Consiliul
Uniunii Europene

Bruxelles, 18 martie 2021
(OR. en)

14308/1/20
REV 1

Dosar interinstituțional:
2018/0331 (COD)

CT 122
ENFOPOL 355
COTER 121
JAI 1135
CYBER 285
TELECOM 281
FREMP 149
AUDIO 70
DROIPEN 127
CODEC 1412
PARLNAT 147

ACTE LEGISLATIVE ȘI ALTE INSTRUMENTE

Subiect:	Poziţie în primă lectură a Consiliului în vederea adoptării REGULAMENTULUI PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind prevenirea diseminării conținutului online cu caracter terorist - Adoptată de Consiliu la 16 martie 2021

REGULAMENTUL (UE) 2021/…
AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din …

privind prevenirea diseminării conținutului online cu caracter terorist

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[1],

hotărând în conformitate cu procedura legislativă ordinară[2],

---

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

[2] Poziția Parlamentului European din 17 aprilie 2019 (nepublicată încă în Jurnalul Oficial) și Poziția în primă lectură a Consiliului din 16 martie 2021 (nepublicată încă în Jurnalul Oficial). Poziția Parlamentului European din … (nepublicată încă în Jurnalul Oficial).

întrucât:

(1) Prezentul regulament urmărește să asigure buna funcționare a pieței unice digitale în cadrul unei societăți deschise și democratice, prin prevenirea utilizării abuzive a serviciilor de găzduire în scopuri teroriste și prin contribuția la siguranța publică în întreaga Uniune. Funcționarea pieței unice digitale ar trebui să fie îmbunătățită prin consolidarea securității juridice pentru furnizorii de servicii de găzduire și a încrederii utilizatorilor în mediul online, precum și prin consolidarea măsurilor de protecție a libertății de exprimare, inclusiv a libertății de a primi și a transmite informații și idei într-o societate deschisă și democratică, și a libertății și a pluralismului mass-mediei.

(2) Măsurile de reglementare pentru prevenirea diseminării conținutului online cu caracter terorist ar trebui să fie completate prin strategiile statelor membre de combatere a terorismului, inclusiv prin consolidarea educației în domeniul mass-mediei și a gândirii critice, unor discursuri alternative și contradiscursuri și prin alte inițiative pentru reducerea impactului conținutului online cu caracter terorist și vulnerabilitatea față de acesta, precum și prin investițiile în activitatea socială, inițiativele de deradicalizare și contactul cu comunitățile afectate pentru a se asigura o prevenție sustenabilă a radicalizării în societate.

(3) Prevenirea conținutului online cu caracter terorist, care face parte din problematica mai amplă a conținutului ilegal online necesită o combinație de măsuri cu caracter legislativ, fără caracter legislativ și voluntare, bazate pe colaborarea dintre autorități și furnizorii de servicii de găzduire, cu deplina respectare a drepturilor fundamentale.

(4) Furnizorilor de servicii de găzduire care activează pe internet le revine un rol esențial în economia digitală, prin crearea de legături între mediul de afaceri și cetățeni și prin facilitarea dezbaterii publice, a difuzării și primirii de informații, de idei și opinii, contribuind în mod semnificativ la inovare, la creșterea economică și la crearea de locuri de muncă în Uniune. Cu toate acestea, serviciile furnizorilor de servicii de găzduire sunt, în anumite situații, utilizate abuziv de către terți în scopul de a desfășura activități ilegale online. Un motiv de preocupare deosebită îl reprezintă utilizarea abuzivă a serviciilor respective 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 adepți, precum și de a facilita și dirija activitățile teroriste.

(5) Deși nu constituie singurul factor, prezența conținutului online cu caracter terorist s-a dovedit a fi decisivă în favorizarea radicalizării persoanelor care poate conduce la 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 de afaceri ale acestora. Din perspectiva rolului lor central și a mijloacelor și capacităților tehnologice asociate serviciilor pe care le oferă, furnizorilor de servicii de găzduire le revin responsabilități societale speciale de a-și proteja serviciile împotriva utilizării abuzive de către teroriști și de a contribui la prevenirea conținutului cu caracter terorist diseminat prin intermediul serviciilor online pe care le oferă, ținând seama totodată de importanța fundamentală a libertății de exprimare, inclusiv a libertății de a primi și transmite informații și idei într-o societate deschisă și democratică.

(6) Eforturile de prevenire a conținutului online cu caracter terorist au fost inițiate la nivelul Uniunii în 2015 prin intermediul unui cadru de cooperare voluntară între statele membre și furnizorii de servicii de găzduire. Eforturile respective trebuie să fie completate de un cadru legislativ clar, pentru a reduce și mai mult accesibilitatea conținutului online cu caracter terorist și pentru a preveni în mod adecvat o provocare care evoluează rapid. Cadrul legislativ își propune să valorifice eforturile voluntare, care au fost consolidate prin Recomandarea (UE) 2018/334 a Comisiei[1], și răspunde solicitărilor formulate de Parlamentul European pentru consolidarea măsurilor de prevenire a conținuturilor online ilegale și dăunătoare, în concordanță cu cadrul orizontal instituit prin Directiva 2000/31/CE a Parlamentului European și a Consiliului[2], precum și de către Consiliul European, de a se îmbunătăți depistarea și eliminarea conținutului online care instigă la acte teroriste.

(7) Prezentul regulament nu ar trebui să aducă atingere aplicării Directivei 2000/31/CE. În special, eventualele măsuri, inclusiv cele specifice, luate de un furnizor de servicii de găzduire în conformitate cu prezentul regulament nu ar trebui să conducă, prin ele însele, la pierderea de către respectivul furnizor de servicii de găzduire a beneficiului exonerării de răspundere prevăzută în directiva respectivă. În plus, prezentul regulament nu aduce atingere competențelor autorităților și instanțelor naționale de a stabili răspunderea furnizorilor de servicii de găzduire atunci când nu sunt îndeplinite condițiile stabilite în directiva respectivă pentru exonerarea de răspundere.

---

1 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).

2 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).

(8) În cazul unui conflict între prezentul regulament și Directiva 2010/13/UE în ceea ce privește dispozițiile care reglementează serviciile mass-media audiovizuale, astfel cum sunt definite la articolul 1 alineatul (1) litera (a) din directiva respectivă, ar trebui să prevaleze Directiva 2010/13/UE. Acest fapt nu ar trebui să aducă atingere obligațiilor care decurg din prezentul regulament, în special cele referitoare la furnizorii de servicii de platforme de partajare a materialelor video.

(9) Prezentul regulament ar trebui să stabilească norme menite să prevină utilizarea abuzivă a serviciilor de găzduire pentru diseminarea conținutului online cu caracter terorist, astfel încât să se asigure buna funcționare a pieței interne. Normele respective ar trebui să respecte pe deplin drepturile fundamentale protejate în Uniune, în special cele garantate prin Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”).

(10) Prezentul regulament urmărește să contribuie la protecția securității publice, stabilind totodată măsuri de salvgardare adecvate și solide în vederea asigurării protecției drepturilor fundamentale, inclusiv dreptul la respectarea vieții private, la protecția datelor cu caracter personal, la libertatea de exprimare, inclusiv la libertatea de a primi și de a transmite informații, la libertatea de a desfășura o activitate comercială, și dreptul la o cale de atac efectivă. În plus, se interzice orice discriminare. Autoritățile competente și furnizorii de servicii de găzduire ar trebui să adopte măsuri numai atunci când acestea sunt necesare, adecvate și proporționale în cadrul unei societăți democratice, luând în considerare importanța deosebită acordată libertății de exprimare și de informare, și libertății și pluralismului mass-mediei, care constituie fundamentele esențiale ale unei societăți pluraliste și democratice și sunt valorile pe care este întemeiată Uniunea. Măsurile care afectează libertatea de exprimare și de informare ar trebui să fie strict direcționate pentru prevenirea diseminării conținutului online cu caracter terorist, respectându-se totodată dreptul de a primi și de a transmite informații în mod legal, având în vedere rolul central care revine 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 eficace de prevenire a conținutului online cu caracter terorist și protecția libertății de exprimare și de informare nu constituie obiective contradictorii, ci se completează și se consolidează reciproc.

(11) Pentru a oferi claritate cu privire la acțiunile pe care furnizorii de servicii de găzduire și autoritățile competente trebuie să le ia pentru a preveni diseminarea conținutului online cu caracter terorist, prezentul regulament ar trebui să stabilească, în scop preventiv, o definiție a „conținutului cu caracter terorist”, în concordanță cu definiția infracțiunilor care intră sub incidența Directivei (UE) 2017/541 a Parlamentului European și a Consiliului[1]. Având în vedere nevoia de a preveni cele mai dăunătoare forme de propagandă teroristă online, definiția respectivă ar trebui să includă materialele care instigă sau solicită unei persoane să comită infracțiuni de terorism sau să contribuie la comiterea acestor infracțiuni, îi solicită să participe la activitățile unui grup terorist sau care glorifică activitățile teroriste, inclusiv prin diseminarea de materiale care prezintă un atac terorist. Definiția ar trebui să includă și materialul care oferă instrucțiuni pentru fabricarea sau 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 cu privire la alte metode ori tehnici specifice, inclusiv selecționarea țintelor, cu scopul de a comite infracțiuni de terorism sau de a contribui la comiterea acestora. Astfel de materiale includ texte, imagini, înregistrări audio și înregistrări video, precum și transmisii în direct ale unor infracțiuni de terorism, care cauzează un pericol de comitere a altor astfel de infracțiuni. Atunci când evaluează dacă un material reprezintă un conținut cu caracter terorist în înțelesul 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 formulate și potențialul acestora de a genera consecințe prejudiciabile pentru securitatea și siguranța persoanelor. Faptul că materialul a fost produs de o persoană, un grup sau o entitate incluse pe lista Uniunii a persoanelor, grupurilor și entităților implicate în acte de terorism și cărora li se aplică măsuri restrictive, sau poate fi atribuit acestora ori este diseminat în numele acestora, ar trebui să constituie un factor important pentru evaluare.

---

[1] 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).

(12) Materialul diseminat în scopuri educative, jurnalistice, artistice sau de cercetare sau în scopul sensibilizării opiniei publice împotriva activității teroriste nu ar trebui să fie considerat conținut cu caracter terorist. Atunci când se stabilește dacă materialul furnizat de un furnizor de conținut constituie „conținut cu caracter terorist” astfel cum este definit în prezentul regulament, ar trebui să se țină seama, în special, de dreptul la libertatea de exprimare și de informare, inclusiv libertatea și pluralismul mass-mediei și de libertatea artelor și a științelor. În special în cazurile în care furnizorul de conținut deține 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, inclusiv cu Carta. În plus, exprimarea unor puncte de vedere radicale, polemice sau controversate în cadrul dezbaterii publice privind chestiuni politice sensibile nu ar trebui să fie considerată drept conținut cu caracter terorist.

(13) Pentru a preveni în mod eficace diseminarea conținutului online cu caracter terorist, asigurând totodată respectarea vieții private a persoanelor fizice, prezentul regulament ar trebui să se aplice furnizorilor de servicii ale societății informaționale care stochează și diseminează către public informații și materiale furnizate de un utilizator al serviciului la cererea acestuia, indiferent dacă stocarea și diseminarea către public a unor astfel de informații și materiale are un caracter pur tehnic, automat și pasiv. Noțiunea de „stocare” ar trebui să fie interpretată în sensul de păstrare de date în memoria unui server fizic sau virtual. Furnizorii de servicii de „simplă transmitere” sau de „înmagazinare cache”, precum și de alte servicii furnizate la alte nivele ale infrastructurii de internet, care nu implică stocare, cum ar fi registrele de nume de domenii sau operatorii de registru, precum și furnizorii de servicii DNS (sistem de nume de domenii), servicii de protecție pentru plăți sau de protecție DDoS (*Distributed Denial of Service*) nu ar trebui să intre, prin urmare, în domeniul de aplicare al prezentului regulament.

(14) Noțiunea de „diseminare către public” ar trebui să implice punerea informațiilor la dispoziția unui număr potențial nelimitat de persoane, adică faptul de a face ca informațiile să fie ușor accesibile utilizatorilor în general fără a fi necesară o acțiune suplimentară din partea furnizorului de conținut, indiferent dacă persoanele respective accesează efectiv sau nu informațiile în cauză. În consecință, în cazul în care accesul la informații necesită înregistrarea sau admiterea într-un grup de utilizatori, informațiile respective ar trebui considerate ca fiind diseminate către public numai în cazul în care utilizatorii care doresc să acceseze informațiile sunt înregistrați sau admiși în mod automat, fără intervenția umană pentru o decizie sau o selecție vizând persoanele cărora li se acordă accesul. Serviciile de comunicații interpersonale, astfel cum sunt definite la articolul 2 punctul 5 din Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului[1], cum ar fi e-mailurile sau serviciile de mesagerie privată, nu ar trebui să intre în domeniul de aplicare al prezentului regulament. Informațiile ar trebui considerate ca fiind stocate și diseminate către public în sensul prezentului regulament numai în cazul în care astfel de activități sunt efectuate la cererea directă a furnizorului de conținut. În consecință, furnizorii de servicii precum infrastructura de tip cloud, care sunt furnizate la cererea altor părți decât furnizorii de conținut și care le aduc beneficii doar în mod indirect acestora din urmă, nu ar trebui să intre sub incidența prezentului regulament. Intră, de exemplu, sub incidența prezentului regulament furnizorii de platforme de comunicare socială, de servicii de partajare de materiale video, de imagini și de materiale audio, precum și de servicii de partajare de fișiere și alte servicii de tip cloud, în măsura în care aceste servicii sunt utilizate pentru a pune informațiile stocate la dispoziția publicului la cererea directă a furnizorului de conținut. În cazul în care un furnizor de servicii de găzduire oferă mai multe servicii, prezentul regulament ar trebui să se aplice numai în ceea ce privește serviciile care intră în domeniul său de aplicare.

[1] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).

(15) Conținutul cu caracter terorist este adesea diseminat către public prin servicii prestate de furnizori de servicii de găzduire stabiliți în țări terțe. Pentru a proteja utilizatorii din Uniune și pentru a se asigura că tuturor furnizorilor de servicii de găzduire care își desfășoară activitatea pe piața unică digitală li se aplică aceleași cerințe, prezentul regulament ar trebui să se aplice tuturor furnizorilor de servicii relevante oferite în Uniune, indiferent de țara în care își au sediul principal. Un furnizor de servicii de găzduire ar trebui să fie considerat ca oferind servicii în Uniune dacă acesta le permite persoanelor fizice sau juridice din unul sau mai multe state membre să îi utilizeze serviciile și dacă are o legătură substanțială cu statul sau statele membre respective.

(16) Ar trebui să existe o legătură substanțială cu Uniunea atunci când furnizorul de servicii de găzduire are un sediu în Uniune, serviciile sale sunt utilizate de un număr semnificativ de utilizatori în unul sau mai multe state membre ori activitățile sale sunt direcționate către unul sau mai multe state membre. Direcționarea activităților către unul sau mai multe state membre ar trebui să fie determinată pe baza tuturor circumstanțelor relevante, inclusiv a factorilor precum utilizarea unei limbi sau a unei monede utilizate în general în statul membru în cauză sau posibilitatea de a comanda bunuri sau servicii dintr-un astfel de stat membru. O asemenea direcționare ar putea să reiasă, de asemenea, din disponibilitatea unei aplicații în magazinul de aplicații național relevant, difuzarea de materiale publicitare locale sau într-o limbă utilizată în general în statul membru respectiv sau din modul de gestionare a relațiilor cu clienții, de exemplu prin oferirea de servicii de relații cu clienții într-o limbă utilizată în general în statul membru respectiv. Ar trebui să se considere că există o legătură substanțială și în cazul în care un furnizor de servicii de găzduire 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[1]. Simplul fapt al accesibilității, în unul sau mai multe state membre, a site-ului de internet al unui furnizor de servicii de găzduire, a unei adrese de e-mail sau a altor date de contact, considerat izolat, nu ar trebui să constituie o condiție suficientă pentru stabilirea unei legături substanțiale. În plus, furnizarea serviciului în vederea simplei respectări a interdicției de discriminare prevăzute în Regulamentul (UE) 2018/302 al Parlamentului European și al Consiliului[2] nu ar trebui să fie considerată drept o legătură substanțială cu Uniunea, exclusiv pe baza acestui motiv.

---

[1] 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).

[2] 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 60 I, 2.3.2018, p. 1).

(17) Procedurile și obligațiile care rezultă din ordinele de eliminare 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, ar trebui să fie armonizate. Având în vedere viteza de diseminare a conținutului cu caracter terorist prin intermediul serviciilor online, ar trebui ca furnizorilor de servicii de găzduire să li se impună obligația de a se asigura că un conținut cu caracter terorist identificat în ordinul de eliminare este eliminat sau accesul la acesta este blocat în toate statele membre în termen de o oră de la primirea ordinului respectiv. Cu excepția unor cazuri de urgență justificate în mod corespunzător, autoritatea competentă ar trebui să pună la dispoziția furnizorului de servicii de găzduire informații cu privire la procedurile și termenele aplicabile cu cel puțin 12 ore înaintea emiterii către furnizorul de servicii de găzduire respectiv a primului ordin de eliminare. Cazuri de urgență justificate corespunzător apar în cazul în care eliminarea conținutului sau blocarea accesului la acesta în mai mult de o oră de la primirea ordinului de eliminare ar avea ca rezultat prejudicii grave, cum ar fi în situația de amenințare iminentă la adresa vieții sau a integrității fizice a unei persoane sau atunci când conținutul respectiv prezintă evenimente în curs de desfășurare care au ca rezultat vătămarea vieții sau integrității fizice a unei persoane. Autoritatea competentă ar trebui să determine care cazuri sunt cazuri de urgență și să justifice corespunzător decizia sa privind ordinul de eliminare. Atunci când furnizorul de servicii de găzduire nu poate executa ordinul de eliminare în termen de o oră de la primirea lui, din motive de forță majoră sau a unei imposibilități *de facto*, inclusiv din motive tehnice sau operaționale justificate în mod obiectiv, acesta ar trebui să informeze autoritatea competentă care a emis ordinul cât mai curând posibil și să execute ordinul de eliminare imediat ce situația se remediază.

(18) Ordinul de eliminare ar trebui să indice motivele care justifică calificarea materialului care urmează să fie eliminat sau al cărui acces urmează să fie blocat, ca având conținut cu caracter terorist și să ofere suficiente informații pentru localizarea conținutului respectiv, prin furnizarea URL-ului exact și, după caz, orice alte informații suplimentare, cum ar fi o captură de ecran a conținutului în cauză. Indicarea motivelor ar trebui să permită furnizorului de servicii de găzduire și, în ultimă instanță, furnizorului de conținut să își exercite efectiv dreptul la o cale de atac contencioasă. Motivele indicate nu ar trebui să dezvăluie informații sensibile care ar putea periclita investigațiile în curs.

(19) Autoritatea competentă ar trebui să transmită ordinul de eliminare direct punctului de contact desemnat sau stabilit de furnizorul de servicii de găzduire în sensul prezentului regulament, prin orice mijloace electronice care permit o înregistrare scrisă, în condiții care îi permit furnizorului de servicii de găzduire să stabilească autenticitatea ordinului, inclusiv exactitatea datei și orei de trimitere și de primire a ordinului, de exemplu prin e-mail ori platforme securizate sau alte canale securizate, inclusiv cele puse la dispoziție de către furnizorul de servicii de găzduire, în conformitate cu dreptul Uniunii privind protecția datelor cu caracter personal. Această cerință ar trebui să poată fi îndeplinită prin utilizarea, printre altele, a serviciilor de distribuție electronică înregistrată calificate, astfel cum sunt prevăzute în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului[1]. Atunci când sediul principal al furnizorului de servicii de găzduire ori reședința sau sediul reprezentantului său legal se află într-un alt stat membru decât statul membru al autorității competente care emite ordinul, o copie a ordinului de eliminare în cauză ar trebui să fie transmisă în același timp și autorității competente din statul membru respectiv.

[1] 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).

(20) Autoritatea competentă a statului membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal ar trebui să poată efectua controlul ordinului de eliminare emis de autoritățile competente ale altui stat membru pentru a stabili dacă acesta încalcă în mod grav sau vădit prezentul regulament sau drepturile fundamentale consacrate în Cartă. Atât furnizorul de conținut, cât și furnizorul de servicii de găzduire ar trebui să aibă dreptul de a cere efectuarea unui astfel de control de către autoritatea competentă din statul membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal. Atunci când se prezintă o astfel de cerere, autoritatea competentă vizată ar trebui să adopte o decizie prin care să stabilească dacă ordinul de eliminare include o astfel de încălcare. Atunci când prin decizia respectivă se constată o astfel de încălcare, ordinul de eliminare ar trebui să înceteze să mai producă efecte juridice. Controlul ar trebui să fie efectuat cu celeritate, astfel încât să se asigure republicarea cât mai rapidă a conținutului eliminat sau blocat în mod eronat.

(21) Furnizorii de servicii de găzduire expuși la conținut cu caracter terorist ar trebui să includă în clauzele și condițiile lor, în cazul în care acestea există, dispoziții care previn utilizarea abuzivă a serviciilor lor pentru diseminarea conținutului online cu caracter terorist către public. Aceștia ar trebui să aplice prevederile respective în mod diligent, transparent, proporțional și nediscriminatoriu.

(22) Având în vedere amploarea preocupării și viteza necesară pentru a identifica și a înlătura în mod eficace conținut cu caracter terorist, un element esențial pentru prevenirea conținutului online cu caracter terorist îl constituie măsurile specifice eficace și proporționale. În vederea reducerii accesibilității conținutului cu caracter terorist în cadrul serviciilor lor, furnizorii de servicii de găzduire expuși la conținutul cu caracter terorist ar trebui să ia măsuri specifice, în funcție de riscuri și de nivelul de expunere la conținutul cu caracter terorist, precum și de efectele asupra drepturilor terților și de interesul public al informațiilor. Furnizorii de servicii de găzduire ar trebui să stabilească care sunt măsurile specifice adecvate, eficace și proporționale care ar trebui să se aplice pentru a identifica și elimina conținutul cu caracter terorist. Printre măsurile specifice s-ar putea include măsuri sau capacități tehnice sau operaționale adecvate, cum ar fi personal sau mijloace tehnice de identificare și eliminare promptă a conținutului cu caracter terorist sau de blocare rapidă a accesului la conținutul respectiv, mecanisme prin care utilizatorii să raporteze sau să semnaleze presupusul conținut cu caracter terorist sau orice alte măsuri pe care furnizorul de servicii de găzduire le consideră adecvate și eficace pentru a preveni disponibilitatea conținutului cu caracter terorist în cadrul serviciilor sale.

(23) Atunci când pun în aplicare măsuri specifice, furnizorii de servicii de găzduire ar trebui să se asigure că se mențin atât dreptul utilizatorilor la libertatea de exprimare și de informare, cât și libertatea și pluralismul mass-mediei, astfel cum sunt protejate prin Cartă. Pe lângă respectarea tuturor 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 protecție, după caz, inclusiv supraveghere și verificări umane, pentru a evita luarea unor decizii neintenționate sau eronate care conduc la eliminarea unui conținut care nu constituie conținut cu caracter terorist sau la blocarea accesului la acesta.

(24) Furnizorul de servicii de găzduire ar trebui să raporteze autorității competente cu privire la măsurile specifice pe care le aplică, pentru a permite autorității respective să stabilească dacă măsurile sunt eficace și proporționale și dacă, în cazul în care sunt utilizate mijloace automatizate, furnizorul de servicii de găzduire deține capacitățile necesare pentru supravegherea și verificarea umane. La evaluarea eficacității și proporționalității măsurilor, autoritățile competente ar trebui să ia în considerare parametrii relevanți, inclusiv numărul de ordine de eliminare adresate furnizorului de servicii de găzduire, dimensiunea și capacitatea economică a furnizorului de servicii de găzduire și impactul serviciilor furnizate de acesta în diseminarea de conținut cu caracter terorist, de exemplu, pe baza numărului de utilizatori din Uniune, precum și măsurile de protecție pe care le aplică pentru a preveni utilizarea abuzivă a serviciilor sale pentru diseminarea conținutului online cu caracter terorist.

(25) Atunci când autoritatea competentă consideră că măsurile specifice luate sunt insuficiente pentru a preveni riscurile, aceasta ar trebui să poată impune adoptarea unor măsuri specifice adecvate, eficace și proporționale suplimentare. Obligația de a pune în aplicare astfel de măsuri specifice suplimentare nu ar trebui să genereze o obligație generală de supraveghere sau de a căuta în mod activ fapte, în sensul articolului 15 alineatul (1) din Directiva 2000/31/CE, și nici la obligația de a utiliza instrumente automatizate. Cu toate acestea, furnizorii de servicii de găzduire ar trebui să poată utiliza instrumente automatizate în cazul în care consideră acest lucru adecvat și necesar pentru a preveni în mod eficace utilizarea abuzivă a serviciilor lor pentru diseminarea conținutului cu caracter terorist.

(26) Obligația care revine 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 la durata necesară. Se impune ca obligația de păstrare să se extindă la datele conexe în măsura în care astfel de date ar fi altfel pierdute ca urmare a eliminării conținutului cu caracter terorist în cauză. Printre datele conexe pot fi date precum datele privind abonații, în special datele referitoare la identitatea furnizorului de conținut, precum și datele privind accesul, inclusiv datele privind data și ora utilizării de către furnizorul de conținut și 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.

(27) Obligația de a păstra conținutul în vederea unor proceduri de control jurisdicțional administrativ sau judecătoresc este necesară și justificată în vederea asigurării existenței unor căi de atac efective la dispoziția furnizorului de conținut a fost eliminat sau la al cărui conținut a fost blocat accesul, precum și pentru a se asigura republicarea conținutului respectiv, în funcție de rezultatul procedurilor respective. Obligația de a păstra materialul în vederea unor proceduri de investigare sau de urmărire penală se justifică și este necesară având în vedere valoarea pe care acest material ar putea să o aibă în contracararea sau prevenirea activității teroriste. Prin urmare, păstrarea conținutului cu caracter terorist eliminat în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism ar trebui să fie, de asemenea, considerată ca fiind justificată. Conținutul cu caracter terorist și datele aferente ar trebui să fie stocate numai pentru o perioada necesară care să permită autorităților de aplicare a legii să verifice conținutul cu caracter terorist și să decidă dacă acesta ar fi necesar în scopurile respective. Pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism, păstrarea obligatorie a datelor ar trebui să se limiteze la datele care sunt susceptibile de a avea legătură cu infracțiuni de terorism și, prin urmare, ar putea contribui la urmărirea penală a infracțiunilor respective sau la prevenirea riscurilor majore la adresa securității publice. Atunci când furnizorii de servicii de găzduire elimină materialul sau blochează accesul la acesta, în special prin măsuri specifice proprii, ar trebui să informeze cu promptitudine autoritățile competente cu privire la conținutul care include informații referitoare la o amenințare iminentă la adresa vieții sau la o presupusă infracțiune de terorism.

(28) În vederea asigurării proporționalității, perioada de păstrare ar trebui să fie limitată la șase luni pentru a acorda furnizorilor de conținut suficient timp să inițieze proceduri de control jurisdicțional administrativ sau judecătoresc și pentru a permite accesul autorităților de aplicare a legii la datele relevante pentru investigarea și urmărirea penală a infracțiunilor de terorism. Totuși, la cererea autorității competente sau a instanței, această perioadă ar trebui să poată fi prelungită cu durata necesară în cazul în care procedurile respective sunt inițiate dar nu sunt finalizate în perioada de șase luni. Durata perioadei de păstrare ar trebui să fie suficientă pentru a permite autorităților de aplicare a legii să conserve materialele necesare în vederea investigațiilor și a urmăririi penale, asigurând în același timp echilibrul cu drepturile fundamentale.

(29) Prezentul regulament nu ar trebui să aducă atingere garanțiilor procedurale sau măsurilor procedurale de investigare care privesc accesul la conținutul și la datele conexe păstrate în vederea investigării și a urmăririi penale a infracțiunilor de terorism, astfel cum sunt reglementate de dreptul Uniunii sau de dreptul intern.

(30) Transparența politicilor furnizorilor de servicii de găzduire în ceea ce privește conținutul cu caracter terorist este esențială pentru a spori gradul de răspundere față de propriii utilizatori și încrederea cetățenilor în piața unică digitală. Furnizorii de servicii de găzduire care au luat măsuri sau au fost obligați să ia astfel de măsuri în temeiul prezentului regulament în cursul unui anumit an calendaristic ar trebui să pună la dispoziția publicului rapoarte anuale privind transparența care includ informații cu privire la măsurile întreprinse în legătură cu identificarea și eliminarea conținutului cu caracter terorist.

(31) Autoritățile competente ar trebui să publice rapoarte anuale privind transparența, care includ informații referitoare la numărul ordinelor de eliminare, numărul cazurilor în care ordinele nu au fost executate, numărul deciziilor referitoare la măsuri specifice, numărul de cazuri care au făcut obiectul unor proceduri de control jurisdicțional administrativ sau judecătoresc și numărul deciziilor prin care s-au aplicat sancțiuni.

(32) Dreptul la o cale de atac efectivă este consacrat la articolul 19 din Tratatul privind Uniunea Europeană (TUE) și la articolul 47 din Cartă. Orice persoană fizică sau juridică are dreptul la o cale de atac efectivă în fața instanței naționale competente împotriva oricărei măsuri luate în temeiul prezentului regulament, care poate aduce atingere drepturilor persoanei respective. Dreptul respectiv ar trebui să includă, în special, posibilitatea ca furnizorii de servicii de găzduire și furnizorii de conținut să conteste efectiv în fața unei instanțe din statul membru a cărui autoritate competentă a emis un ordin de eliminare sau a adoptat o decizie, ordinul respectiv sau orice decizie care rezultă în urma controlului ordinelor de eliminare în temeiul prezentului regulament precum și posibilitatea ca furnizorii de servicii de găzduire să conteste efectiv o decizie privind măsuri specifice sau sancțiuni în fața unei instanțe din statul membru a cărui autoritate competentă a luat decizia respectivă.

(33) Procedurile de contestație constituie o măsură de protecție necesară împotriva eliminării conținutului online sau a blocării accesului la conținutul online, în mod eronat, atunci când conținutul respectiv este protejat în temeiul libertății de exprimare și de informare. Furnizorii de servicii de găzduire ar trebui, așadar, să stabilească proceduri de contestație accesibile și să se asigure că contestațiile sunt tratate cu celeritate și în deplină transparență în raport cu furnizorul de conținut. Cerința ca furnizorul de servicii de găzduire să republice conținutul care a fost eliminat în mod eronat sau să restabilească accesul care a fost blocat în mod eronat nu ar trebui să aducă atingere posibilității furnizorilor de servicii de găzduire de a aplica propriile clauze și condiții.

(34) Pentru o protecție jurisdicțională efectivă în conformitate cu articolul 19 din TUE și cu articolul 47 din Cartă, furnizorii de conținut trebuie să poată cunoaște motivele care au dus la eliminarea conținutului pe care l-au furnizat 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 care să îi permită acestuia din urmă să conteste eliminarea conținutului sau blocarea accesului la acesta. În funcție de circumstanțe, furnizorii de servicii de găzduire ar putea să înlocuiască conținutul care a fost eliminat sau la care accesul a fost blocat cu un mesaj care să indice eliminarea conținutului sau blocarea accesului la acesta în conformitate cu prezentul regulament. La cererea furnizorului de conținut, acestuia ar trebui să-i fie furnizate informații suplimentare cu privire la motivele eliminării sau blocării accesului, precum și cu privire la căile de atac împotriva eliminării sau blocării accesului. Atunci când autoritățile competente decid că, din motive de siguranță publică, inclusiv în contextul unei investigații, ar fi inoportun sau contraproductiv ca furnizorului de conținut să i se notifice direct eliminarea conținutului sau blocarea accesului la acesta, autoritățile respective ar trebui să informeze în acest sens furnizorul de servicii de găzduire.

(35) Statele membre ar trebui să desemneze autorități competente în sensul prezentului regulament. Această cerință nu ar trebui să impună constituirea unei noi autorități, iar funcțiile stabilite în prezentul regulament ar trebui să poată fi încredințate unui organism existent. Prezentul regulament ar trebui să impună desemnarea unor autorități competente pentru emiterea și pentru controlul ordinelor de eliminare, pentru supravegherea măsurilor specifice și pentru aplicarea unor sancțiuni, dar ar trebui să rămână la latitudinea fiecărui stat membru să decidă numărul autorităților competente pe care doresc să le desemneze, fie că sunt autorități administrative, autorități de aplicare a legii sau autorități judiciare. Statele membre ar trebui să garanteze îndeplinirea în mod obiectiv și nediscriminatoriu de către autoritățile competente a sarcinilor care le revin și faptul că acestea nu solicită și nu acceptă instrucțiuni de la niciun alt organism în îndeplinirea sarcinilor care le revin în temeiul prezentului regulament. Acest lucru nu ar trebui să excludă supravegherea în conformitate cu dreptul constituțional intern. Statele membre ar trebui să comunice Comisiei care sunt autoritățile competente desemnate în temeiul prezentului regulament, iar Comisia ar trebui să publice un registru online al autoritățile competente. Registrul online respectiv ar trebui să fie ușor de accesat pentru a facilita furnizorilor de servicii de găzduire verificarea rapidă a autenticității ordinelor de eliminare.

(36) Pentru a evita suprapunerea eforturilor și eventualele imixtiuni în investigații și pentru a minimiza costurile pentru furnizorii de servicii de găzduire afectați, autoritățile competente ar trebui să facă schimb de informații, să se coordoneze și să coopereze între ele și, după caz, cu Europol înainte de a emite ordine de eliminare. Atunci când decide cu privire la emiterea unui ordin de eliminare, autoritatea competentă ar trebui să țină seama în mod corespunzător de orice notificare a unei imixtiuni cu interesele investigației (deconflictualizare). Atunci când este informată de către o autoritate competentă din alt stat membru cu privire la un ordin de eliminare existent, o autoritate competentă nu ar trebui să emită un ordin de eliminare cu același obiect. În vederea punerii în aplicare a dispozițiilor prezentului regulament, Europol ar putea să ofere sprijin în conformitate cu mandatul său actual și cu cadrul juridic existent.

(37) Pentru a asigura punerea în aplicare efectivă și suficient de coerentă a măsurilor specifice luate de către furnizorii de servicii de găzduire, autoritățile competente ar trebui să se coordoneze și să coopereze între ele cu privire la schimbul de informații cu furnizorii de servicii de găzduire referitoare la ordinele de eliminare și identificarea, la punerea în aplicare și la evaluarea măsurilor specifice. Coordonarea și cooperarea se impun și în ceea ce privește alte măsuri pentru punerea în aplicare a prezentului regulament, inclusiv în ceea ce privește adoptarea normelor privind sancțiunile și aplicarea acestora. Comisia ar trebui să faciliteze coordonarea și cooperarea în cauză.

(38) Este esențial ca autoritatea competentă din statul membru responsabil de aplicarea unor sancțiuni să fie pe deplin informată cu privire la emiterea de ordine de eliminare, precum și cu privire la schimbul ulterior de informații desfășurat între furnizorul de servicii de găzduire și autoritățile competente din alte state membre. În acest scop, statele membre ar trebui să asigure canale și mecanisme de comunicare adecvate și securizate care să permită schimbul de informații relevante în timp util.

(39) Pentru a facilita schimbul rapid între autoritățile competente, precum și cu furnizorii de servicii de găzduire, și pentru a evita suprapunerea eforturilor, statele membre ar trebui să fie încurajate să utilizeze instrumentele dedicate elaborate de Europol, cum ar fi actuala aplicație de gestionare a sesizărilor privind conținuturi online sau instrumentele care îi vor succede.

(40) Sesizările emise de statele membre și de Europol s-au dovedit a fi un mijloc eficace și rapid de a sensibiliza furnizorii de servicii de găzduire cu privire la un conținut specific disponibil în cadrul serviciilor lor și de a le permite să ia măsuri rapide. Sesizările respective, care constituie un mecanism de alertare a furnizorilor de servicii de găzduire cu privire la informații care ar putea fi considerate cu caracter terorist, care îi permit furnizorului să evalueze, în mod voluntar, compatibilitatea conținutului în cauză cu propriile clauze și condiții, ar trebui să rămână disponibil în plus față de ordinele de eliminare. Decizia finală de a elimina sau nu conținutul, ca nefiind compatibil cu clauzele și condițiile sale, revine furnizorului de servicii de găzduire. Prezentul regulament nu ar trebui să aducă atingere mandatului Europol, astfel cum este prevăzut în Regulamentul (UE) 2016/794al Parlamentului European și al Consiliului[1]. Prin urmare, nicio dispoziție din prezentul regulament nu ar trebui să fie interpretată ca împiedicând statele membre și Europol să utilizeze sesizările ca instrument de prevenire a conținutului online cu caracter terorist.

[1] 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).

(41) Având în vedere consecințele deosebit de grave ale anumitor conținuturi online cu caracter terorist, furnizorii de servicii de găzduire ar trebui să informeze cu promptitudine autoritățile relevante din statul membru vizat sau autoritățile competente din statul membru în care au sediul sau au un reprezentant legal cu privire la conținutul cu caracter terorist care presupune o amenințare iminentă la adresa vieții sau o infracțiune de terorism. Pentru a asigura proporționalitatea, obligația respectivă ar trebui să se limiteze la infracțiunile de terorism, astfel cum sunt definite la articolul 3 alineatul (1) din Directiva (UE) 2017/541. Respectiva obligația de informare nu ar trebui să implice obligația furnizorilor de servicii de găzduire de a căuta în mod activ dovezi cu privire la o amenințare iminentă la adresa vieții sau o infracțiune de terorism. Statul membru vizat ar trebui să fie considerat ca fiind statul membru care are competența de a investiga și urmări penal infracțiunile de terorism respective pe baza cetățeniei infractorului sau a potențialei victime a infracțiunii sau a locației vizate de actul de terorism. În caz de îndoială, furnizorii de servicii de găzduire ar trebui să transmită informațiile către Europol, care ar trebui să ia măsurile subsecvente necesare în conformitate cu mandatul său, inclusiv să transmită informațiile respective autorităților naționale competente. Autoritățile competente ale statelor membre ar trebui să poată utiliza astfel de informații pentru a desfășura măsurile de investigare prevăzute în dreptul Uniunii sau în dreptul intern.

(42) Furnizorii de servicii de găzduire ar trebui să desemneze sau să stabilească puncte de contact pentru a facilita prelucrarea promptă a ordinelor de eliminare. Punctele de contact ar trebui să servească doar în scopuri operaționale. Punctele de contact ar trebui să dispună de orice mijloace specifice, elaborate intern sau prin externalizare, care permit depunerea electronică a ordinelor de eliminare, precum și de resurse tehnice sau umane care permit prelucrarea promptă a acestora. Punctul de contact nu este necesar să fie situat în Uniune. Furnizorul de servicii de găzduire ar trebui să aibă libertatea de a utiliza orice punct de contact existent în scopul prezentului regulament, cu condiția ca punctul de contact să fie în măsură să își exercite funcțiile prevăzute în prezentul regulament. Pentru a asigura eliminarea conținutului cu caracter terorist sau blocarea accesului la acesta în termen de o oră de la primirea ordinului de eliminare, punctul de contact al furnizorilor de servicii de găzduire care au fost expuși la conținutul cu caracter terorist ar trebui să fie accesibil în orice moment. 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 permită comunicarea într-una dintre limbile oficiale ale instituțiilor Uniunii în care sunt disponibile clauzele și condițiile lor.

(43) În absența unei obligații generale pentru furnizorii de servicii de găzduire de a asigura o prezență fizică pe teritoriul Uniunii, ar trebui să fie stabilită cu precizie sub incidența jurisdicției cărui stat membru intră furnizorul de servicii de găzduire care oferă servicii pe teritoriul Uniunii. Ca regulă generală, furnizorul de servicii de găzduire intră sub incidența jurisdicției statului membru în care își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal. Această dispoziție nu ar trebui să aducă atingere normelor privind competența care se aplică ordinelor de eliminare și deciziilor care rezultă din controlul ordinelor de eliminare în temeiul prezentului regulament. Un furnizor de servicii de găzduire care nu are niciun sediu în Uniune și care nu își desemnează un reprezentant legal ar trebui, cu toate acestea, să intre sub jurisdicția oricărui stat membru și orice stat membru ar trebui să-i poată aplica sancțiuni, cu condiția respectării principiului *ne bis in idem*.

(44) Furnizorii de servicii de găzduire care nu au sediul în Uniune ar trebui să își desemneze în scris un reprezentant legal în scopul respectării prezentului regulament și al îndeplinirii obligațiilor care le revin în temeiul acestuia. Furnizorii de servicii de găzduire ar trebui să poată desemna în sensul prezentului regulament un reprezentant legal deja desemnat în alte scopuri, cu condiția ca respectivul reprezentant legal să fie în măsură să își exercite funcțiile prevăzute în prezentul regulament. Reprezentantul legal ar trebui să fie împuternicit să acționeze în numele furnizorului de servicii de găzduire.

(45) Pentru a asigura punerea efectivă în aplicare a prezentului regulament de către furnizorii de servicii de găzduire, se impune stabilirea unui regim de sancțiuni. Statele membre ar trebui să adopte regimul de sancțiuni, care pot fi de natură administrativă sau penală, precum și, după caz, un ghid privind amenzile. Pentru nerespectarea normelor în cazuri individuale s-ar putea aplica sancțiuni, respectându-se principiul *ne bis in idem* și principiul proporționalității și asigurându-se faptul că sancțiunile respective iau în considerare neîndeplinirea sistematică a obligațiilor. Sancțiunile ar putea lua diferite forme, inclusiv avertismente formale în cazul unor încălcări minore sau sancțiuni financiare în cazul unor încălcări mai grave sau sistematice. Sancțiuni deosebit de aspre ar trebui să se aplice în cazul în care furnizorul de servicii de găzduire omite în mod sistematic sau constant să elimine conținutul cu caracter terorist sau să blocheze accesul la acesta în termen de o oră de la primirea ordinului de eliminare. Pentru a garanta securitatea juridică, prezentul regulament ar trebui să stabilească căror încălcări li se aplică sancțiuni și ce fel de circumstanțe sunt relevante pentru a evalua tipul și nivelul de gravitate al sancțiunilor respective. Atunci când se stabilește pertinența aplicării unor sancțiuni financiare, ar trebui să se țină seama în mod corespunzător de resursele financiare ale furnizorului de servicii de găzduire. În plus, autoritatea competentă ar trebui să ia în considerare dacă furnizorul de servicii de găzduire este o întreprindere nou-înființată (start-up) sau microîntreprindere ori o întreprindere din categoria întreprinderilor mici și mijlocii astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei[1]. De asemenea, ar trebui să fie luate în considerare circumstanțe suplimentare, cum ar fi dacă comportamentul furnizorului de servicii de găzduire a fost în mod obiectiv imprudent sau reprobabil sau dacă încălcarea a fost comisă din neglijență sau în mod intenționat. Statele membre ar trebui să garanteze că sancțiunile care se aplică în cazul încălcării prezentului regulament nu încurajează eliminarea materialului care nu este conținut cu caracter terorist.

[1] Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

(46) Utilizarea unor formulare standardizate facilitează cooperarea și schimbul de informații între autoritățile competente și furnizorii de servicii de găzduire, permițându-le să comunice într-un mod mai rapid și mai eficace. Este deosebit de important să se asigure luarea de măsuri prompte în urma primirii ordinelor de eliminare. Formularele reduc costurile de traducere și contribuie la asigurarea unui nivel mai ridicat de calitate al întregii acțiuni. Formularele standardizate pentru transmiterea de observații permit un schimb standardizat de informații și prezintă o importanță deosebită atunci când furnizorii de servicii de găzduire nu pot respecta ordinele de eliminare. 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.

(47) Pentru a permite modificarea promptă, atunci când este necesară, a conținutului formularelor de utilizat 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 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[1]. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(48) Statele membre ar trebui să colecteze informații privind punerea în aplicare a prezentului regulament. Statele membre ar trebui să poată utiliza rapoartele privind transparența ale furnizorilor de servicii de găzduire și să le poată completa, după caz, cu informații mai detaliate, cum ar fi propriile lor rapoarte privind transparența în temeiul prezentului regulament. Ar trebui stabilit un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament, pentru a contribui la evaluarea punerii lui în aplicare.

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

(49) 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 în termen de trei ani de la data intrării sale în vigoare. Evaluarea ar trebui să se bazeze pe următoarele criterii: eficiență, necesitate, eficacitate, proporționalitate, relevanță, coerență și valoare adăugată pentru Uniune. Evaluarea ar trebui să vizeze funcționarea diferitelor măsuri operaționale și tehnice prevăzute în prezentul regulament, inclusiv eficacitatea măsurilor de îmbunătățire a depistării, identificării și eliminării conținutului cu caracter terorist, eficacitatea mecanismelor de protecție, precum și impactul asupra drepturilor fundamentale care ar putea fi afectate, cum sunt libertatea de exprimare și de informare, inclusiv libertatea și pluralismul mass-mediei, libertatea de a desfășura o activitate comercială, dreptul la viață privată și la protecția datelor cu caracter personal. Comisia ar trebui, de asemenea, să evalueze impactul asupra intereselor părților terțe care ar putea fi afectate.

(50) Întrucât obiectivul prezentului regulament, și anume asigurarea bunei 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 sale, poate fi realizat mai bine la nivelul Uniunii, aceasta din urmă poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din TUE. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea acestui obiectiv,

ADOPTĂ PREZENTUL REGULAMENT:

SECȚIUNEA I

DISPOZIȚII GENERALE

Articolul 1

Obiect și domeniu de aplicare

(1) Prezentul regulament stabilește norme uniforme pentru a preveni utilizarea abuzivă a serviciilor de găzduire pentru diseminarea către public a conținutului online cu caracter terorist, în special în ceea ce privește:

(a) obligațiile de diligență rezonabile și proporționale care le revin furnizorilor de servicii de găzduire pentru a preveni diseminarea către public a conținutului cu caracter terorist prin intermediul serviciilor lor și pentru a asigura, atunci când este necesar, eliminarea promptă a acestuia sau blocarea promptă a accesului la acesta;

(b) măsuri pe care să le aplice statele membre, în conformitate cu dreptul Uniunii și sub rezerva unor măsuri adecvate de protecție a drepturilor fundamentale, în special libertatea de exprimare și de informare într-o societate deschisă și democratică, pentru:

(i) identificarea și asigurarea eliminării prompte a conținutului cu caracter terorist de către furnizorii de servicii de găzduire; și

(ii) facilitarea cooperării dintre autoritățile competente ale statelor membre, cu furnizorii de servicii de găzduire și, după caz, cu Europol.

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

(3) Nu este considerat conținut cu caracter terorist materialul diseminat publicului în scopuri educaționale, jurnalistice, artistice sau de cercetare ori în scopul prevenirii sau combaterii terorismului, inclusiv materialul care reprezintă exprimarea unor opinii polemice sau controversate în cursul dezbaterii publice. Scopul real al diseminării respective și dacă materialul este diseminat publicului în scopurile respective se stabilește prin intermediul unei evaluări.

(4) Prezentul regulament nu are ca efect modificarea obligației de a respecta drepturile, libertățile și principiile prevăzute la articolul 6 din TUE și se aplică fără a aduce atingere principiilor fundamentale care privesc libertatea de exprimare și de informare, inclusiv libertatea și pluralismul mass-mediei.

(5) Prezentul regulament nu aduce atingere Directivelor 2000/31/CE și 2010/13/UE. În ceea ce privește serviciile mass-media audiovizuale, astfel cum sunt definite la articolul 1 alineatul (1) litera (a) din Directiva 2010/13/UE, prevalează Directiva 2010/13/UE.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „furnizor de servicii de găzduire” înseamnă un furnizor de servicii astfel cum sunt definite la articolul 1 litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului[1] care constau în stocarea informațiilor furnizate de furnizorul conținutului la cererea acestuia ;

2. „furnizor de conținut” înseamnă un utilizator care a furnizat informații care sunt stocate sau care au fost stocate și diseminate către public de către un furnizor de servicii de găzduire;

3. „diseminare către public ” înseamnă punerea unor informații la dispoziția unui număr potențial nelimitat de persoane, la cererea unui furnizor de conținut;

4. „oferirea de servicii în Uniune” înseamnă oferirea posibilității ca persoane fizice sau juridice din unul sau mai multe state membre să utilizeze serviciile unui furnizor de servicii de găzduire care are o legătură substanțială cu statul membru sau cu statele membre în cauză ;

5. „legătură substanțială” înseamnă legătura dintre un furnizor de servicii de găzduire și unul sau mai multe state membre care rezultă fie din existența sediului furnizorului de servicii în Uniune, fie din criterii concrete specifice, precum:

[1] Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

(a) existența unui număr semnificativ de utilizatori ai serviciilor sale într-unul sau mai multe state membre; sau

(b) direcționarea activităților sale către unul sau mai multe state membre;

6. „infracțiuni de terorism” înseamnă infracțiuni în înțelesul definiției de la articolul 3 din Directiva (UE) 2017/541;

7. „conținut cu caracter terorist” înseamnă unul sau mai multe dintre următoarele tipuri de materiale, și anume:

(a) materiale care instigă la săvârșirea uneia dintre infracțiunile prevăzute la articolul 3 alineatul (1) literele (a)-(i) din Directiva (UE) 2017/541, în cazul în care astfel de materiale promovează direct sau indirect săvârșirea unor infracțiuni de terorism, cum ar fi prin glorificarea actelor teroriste, generând astfel un pericol de săvârșire a uneia sau mai multor astfel de infracțiuni;

(b) materiale care solicită unei persoane sau unui grup de persoane să săvârșească sau să contribuie la săvârșirea uneia dintre infracțiunile prevăzute la articolul 3 alineatul (1) literele (a)-(i) din Directiva (UE) 2017/541;

(c) materiale care solicită unei persoane sau unui grup de persoane să participe la activitățile unui grup terorist, în sensul articolului 4 litera (b) din Directiva (UE) 2017/541;

(d) materiale care oferă 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 sau contribuirii la săvârșirea uneia dintre infracțiunile de terorism prevăzute la articolul 3 alineatul (1) literele (a)-(i) din Directiva (UE) 2017/541;

(e) materiale care constituie o amenințare de săvârșire a uneia dintre infracțiunile prevăzute la articolul 3 alineatul (1) literele (a)-(i) din Directiva (UE) 2017/541.

8. „clauze și condiții” înseamnă toate clauzele și condițiile, indiferent de denumirea sau forma acestora, care reglementează relația contractuală dintre furnizorul de servicii de găzduire și utilizatorii serviciilor sale;

9. „sediu principal” înseamnă sediul central sau sediul social al furnizorului de servicii de găzduire în cadrul căruia se exercită principalele funcții financiare și controlul operațional.

SECȚIUNEA II

MĂSURI DE PREVENIRE A DISEMINĂRII CONȚINUTULUI ONLINE CU CARACTER TERORIST

Articolul 3

Ordine de eliminare

(1) Autoritatea competentă a fiecărui stat membru are competența de a emite un ordin de eliminare care solicită furnizorilor de servicii de găzduire să elimine conținut cu caracter terorist sau să blocheze accesul la conținutul cu caracter terorist în toate statele membre.

(2) Atunci când autoritatea competentă nu a emis anterior un ordin de eliminare către un furnizor de servicii de găzduire, aceasta îi pune la dispoziție furnizorului de servicii de găzduire respectiv informații cu privire la procedurile și termenele aplicabile, cu cel puțin 12 ore înainte de emiterea ordinului de eliminare.

Primul paragraf nu se aplică în cazurile de urgență justificate în mod corespunzător.

(3) Furnizorii de servicii de găzduire elimină conținutul cu caracter terorist sau blochează accesul la conținutul cu caracter terorist în toate statele membre în cel mai scurt timp posibil și, în orice caz, în termen de o oră de la primirea ordinului de eliminare.

(4) Autoritățile competente emit ordine de eliminare utilizând formularul prevăzut în anexa I. Ordinele de eliminare conțin următoarele elemente:

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

(b) o expunere suficient de detaliată a motivelor care să explice de ce conținutul este considerat conținut cu caracter terorist și menționarea tipurilor de materiale relevante menționate la articolul 2 punctul 7;

(c) o adresă URL (*Uniform Resource Locator*) exactă și, în cazul în care este necesar, informații suplimentare pentru identificarea conținutului cu caracter terorist;

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

(e) indicarea datei, a orei și a semnăturii electronice a autorității competente care a emis ordinul de eliminare;

(f) informații ușor de înțeles privind căile de atac de care dispune furnizorul de servicii de găzduire și furnizorul de conținut, inclusiv căile de atac în fața autorității competente, în fața unei instanțe și termenele pentru introducerea căii de atac;

(g) în cazul în care este necesar și proporțional, decizia de a nu dezvălui informațiile cu privire la eliminarea conținutului cu caracter terorist sau la blocarea accesului la acesta, în conformitate cu articolul 11 alineatul (3).

(5) Autoritatea competentă adresează ordinul de eliminare către sediul principal al furnizorului de servicii de găzduire sau către reprezentantul legal desemnat de acesta în conformitate cu articolul 17.

Autoritatea competentă transmite ordinul de eliminare către punctul de contact menționat la articolul 15 alineatul (1) prin mijloace electronice capabile să producă o înregistrare scrisă și în condiții care permit autentificarea expeditorului, inclusiv exactitatea datei și a orei la care s-a trimis și la care s-a primit ordinul.

(6) Furnizorul de servicii de găzduire informează, fără întârzieri nejustificate, autoritatea competentă, prin intermediul formularului prevăzut în anexa II, cu privire la eliminarea conținutului cu caracter terorist sau la blocarea accesului la conținutul cu caracter terorist în toate statele membre, indicând, în special, data și ora eliminării sau blocării respective.

(7) În cazul în care furnizorul de servicii de găzduire nu poate respecta ordinul de eliminare din motive de forță majoră sau dintr-o imposibilitate *de facto* care nu îi este imputabilă, inclusiv din motive tehnice sau operaționale justificate în mod obiectiv, acesta prezintă motivele respective fără întârzieri nejustificate autorității competente care a emis ordinul de eliminare, prin intermediul formularului prevăzut în anexa III.

Termenul prevăzut la alineatul (3) se aplică de îndată ce motivele menționate la primul paragraf de la prezentul alineat încetează să mai existe.

(8) Dacă furnizorul de servicii de găzduire nu poate respecta ordinul de eliminare deoarece documentul conține erori evidente sau nu conține informații suficiente pentru a permite executarea sa, acesta informează fără întârzieri nejustificate autoritatea competentă care a emis ordinul de eliminare, solicitând precizările necesare prin intermediul formularului prevăzut în anexa III.

Termenul prevăzut la alineatul (3) începe să curgă de îndată ce furnizorul de servicii de găzduire primește precizările necesare.

(9) Un ordin de eliminare devine definitiv la expirarea termenului pentru exercitarea căii de atac prevăzut de dreptul intern aplicabil, atunci când nu a fost introdusă nicio cale de atac, ori atunci când ordinul este confirmat în urma exercitării unei căi de atac.

Atunci când ordinul de eliminare devine definitiv, autoritatea competentă care a emis ordinul de eliminare informează autoritatea competentă menționată la articolul 12 alineatul (1) litera (c) din statul membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal.

Articolul 4

Procedura privind ordinele de eliminare transfrontaliere

(1) Sub rezerva articolului 3, atunci când furnizorul de servicii de găzduire nu își are sediul principal sau nu are reprezentant legal în statul membru al autorității competente care a emis ordinul de eliminare, autoritatea respectivă transmite în același timp o copie a ordinului de eliminare autorității competente din statul membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal.

(2) Atunci când un furnizor de servicii de găzduire primește un ordin de eliminare astfel cum este prevăzut în prezentul articol, acesta ia măsurile prevăzute la articolul 3 și măsurile necesare pentru a putea republica conținutul sau pentru a restabili accesul la conținutul în cauză, în conformitate cu alineatul (7) de la prezentul articol.

(3) Autoritatea competentă a statului membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal poate, din proprie inițiativă, în termen de 72 de ore de la primirea copiei ordinului de eliminare în conformitate cu alineatul (1), să efectueze controlul ordinului de eliminare pentru a stabili dacă acesta încalcă în mod grav sau evident prezentul regulament sau drepturile și libertățile fundamentale garantate de Cartă.

Atunci când constată o încălcare, respectiva autoritate competentă adoptă în același termen o decizie motivată în acest sens.

(4) Furnizorii de servicii de găzduire și furnizorii de conținut au dreptul de a transmite, în termen de 48 de ore de la primirea fie a unui ordin de eliminare, fie a informațiilor în temeiul articolului 11 alineatul (2), o cerere motivată prin care solicită autorității competente din statul membru în care furnizorul de servicii de găzduire își are sediul principal, sau în care își are reședința sau sediul reprezentantul său legal, să efectueze controlul ordinului de eliminare astfel cum este menționat la alineatul (3) primul paragraf de la prezentul articol.

În termen de 72 de ore de la primirea cererii respective, autoritatea competentă adoptă, în urma controlului ordinului de eliminare, o decizie motivată prin care constată existența sau inexistența unei încălcări.

(5) Înainte de a adopta o decizie în temeiul celui de al doilea paragraf de la alineatul (3) sau o decizie prin care constată existența unei încălcări în temeiul celui de al doilea paragraf de la alineatul (4), autoritatea competentă informează autoritatea competentă care a emis ordinul de eliminare cu privire la intenția sa de a adopta decizia și motivele deciziei sale.

(6) În cazul în care autoritatea competentă a statului membru în care furnizorul de servicii de găzduire își are sediul principal, sau în care își are reședința sau sediul reprezentantul său legal, adoptă o decizie motivată în conformitate cu alineatul (3) sau (4) de la prezentul articol, aceasta comunică de îndată decizia respectivă autorității competente care a emis ordinul de eliminare, furnizorului de servicii de găzduire, furnizorului de conținut care a solicitat efectuarea controlului în temeiul alineatului (4) de la prezentul articol și, în conformitate cu articolul 14, Europolului. Atunci când prin decizie se constată o încălcare în temeiul alineatului (3) sau (4) de la prezentul articol, ordinul de eliminare încetează să mai producă efecte juridice.

(7) La primirea deciziei prin care se constată o încălcare, care i-a fost comunicată în conformitate cu alineatul (6), furnizorul de servicii de găzduire în cauză republică imediat conținutul sau restabilește accesul la acesta, fără a aduce atingere posibilității de a-și pune în aplicare clauzele și condițiile în conformitate cu dreptul Uniunii și cu dreptul intern.

Articolul 5

Măsuri specifice

(1) Un furnizor de servicii de găzduire expus la conținut cu caracter terorist astfel cum se menționează la alineatul (4), include în clauzele și condițiile sale și, după caz, aplică prevederi care previn utilizarea abuzivă a serviciilor sale pentru diseminarea conținutului cu caracter terorist către public.

Acesta acționează în mod diligent, proporțional și nediscriminatoriu, luând în considerare în mod corespunzător și în toate împrejurările drepturile fundamentale ale utilizatorilor, și ținând cont, în special, de importanța fundamentală a libertății de exprimare și de informare într-o societate deschisă și democratică, pentru a evita eliminarea materialelor care nu reprezintă conținut cu caracter terorist.

(2) Un furnizor de servicii de găzduire expus la conținut cu caracter terorist astfel cum se menționează la alineatul (4), ia măsuri specifice pentru a își proteja serviciile împotriva diseminării conținutului cu caracter terorist către public.

Decizia cu privire la alegerea măsurilor specifice rămâne la latitudinea furnizorului de servicii de găzduire. Măsurile specifice respective pot include una sau mai multe dintre următoarele:

(a) măsuri sau capacități tehnice sau operaționale adecvate, cum ar fi personal sau mijloace tehnice adecvate de identificare și de eliminare sau blocare promptă a accesului la conținutul cu caracter terorist;

(b) mecanisme ușor accesibile și ușor de utilizat pentru ca utilizatorii să raporteze sau să semnaleze furnizorului de servicii de găzduire un presupus conținut cu caracter terorist;

(c) alte mecanisme pentru o mai bună sensibilizare cu privire la conținutul cu caracter terorist în cadrul serviciilor sale, cum ar fi mecanismele de moderare a utilizatorilor;

(d) orice altă măsură pe care furnizorul de servicii de găzduire o consideră adecvată pentru a preveni disponibilitatea unui conținut cu caracter terorist în cadrul serviciilor sale.

(3) Măsurile specifice îndeplinesc toate cerințele următoare:

(a) sunt eficace în atenuarea nivelului de expunere al serviciilor furnizorului de servicii de găzduire la conținut cu caracter terorist;

(b) sunt orientate și proporționale, ținând seama, în special, de gravitatea nivelului de expunere al serviciilor furnizorului de servicii de găzduire la conținutul cu caracter terorist, precum și de capacitățile tehnice și operaționale, de capacitatea financiară, de numărul de utilizatori ai furnizorului de servicii de găzduire și de volumul de conținut pe care îl furnizează;

(c) sunt aplicate astfel încât să se țină seama pe deplin de drepturile și interesele legitime ale utilizatorilor, în special de drepturile fundamentale ale utilizatorilor privind libertatea de exprimare și de informare, respectarea vieții private și protecția datelor cu caracter personal;

(d) sunt aplicate în mod diligent și nediscriminatoriu.

Atunci când măsurile specifice implică utilizarea unor măsuri tehnice, se oferă garanții adecvate și eficace, în special prin intermediul supravegherii și al verificării umane, pentru a se asigura acuratețea și pentru a se evita eliminarea materialului care nu reprezintă conținut cu caracter terorist.

(4) Un furnizor de servicii de găzduire este expus la conținut cu caracter terorist atunci când autoritatea competentă a statului membru în care își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal:

(a) a luat o decizie, pe baza unor factori obiectivi, cum ar fi faptul că furnizorul de servicii de găzduire a primit două sau mai multe ordine definitive de eliminare în ultimele 12 luni, prin care constată că furnizorul de servicii de găzduire este expus la conținut cu caracter terorist; și

(b) a notificat furnizorului de servicii de găzduire decizia menționată la litera (a).

(5) După primirea deciziei menționate la alineatul (4) sau la alineatul (6), după caz, furnizorul de servicii de găzduire raportează autorității competente cu privire la măsurile specifice pe care le-a luat și pe care intenționează să le ia pentru a respecta alineatele (2) și (3). Furnizorul de servicii de găzduire raportează în termen de trei luni de la primirea deciziei și, ulterior, anual. Obligația de a raporta încetează de îndată ce autoritatea competentă a decis, în urma unei cereri formulate în temeiul alineatului (7), că furnizorul de servicii de găzduire nu mai este expus la conținut cu caracter terorist.

(6) Atunci când, pe baza rapoartelor menționate la alineatul (5) și a oricăror alți factori obiectivi, după caz, autoritatea competentă consideră că măsurile specifice luate nu respectă alineatele (2) și (3), aceasta adresează furnizorului de servicii de găzduire o decizie prin care îi solicită să ia măsurile necesare pentru a asigura respectarea alineatelor (2) și (3).

Alegerea tipului de măsuri specifice care trebuie să fie luate rămâne la latitudinea furnizorului de servicii de găzduire.

(7) Un furnizor de servicii de găzduire poate, în orice moment, să solicite autorității competente să reexamineze și, după caz, să modifice sau să revoce decizia menționată la alineatul (4) sau (6).

În termen de trei luni de la primirea cererii, autoritatea competentă adoptă o decizie motivată, pe baza unor factori obiectivi cu privire la cerere, și notifică decizia respectivă furnizorului de servicii de găzduire.

(8) Nicio cerință de a lua măsuri specifice nu aduce atingere articolului 15 alineatul (1) din Directiva 2000/31/CE și nu impune furnizorilor de servicii de găzduire o obligație generală de a supraveghere a informațiile pe care le transmit sau le stochează și nici o obligație generală de a căuta în mod activ fapte sau circumstanțe care indică o activitate ilegală.

Nicio cerință de a lua măsuri specifice nu impune furnizorului de servicii de găzduire obligația de a utiliza instrumente automatizate.

Articolul 6

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, sau a unor măsuri specifice în temeiul articolului 3 sau 5, precum și datele conexe eliminate ca urmare a eliminării conținutului cu caracter terorist, care sunt necesare în vederea:

(a) unor proceduri de control jurisdicțional administrativ sau judecătoresc, de soluționare a contestațiilor în temeiul articolului 10 împotriva unei decizii de a elimina conținutul cu caracter terorist și datele conexe sau de a bloca accesul la acestea; sau

(b) prevenirii, depistării, investigării și urmăririi penale a infracțiunilor de terorism.

(2) Conținutul cu caracter terorist și datele conexe menționate la alineatul (1) se păstrează timp de șase luni de la eliminare sau blocare. La cererea autorității sau a instanței competente, conținutul cu caracter terorist se păstrează pentru o durată suplimentară determinată numai dacă și atât timp cât acest lucru este necesar pentru procedurile de control jurisdicțional administrativ sau judecătoresc menționate la alineatul (1) litera (a) aflate în desfășurare.

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

Respectivele măsuri de protecție tehnice și organizatorice asigură faptul că accesul la conținutul cu caracter terorist și la datele conexe păstrate și prelucrarea acestora au loc 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 protecție atunci când este necesar.

SECȚIUNEA III

MĂSURI DE PROTECȚIE ȘI RĂSPUNDEREA

Articolul 7

Obligații în materie de transparență

care revin furnizorilor de servicii de găzduire

(1) Furnizorii de servicii de găzduire prezintă clar, în clauzele și condițiile lor, politica lor de prevenire a diseminării conținutului cu caracter terorist, inclusiv, după caz, o explicație pertinentă cu privire la funcționarea măsurilor specifice, inclusiv, după caz, la utilizarea unor instrumente automatizate.

(2) Un furnizor de servicii de găzduire care a luat măsuri de prevenire a diseminării conținutului cu caracter terorist sau a fost obligat să ia măsuri în temeiul prezentului regulament într-un anumit an calendaristic publică un raport privind transparența acțiunilor întreprinse în anul respectiv. Furnizorul de servicii de găzduire publică raportul respectiv până la data de 1 martie a anului următor.

(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 identificarea și eliminarea sau blocarea accesului la conținut cu caracter terorist;

(b) informații referitoare la măsurile luate de furnizorul de servicii de găzduire pentru a preveni reapariția materialului online care a fost eliminat sau la care accesul a fost blocat deoarece a fost considerat ca fiind conținut cu caracter terorist, în special atunci când au fost utilizate instrumente automatizate;

(c) numărul de elemente de conținut cu caracter terorist care au fost eliminate sau la care accesul a fost blocat ca urmare a unor ordine de eliminare sau a unor măsuri specifice și numărul de ordine de eliminare în urma cărora conținutul nu a fost eliminat sau accesul la acesta nu a fost blocat în temeiul articolului 3 alineatul (7) primul paragraf și al articolului 3 alineatul (8) primul paragraf, precum și motivele pentru aceasta;

(d) numărul și rezultatul contestațiilor prelucrate de furnizorul de servicii de găzduire în conformitate cu articolul 10;

(e) numărul și rezultatul procedurilor de control jurisdicțional administrativ sau judecătoresc inițiate de furnizorul de servicii de găzduire;

(f) numărul de cazuri în care furnizorul de servicii de găzduire a fost obligat să republice sau să redea accesul la conținut ca rezultat al unor proceduri de control jurisdicțional administrativ sau judecătoresc ;

(g) numărul de cazuri în care furnizorul de servicii de găzduire a republicat sau a redat accesul la conținut în urma unei contestații din partea furnizorului de conținut.

Articolul 8

Rapoartele privind transparența ale autorităților competente

(1) Autoritățile competente publică rapoarte anuale privind transparența referitoare la activitățile desfășurate în temeiul prezentului regulament. Rapoartele respective conțin cel puțin următoarele informații referitoare la anul calendaristic dat:

(a) numărul de ordine de eliminare emise în temeiul articolului 3, numărul de ordine de eliminare care intră sub incidența articolului 4 alineatul (1), numărul de ordine de eliminare care au făcut obiectul controlului în temeiul articolului 4, precum și informațiile privind modul în care furnizorii de servicii de găzduire în cauză au pus în aplicare ordinele de eliminare respective, inclusiv numărul de cazuri în care conținutul cu caracter terorist a fost eliminat sau accesul la acesta a fost blocat și numărul de cazuri în care conținutul cu caracter terorist nu a fost eliminat sau accesul la acesta nu a fost blocat;

(b) numărul de decizii luate în conformitate cu articolul 5 alineatul (4), (6) sau (7) și informațiile privind modul în care furnizorii de servicii de găzduire au pus în aplicare deciziile respective, inclusiv o descriere a măsurilor specifice;

(c) numărul de cazuri în care ordinele de eliminare și deciziile luate în conformitate cu articolul 5 alineatele (4) și (6) au făcut obiectul unor proceduri de control jurisdicțional administrativ sau judecătoresc și informațiile privind rezultatul procedurilor relevante;

(d) numărul de decizii prin care s-au aplicat sancțiuni în temeiul articolului 18, și o descriere a tipului de sancțiune aplicată.

(2) Rapoartele anuale privind transparența menționate la alineatul (1) nu conțin informații care ar putea afecta activitățile în curs vizând prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor de terorism sau în scopuri legate de interesele de siguranță națională.

Articolul 9

Căi de atac

(1) Furnizorii de servicii de găzduire care au primit un ordin de eliminare emis în temeiul articolului 3 alineatul (1) sau o decizie în temeiul articolului 4 alineatul (4) sau al articolului 5 alineatul (4), (6) sau (7) au dreptul la o cale de atac efectivă. Acest drept include dreptul de a contesta un asemenea ordin de eliminare în fața instanțelor statului membru al autorității competente care a emis ordinul de eliminare sau dreptul de a contesta decizia în temeiul articolului 4 alineatul (4) sau al articolului 5 alineatul (4), (6) sau (7) în fața instanțelor statului membru al autorității competente care a adoptat decizia respectivă .

(2) Furnizorii de conținut al căror conținut a fost eliminat sau la care accesul a fost blocat ca urmare a unui ordin de eliminare au dreptul la o cale de atac efectivă. Acest drept include dreptul de a contesta ordinul de eliminare emis în temeiul articolului 3 alineatul (1) în fața instanțelor statului membru al autorității competente care a emis respectivul ordin de eliminare și dreptul de a contesta decizia adoptată în temeiul articolului 4 alineatul (4) în fața instanțelor statului membru al autorității competente care a adoptat decizia respectivă.

(3) Statele membre stabilesc proceduri eficace pentru exercitarea drepturilor prevăzute în prezentul articol.

Articolul 10

Mecanisme de prezentare a contestațiilor

(1) Furnizorii de servicii de găzduire stabilesc un mecanism eficace și accesibil care să le permită furnizorilor de conținut al căror conținut a fost eliminat sau la care accesul a fost blocat ca urmare a unor măsuri specifice luate în temeiul articolului 5 să conteste eliminarea sau blocarea accesului la conținutul respectiv și să solicite republicarea conținutului eliminat sau la care accesul a fost blocat.

(2) Fiecare furnizor de servicii de găzduire analizează prompt toate contestațiile primite prin intermediul mecanismului menționat la alineatul (1) și republică conținutul sau deblochează accesul la acesta, fără întârzieri nejustificate, atunci când eliminarea conținutului sau blocarea accesului la acesta a fost nejustificată. Furnizorul de servicii de găzduire informează autorul contestației cu privire la rezultatul contestației, în termen de două săptămâni de la primirea acesteia.

Atunci când contestația este respinsă, furnizorul de servicii de găzduire comunică autorului contestației motivele care stau la baza deciziei sale.

Republicarea conținutului sau deblocarea accesului la acesta nu împiedică exercitarea unor proceduri de control jurisdicțional administrativ sau judecătoresc împotriva deciziei furnizorului de servicii de găzduire sau a autorității competente.

Articolul 11

Informarea furnizorilor de conținut

(1) Atunci când un furnizor de servicii de găzduire a eliminat sau a blocat accesul la un conținut cu caracter terorist, acesta informează furnizorul de conținut cu privire la o astfel de eliminare sau blocare.

(2) La cererea furnizorului de conținut, furnizorul de servicii de găzduire îi comunică acestuia motivele eliminării sau ale blocării accesului și dreptul de contestare a ordinului de eliminare sau îi furnizează acestuia o copie a ordinului de eliminare.

(3) Obligația în temeiul alineatelor (1) și (2) nu se aplică atunci când autoritatea competentă care a emis ordinul de eliminare decide că este necesar și proporțional să nu fie dezvăluite niciun fel de informații din motive de siguranță publică, cum ar fi prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor de terorism, atât timp cât este necesar, dar nu mai mult de șase săptămâni de la data deciziei respective. În acest caz, furnizorul de servicii de găzduire nu dezvăluie nicio informație privind eliminarea conținutului cu caracter terorist sau blocarea accesului la acesta.

Respectiva autoritate competentă poate prelungi perioada menționată cu încă șase săptămâni, în cazul în care există în continuare motive pentru o astfel de nedivulgare.

SECȚIUNEA IV

AUTORITĂȚI COMPETENTE ȘI COOPERARE

Articolul 12

Desemnarea autorităților competente

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

(a) a emite ordine de eliminare în temeiul articolului 3;

(b) a efectua controlul ordinelor de eliminare în temeiul articolului 4;

(c) a supraveghea punerea în aplicare a măsurilor specifice în temeiul articolului 5;

(d) a aplica sancțiuni în temeiul articolului 18.

(2) Fiecare stat membru se asigură că în cadrul autorității competente menționate la alineatul 1 litera (a) este desemnat sau stabilit un punct de contact care să soluționeze cererile de clarificare și observațiile cu privire la ordinele de eliminare pe care le emite respectiva autoritate competentă.

Statele membre se asigură că informațiile referitoare la punctul de contact sunt puse la dispoziția publicului.

(3) Până la … [12 *luni de la intrarea în vigoare a prezentului regulament*], statele membre îi notifică Comisiei autoritatea sau autoritățile competente menționate la alineatul (1) și eventualele schimbări referitoare la acestea. Comisia publică această notificare și eventualele schimbări referitoare la acestea în *Jurnalul Oficial al Uniunii Europene*.

(4) Până la … [*12 luni de la intrarea în vigoare a prezentului regulament*], Comisia întocmește un registru online în care sunt înscrise toate autoritățile competente menționate la alineatul (1) și punctul de contact desemnat sau stabilit în temeiul alineatului (2) de fiecare autoritate competentă. Comisia publică periodic eventualele schimbări referitoare la acestea.

Articolul 13

Autoritățile competente

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

(2) Statele membre se asigură că autoritățile lor competente își exercită sarcinile care le revin în temeiul prezentului regulament în mod obiectiv, nediscriminatoriu și cu respectarea deplină a drepturilor fundamentale. Autoritățile competente nu solicită și nu acceptă instrucțiuni de la niciun alt organism în legătură cu îndeplinirea sarcinilor care le revin în temeiul articolului 12 alineatul (1).

Primul paragraf de la prezentul alineat nu exclude supravegherea în conformitate cu dreptul constituțional intern.

Articolul 14

Cooperarea dintre furnizorii de servicii de găzduire,
autoritățile competente și Europol

(1) Autoritățile competente fac schimb de informații, se coordonează și cooperează între ele și, după caz, cu Europolul, în ceea ce privește ordinele de eliminare, în special în scopul de a evita suprapunerea eforturilor, de a spori coordonarea și de a evita interferențele cu investigațiile din diferitele state membre.

(2) Autoritățile competente din statele membre fac schimb de informații, se coordonează și cooperează cu autoritățile competente menționate la articolul 12 alineatul (1) literele (c) și (d) în ceea ce privește măsurile specifice luate în temeiul articolului 5 și sancțiunile aplicate în temeiul articolului 18. Statele membre se asigură că autoritățile competente menționate la articolul 12 alineatul (1) literele (c) și (d) dețin toate informațiile relevante.

(3) În sensul alineatului (1), statele membre stabilesc canale sau mecanisme de comunicare adecvate și sigure care să asigure schimbul de informații relevante în timp util.

(4) Pentru punerea în aplicare eficace a prezentului regulament, precum și pentru a se evita suprapunerea eforturilor, statele membre și furnizorii de servicii de găzduire pot să utilizeze instrumente specifice, inclusiv cele stabilite de Europol, pentru a facilita în special:

(a) prelucrarea ordinelor de eliminare și observațiile privind acestea în temeiul articolului 3; și

(b) cooperarea în vederea identificării și punerii în aplicare a măsurilor specifice în temeiul articolului 5.

(5) Atunci când furnizorii de servicii de găzduire iau cunoștință de conținut cu caracter terorist care implică o amenințare iminentă la adresa vieții, aceștia informează prompt autoritățile competente să investigheze și să urmărească penal infracțiunile din statele membre vizate. În cazul în care este imposibilă identificarea statelor membre vizate, furnizorii de servicii de găzduire informează punctul de contact în temeiul articolului 12 alineatul (2) din statul membru în care au sediul principal sau în care își are reședința sau sediul reprezentantul lor legal și transmit informațiile privind conținutul cu caracter terorist către Europol, în vederea luării unor măsuri corespunzătoare.

(6) Autoritățile competente sunt încurajate să transmită către Europol copii ale ordinelor de eliminare, pentru a-i permite acestuia să prezinte un raport anual care să conțină o analiză a tipurilor de conținut cu caracter terorist care fac obiectul unui ordin de eliminare sau de blocare a accesului în temeiul prezentului regulament.

Articolul 15

Puncte de contact ale furnizorilor de servicii de găzduire

(1) Fiecare furnizor de servicii de găzduire desemnează sau stabilește un punct de contact care primește ordinele de eliminare prin mijloace electronice și asigură prelucrarea promptă a acestora în temeiul articolelor 3 și 4. Furnizorul de servicii de găzduire se asigură că informațiile referitoare la punctul de contact sunt făcute publice.

(2) În informațiile menționate la alineatul (1) de la prezentul articol se precizează limbile oficiale ale instituțiilor Uniunii, astfel cum sunt menționate în Regulamentul 1/58[1], în care se poate desfășura comunicarea cu punctul de contact și în care are loc corespondența ulterioară privind ordinele de eliminare în temeiul articolului 3. Printre limbile respective 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.

[1] Regulamentul nr. 1 de stabilire a regimului lingvistic al Comunității Economice Europene (JO 17, 6.10.1958, p. 385).

SECȚIUNEA V

PUNERE ÎN APLICARE ȘI EXECUTARE

Articolul 16

Competență

(1) Statul membru în care se află sediul principal al furnizorului de servicii de găzduire este competent în sensul articolelor 5, 18 și 21. Competența cu privire la un furnizor de servicii de găzduire al cărui sediu principal nu se află în Uniune revine statului membru în care își are reședința sau sediul reprezentantul său legal.

(2) Atunci când un furnizor de servicii de găzduire care nu își are sediul principal în Uniune nu își desemnează un reprezentant legal, sunt competente toate statele membre.

(3) Atunci când o autoritate competentă dintr-un stat membru își exercită competența în temeiul alineatului (2), acesta informează autoritățile competente din toate celelalte state membre.

Articolul 17

Reprezentantul legal

(1) Un furnizor de servicii de găzduire care nu are un sediu principal 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 și a deciziilor emise de autoritățile competente.

(2) Furnizorul de servicii de găzduire îi conferă reprezentantului său legal competențele și resursele necesare pentru a îndeplini ordinele de eliminare și deciziile respective și pentru a coopera cu autoritățile competente.

Reprezentantul legal își are reședința sau sediul într-unul din statele membre în care furnizorul de servicii de găzduire își oferă serviciile.

(3) Reprezentantul legal poate fi considerat răspunzător pentru încălcarea prezentului regulament, fără a se aduce atingere răspunderii furnizorului de servicii de găzduire sau acțiunilor în justiție împotriva acestuia.

(4) Furnizorul de servicii de găzduire notifică desemnarea reprezentantului său legal autorității competente menționate la articolul 12 alineatul (1) litera (d) din statul membru în care își are reședința sau sediul reprezentantul legal.

Furnizorul de servicii de găzduire pune la dispoziția publicului informațiile referitoare la reprezentantul său legal.

SECȚIUNEA VI

DISPOZIȚII FINALE

Articolul 18

Sancțiuni

(1) Statele membre stabilesc regimul sancțiunilor care se aplică în cazul încălcării prezentului regulament de către furnizorii de servicii de găzduire și iau toate măsurile necesare pentru a asigura aplicarea acestora. Sancțiunile respective se limitează la încălcarea articolului 3 alineatele (3) și (6), a articolului 4 alineatele (2) și (7), a articolului 5 alineatele (1), (2), (3), (5) și (6), a articolelor 6, 7, 10 și 11, a articolului 14 alineatul (5), a articolului 15 alineatul (1) și a articolului 17.

Sancțiunile menționate la primul paragraf sunt efective, proporționale și disuasive. Statele membre notifică normele și măsurile respective Comisiei până la … [12 luni de la data intrării în vigoare a prezentului regulament], și îi comunică acesteia, fără întârziere, orice modificare ulterioară a acestora.

(2) Statele membre se asigură că autoritățile competente, atunci când decid dacă să aplice o sancțiune, precum și atunci când stabilesc tipul și nivelul de gravitate ale sancțiunii, țin cont de toate circumstanțele relevante, inclusiv de:

(a) natura, gravitatea și durata încălcării;

(b) dacă încălcarea a fost comisă cu intenție sau din neglijență;

(c) încălcările anterioare comise de furnizorul de servicii de găzduire;

(d) capacitatea financiară a furnizorului de servicii de găzduire ;

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

(f) natura și dimensiunea furnizorului de servicii de găzduire , în special dacă acesta constituie o microîntreprindere sau o întreprindere mică sau mijlocie;

(g) gradul de vinovăție a furnizorului de servicii de găzduire , ținând seama de măsurile tehnice și organizatorice luate de acesta pentru a se conforma prezentului regulament.

(3) Statele membre se asigură că pentru nerespectarea sistematică sau continuă a obligațiilor în temeiul articolului 3 alineatul (3) se aplică sancțiuni financiare de până la 4 % din cifra de afaceri globală a furnizorului de servicii de găzduire corespunzătoare precedentului exercițiu financiar.

Articolul 19

Cerințe tehnice și modificarea anexelor

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

(2) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 20 pentru a modifica anexele, cu scopul de a aborda efectiv eventuala necesitate de îmbunătățire a conținutului formularelor aferente ordinelor de eliminare și pentru furnizarea de informații cu privire la imposibilitatea de a executa ordinele de eliminare.

Articolul 20

Exercitarea delegării

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

(2) Competența de a adopta acte delegate menționată la articolul 19 se conferă Comisiei pe o perioadă nedeterminată de la … [un an de la data intrării în vigoare a prezentului regulament].

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

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

(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 în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul 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 intră sub jurisdicția lor informații privind măsurile pe care le-au luat în conformitate cu prezentul regulament în anul calendaristic precedent și le trimit Comisiei anual până la data de 31 martie. Informațiile respective cuprind:

(a) numărul de ordine de eliminare emise și numărul de elemente de conținut cu caracter terorist care au fost eliminate sau la care accesul a fost blocat, precum și promptitudinea eliminării sau blocării acestora;

(b) măsurile specifice luate în temeiul articolului 5, inclusiv informații privind numărul de elemente de conținut cu caracter terorist care au fost eliminate sau la care accesul a fost blocat, precum și promptitudinea eliminării sau blocării acestora;

(c) numărul de solicitări de acces emise de autoritățile naționale competente cu privire la conținutul păstrat de furnizorii de servicii de găzduire în temeiul articolului 6;

(d) numărul procedurilor de contestație inițiate și măsurile luate de furnizorii de servicii de găzduire în temeiul articolului 10;

(e) numărul procedurilor de control jurisdicțional administrativ sau judecătoresc și deciziile luate de autoritatea competentă în conformitate cu dreptul intern.

(2) Până la … [doi ani de la data intrării în vigoare a prezentului regulament], Comisia stabilește un program detaliat de monitorizare a performanțelor, a rezultatelor și a impactului prezentului regulament. Programul de monitorizare stabilește indicatorii și mijloacele care trebuie să fie utilizate și intervalele pentru colectarea de date și de alte dovezi necesare. Programul precizează 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 la ... [doi ani de la data intrării în vigoare a prezentului regulament], Comisia prezintă Parlamentului European și Consiliului un raport privind aplicarea prezentului regulament. Raportul respectiv conține informații privind monitorizarea în temeiul articolului 21 și informațiile care rezultă din obligațiile în materie de transparență în temeiul articolului 8. Statele membre furnizează Comisiei informațiile necesare pentru elaborarea raportului respectiv.

Articolul 23

Evaluare

Până la … [trei ani de la data intrării în vigoare a prezentului regulament], Comisia efectuează o evaluare a prezentului regulament și prezintă Parlamentului European și Consiliului un raport referitor la aplicarea acestuia, care include:

(a) funcționarea și eficacitatea mecanismelor de protecție, în special a celor prevăzute la articolul 4 alineatul (4), la articolul 6 alineatul (3) și la articolele 7-11;

(b) impactul pe care îl are prezentul regulament asupra drepturilor fundamentale, în special asupra libertății de exprimare și de informare, respectării vieții private și protecției datelor cu caracter personal; și

(c) contribuția prezentului regulament la protecția siguranței publice.

Dacă este cazul, raportul este însoțit de propuneri legislative.

Statele membre furnizează Comisiei informațiile necesare pentru elaborarea raportului respectiv.

Comisia evaluează, de asemenea, necesitatea și fezabilitatea înființării unei platforme europene cu privire la conținutul cu caracter terorist online, pentru a facilita comunicarea și cooperarea în temeiul prezentului regulament.

Articolul 24

Intrarea în vigoare și aplicarea

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

Acesta se aplică de la ... [12 luni de la data intrării în vigoare a prezentului regulament].

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

Adoptat la …,

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*

ANEXA I

ORDIN DE ELIMINARE [articolul 3 din Regulamentul (UE) 2021/…

al Parlamentului European și al Consiliului[+]]

În temeiul articolului 3 din Regulamentul (UE) 2021/…[++] (denumit în continuare „regulamentul”), destinatarul prezentului ordin de eliminare trebuie să elimine conținutul cu caracter terorist sau să blocheze accesul la conținutul cu caracter terorist în toate statele membre în cel mai scurt timp și, în orice caz, în termen de o oră de la primirea ordinului de eliminare.

În temeiul articolului 6 din regulament, 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 accesul a fost blocat.

În temeiul articolului 15 alineatul (2) din regulament, ordinul de eliminare se transmite într-una din limbile desemnate de destinatar.

[+] JO: a se introduce numărul regulamentului din documentul ST 14308/20 [2018/0331 (COD)] și a se introduce numărul, data, titlul și referința JO aferente în nota de subsol corespunzătoare.

[++] JO: a se introduce numărul regulamentului din documentul ST 14308/20 [2018/0331 (COD)].

SECȚIUNEA A:

Statul membru al autorității competente emitente:

……..……...

NB: detaliile despre autoritatea competentă emitentă care sunt indicate în secțiunile E și F

Destinatarul și, după caz, reprezentantul legal:

……..……..……..

Punctul de contact:

……..……...

Statul membru în care își are sediul principal furnizorul de servicii de găzduire sau în care își are reședința sau sediul reprezentantul său legal:

……..……..…..

Data și ora emiterii ordinului de eliminare:

……..……..……..

Numărul de referință al ordinului de eliminare:

……..……..……..

SECȚIUNEA B: Conținutul cu caracter terorist care trebuie eliminat sau la care accesul trebuie blocat în toate statele membre în cel mai scurt timp și, în orice caz, în termen de o oră:

Adresa URL și informații suplimentare care permit identificarea și locația precisă a conținutului cu caracter terorist:

……

Motivele pentru care materialul este considerat drept conținut cu caracter terorist în conformitate cu articolul 2 punctul 7 din regulament.

Materialul [a se bifa rubrica (rubricile) corespunzătoare]:

□ instigă alte persoane la săvârșirea unor infracțiuni de terorism, de exemplu prin glorificarea actelor de terorism, prin apologia săvârșirii unor astfel de infracțiuni [articolul 2 punctul 7 litera (a) din regulament]

□ solicită altor persoane să săvârşească, sau să contribuie la săvârşirea, unor infracțiuni de terorism [articolul 2 punctul 7 litera (b) din regulament]

□ solicită altor persoane să participe la activitățile unui grup terorist [articolul 2 punctul 7 litera (c) din regulament]

□ oferă 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 sau contribuirii la săvârșirea unor infracțiuni de terorism [articolul 2 punctul 7 litera (d) din regulament]

□ constituie o amenințare de a săvârși o infracțiune de terorism [articolul 2 punctul 7 litera (e) din Regulament].

Informații suplimentare pentru care materialul este considerat drept conținut cu caracter terorist:

……

……

……

SECȚIUNEA C: Informarea furnizorului de conținut

Vă rugăm să rețineți că (a se bifa rubrica, după caz):

□ din motive de siguranță publică, destinatarul trebuie să se abțină de a informa furnizorul de conținut al cărui conținut cu caracter terorist este eliminat sau la care accesul a fost blocat.

Dacă rubrica nu este pertinentă, a se vedea secțiunea G pentru informațiile privind posibilitățile de a contesta ordinul de eliminare în statul membru al autorității competente emitente în temeiul dreptului intern (o copie a ordinului de eliminare poate fi transmisă, la cerere, furnizorului de conținut).

SECȚIUNEA D: Informarea autorității competente a statului membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal

A se bifa rubrica (rubricile) corespunzătoare

□ Statul membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal este diferit de statul membru al autorității competente emitente:

□ O copie a ordinului de eliminare se transmite autorității competente a statului membru în care furnizorul de servicii de găzduire își are sediul principal sau în care își are reședința sau sediul reprezentantul său legal

SECȚIUNEA E: Date de contact ale autorității competente emitente

Tipul (a se bifa rubrica corespunzătoare):

□ judecător, instanță judecătorească sau judecător de instrucție

□ autoritate de aplicare a legii

□ altă autoritate competentă→ vă rugăm să completați și secțiunea F

Date de contact ale autorității competente emitente sau ale reprezentatului acesteia care atestă exactitatea și corectitudinea ordinului de eliminare:

Denumirea autorității emitente competente:
……..……..…

Numele reprezentantului său, funcția (titlul și gradul):
……..……..……

Numărul dosarului:….……..……..…….….

Adresa:….……..……..……...……..…

Numărul de telefon: (prefixul țării) (prefixul regiunii/localității) ……..….

Fax: (prefixul țării) (prefixul regiunii/localității) …….

Adresa de e-mail: …….....……..…….…….

Data: ……..……

Ștampila oficială (dacă există) și semnătura : ……...…..…

SECȚIUNEA F: Date de contact pentru acțiuni subsecvente

Datele de contact ale autorității competente emitente pentru transmiterea observațiilor privind momentul eliminării sau al blocării accesului sau pentru obținerea unor clarificări suplimentare:

……..…….

Date de contact ale autorității competente din statul membru în care își are sediul principal furnizorul de servicii de găzduire sau în care își are reședința sau sediul reprezentantul său legal:

……..…….

SECȚIUNEA G: Informații privind controlul jurisdicțional

Informații privind organismul sau instanța competentă, termenele și procedurile de contestare a ordinului de eliminare:

Organismul sau instanța competentă în fața căreia se poate contesta ordinul de eliminare:

…….…….

Termenul pentru contestarea ordinului de eliminare:

[zile/luni începând de la]

…….……..

Trimitere la dispozițiile de drept intern:

……...…….

ANEXA II

FORMULAR PENTRU TRANSMITEREA DE OBSERVAȚII
ÎN URMA ELIMINĂRII CONȚINUTULUI CU CARACTER TERORIST
SAU A BLOCĂRII ACCESULUI LA ACESTA
[articolul 3 alineatul (6) din Regulamentul (UE) 2021/…
al Parlamentului European și al Consiliului+]

SECȚIUNEA A:

Destinatarul ordinului de eliminare:

……..……..……..

Autoritatea competentă care a emis ordinul de eliminare:

……..……..…...

Numărul de referință al dosarului autorității competente care a emis ordinul de eliminare:

……..……....

Numărul de referință al dosarului destinatarului:

……..……..…..

Data și ora primirii ordinului de eliminare:

……..……..……..

+ JO: a se introduce în text numărul regulamentului din documentul ST 14308/20 [2018/0331 (COD)] și a se introduce numărul, data, titlul și referința JO aferente regulamentului respectiv în nota de subsol.

SECȚIUNEA B:

Măsurile luate în conformitate cu ordinul de eliminare

(a se bifa rubrica corespunzătoare):

□ conținutul cu caracter terorist a fost eliminat

□ conținutul cu caracter terorist a fost blocat în toate statele membre

Ora și data măsurii luate:

…….

SECȚIUNEA C: Datele de contact ale destinatarului

Denumirea/numele furnizorului de servicii de găzduire

……..……..……..

SAU

Denumirea/numele reprezentantului legal al furnizorului de servicii de găzduire:

……..……..…..

Statul membru în care se află sediul principal al furnizorului de servicii de găzduire:

……..……..…..

SAU

Statul membru în care își are reședința sau sediul reprezentantul legal al furnizorului de servicii de găzduire:

……..……..…..

Numele persoanei autorizate:

……..……...

Adresa de e-mail al punctului de contact:

…….

Data:

……..……..

ANEXA III

INFORMAȚII PRIVIND IMPOSIBILITATEA
DE A EXECUTA ORDINUL DE ELIMINARE
[articolul 3 alineatele (7) și (8) din Regulamentul (UE) 2021/…
al Parlamentului European și al Consiliului[+]]

SECȚIUNEA A:

Destinatarul ordinului de eliminare:

……..……....

Autoritatea competentă care a emis ordinul de eliminare:

……..……...

Numărul de referință al dosarului autorității competente care a emis ordinul de eliminare:

……..……...

Numărul de referință al dosarului destinatarului:

……..……..

Data și ora primirii ordinului de eliminare:

……..……..

[+] JO: a se introduce în text numărul regulamentului din documentul ST 14308/20 [2018/0331 (COD)] și a se introduce numărul, data, titlul și referința JO aferente regulamentului respectiv în nota de subsol.

SECȚIUNEA B: Neexecutare

1. Ordinul de eliminare nu poate fi executat în termen din următorul (următoarele) motiv(e) [a se bifa rubrica (rubricile) corespunzătoare]:

   □ caz de forță majoră sau imposibilitate de facto imputabile destinatarului sau furnizorului de servicii, inclusiv din motive tehnice sau operaționale justificabile în mod obiectiv

   □ ordinul de eliminare conține erori evidente

   □ ordinul de eliminare nu conține suficiente informații

2. Vă rugăm să furnizați informații suplimentare cu privire la motivele neexecutării:

……...

3. Dacă ordinul de eliminare conține erori evidente și/sau nu conține informații suficiente, vă rugăm să precizați erorile și informațiile sau clarificările suplimentare care sunt necesare:

……

SECȚIUNEA C: Datele de contact ale furnizorului de servicii de găzduire sau ale reprezentantului său legal

Denumirea/numele furnizorului de servicii de găzduire:

……..……....

SAU

Denumirea/numele reprezentantului legal al furnizorului de servicii de găzduire:

……..……..……..

Numele persoanei autorizate:

……..……..……..

Date de contact (adresa de e-mail):

……..……..……..

Semnătura:

……..……..……..

Data și ora:

……..……..…..