de servicii de găzduire***,~~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 ***ordinele de eliminare și*** 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. **[AM 32]**

(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 ***autoritățile competente pertinente din alte state membre*** ~~autoritatea competentă relevantă~~. În acest scop, statele membre ar trebui să se asigure că dispun de canale și mecanisme de comunicare adecvate ***și securizate*** care să permită schimbul de informații relevante în timp util. **[AM 33]**

(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[11].

11 COM(2018)0225.

(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. **[AM 34]**

(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*. **[AM 35]**

(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.*** **[AM 36]**

(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 ***o autoritate judiciară sau administrativă, funcțională și independentă, unică. Această cerință*** ~~autorități competente. Cerința de desemnare a unor autorități competente~~ nu ***necesită*** ~~presupune neapărat~~ instituirea ~~de~~ unei noi autorități, funcțiile stabilite în prezentul regulament putând fi încredințate ***unui organ existent***.~~unor organisme existente.~~ Prezentul regulament impune desemnarea ~~de~~ ***unei*** autorități competente pentru emiterea ordinelor de eliminare ~~și a semnalărilor~~, pentru supravegherea măsurilor ***specifice*** ~~proactive~~ și pentru impunerea de sancțiuni. ***Statele membre ar trebui să comunice Comisiei care este autoritatea competentă desemnată în temeiul prezentului regulament, iar cea dintâi ar trebui*** să ***publice online o compilație cu autoritățile competente din fiecare stat membru. Registrul online ar trebui să fie ușor accesibil pentru a facilita verificarea rapidă a autenticității ordinelor de eliminare de către furnizorii de servicii de găzduire.*** ~~Este la latitudinea statelor membre să decidă numărul de autorități pe care doresc să le desemneze pentru îndeplinirea acestor sarcini.~~ **[AM 37]**

(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. ***Ar trebui stabilite*** ~~Este necesar să se stabilească~~ sancțiuni ***în cazul*** ~~deosebit de aspre pentru cazurile~~ în care ***furnizorii*** ~~furnizorul~~ de servicii de găzduire ***nu își respectă*** ~~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.~~ ***mod sistematic*** și ***persistent obligațiile care le revin*** în ***temeiul prezentului regulament***. În cazul nerespectării articolului 6, ar trebui să se adopte sancțiuni numai în ceea ce privește obligațiile care decurg dintr-o solicitare de ***aplicare*** ~~raportare efectuată în temeiul articolului 6 alineatul (2) sau dintr-o decizie de impunere~~ a unor măsuri ***specifice*** ~~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. ***În plus, autoritatea competentă ar trebui să ia în considerare dacă furnizorul de servicii de găzduire este o întreprindere nou-înființată sau o întreprindere mică și mijlocie și ar trebui să stabilească, de la caz la caz, dacă acesta este în măsură să respecte în mod corespunzător ordinul emis.*** Statele membre ar trebui să se asigure că sancțiunile nu încurajează eliminarea conținutului care nu este conținut cu caracter terorist.
[AM 38]

(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[12]. 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.

12 JO L 123, 12.5.2016, p. 1.

(41) Statele membre ar trebui să colecteze informații privind punerea în aplicare a legislației***, inclusiv informații privind numărul de cazuri de depistare, investigare și urmărire penală reușită a infracțiunilor teroriste ca urmare a aplicării prezentului regulament***. 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. **[AM 39]**

(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~~ ***un an*** după intrarea sa în vigoare. Evaluarea ar trebui să se bazeze pe următoarele ~~cinci~~ ***șapte*** criterii: eficiență, ***necesitate, proporționalitate***, eficacitate, relevanță, coerență și valoare adăugată europeană. Aceasta ***ar trebui să vizeze*** ~~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 ***fundamentale care ar putea fi afectate, inclusiv libertatea de exprimare*** și cea de a ***primi și disemina informații, libertatea și pluralismul mass media, libertatea de a desfășura o activitate comercială și dreptul la viață privată și la protecția datelor cu caracter personal. Comisia ar trebui, de asemenea, să evalueze efectul asupra*** ~~și intereselor~~ părților terțe care ar putea fi afectate, și va include o reexaminare a cerinței de informare a furnizorilor de conținut. **[AM 40]**

(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 ***specifice*** uniforme pentru a ***combate*** ~~preveni~~ utilizarea abuzivă a serviciilor de găzduire pentru diseminarea ***publică a*** conținutului online cu caracter terorist. Acesta prevede în special: **[AM 41]**

(a) norme ***rezonabile și proporționale*** privind obligațiile de diligență pe care trebuie să le aplice furnizorii de servicii de găzduire pentru ***combate*** ~~a preveni~~ diseminarea ***publică a*** conținutului cu caracter terorist prin intermediul serviciilor lor și pentru a asigura, atunci când este necesar, eliminarea rapidă a acestuia; **[AM 42]**

(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 ***în concordanță cu legislația Uniunii care oferă garanții adecvate exercitării libertății de exprimare și libertății de a primi și difuza informații și idei într-o societate deschisă și democratică*** 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. **[AM 43]**

(2) Prezentul regulament se aplică furnizorilor de servicii de găzduire care oferă servicii ***publice*** în Uniune, indiferent de locul unde se află sediul lor principal. **[AM 44]**

2a. ***Prezentul regulament nu se aplică conținutului care este difuzat în scopuri educaționale, artistice, jurnalistice sau de cercetare sau în scopul sensibilizării față de activitățile teroriste, nici conținutului care reprezintă o expresie a opiniilor polemice sau controverselor din cursul unei dezbateri publice.*** **[AM 45]**

2b. ***Prezentul regulament nu are ca efect modificarea obligației de a respecta drepturile, libertățile și principiile prevăzute la articolul 6 din Tratatul privind Uniunea Europeană și se aplică fără a aduce atingere principiilor fundamentale din legislația Uniunii și din legislația internă privind libertatea de exprimare, libertatea presei și libertatea și pluralismul mijloacelor de informare în masă.*** **[AM 46]**

2c. ***Prezentul regulament nu aduce atingere Directivei 2000/31/CE.*** **[AM 47]**

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(-1) ***„servicii ale societății informaționale” înseamnă serviciile astfel cum sunt definite la articolul 2 litera (a) din Directiva 2000/31/CE.*** **[AM 48]**

(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~~ ***publicului. Acest lucru se aplică numai serviciilor furnizate publicului la nivelul aplicației. Furnizorii de infrastructură de tip cloud și furnizorii de servicii de cloud nu sunt considerați furnizori de servicii de găzduire. Nu se aplică nici serviciilor de comunicații electronice, astfel cum sunt definite în Directiva (UE) 2018/1972***; **[AM 49]**

(2) „furnizor de conținut” înseamnă un utilizator care a furnizat informații care sunt stocate sau care au fost stocate ***și puse la dispoziția publicului*** la cererea sa de către un furnizor de servicii de găzduire; **[AM 50]**

(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;~~ **[AM 51]**

(5) „conținut cu caracter terorist” înseamnă ~~una~~ ***unul*** sau mai multe dintre următoarele ***materiale*** ~~informații~~ care: **[AM 52]**

(a) instigă la săvârșirea ***uneia dintre infracțiunile prevăzute la articolul 3 alineatul (1) literele (a) - (i) din Directiva (UE) 2017/541, atunci când un*** ~~de infracțiuni de terorism sau promovează săvârșirea unor~~ astfel de ***comportament promovează direct sau indirect***, ***cum ar fi*** ~~infracțiuni, inclusiv prin~~ glorificarea ***actelor teroriste, săvârșirea unor infracțiuni teroriste***, ~~lor,~~ generând astfel un pericol de săvârșire ***intenționată*** a ***uneia sau a mai multor*** ~~unor~~ astfel de infracțiuni; **[AM 53]**

(b) ~~încurajează contribuirea la infracțiuni de terorism;~~ ***determinarea unei alte persoane sau a unui grup de persoane să săvârșească sau să contribuie*** la ***săvârșirea uneia dintre infracțiunile enumerate la articolul 3 alineatul (1) literele (a) — (i) din Directiva (UE) 2017/541, generând astfel pericolul ca una sau mai multe astfel*** de ***infracțiuni să fie comise intenționat***; **[AM 54]**

(c) ***determinarea unei alte persoane sau a unui grup de persoane să participe la*** ~~promovează~~ activitățile unui grup terorist, ~~în special prin încurajarea participării la un grup terorist~~ ***inclusiv prin furnizarea de informații sau de resurse materiale*** sau ***prin finanțarea în orice fel a activităților acestuia,*** ~~a sprijinirii unui grup terorist~~ în sensul ***articolul 4*** ~~articolului 2 punctul 3~~ din Directiva (UE) 2017/541***, generând astfel pericolul ca una sau mai multe astfel de infracțiuni să fie comise intenționat***; **[AM 55]**

(d) ~~oferă~~ ***oferirea de*** instrucțiuni referitoare la ***fabricarea sau folosirea explozivilor, a armelor de foc sau a altor arme sau substanțe nocive sau periculoase sau la alte*** metode sau tehnici ***specifice*** cu scopul ***săvârșirii unor infracțiuni*** ~~săvârșirii unor infracțiuni~~ de terorism ***sau a contribuirii la săvârșirea uneia dintre infracțiunile de terorism enumerate la articolul 3 alineatul (1) literele (a)-(i) din Directiva (UE) 2017/541***; **[AM 56]**

(da) prezentarea comiterii uneia sau mai multora dintre infracțiunile enumerate la articolul 3 alineatul (1) literele (a) — (i) din Directiva (UE) 2017/541, generând astfel pericolul ca una sau mai multe astfel de infracțiuni să fie comise intenționat; **[AM 57]**

(6) „diseminarea conținutului cu caracter terorist” înseamnă punerea conținutului cu caracter terorist la dispoziția ***publicului*** ~~unor părți terțe~~ prin intermediul serviciilor furnizorilor de servicii de găzduire; **[AM 58]**

(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~~; **[AM 59]**

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

9a. ***„autoritate competentă” înseamnă o autoritate națională judiciară unică sau o autoritate administrativă independentă din punct de vedere funcțional din statul membru.*** **[AM 60]**

SECȚIUNEA II

Măsuri de prevenire a diseminării conținutului online cu caracter terorist

Articolul 3

Obligații de diligență

(1) Furnizorii de servicii de găzduire ***acționează*** ~~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 ***și în toate împrejurările*** drepturile fundamentale ale utilizatorilor, și țin cont de importanța fundamentală a libertății de exprimare și ***a libertății*** de ***a primi și a comunica informații și idei*** ~~de informare~~ într-o societate deschisă și democratică***, în vederea evitării eliminării de conținut fără caracter terorist***. **[AM 61]**

1a. Aceste obligații de diligență nu constituie o obligație generală a furnizorilor de servicii de găzduire de a monitoriza informațiile pe care le stochează și nici o obligație generală de a căuta în mod activ fapte sau circumstanțe care să indice o activitate ilegală. **[AM 62]**

~~(2) Furnizorii de servicii de găzduire includ în clauzele și condițiile lor dispoziții menite să prevină diseminarea conținutului cu caracter terorist și le aplică.~~ **[AM 63]**

2a. Dacă furnizorii de servicii de găzduire iau cunoștință de un conținut cu caracter terorist diseminat prin intermediul serviciilor lor, aceștia informează autoritățile competente cu privire la respectivul conținut și îl elimină prompt. **[AM 64]**

2b. Furnizorii de servicii de găzduire care îndeplinesc criteriile definiției furnizorilor de platforme de partajare a materialelor video conform Directivei (UE) 2018/1808 iau măsurile adecvate pentru a combate diseminarea conținutului cu caracter terorist în conformitate cu articolul 28b alineatul (1) litera (c) și alineatul (3) din Directiva (UE) 2018/1808. **[AM 65]**

Articolul 4

Ordine de eliminare

(1) Autoritatea competentă ***a statului membru în care se află sediul principal al furnizorului de servicii de găzduire*** are competența de a emite ~~o decizie~~ ***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 ***în toate statele membre***. **[AM 66]**

1a. ***Autoritatea competentă a unui stat membru în care furnizorul de servicii de găzduire nu are sediul principal sau nu are un reprezentant legal poate solicita ca accesul la conținutul terorist să fie blocat și poate asigura respectarea prezentei cereri pe teritoriul său.*** **[AM 67]**

1b. ***Dacă autoritatea competentă relevantă nu a emis anterior un ordin de eliminare către un furnizor de servicii de găzduire, aceasta contactează furnizorul de servicii de găzduire, punându-i la dispoziție informații cu privire la proceduri și termene aplicabile, cu cel puțin 12 de ore înainte de emiterea unui ordin de eliminare.*** **[AM 68]**

(2) Furnizorii de servicii de găzduire elimină conținutul cu caracter terorist sau blochează accesul la acesta în ***cel mai scurt termen posibil și în*** termen de o oră de la primirea ordinului de eliminare. **[AM 69]**

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

(a) identificarea autorității competente care emite ordinul de eliminare ***prin semnătură digitală*** și autentificarea ordinului de eliminare de către autoritatea competentă; **[AM 70]**

(b) o expunere ***detaliată*** a motivelor care să explice de ce conținutul este considerat conținut cu caracter terorist ***și o*** ~~cel puțin prin~~ referire ***concretă*** la categoriile de conținuturi cu caracter terorist enumerate la articolul 2 punctul 5; **[AM 71]**

(c) o adresă URL (*Uniform Resource Locator*) ***exactă*** și, dacă este necesar, informații suplimentare care să permită identificarea conținutului menționat; **[AM 72]**

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

(e) marca temporală a emiterii ordinului;

(f) informații ***ușor de înțeles*** privind căile de atac de care dispun furnizorul de servicii de găzduire și furnizorul de conținut***, inclusiv căile de atac la autoritatea competentă, precum și recurgerea la o instanță și termene-limită pentru introducerea apelului***; **[AM 73]**

(g) dacă este ~~relevant~~ ***necesar și potrivit***, 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. **[AM 74]**

~~(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).~~ **[AM 75]**

(5) ***Autoritatea competentă*** ~~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. **[AM 76]**

(6) Furnizorii de servicii de găzduire ***informează*** ~~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. **[AM 77]**

(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, ***inclusiv din motive tehnice sau operaționale,*** 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. **[AM 78]**

(8) ~~În cazul în care furnizorul~~ ***Furnizorul*** de servicii de găzduire ~~nu~~ poate ***refuza executarea ordinului*** ~~respecta ordinul~~ de eliminare ***dacă*** ~~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. **[AM 79]**

(9) Autoritatea competentă care a emis ordinul de eliminare informează autoritatea competentă care supraveghează punerea în aplicare a măsurilor ***specifice*** ~~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. **[AM 80]**

Articolul 4a

Procedura de consultare pentru ordinele de eliminare

(1) *Autoritatea judiciară competentă care emite un ordin de eliminare conform articolului 4 alineatul (1a) transmite o copie a ordinului de eliminare autorității judiciare competente menționate la articolul 17 alineatul (1) litera (a) din statul membru în care se află sediul principal al furnizorului de servicii de găzduire, simultan cu transmiterea acestuia furnizorului 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. Autoritatea emitentă ia în considerare aceste circumstanțe și, după caz, retrage sau adaptează ordinul de eliminare.* **[AM 81]**

Articolul 4b

Procedura de cooperare pentru emiterea unui ordin de eliminare suplimentar

1. ***În cazul în care o autoritate competentă a emis un ordin de eliminare în temeiul articolul 4 alineatul (1a), autoritatea respectivă poate contacta autoritatea competentă a statului membru în care furnizorul de servicii de găzduire își are sediul principal pentru a solicita ca aceasta din urmă să emită, la rândul său, un ordin de eliminare în temeiul articolul 4 alineatul (1).***

2. ***Autoritatea competentă din statul membru în care este situat sediul principal al furnizorului de servicii de găzduire fie emite un ordin de îndepărtare, fie refuză cât de rapid posibil să emită un ordin, dar nu mai târziu de o oră de la momentul la care este contactată în conformitate cu alineatul (1) și informează autoritatea competentă care a emis prima decizie cu privire la decizia sa.***

3. ***În cazurile în care autoritatea competentă din statul membru în care se află sediul principal are nevoie de mai mult de o oră pentru a efectua propria evaluare a conținutului, aceasta trimite furnizorului de servicii de găzduire în cauză o cerere de blocare temporară a accesului la conținut pentru o perioadă de până la 24 ore, perioadă în care autoritatea competentă efectuează evaluarea și trimite ordinul de eliminare sau retrage cererea de blocare a accesului.*** **[Am. 82]**

~~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.~~ **[AM 83]**

Articolul 6

Măsuri ~~proactive~~ ***specifice*** **[AM 84]**

(1) ~~Furnizorii de servicii de găzduire iau măsuri proactive, atunci când acestea se impun,~~ ***Fără a aduce atingere Directivei (UE) 2018/1808 și Directivei 2000/31/CE***, ***furnizorii de servicii de găzduire pot lua măsuri specifice*** pentru a-și proteja serviciile împotriva diseminării ***publice*** de conținut cu caracter terorist. Măsurile trebuie să fie eficace***, orientate*** și proporționale, ținând seama ***în mod special*** de riscul și nivelul de expunere la conținutul cu caracter terorist, de drepturile fundamentale ale utilizatorilor și de importanța fundamentală ***dreptului de exercitare*** a libertății de exprimare și de ***primire și transmitere a informațiilor și ideilor*** ~~informare~~ într-o societate deschisă și democratică. **[AM 85]**

(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~~. **[AM 86]**

~~(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.~~ **[AM 87]**

(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),~~ ***După ce a stabilit că un furnizor de servicii de găzduire a primit un număr substanțial*** de ***ordine de eliminare***, autoritatea competentă menționată la articolul 17 alineatul (1) litera (c) poate ***înainta*** o ***solicitare de*** ~~emite o decizie prin care să impună~~ măsuri ~~proactive~~ specifice suplimentare, necesare***, proporționale*** și ***eficace pe care furnizorul de servicii de găzduire va trebui să le pună în practică.*** ~~proporționale. Atunci când adoptă această decizie,~~ Autoritatea competentă ***nu impune o obligație generală de supraveghere, nici utilizarea de instrumente automatizate. Solicitarea*** ține cont în special de ***fezabilitatea tehnică a măsurilor, de dimensiunea și*** 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 ***primire și transmitere de informații și idei într-o societate deschisă și democratică***. ***Această solicitare*** ~~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). **[AM 88]**

(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,~~ ***alineatului*** (4). Autoritatea competentă emite o decizie motivată într-un termen rezonabil de la primirea solicitării din partea furnizorului de servicii de găzduire. **[AM 89]**

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 ***specifice*** ~~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: **[AM 90]**

(a) proceduri de reexaminare administrativă ~~sau~~ de control judiciar ***sau de exercitare a căilor de atac***; **[AM 91]**

(b) prevenirea, depistarea, investigarea și urmărirea penală ***de către autoritățile însărcinate cu aplicarea legii*** a infracțiunilor de terorism. **[AM 92]**

(2) Conținutul cu caracter terorist și datele conexe menționate la alineatul (1) ***litera (a)*** se păstrează timp de șase luni ***și se distruge după această perioadă***. La cererea autorității sau a instanței competente, conținutul cu caracter terorist se păstrează ***încă*** o perioadă ~~mai lungă~~ ***specificată***, ***doar***în cazul în care și atât timp cât acest lucru este necesar pentru desfășurarea procedurilor de reexaminare administrativă***, de control judiciar*** sau de ***exercitare a căilor de atac menționate la alineatul (1) litera (a). Furnizorii de servicii de găzduire trebuie să păstreze conținutul cu caracter terorist și datele conexe menționate la alineatul (1) litera (b) până când autoritatea de aplicare a legii reacționează la notificarea efectuată de către furnizorul de servicii de găzduire*** ~~control judiciar~~ ***în conformitate cu articolul 13 alineatul (4), dar nu mai târziu de șase luni.*** ~~menționate la alineatul (1) litera (a).~~ **[AM 93]**

(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 ***pentru furnizorii de servicii de găzduire*** **[AM 94]**

(1) ~~Furnizorii~~ ***Dacă este cazul, furnizorii*** de servicii de găzduire prezintă ***clar***, în clauzele și condițiile lor, politica pe care o aplică pentru prevenirea diseminării conținutului cu caracter terorist, inclusiv, ~~*dacă este cazul* după caz,~~ o explicație pertinentă privind funcționarea măsurilor ***specifice*** ~~proactive și utilizarea instrumentelor automatizate~~. **[AM 95]**

(2) Furnizorii de servicii de găzduire ***care fac sau au făcut obiectul unor ordine de eliminare în anul respectiv*** publică anual ***rapoarte*** ~~un raport~~ privind transparența ~~referitor~~ ***referitoare*** la măsurile întreprinse pentru combaterea diseminării conținutului cu caracter terorist. **[AM 96]**

(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***, în special în cazurile în care s-a folosit tehnologie automatizată***; **[AM 97]**

(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 ***specifice și numărul de ordine în cazul cărora conținutul nu a fost eliminat în conformitate cu articolul 4 alineatele (7) și (8), împreună cu motivele refuzului*** ~~proactive~~; **[AM 98]**

(d) ~~o prezentare generală~~ ***numărul*** și rezultatele procedurilor de depunere a plângerilor ***și acțiunilor de control judiciar, inclusiv numărul de cazuri în care s-a stabilit că conținutul a fost identificat în mod eronat ca având caracter terorist***. **[AM 99]**

Articolul 8a

Obligațiile autorităților competente în ceea ce privește transparența

1. Autoritățile competente publică rapoarte anuale de transparență care includ cel puțin următoarele informații:

(a) numărul de ordine de eliminare emise, numărul eliminări și numărul de ordine de eliminare refuzate sau ignorate;

(b) numărul identificărilor de conținut terorist care au condus la cercetare și urmărire penală și numărul materialelor identificate în mod eronat ca având caracter terorist;

(c) o descriere a măsurilor solicitate de autoritățile competente în temeiul articolul 6 alineatul (4). **[AM 100]**

Articolul 9

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

[AM 101]

(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. **[AM 102]**

(2) Măsurile de salvgardare respective constau în special în supravegherea și efectuarea de verificări ***a caracterului adecvat al deciziei*** de ***a elimina conținutul sau de a refuza accesul la acesta***, ***în special având în vedere libertatea de exprimare și libertatea de*** a ***primi și transmite informații într-o societate deschisă și democratică*** ~~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~~. **[AM 103]**

Articolul 9a

Căi de atac eficiente

1. Furnizorii de conținut al căror conținut a fost eliminat sau la care accesul a fost blocat ca urmare a unui ordin de eliminare și furnizorii de servicii de găzduire care au primit un ordin de eliminare au dreptul de a recurge la o cale de atac eficace. Statele membre instituie proceduri eficace pentru exercitarea acestui drept. **[AM 104]**

Articolul 10

Mecanisme de depunere a plângerilor

(1) Furnizorii de servicii de găzduire instituie ***un mecanism***~~mecanisme~~ eficace și ***accesibil*** 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 ***specifice*** ~~proactive~~ luate în temeiul articolului 6 să depună o plângere împotriva acțiunii furnizorului de servicii de găzduire prin care să solicite republicarea conținutului. **[AM 105]**

(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. Aceştia informează autorul plângerii cu privire la rezultatul examinării***, în termen de două săptămâni de la primirea plângerii, oferind o explicație clară în cazurile în care furnizorii de servicii de găzduire decid să nu republice conținutul. O republicare a conținutului nu împiedică luarea de măsuri judiciare ulterioare împotriva deciziei furnizorului de servicii de găzduire sau a autorității competente***. **[AM 106]**

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, aceştia informează ***complet și concis*** furnizorul de conținut cu privire la eliminarea conținutului cu caracter terorist sau la blocarea accesului la acesta ***și cu privire la contestarea deciziei și îi transmit, la cerere, un exemplar al ordinului de eliminare emis în conformitate cu articolul 4***. **[AM 107]**

~~(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.~~ **[AM 108]**

(3) Obligația prevăzută la ***alineatul*** ~~alineatele~~ (1) ~~și (2)~~ nu se aplică în cazul în care autoritatea competentă decide***, pe baza unor dovezi obiective și luând în considerare proporționalitatea și necesitatea unei astfel de decizii,*** 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*** ~~[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. **[AM 109]**

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***, oferind garanții solide de independență***. **[AM 110]**

Articolul 13

Cooperarea dintre furnizorii de servicii de găzduire, autoritățile competente și, după caz, organismele ~~relevante~~ ***competente*** ale Uniunii **[AM 111]**

(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. **[AM 112]**

(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 ***și sigure*** care să asigure schimbul de informații relevante în timp util. **[AM 113]**

(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: **[AM 114]**

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

~~(b) prelucrarea și feedback-ul privind semnalările prevăzute la articolul 5;~~ **[AM 115]**

(c) cooperarea în vederea identificării și punerii în aplicare a măsurilor ~~proactive~~ ***specifice*** prevăzute la articolul 6. **[AM 116]**

(4) În cazul în care furnizorii de servicii de găzduire iau cunoștință de ***existența unui conținut terorist*** ~~vreo dovadă referitoare la infracțiuni de terorism~~, aceștia informează prompt autoritățile competente pentru investigarea și urmărirea penală a infracțiunilor din statul membru în cauză. ***În cazul în care este imposibil să se identifice statul membru vizat, furnizorul de servicii de găzduire notifică*** ~~sau~~ punctul de contact din statul membru în care au sediul principal sau un reprezentant legal, în conformitate cu articolul ~~14~~ ***17*** alineatul (2)***, și,*** ~~În caz~~ de ***asemenea***, ***transmite*** ~~îndoială, furnizorii de servicii de găzduire pot transmite~~ aceste informații către Europol, care urmează să ia măsuri corespunzătoare. **[AM 117]**

4a. Furnizorii de servicii de găzduire cooperează cu autoritățile competente. **[AM 118]**

Articolul 14

Puncte de contact

(1) Furnizorii de servicii de găzduire ***care au primit deja unul sau mai multe ordine de eliminare*** 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~~ ***articolul*** 4 ~~și 5~~. Aceștia se asigură că informațiile privind punctul de contact sunt făcute publice. **[AM 119]**

(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~~ ***prevăzută*** la ***articolul*** 4.~~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. **[AM 120]**

~~(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~~. **[AM 121]**

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 ***care nu își are sediul principal în unul dintre statele membre*** nu desemnează un reprezentant legal, sunt competente toate statele membre. ***În cazul în care un stat membru decide să își exercite această competență, acesta informează toate celelalte state membre în acest sens.***
[AM 122]

~~(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.~~ **[AM 123]**

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 ***solicitărilor*** ~~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. **[AM 124]**

(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 ***solicitările*** ~~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. **[AM 125]**

(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~~ ***o autoritate judiciară*** sau ***administrativă independentă din punct de vedere funcțional*** ~~autoritățile competente~~ pentru: **[AM 126]**

(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;~~ **[AM 127]**

(c) a supraveghea punerea în aplicare a măsurilor ***specifice*** ~~proactive~~ în temeiul articolului 6; **[AM 128]**

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

1a. ***Statele membre stabilesc un punct de contact care să trateze solicitările de clarificare și feedback cu privire la ordinele de eliminare pe care le emit. Informațiile referitoare la punctul de contact se fac publice.*** **[AM 129]**

(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 ***creează un registru online în care sunt enumerate toate autoritățile competente și punctul de contact desemnat pentru fiecare autoritate competentă. Comisia*** publică această notificare și eventualele modificări ale acesteia în *Jurnalul Oficial al Uniunii Europene*. **[AM 130]**

Articolul 18

Sancțiuni

(1) Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării ***sistematice și continue ale*** 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: **[AM 131]**

~~(a) articolul 3 alineatul (2) (clauzele și condițiile furnizorilor de servicii de găzduire);~~ **[AM 132]**

(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);~~ **[AM 133]**

(d) articolul 6 ***alineatul*** ~~alineatele (2) și~~ (4) (rapoartele privind măsurile ***specifice*** ~~proactive~~ și adoptarea de măsuri în urma unei ***solicitări*** ~~decizii~~ de impunere a unor măsuri ***suplimentare*** ~~proactive~~ specifice); **[AM 134]**

(e) articolul 7 (păstrarea datelor);

(f) articolul 8 (***obligații în materie de*** transparență ***pentru furnizorii de servicii de găzduire)***~~(transparență)~~; **[AM 135]**

(g) articolul 9 (măsurile de salvgardare ~~legate~~ ~~de~~ ***privind ~~utilizarea și~~ punerea în aplicare*** de ***măsuri specifice***~~proactive~~); **[AM 136]**

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

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

(j) articolul 13 alineatul (4) (informarea privind ***conținutul cu caracter terorist*** ~~dovezile referitoare la infracțiuni de terorism~~); **[AM 137]**

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

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

(2) Sancțiunile prevăzute ***la alineatul (1)*** 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. **[AM 138]**

(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~~.~~ ***;*** **[AM 139]**

(ea) natura și dimensiunea furnizorilor de servicii de găzduire, în special în cazul microîntreprinderilor sau al întreprinderilor mici, în sensul Recomandării 2003/361/CE a Comisiei[13]. **[AM 140]**

(4) Statele membre se asigură că nerespectarea sistematică ***și continuă*** 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. **[AM 141]**

Articolul 19

Cerințe tehnice***, criterii de evaluare a importanței*** și modificări ale formularelor pentru ordinele de eliminare **[AM 142]**

(1) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 20 pentru a completa prezentul regulament cu cerințe tehnice ***necesare*** privind mijloacele electronice pe care autoritățile competente trebuie să le utilizeze pentru transmiterea ordinelor de eliminare. **[AM 143]**

13 ***Recomandarea Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).***

1a. ***Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 20 pentru a completa prezentul regulament cu criterii și cifre care urmează să fie utilizate de autoritățile competente pentru a stabili ceea ce corespunde unui număr semnificativ de ordine de eliminare necontestate, astfel cum se menționează în prezentul regulament.*** **[AM 144]**

(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 ***articolul*** ~~articolele~~ 4 ~~și 5~~ ***informații privind numărul de cazuri corespunzătoare reușite de depistare, investigare și urmărire penală a infracțiunilor de terorism***; **[AM 145]**

(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;

(ba) informații privind numărul de solicitări de acces emise de autoritățile naționale competente cu privire la conținutul păstrat de furnizorii de servicii de găzduire în temeiul articolului 7; **[AM 146]**

(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*~~ ***La un an*** ~~–~~de la data aplicării prezentului ***regulament*** ~~*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***, precum și la impactul asupra drepturilor fundamentale, inclusiv asupra libertății de exprimare, a libertății de a primi și a comunica informații și asupra dreptului la respectarea vieții private***. ***În contextul prezentei evaluări, Comisia prezintă și un raport referitor la necesitatea, fezabilitatea și eficacitatea creării unei platforme europene privind conținutul cu caracter terorist online, care ar permite tuturor statelor membre să utilizeze un singur canal de comunicare securizat pentru a trimite furnizorilor de servicii de găzduire și ordine de eliminare a conținutului cu caracter terorist.*** Dacă este cazul, raportul este însoțit de propuneri legislative. Statele membre furnizează Comisiei informațiile necesare pentru elaborarea raportului respectiv. **[AM 147]**

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~~ ***12*** luni de la intrarea sa în vigoare]. **[AM 148]**

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*

ANEXA I

ORDIN DE ELIMINARE A CONȚINUTULUI CU CARACTER TERORIST [articolul 4 din Regulamentul (UE) xxx]

În temeiul articolului 4 din Regulamentul (UE)...[14], destinatarul unui ordin de eliminare elimină conținutul cu caracter terorist sau blochează accesul la acesta în termen de o oră de la primirea ordinului de eliminare de la autoritatea competentă.
În conformitate cu articolul 7 din Regulamentul (UE)...[15], la cererea autorităților sau a instanțelor competente, destinatarul trebuie să păstreze timp de șase luni sau mai mult conținutul și datele conexe care au fost eliminate sau la care s-a blocat accesul.
Ordinul de eliminare ar trebui transmis într-una din limbile desemnate de destinatar în temeiul articolului 14 alineatul (2).

SECȚIUNEA A:
Statul membru emitent:
……..……..
NB: Datele de contact privind autoritatea emitentă trebuie prezentate la sfârșit (secțiunile E și F)
Destinatarul (reprezentantul legal)
……..……..
Destinatarul (punctul de contact)
……..……..
Statul membru sub a cărui jurisdicție se află destinatarul (statul competent): [dacă diferă de statul emitent]
……..……..
Data și ora emiterii ordinului de eliminare
……..……..
Numărul de referință al ordinului de eliminare:
……..……..

14 Regulamentul Parlamentului European și al Consiliului privind prevenirea diseminării conținutului online cu caracter terorist(*JO L* …).

15 Regulamentul Parlamentului European și al Consiliului privind prevenirea diseminării conținutului online cu caracter terorist(*JO L* …).

SECȚIUNEA B: Conținutul care trebuie eliminat sau la care accesul trebuie blocat ~~în termen de o oră~~ ***fără întârzieri nejustificate:*** **[AM 162]**
O adresă URL și informații suplimentare care să permită identificarea și locația exactă a conținutului cu caracter terorist semnalat:
……..……
Motivul (motivele) care explică de ce conținutul este considerat conținut cu caracter terorist, în conformitate cu articolul 2 alineatul (5) din Regulamentul (UE) xxx. Conținutul [a se bifa caseta (casetele) corespunzătoare]:
□ incită, ~~promovează sau glorifică~~ ***la*** săvârșirea ~~unor~~ ***de*** infracțiuni de terorism ***enumerate la articolul 3 alineatul (1) literele (a) — (i) din Directiva (UE) 2017/541*** [articolul 2 alineatul (5) litera (a)] **[AM 149]**
□ ~~încurajează contribuirea la~~ ***determină o persoană sau un grup de persoane să săvârșească*** infracțiuni de terorism ***enumerate la articolul 3 alineatul (1) literele (a) — (i) din Directiva (UE) 2017/541*** [articolul 2 alineatul (5) litera (b)] ***sau să contribuie la săvârșirea acestora;*** **[AM 150]**
□ ~~promovează activitățile unui~~ ***determină o persoană sau un*** grup ~~terorist, încurajând~~ participarea la ~~un grup terorist sau sprijinirea acestuia~~ [articolul 2 alineatul (5) litera (c)]; **[AM 151]**
□ furnizează instrucțiuni sau tehnici ***de confecționare sau utilizare a explozivilor, armelor de foc sau a altor arme sau substanțe nocive sau periculoase sau alte tehnici și metode concrete de săvârșire a*** ~~pentru săvârșirea~~ unor infracțiuni de terorism ***enumerate la articolul 3 alineatul (1) literele (a)-(i) din Directiva (UE) 2017/541*** [articolul 2 alineatul (5) litera (d)]; **[AM 152]**
[ ] prezintă săvârșirea de infracțiuni de terorism enumerate la articolul 3 alineatul (1) literele (a) — (i) din Directiva (UE) 2017/541 [articolul 2 alineatul (5) litera (e)]; **[AM 153]**
Informații suplimentare privind motivele pentru care conținutul este considerat conținut cu caracter terorist (opțional): ……
……..
…….

SECȚIUNEA C: Informarea furnizorului de conținut
Vă rugăm să rețineți că (a se bifa, după caz):
□ din motive de siguranță publică, destinatarul **nu are voie să informeze furnizorul de conținut** al cărui conținut este eliminat sau la care s-a blocat accesul.

Sau: Informații privind posibilitățile de contestare a ordinului de eliminare în statul membru emitent (care pot fi transmise furnizorului de conținut, la cerere) în temeiul dreptului național; a se vedea secțiunea G de mai jos.

SECȚIUNEA D: Informarea statului membru competent
□ A se bifa dacă statul membru competent este diferit de statul membru emitent:
□ o copie a ordinului de eliminare este trimisă autorității competente a statului membru competent

SECȚIUNEA E: Date de contact ale autorității care a emis ordinul de eliminare
Tipul de autoritate care a emis ordinul de eliminare (a se bifa caseta corespunzătoare):
□ un judecător, o instanță judecătorească sau un judecător de instrucție
□ o autoritate de asigurare a respectării legii
□ altă autoritate competentă→ vă rugăm să completați și secțiunea F

Date de contact privind autoritatea emitentă și/sau reprezentatul acesteia care atestă exactitatea și corectitudinea ordinului de eliminare:
Denumirea autorității:
……
Numele reprezentantului:
……
Funcția deținută (titlu/grad):
……
Numărul dosarului:……
Adresa:……
Numărul de telefon: (prefixul țării) (prefixul regiunii/localității)……
Fax: (prefixul țării) (prefixul regiunii/localității)……
E-mail: ……
Data:
……
Ștampila oficială (dacă există) și semnătura[16]:
……

16 Semnătura nu este necesară în cazul transmiterii prin canale autentificate.

SECȚIUNEA F: Date de contact pentru acțiuni subsecvente

Datele de contact la care autoritatea emitentă poate fi contactată pentru a primi feedback privind momentul eliminării sau al blocării accesului sau pentru a furniza clarificări suplimentare:

……..…….

Date de contact ale autorității din statul competent [dacă diferă de statul membru emitent]

……..…….

SECȚIUNEA G: Informații privind căile de atac

Informații privind organismul sau instanța competentă, termenele și procedurile ~~de contestare a~~ ***, inclusiv cerințele oficiale pentru contestarea*** ordinului de eliminare:

[AM 154]

Organismul sau instanța competentă la care se poate contesta ordinul de eliminare:

…….…….

Termenul pentru contestarea deciziei:

xxx luni începând de la xxxx

Link la dispozițiile din legislația națională:

…….…….

ANEXA II

FORMULAR DE FEEDBACK ÎN URMA UNUI ORDIN DE ELIMINARE A CONȚINUTULUI CU CARACTER TERORIST SAU DE BLOCARE A ACCESULUI LA ACESTA [articolul 4 alineatul (5) din Regulamentul (UE) xxx]

SECȚIUNEA A:
Destinatarul ordinului de eliminare:
……..……..
Autoritatea care a emis ordinul de eliminare:
……..……..
Numărul de referință al dosarului autorității emitente:
……..……..
Numărul de referință al dosarului destinatarului:
……..……..
Data și ora primirii ordinului de eliminare:
……..……..

SECȚIUNEA B:
Conținutul cu caracter terorist/accesul la conținutul cu caracter terorist care face obiectul ordinului de eliminare a fost (a se bifa caseta corespunzătoare):

- □ eliminat
- □ blocat

Ora și data eliminării sau a blocării accesului ……..

SECȚIUNEA C: Datele de contact ale destinatarului

Numele furnizorului de servicii de găzduire/reprezentantului legal:

……..……..

Statul membru în care se află sediul principal sau în care este stabilit reprezentantul legal:

……..……..

Numele persoanei autorizate:

……..……..

Datele de contact ale punctului de contact (e-mail):

…….

Data:

……..……..

_____

ANEXA III

INFORMAȚII PRIVIND IMPOSIBILITATEA DE A EXECUTA ORDINUL DE ELIMINARE [articolul 4 alineatele (6) și (7) din Regulamentul (UE) xxx]

SECȚIUNEA A:
Destinatarul ordinului de eliminare:
……..……..
Autoritatea care a emis ordinul de eliminare:
……..……..
Numărul de referință al dosarului autorității emitente:
……..……..
Numărul de referință al dosarului destinatarului:
……..……..
Data și ora primirii ordinului de eliminare:
……..……..

SECȚIUNEA B: Motivele neexecutării
(i) Ordinul de eliminare nu poate fi executat sau nu poate fi executat în termenul solicitat din următorul (următoarele) motiv(e):

□ caz de forță majoră sau imposibilitate *de facto* care nu pot fi imputate destinatarului sau furnizorului de servicii***, inclusiv din motive tehnice sau operaționale*** **[AM 155]**

□ ordinul de eliminare conține erori evidente

□ ordinul de eliminare nu conține suficiente informații

(ii) Vă rugăm să furnizați informații suplimentare cu privire la motivele neexecutării:
…….
(iii) În cazul în care ordinul de eliminare conține erori evidente și/sau nu conține informații suficiente, a se preciza erorile și informațiile sau clarificările suplimentare care sunt necesare:
…….

SECȚIUNEA C: Datele de contact ale furnizorului de servicii/reprezentantului său legal
Numele furnizorului de servicii/reprezentantului legal:
……..……..
Numele persoanei autorizate:
……..……..
Date de contact (e-mail):
……..……..
Semnătura:
……..……..
Data și ora:
……..……..