RECOMANDĂRI

RECOMANDAREA (UE) 2018/334 A COMISIEI

din 1 martie 2018

privind măsuri de combatere eficace a conținutului ilegal online

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 292,

întrucât:

(1) Internetul și furnizorii de servicii care își desfășoară activitatea pe internet contribuie în mod semnificativ la inovare, creștere economică și crearea de locuri de muncă în Uniune. Mulți dintre acești furnizori de servicii joacă un rol esențial în economia digitală, creând legături între întreprinderi și cetățeni și facilitând dezbaterea publică, precum și difuzarea și primirea de informații factuale, de idei și opinii. În anumite cazuri însă, serviciile lor sunt utilizate în mod abuziv de către terți pentru a desfășura activități ilegale online, de exemplu pentru a difuza informații legate de terorism, pentru abuzul sexual asupra minorilor, pentru a publica discursuri ilegale de incitare la ură sau pentru a încălca normele de protecție a consumatorilor, activități care pot submina încrederea utilizatorilor și care pot prejudicia modelele lor de afaceri. În anumite cazuri, furnizorii de servicii în cauză ar putea chiar obține unele avantaje ca urmare a unor astfel de activități, de exemplu ca urmare a punerii la dispoziție a unor conținuturi protejate prin drepturi de autor fără o autorizare din partea titularilor drepturilor respective.

(2) Prezența conținutului ilegal online are consecințe negative grave pentru utilizatori, pentru cetățenii afectați și întreprinderile afectate, precum și pentru societate în general. Ținând cont de rolul lor central și de mijloacele și capacitățile tehnologice asociate serviciilor pe care le furnizează, furnizorii de servicii online au responsabilități societale specifice de a contribui la combaterea conținutului ilegal difuzat prin utilizarea serviciilor lor.

(3) Având în vedere că eliminarea rapidă a conținutului ilegal sau blocarea rapidă a accesului la acesta este adesea esențială pentru a limita extinderea difuzării sale și a prejudiciilor cauzate, aceste responsabilități implică, printre altele, ca furnizorii de servicii în cauză să fie în măsură să ia decizii prompte cu privire la acțiunile posibile legate de conținutul ilegal online. Furnizorii de servicii ar trebui, de asemenea, să aibă responsabilitatea de a institui garanții eficace și adecvate, în special pentru a se asigura faptul că aceștia acționează cu diligență și în mod proporțional și pentru a se preveni eliminarea neintenționată a conținutului care nu este ilegal.

(4) Mulți dintre furnizorii de servicii online au recunoscut și și-au asumat aceste responsabilități. La nivel colectiv, s-au făcut progrese importante prin încheierea unor acorduri voluntare de diverse tipuri, printre care se numără Forumul UE pentru internet privind conținutul online cu caracter terorist, Codul de conduită privind combaterea discursurilor ilegale de incitare la ură din mediul online și Memorandumul de înțelegere privind vânzarea mărfurilor contrafăcute. Însă, în pofida acestor angajamente și progrese, conținutul ilegal online rămâne o problemă gravă la nivelul Uniunii.

(5) Îngrijorat de seria de atacuri teroriste comise în UE și de proliferarea propagandei teroriste online, Consiliul European din 22-23 iunie 2017 a declarat că „așteaptă din partea industriei de sector […] să dezvolte tehnologii și instrumente noi care să îmbunătățească detectarea automată și eliminarea conținutului care incită la acte teroriste.” Parlamentul European, în Rezoluția sa din 15 iunie 2017, a îndemnat respectivele platforme online „să adopte măsuri mai stricte pentru a combate conținutul ilegal și dăunător”. Miniștrii din statele membre, în cadrul Forumului UE pentru internet, au reiterat apelul adresat întreprinderilor de a adopta o abordare mai proactivă în ceea ce privește protejarea utilizatorilor de conținutul cu caracter terorist. În ceea ce privește drepturile de proprietate intelectuală, în Concluziile sale din 4 decembrie 2014 privind asigurarea respectării acestor drepturi, Consiliul a invitat Comisia să analizeze posibilitatea de a utiliza instrumentele disponibile pentru a identifica autorii încălcărilor drepturilor de proprietate intelectuală și rolul intermediarilor în sprijinirea luptei împotriva încălcării drepturilor de proprietate intelectuală.

(6) La 28 septembrie 2017, Comisia a adoptat o Comunicare conținând orientări referitoare la responsabilitățile furnizorilor de servicii online cu privire la conținutul ilegal online ([1]). În comunicarea respectivă, Comisia a explicat că va analiza dacă sunt necesare măsuri suplimentare, printre altele prin monitorizarea progreselor pe baza unor acorduri voluntare. Prezenta recomandare se înscrie în continuarea comunicării respective, reflectând nivelul ambiției stabilit în aceasta și punându-l în aplicare, ținând cont totodată de progresele importante înregistrate datorită acordurilor voluntare menționate și valorificându-le.

(7) Prezenta recomandare recunoaște că ar trebui să se țină seama în mod corespunzător de particularitățile combaterii diferitelor tipuri de conținut ilegal online, precum și de acțiunile caracteristice care ar putea fi necesare ca răspuns la această problemă, care pot include adoptarea de măsuri legislative specifice. Spre exemplu, recunoscând necesitatea unor astfel de măsuri legislative specifice, la 25 mai 2016 Comisia a adoptat o Propunere de modificare a Directivei 2010/13/UE a Parlamentului European și a Consiliului ([2]) având în vedere evoluția realităților pieței. La 14 septembrie 2016, Comisia a adoptat, de asemenea, o Propunere de directivă privind dreptul de autor pe piața unică digitală ([3]), care prevede obligația anumitor furnizori de servicii de a lua, în cooperare cu titularii de drepturi, măsuri pentru a asigura funcționarea acordurilor încheiate cu titularii de drepturi pentru utilizarea operelor lor sau a altor obiecte protejate sau pentru a împiedica punerea la dispoziție, prin intermediul serviciilor lor, a operelor sau a altor obiecte protejate identificate de către titularii de drepturi în cadrul cooperării cu furnizorii de servicii. Prezenta recomandare nu aduce atingere acestor măsuri și propuneri legislative.

(8) Directiva 2000/31/CE a Parlamentului European și a Consiliului ([4]) prevede derogări în materie de răspundere de care pot beneficia, în anumite condiții, unii furnizori de servicii online, printre care și furnizorii de servicii de găzduire în sensul articolului 14. Pentru a putea beneficia de respectiva derogare în materie de răspundere, furnizorii de servicii de găzduire trebuie să acționeze prompt pentru a elimina informațiile ilicite pe care le stochează sau pentru a bloca accesul la acestea, de îndată ce iau cunoștință de acestea și, în ceea ce privește acțiunile în daune, de îndată ce iau cunoștință de fapte sau circumstanțe din care să rezulte că activitatea sau informația este vădit ilicită. Furnizorii respectivi pot lua cunoștință de aceste informații, fapte sau circumstanțe, printre altele, prin notificările care le sunt transmise. Directiva 2000/31/CE constituie, așadar, baza elaborării unor proceduri prin care să se elimine informațiile ilicite și să se blocheze accesul la acestea. Directiva menționată prevede, de asemenea, posibilitatea ca statele membre să impună furnizorilor de servicii în cauză să respecte o obligație de diligență cu privire la conținutul ilegal pe care l-ar putea stoca.

(9) Atunci când adoptă măsuri legate de conținutul ilegal online, statele membre trebuie să respecte principiul țării de origine prevăzut în Directiva 2000/31/CE. În consecință, statele membre nu pot, din motive care țin de domeniul coordonat, astfel cum este specificat în directiva menționată, să restrângă libertatea de a furniza servicii ale societății informaționale de către furnizori stabiliți în alt stat membru, sub rezerva însă a aplicării unor derogări în anumite condiții stabilite în directiva respectivă.

(10) În plus, mai multe alte instrumente legislative ale Uniunii prevăd un cadru juridic pentru anumite tipuri de conținut ilegal care sunt disponibile online și difuzate în acest mediu. Mai precis, Directiva 2011/93/UE a Parlamentului European și a Consiliului ([5]) impune statelor membre să ia măsuri pentru eliminarea paginilor web care conțin sau difuzează pornografie infantilă și le permite să blocheze accesul la astfel de pagini web, sub rezerva anumitor garanții. Directiva (UE) 2017/541 a Parlamentului European și a Consiliului ([6]), care trebuie să fie transpusă în legislația națională până la 8 septembrie 2018, conține dispoziții similare în ceea ce privește conținutul online care constituie o instigare publică la săvârșirea unei infracțiuni de terorism. De asemenea, Directiva (UE) 2017/541 stabilește norme minime privind definiția infracțiunilor în domeniul infracțiunilor de terorism, al infracțiunilor legate de un grup terorist și al infracțiunilor legate de activități de terorism. În temeiul

([1]) COM(2017) 555 final din 28 septembrie 2017.

([2]) Directivei 2010/13/UE a Parlamentului European și a Consiliului din 10 martie 2010 privind coordonarea anumitor dispoziții stabilite prin acte cu putere de lege sau acte administrative în cadrul statelor membre cu privire la furnizarea de servicii mass-media audiovizuale având în vedere evoluția realităților pieței (Directiva serviciilor mass-media audiovizuale) (JO L 95, 15.4.2010, p. 1). COM(2016) 287 final.

([3]) COM(2016) 593 final din 14 septembrie 2016.

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

([5]) Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

([6]) 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).

Directivei 2004/48/CE a Parlamentului European și a Consiliului ([1]), autoritățile judiciare competente au posibilitatea de a emite ordine judecătorești împotriva intermediarilor ale căror servicii sunt utilizate de către un terț pentru a încălca un drept de proprietate intelectuală.

(11) În special în acest context, pe lângă măsurile voluntare luate de anumiți furnizori de servicii online, unele state membre au adoptat norme privind mecanismele de „notificare și acțiune" în intervalul scurs de la adoptarea Directivei 2000/31/CE. Alte state membre analizează, la rândul lor, posibilitatea de a adopta astfel de norme. Mecanismele respective urmăresc în general să faciliteze notificarea conținutului pe care partea care efectuează notificarea îl consideră ilegal către furnizorul de servicii de găzduire în cauză („notificare"). În urma primirii notificării, furnizorul poate decide dacă este de acord sau nu cu această evaluare și dacă dorește să elimine conținutul sau să blocheze accesul la acesta („acțiune"). Există diferențe din ce în ce mai mari între normele naționale din acest domeniu. În consecință, furnizorii de servicii în cauză pot fi supuși mai multor cerințe legale cu conținuturi și domenii de aplicare divergente.

(12) În interesul pieței interne și al combaterii eficace a conținutului ilegal online, precum și pentru a proteja abordarea echilibrată pe care urmărește să o asigure Directiva 2000/31/CE, este necesar să se stabilească anumite principii de bază care să ghideze activitățile statelor membre și ale furnizorilor de servicii în cauză în această privință.

(13) Aceste principii ar trebui stabilite și aplicate cu respectarea deplină a drepturilor fundamentale protejate în ordinea juridică a Uniunii, în special a celor garantate în Carta drepturilor fundamentale a Uniunii Europene („carta"). Combaterea conținutului ilegal online ar trebui însoțită de aplicarea unor garanții adecvate și solide, care să asigure protecția diferitelor drepturi fundamentale vizate ale tuturor părților implicate. Printre aceste drepturi se numără, după caz, libertatea de exprimare, inclusiv libertatea de a primi și de a comunica informații, dreptul la respectarea vieții private a unei persoane și la protecția datelor cu caracter personal, precum și dreptul la protecția judiciară efectivă a utilizatorilor serviciilor respective. Aceste drepturi pot include, de asemenea, libertatea de a desfășura o activitate economică, inclusiv libertatea contractuală, a furnizorilor de servicii de găzduire, drepturile copilului și drepturile la protecția proprietății, inclusiv a proprietății intelectuale, precum și drepturile la demnitate umană și la nediscriminare ale altor părți afectate. În special, deciziile luate de furnizorii de servicii de găzduire de a elimina sau a bloca accesul la conținutul pe care îl stochează ar trebui să țină seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale utilizatorilor lor, precum și de rolul central pe care tind să îl aibă acești furnizori în ceea ce privește facilitarea dezbaterii publice și difuzarea și primirea de fapte, opinii și idei în conformitate cu legea.

(14) În concordanță cu abordarea orizontală care stă la baza derogării în materie de răspundere prevăzute la articolul 14 din Directiva 2000/31/CE, prezenta recomandare ar trebui să se aplice oricărui tip de conținut care nu este conform cu legislația Uniunii sau cu legislațiile statelor membre, indiferent de obiectul sau natura exactă a instrumentelor legislative respective. Este suficient să se ia în considerare legislațiile statelor membre care sunt vizate de furnizarea de servicii în discuție, și anume legislațiile statelor membre pe al căror teritoriu este stabilit furnizorul de servicii de găzduire sau pe al căror teritoriu sunt furnizate serviciile. În plus, la punerea în aplicare a prezentei recomandări ar trebui să se țină cont în mod corespunzător de gravitatea conținutului ilegal și de orice tip de prejudiciu potențial cauzat de acesta, care poate fi strâns corelat cu promptitudinea eventualelor acțiuni întreprinse, precum și de ce anume poate fi așteptat în mod rezonabil de la furnizorii de servicii de găzduire, având în vedere, dacă este cazul, stadiul de dezvoltare și folosirea posibilă a tehnologiilor. Ar trebui să se țină cont în mod corespunzător și de diferențele relevante care ar putea exista între diferitele tipuri de conținut ilegal și acțiunile care ar trebui întreprinse pentru a le combate.

(15) Furnizorii de servicii de găzduire joacă un rol deosebit de important în combaterea conținutului ilegal online, întrucât aceștia stochează informațiile transmise de utilizatorii lor, la cererea acestora, și oferă altor utilizatori acces la informațiile respective, deseori pe scară largă. Prin urmare, prezenta recomandare se referă în principal la activitățile și responsabilitățile acestor furnizori. Cu toate acestea, atunci când este cazul, recomandările formulate pot fi aplicate, *mutatis mutandis*, și în cazul altor furnizori de servicii online afectați. Având în vedere că obiectivul prezentei recomandări este de a aborda riscurile legate de conținutul ilegal online care afectează consumatorii din Uniune, aceasta se referă la activitățile tuturor furnizorilor de servicii de găzduire, indiferent dacă sunt stabiliți în Uniune sau într-o țară terță, cu condiția ca aceștia să își orienteze activitățile către consumatori cu reședința în Uniune.

(16) Un mijloc important de combatere a conținutului ilegal online îl constituie mecanismele prin care furnizorilor de servicii de găzduire li se transmit notificări privind conținutul care este considerat conținut ilegal. Astfel de mecanisme ar trebui să faciliteze transmiterea de notificări de către toate persoanele sau entitățile care doresc să

([1]) Directiva 2004/48/CE a Parlamentului European și a Consiliului din 29 aprilie 2004 privind respectarea drepturilor de proprietate intelectuală (JO L 157, 30.4.2004, p. 45).

facă acest lucru. Prin urmare, aceste mecanisme ar trebui să fie ușor de accesat și de folosit de către toți utilizatorii. Cu toate acestea, furnizorii de servicii de găzduire ar trebui să beneficieze de o anumită flexibilitate, de exemplu în ceea ce privește formatul de raportare sau tehnologia care urmează să fie utilizată, pentru a permite aplicarea unor soluții eficiente și a se evita impunerea unor sarcini disproporționate acestor furnizori.

(17) În conformitate cu jurisprudența Curții de Justiție referitoare la articolul 14 din Directiva 2000/31/CE, notificările ar trebui să fie suficient de precise și argumentate în mod corespunzător, astfel încât să permită furnizorului de servicii de găzduire care le primește să ia o decizie avizată și cu toată diligența necesară în ceea ce privește acțiunile care trebuie întreprinse pentru a da curs notificărilor. Prin urmare, ar trebui să se asigure cât mai mult posibil respectarea criteriilor menționate mai sus. Cu toate acestea, măsura în care, în urma primirii unei anumite notificări, furnizorul de servicii de găzduire ia cunoștință de informații, fapte sau circumstanțe în sensul articolului 14 din directiva menționată ar trebui să fie evaluată în funcție de particularitățile fiecărui caz în parte, având în vedere că informațiile, faptele sau circumstanțele de care se ia astfel cunoștință pot fi aflate și în alte moduri decât prin notificări.

(18) În general, cunoașterea datelor de contact ale autorului notificării nu este necesară pentru ca furnizorul de servicii de găzduire să poată lua o decizie avizată și cu toată diligența necesară cu privire la acțiunile care ar trebui întreprinse ca urmare a notificării primite. Condiționarea transmiterii unei notificări de comunicarea datelor de contact ar constitui un obstacol în calea notificării. Cu toate acestea, includerea datelor de contact este necesară pentru ca furnizorul de servicii de găzduire să poată oferi un răspuns. Autorul notificării ar trebui, așadar, să aibă posibilitatea, dar nu și obligația de a-și comunica datele de contact.

(19) Pentru a se îmbunătăți transparența și precizia mecanismelor de notificare și acțiune și a permite contestarea deciziilor luate, dacă este cazul, furnizorii de servicii de găzduire, atunci când dispun de datele de contact ale autorilor notificărilor și/sau ale furnizorilor conținutului, ar trebui să informeze în timp util și în mod corespunzător aceste persoane cu privire la măsurile luate în contextul mecanismelor menționate, în special cu privire la deciziile lor referitoare la cererea de eliminare a conținutului în cauză sau de blocare a accesului la acesta. Informațiile care urmează să fie comunicate ar trebui să fie proporționale, în sensul că acestea ar trebui să corespundă afirmațiilor făcute de persoanele în cauză în notificările sau contranotificările lor, permițând totodată adoptarea unor soluții adecvate și diferențiate, fără a impune furnizorilor o sarcină excesivă.

(20) Pentru a se asigura transparența și echitatea și a se evita eliminarea neintenționată a conținutului care nu este conținut ilegal, furnizorii de conținut ar trebui, în principiu, să fie informați cu privire la decizia de a elimina sau a bloca accesul la conținutul stocat la cererea lor și ar trebui să li se ofere posibilitatea de a contesta decizia printr-o contranotificare, în vederea anulării deciziei respective, atunci când este cazul, indiferent dacă decizia a fost luată pe baza unei notificări sau a unei semnalări ori ca urmare a unor măsuri proactive luate de către furnizorul de servicii de găzduire.

(21) Cu toate acestea, având în vedere natura conținutului în cauză, scopul unei astfel de proceduri de contranotificare și sarcina suplimentară pe care aceasta o implică pentru furnizorii de servicii de găzduire, atunci când conținutul în cauză este în mod evident ilegal și se referă la infracțiuni grave care implică o amenințare la adresa vieții sau a siguranței persoanelor, cum ar fi infracțiunile specificate în Directiva (UE) 2017/541 și în Directiva 2011/93/UE, nu se justifică recomandarea de a comunica astfel de informații despre decizia respectivă și posibilitatea de a contesta decizia. În plus, în anumite cazuri, din motive de ordine publică și de siguranță publică, în special din motive legate de prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor, poate fi justificat ca informațiile respective să nu fie comunicate direct furnizorilor de conținut în cauză. Prin urmare, furnizorii de servicii de găzduire nu ar trebui să comunice aceste informații atunci când o autoritate competentă a formulat o cerere în acest sens bazată pe motive de ordine publică și siguranță publică, pentru întreaga perioadă solicitată de autoritatea respectivă în lumina acestor motive. În măsura în care acest lucru implică o limitare a dreptului de a fi informat în legătură cu prelucrarea datelor cu caracter personal, ar trebui să se respecte condițiile relevante prevăzute în Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([1]).

(22) Mecanismele de notificare și acțiune nu ar trebui să aducă atingere în niciun fel drepturilor părților implicate de a iniția proceduri judiciare, în conformitate cu legislația aplicabilă, cu privire la orice conținut care este considerat conținut ilegal sau orice măsuri luate în această privință de către furnizorii de servicii de găzduire. Mecanismele de soluționare alternativă a litigiilor care pot apărea în acest context pot oferi un instrument complementar important pe lângă procedurile judiciare, în special în cazul în care acestea permit soluționarea eficace, rapidă și la un cost accesibil a litigiilor respective. Soluționarea alternativă a litigiilor ar trebui, așadar, să fie încurajată, cu condiția ca mecanismele relevante să îndeplinească anumite standarde, în special în ceea ce privește echitatea procedurală, ca accesul părților la justiție să nu fie afectat și ca abuzurile să fie evitate.

([1]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

(23) Pentru a se evalua mai bine eficacitatea mecanismelor de notificare și acțiune și a altor activități ale furnizorilor de servicii de găzduire în ceea ce privește conținutul considerat conținut ilegal și pentru a se asigura tragerea lor la răspundere, ar trebui să existe transparență față de publicul larg. Furnizorii de servicii de găzduire ar trebui, prin urmare, să publice periodic rapoarte referitoare la aceste mecanisme și alte activități, care ar trebui să fie suficient de complete și detaliate pentru a permite o înțelegere adecvată. Aceștia ar trebui, de asemenea, să indice *ex ante* cu claritate, în condițiile de utilizare a serviciilor, care sunt politicile lor privind eliminarea oricărui conținut pe care îl stochează, inclusiv conținutul ilegal, sau privind blocarea accesului la acesta.

(24) Pe lângă mecanismele de notificare și acțiune, măsurile proactive proporționale și specifice luate în mod voluntar de către furnizorii de servicii de găzduire, inclusiv prin utilizarea de mijloace automatizate în anumite cazuri, pot fi, de asemenea, un element important în combaterea conținutului ilegal online, fără a se aduce atingere articolului 15 alineatul (1) din Directiva 2000/31/CE. În cazul acestor măsuri proactive, ar trebui să se țină seama de situația furnizorilor de servicii de găzduire care, date fiind dimensiunile și anvergura activității lor, dispun de resurse și competențe de specialitate limitate, precum și de necesitatea ca astfel de măsuri să fie însoțite de garanții eficace și adecvate.

(25) Luarea unor astfel de măsuri proactive poate fi oportună în special atunci când a fost deja stabilit caracterul ilegal al conținutului sau când tipul de conținut nu necesită neapărat contextualizarea. De asemenea, oportunitatea luării unor astfel de măsuri poate depinde de următoarele aspecte: natura, amploarea și scopul măsurilor preconizate, tipul de conținut în cauză, dacă notificarea conținutului a fost efectuată de către autorități de aplicare a legii sau de către Europol, dacă s-au întreprins deja acțiuni cu privire la conținutul în cauză deoarece este considerat conținut ilegal. În cazul materialelor privind abuzuri sexuale asupra copiilor în special, furnizorii de servicii de găzduire ar trebui să ia măsuri proactive pentru a depista și a împiedica difuzarea unor asemenea materiale, în concordanță cu angajamentele asumate în cadrul Alianței mondiale împotriva abuzurilor sexuale asupra copiilor pe internet.

(26) În acest context, în Comunicarea sa din 28 septembrie 2017 privind combaterea conținutului ilegal online, Comisia a precizat că, în opinia sa, luarea unor astfel de măsuri voluntare proactive nu conduce automat la pierderea de către furnizorul de servicii de găzduire a beneficiului derogării în materie de răspundere prevăzute la articolul 14 din Directiva 2000/31/CE.

(27) Este esențial ca orice măsură de combatere a conținutului ilegal online să facă obiectul unor garanții eficace și adecvate, menite să asigure faptul că furnizorii de servicii de găzduire acționează cu diligență și în mod proporțional atunci când își stabilesc și aplică politicile legate de conținutul pe care îl stochează, inclusiv conținutul ilegal, astfel încât să se asigure în special că utilizatorii pot primi și comunica în mod liber informații online în conformitate cu legislația aplicabilă. Pe lângă eventualele garanții prevăzute în legislația aplicabilă, de exemplu în ceea ce privește protecția datelor cu caracter personal, ar trebui să se prevadă garanții speciale, și anume supravegherea și efectuarea de verificări de către o persoană, care să se aplice, dacă este cazul, în legătură cu utilizarea mijloacelor automatizate, astfel încât să se evite eventualele decizii neintenționate și eronate.

(28) Ar trebui să se asigure o cooperare eficientă, eficace și adecvată între autoritățile competente și furnizorii de servicii de găzduire în ceea ce privește combaterea conținutului ilegal online. Această cooperare ar putea beneficia de asistența Europolului atunci când este cazul, de exemplu cu scopul de a combate terorismul, abuzurile sexuale asupra copiilor și exploatarea sexuală a acestora, pornografia infantilă și ademenirea copiilor în scopuri sexuale. Pentru facilitarea acestei cooperări, statele membre și furnizorii de servicii de găzduire ar trebui să desemneze puncte de contact și ar trebui stabilite proceduri pentru prelucrarea notificărilor transmise de aceste autorități cu prioritate și cu un grad adecvat de încredere în ceea ce privește exactitatea acestora, ținând seama de competențele și responsabilitățile speciale ale autorităților respective. Pentru a combate în mod eficace anumite infracțiuni deosebit de grave, cum ar fi infracțiunile specificate în Directiva (UE) 2017/541 și în Directiva 2011/93/UE, care ar putea intra în atenția furnizorilor de servicii de găzduire în cursul desfășurării activității lor, statele membre ar trebui să fie încurajate să recurgă la posibilitatea prevăzută la articolul 15 alineatul (2) din Directiva 2000/31/CE de a institui obligații juridice de raportare, în conformitate cu legislația aplicabilă, în special cu Regulamentul (UE) 2016/679.

(29) Pe lângă autoritățile competente, anumite persoane sau entități, inclusiv organizații neguvernamentale și organisme profesionale, ar putea avea, la rândul lor, competențe de specialitate relevante și ar putea dori să își asume, în mod voluntar, anumite responsabilități legate de combaterea conținutului ilegal online. Având în vedere valoarea lor adăugată și uneori numărul mare de notificări implicate, cooperarea dintre astfel de notificatori de încredere și furnizorii de servicii de găzduire ar trebui să fie încurajată, în special prin tratarea cu prioritate și cu un grad adecvat de încredere în ceea ce privește exactitatea acestora și a notificărilor transmise de astfel de

persoane sau entități. Cu toate acestea, având în vedere statutul lor special, cooperarea ar trebui să fie deschisă exclusiv persoanelor și entităților care respectă valorile pe care se întemeiază Uniunea, astfel cum sunt prevăzute la articolul 2 din Tratatul privind Uniunea Europeană, și care îndeplinesc anumite condiții adecvate, care ar trebui, de asemenea, să fie clare și obiective și să fie făcute publice.

(30) Combaterea conținutului ilegal online necesită o abordare cuprinzătoare, dat fiind că, deseori, acest conținut migrează ușor de la un furnizor de servicii de găzduire la altul și tinde să exploateze verigile cele mai slabe ale lanțului. Cooperarea este, așadar, esențială și ar trebui să constea în special în schimbul voluntar de experiență, soluții tehnologice și cele mai bune practici. Această cooperare este deosebit de importantă în cazul furnizorilor de servicii de găzduire care, date fiind dimensiunile și anvergura activității lor, dispun de resurse și competențe de specialitate limitate.

(31) Terorismul presupune utilizarea ilegală și fără discernământ a violenței și a intimidării împotriva cetățenilor. Teroriștii se bazează din ce în ce mai mult pe internet pentru a difuza propagandă teroristă, utilizând frecvent metode sofisticate pentru a asigura o difuzare rapidă și amplă a acestor conținuturi. Deși s-au făcut progrese, în special în cadrul Forumului UE pentru internet, este în continuare urgent să se combată mai rapid și mai eficace conținutul online cu caracter terorist, iar furnizorii de servicii de găzduire care participă la Forumul UE pentru internet trebuie să își îndeplinească integral angajamentele asumate cu privire la raportarea efectivă și cuprinzătoare.

(32) Având în vedere particularitățile legate de combaterea conținutului online cu caracter terorist, recomandările referitoare la combaterea conținutului ilegal în general ar trebui să fie completate cu anumite recomandări legate specific de combaterea conținutului online cu caracter terorist, care să se bazeze pe eforturile întreprinse în cadrul Forumului UE pentru internet și să le consolideze.

(33) Având în vedere riscurile deosebit de grave asociate conținutului cu caracter terorist și rolul central al furnizorilor de servicii de găzduire în difuzarea acestui conținut, aceștia ar trebui să ia toate măsurile rezonabile pentru a nu permite difuzarea conținutului cu caracter terorist și, dacă este posibil, să împiedice găzduirea acestuia, sub rezerva posibilității lor de a stabili și de a asigura respectarea condițiilor de utilizare a serviciilor lor și a necesității prevederii unor garanții eficace și adecvate și fără a se aduce atingere articolului 14 din Directiva 2000/31/CE.

(34) Măsurile respective ar trebui să constea în special în cooperarea cu autoritățile competente și cu Europol în ceea ce privește semnalările, care sunt un mijloc specific de notificare a furnizorilor de servicii de găzduire, adaptat la particularitățile combaterii conținutului cu caracter terorist. Atunci când transmit semnalări, autoritățile competente și Europol ar trebui să poată solicita eliminarea conținutului pe care îl consideră conținut cu caracter terorist sau blocarea accesului la acesta, fie în temeiul legilor aplicabile relevante, fie al condițiilor de utilizare stabilite de furnizorul de servicii de găzduire în cauză. Aceste mecanisme de semnalare ar trebui să existe în plus față de mecanismele de transmitere a notificărilor, inclusiv de către notificatorii de încredere, care pot fi utilizate și pentru notificarea conținutului considerat conținut cu caracter terorist.

(35) Având în vedere că acest conținut cu caracter terorist este de obicei cel mai dăunător în prima oră de la apariția sa online și date fiind competențele și responsabilitățile specifice ale autorităților competente și ale Europol, ca regulă generală, semnalările ar trebui să fie evaluate și, dacă este cazul, ar trebui să se ia măsuri în privința lor în decurs de o oră.

(36) Măsurile de combatere a conținutului cu caracter terorist ar trebui să constea, de asemenea, în măsuri proactive proporționale și specifice, inclusiv prin utilizarea de mijloace automatizate, pentru a depista, a identifica și a elimina prompt conținutul cu caracter terorist sau a bloca accesul la acesta și a se asigura că respectivul conținut cu caracter terorist nu reapare, fără a se aduce atingere articolului 15 alineatul (1) din Directiva 2000/31/CE. În această privință, este necesar ca astfel de măsuri să fie însoțite de garanții adecvate și eficace, în special cele recomandate în capitolul II din prezenta recomandare.

(37) Cooperarea, atât între furnizorii de servicii de găzduire, cât și între aceștia și autoritățile competente este extrem de importantă atunci când se urmărește combaterea conținutului online cu caracter terorist. În special, instrumentele tehnologice care permit detectarea automată a conținutului, cum ar fi Baza de date a valorilor hash, pot contribui la realizarea obiectivului de a împiedica difuzarea conținutului cu caracter terorist între diferitele servicii de găzduire. Această cooperare, precum și dezvoltarea, utilizarea și schimbul de astfel de instrumente tehnologice ar trebui încurajate, recurgându-se la competențele de specialitate ale Europol, dacă este cazul. Aceste eforturi de cooperare sunt deosebit de importante pentru a le oferi mijloace suplimentare de acțiune furnizorilor de servicii de găzduire care, date fiind dimensiunile și anvergura activității lor, dispun de resurse și competențe de specialitate limitate pentru a reacționa de urgență și în mod eficace la semnalări și a lua măsuri proactive conform recomandărilor.

(38) Un număr cât mai mare de furnizori relevanți de servicii de găzduire ar trebui să participe la aceste eforturi de cooperare și toți furnizorii de servicii de găzduire participanți ar trebui să contribuie la optimizarea și maximizarea utilizării instrumentelor respective. Încheierea de acorduri de lucru între toate părțile relevante, inclusiv, dacă este cazul, cu Europol ar trebui, de asemenea, să fie încurajată, dat fiind că astfel de acorduri pot contribui la asigurarea unei abordări coerente și eficace și pot permite schimbul de experiență și cunoștințe de specialitate relevante.

(39) Pentru a se asigura respectarea dreptului fundamental la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și libera circulație a acestor date, prelucrarea datelor cu caracter personal în contextul tuturor măsurilor luate pentru punerea în aplicare a prezentei recomandări ar trebui să fie conformă pe deplin cu normele privind protecția datelor, în special cu Regulamentul (UE) 2016/679 și cu Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([1]), și ar trebui să fie monitorizată de autoritățile de supraveghere competente.

(40) Prezenta recomandare respectă drepturile fundamentale și principiile recunoscute în special în cartă. Prezenta recomandare urmărește mai ales să asigure respectarea deplină a articolelor 1, 7, 8, 10, 11, 16, 17, 21, 24 și 47 din cartă.

(41) Comisia intenționează să monitorizeze îndeaproape toate acțiunile întreprinse ca răspuns la prezenta recomandare. Statele membre și furnizorii de servicii de găzduire ar trebui, prin urmare, să fie pregătiți să comunice Comisiei, la solicitarea acesteia, toate informațiile relevante despre care se poate preconiza în mod rezonabil că vor trebui să le comunice pentru a permite această monitorizare. Pe baza informațiilor obținute astfel, precum și a tuturor celorlalte informații disponibile, inclusiv a celor raportate în temeiul diverselor acorduri voluntare, Comisia va evalua acțiunile întreprinse pentru a da curs prezentei recomandări și va stabili dacă sunt necesare măsuri suplimentare, inclusiv propunerea unor instrumente legislative cu caracter obligatoriu ale Uniunii. Având în vedere particularitățile și urgența combaterii conținutului online cu caracter terorist, monitorizarea și evaluarea respective ar trebui să se efectueze pe baza unor informații detaliate și foarte rapid, în termen de trei luni de la data publicării prezentei recomandări, în timp ce pentru alte tipuri de conținut ilegal este oportun ca acestea să se efectueze în termen de șase luni de la data publicării,

ADOPTĂ PREZENTA RECOMANDARE:

CAPITOLUL I

Scop și termeni utilizați

1. Statele membre și furnizorii de servicii de găzduire, în ceea ce privește conținutul furnizat de furnizorii de conținut pe care îl stochează la solicitarea respectivilor furnizori de conținut, sunt încurajați să ia măsuri eficace, adecvate și proporționale pentru a combate conținutul ilegal online, în conformitate cu principiile descrise în prezenta recomandare și în deplină conformitate cu Carta drepturilor fundamentale, în special cu dreptul la libertatea de exprimare și de informare, precum și cu alte dispoziții aplicabile din legislația Uniunii, mai ales cele referitoare la protecția datelor cu caracter personal, la aspectele de concurență și la comerțul electronic.

2. Prezenta recomandare se bazează pe progresele legate de diferitele tipuri de conținut ilegal realizate în contextul acordurilor voluntare dintre furnizorii de servicii de găzduire și alți furnizori de servicii afectați și consolidează aceste progrese. În domeniul terorismului, recomandarea se bazează pe progresele realizate în cadrul Forumului UE pentru internet și consolidează aceste progrese.

3. Prezenta recomandare nu aduce atingere drepturilor și obligațiilor statelor membre de a lua măsuri în ceea ce privește conținutul ilegal online în conformitate cu dreptul Uniunii și nici posibilității pe care o au instanțele sau autoritățile administrative ale statelor membre, în conformitate cu sistemele lor juridice, de a cere furnizorilor de servicii de găzduire să elimine conținutul ilegal sau să blocheze accesul la acesta. De asemenea, prezenta recomandare nu aduce atingere statutului furnizorilor de servicii de găzduire, astfel cum este prevăzut în Directiva 2000/31/CE, și nici posibilității pe care o au aceștia de a stabili și a asigura respectarea condițiilor de utilizare a serviciilor lor în conformitate cu legislația Uniunii și cu legile statelor membre.

([1]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

4. În sensul prezentei recomandări, se utilizează următorii termeni:

(a) „furnizor de servicii de găzduire” înseamnă un furnizor de servicii ale societății informaționale care constau în stocarea informațiilor furnizate de destinatarul serviciilor la cererea sa, în sensul articolului 14 din Directiva 2000/31/CE, indiferent de locul în care este stabilit respectivul furnizor, care își orientează activitățile către consumatorii cu reședința în Uniune;

(b) „conținut ilegal” înseamnă orice informație care nu este conformă cu legislația Uniunii sau cu legislația statului membru în cauză;

(c) „utilizator” înseamnă orice persoană fizică sau juridică care este destinatarul serviciilor furnizate de un furnizor de servicii de găzduire;

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

(e) „notificare” înseamnă orice comunicare adresată unui furnizor de servicii de găzduire, transmisă de către un autor de notificări cu privire la conținutul stocat de respectivul furnizor de servicii de găzduire și pe care autorul notificării îl consideră a fi conținut ilegal, comunicare prin care i se cere furnizorului de servicii de găzduire să elimine în mod voluntar conținutul în cauză sau să blocheze accesul la acesta;

(f) „autor al notificării” înseamnă o persoană sau o entitate care a transmis o notificare unui furnizor de servicii de găzduire;

(g) „notificator de încredere” înseamnă o persoană sau o entitate care este considerată de către un furnizor de servicii de găzduire ca având competențe și responsabilități deosebite în ceea ce privește combaterea conținutului ilegal online;

(h) „conținut cu caracter terorist” înseamnă orice informație a cărei difuzare constituie o infracțiune în sensul Directivei (UE) 2017/541 sau o infracțiune de terorism în sensul legislației statului membru în cauză, inclusiv difuzarea de informații relevante produse de grupuri ori entități teroriste incluse în listele relevante stabilite de Uniune sau de Organizația Națiunilor Unite ori care pot fi atribuite acestor grupuri sau entități;

(i) „autorități de aplicare a legii” înseamnă autoritățile competente desemnate de statele membre în conformitate cu legislația lor națională pentru a îndeplini sarcini în domeniul asigurării respectării legii, în scopul prevenirii, al depistării, al investigării sau al urmăririi penale a unor infracțiuni legate de conținutul ilegal online;

(j) „autorități competente” înseamnă autoritățile competente desemnate de statele membre în conformitate cu legislația lor națională pentru a îndeplini sarcini precum combaterea conținutului ilegal online, inclusiv autoritățile de aplicare a legii și autoritățile administrative însărcinate cu asigurarea respectării legii, indiferent de natura sau de obiectul specific al legislației respective, care se aplică în anumite domenii specifice;

(k) „semnalare” înseamnă orice comunicare adresată unui furnizor de servicii de găzduire, transmisă de către o autoritate competentă sau de către Europol cu privire la conținutul stocat de furnizorul de servicii de găzduire respectiv și pe care autoritatea în cauză sau Europol îl consideră a fi conținut cu caracter terorist, prin care i se cere furnizorului de servicii de găzduire să elimine în mod voluntar conținutul în cauză sau să blocheze accesul la acesta.

CAPITOLUL II

Recomandări generale referitoare la toate tipurile de conținut ilegal

Transmiterea și prelucrarea notificărilor

5. Ar trebui prevăzute mecanisme pentru transmiterea notificărilor. Aceste mecanisme ar trebui să fie ușor de accesat și de utilizat și să permită transmiterea notificărilor prin mijloace electronice.

6. Mecanismele respective ar trebui să permită și să încurajeze transmiterea de notificări care să fie suficient de precise și argumentate în mod corespunzător, astfel încât să se dea furnizorului de servicii de găzduire în cauză posibilitatea de a lua o decizie avizată și cu toată diligența necesară cu privire la conținutul la care se referă notificarea, în special cu privire la considerarea sau nu a conținutului respectiv drept conținut ilegal și la eliminarea sa ori blocarea accesului la acesta. Mecanismele menționate ar trebui să fie de așa natură încât să faciliteze transmiterea de notificări în care să se explice motivele pentru care autorul notificării consideră că respectivul conținut este ilegal și să se indice clar locul în care se găsește conținutul respectiv.

7. Autorii de notificări ar trebui să aibă posibilitatea de a-și include datele de contact în notificare, fără însă să existe o obligație formală în acest sens. În cazul în care un autor al notificării decide să includă datele respective în notificare, ar trebui garantată anonimitatea sa în raport cu furnizorul de conținut.

8. În cazul în care datele de contact ale autorului notificării sunt cunoscute de către furnizorul de servicii de găzduire, acesta din urmă ar trebui să trimită o confirmare de primire autorului notificării și să îl informeze pe acesta, fără întârzieri nejustificate și în mod proporțional, cu privire la decizia sa legată de conținutul la care se face referire în notificare.

Informarea furnizorilor de conținut și contranotificările

9. În cazul în care un furnizor de servicii de găzduire hotărăște să elimine sau să blocheze accesul la un conținut pe care îl stochează întrucât consideră că respectivul conținut este ilegal, indiferent de mijloacele utilizate pentru detectarea, identificarea sau eliminarea ori blocarea accesului la conținutul în cauză și în cazul în care datele de contact ale furnizorului de conținut sunt cunoscute de către furnizorul de servicii de găzduire, furnizorul de conținut ar trebui, fără întârzieri nejustificate, să fie informat în mod proporțional cu privire la decizia respectivă și la motivele care au stat la baza sa, precum și cu privire la posibilitatea, menționată la punctul 11, de a contesta decizia.

10. Cu toate acestea, punctul 9 nu ar trebui să se aplice în cazul în care este evident că respectivul conținut este ilegal și se referă la o infracțiune gravă care implică o amenințare la adresa vieții sau a siguranței persoanelor. În plus, furnizorii de servicii de găzduire nu ar trebui să furnizeze informațiile menționate la punctul respectiv în cazul în care o autoritate competentă a formulat o cerere în acest sens, bazată pe motive de ordine publică și de siguranță publică, în special în scopul prevenirii, al depistării, al investigării și al urmăririi penale a infracțiunilor. Această exceptare de la obligația de informare ar trebui să se aplice pentru întreaga perioada solicitată de autoritatea respectivă.

11. Furnizorii de conținut ar trebui să aibă posibilitatea să conteste decizia furnizorului de servicii de găzduire menționată la punctul 9 într-un interval de timp rezonabil, prin transmiterea unei contranotificări furnizorului de servicii de găzduire respectiv. Mecanismul folosit pentru transmiterea acestor contranotificări ar trebui să fie ușor de utilizat și să permită transmiterea lor prin mijloace electronice.

12. Ar trebui să se asigure faptul că furnizorii de servicii de găzduire țin seama în mod corespunzător de orice contranotificare primită. În cazul în care contranotificarea conține motive care îl determină pe furnizorul de servicii de găzduire să considere că conținutul la care se referă contranotificarea nu trebuie considerat conținut ilegal, acesta ar trebui să revină, fără întârzieri nejustificate, asupra deciziei sale de a elimina conținutul în cauză sau de a bloca accesul la acesta, fără a se aduce atingere posibilității sale de a stabili și a asigura respectarea condițiilor de utilizare a serviciilor sale în conformitate cu legislația Uniunii și cu legile statelor membre.

13. În cazul în care datele lor de contact sunt cunoscute de către furnizorul de servicii de găzduire, furnizorul de conținut care a transmis o contranotificare și autorul notificării în cauză ar trebui informați fără întârzieri nejustificate cu privire la decizia luată de furnizorul de servicii de găzduire referitor la conținutul în cauză.

Soluționarea alternativă a litigiilor

14. Statele membre sunt încurajate să faciliteze, atunci când este cazul, soluționarea alternativă a litigiilor legate de eliminarea conținutului ilegal ori de blocarea accesului la acesta. Mecanismele disponibile pentru soluționarea alternativă a litigiilor ar trebui să fie ușor de accesat, eficace, transparente și imparțiale și să asigure faptul că înțelegerea la care se ajunge este corectă și conformă cu legislația aplicabilă. Încercările de soluționare alternativă a litigiilor nu ar trebui să afecteze accesul la justiție al părților în cauză.

15. Atunci când astfel de mecanisme de soluționare alternativă a litigiilor sunt disponibile în statul membru în cauză, furnizorii de servicii de găzduire sunt încurajați să permită recurgerea la acestea.

Transparență

16. Furnizorii de servicii de găzduire ar trebui să fie încurajați să publice explicații clare, ușor de înțeles și suficient de detaliate cu privire la politica pe care o aplică referitor la eliminarea conținutului stocat, inclusiv a conținutului considerat ilegal, sau la blocarea accesului la acesta.

17. Furnizorii de servicii de găzduire ar trebui să fie încurajați să publice, la intervale regulate, preferabil cel puțin anual, rapoarte privind activitățile lor legate de eliminarea conținutului considerat ilegal și de blocarea accesului la un astfel de conținut. Rapoartele respective ar trebui să includă în special informații referitoare la volumul și tipul conținutului eliminat, la numărul de notificări și contranotificări primite și la intervalul de timp necesar pentru luarea de măsuri.

Măsuri proactive

18. Furnizorii de servicii de găzduire ar trebui să fie încurajați să ia, dacă este cazul, măsuri proactive proporționale și specifice cu privire la conținutul ilegal. Astfel de măsuri proactive ar putea include utilizarea de mijloace automatizate pentru detectarea conținutului ilegal numai în situațiile în care acest lucru este oportun și proporțional și cu condiția aplicării unor garanții eficace și adecvate, în special cele menționate la punctele 19 și 20.

Garanții

19. Pentru a se evita eliminarea conținutului care nu este conținut ilegal, fără a se aduce atingere posibilității furnizorilor de servicii de găzduire de a stabili și a asigura respectarea condițiilor de utilizare a serviciilor lor în conformitate cu legislația Uniunii și cu legile statelor membre, ar trebui să se prevadă garanții eficace și adecvate, astfel încât să se asigure faptul că furnizorii de servicii de găzduire acționează cu diligență și într-un mod proporțional cu privire la conținutul pe care îl stochează, mai ales atunci când prelucrează notificări și contranotificări și când iau o decizie cu privire la eventuala eliminare a conținutului considerat conținut ilegal sau la blocarea accesului la acesta.

20. În cazul în care furnizorii de servicii de găzduire utilizează mijloace automatizate cu privire la conținutul pe care îl stochează, ar trebui prevăzute garanții eficace și adecvate, astfel încât deciziile luate privind conținutul în cauză, în special deciziile de a elimina conținutul considerat ilegal sau de a bloca accesul la acesta, să fie corecte și întemeiate. Garanțiile respective ar trebui să constea în special în supravegherea și efectuarea de verificări de către o persoană, dacă este nevoie, și, în orice caz, atunci când este necesară o evaluare detaliată a contextului relevant pentru a se stabili dacă respectivul conținut trebuie considerat ilegal.

Protecție împotriva comportamentului abuziv

21. Ar trebui luate măsuri eficace și adecvate pentru a se preveni transmiterea de notificări sau contranotificări cu rea-credință sau luarea de măsuri în urma primirii unor astfel de notificări sau contranotificări, precum și pentru a descuraja alte forme de comportament abuziv legat de măsurile recomandate pentru combaterea conținutului ilegal online descrise în prezenta recomandare.

Cooperarea dintre furnizorii de servicii de găzduire și statele membre

22. Statele membre și furnizorii de servicii de găzduire ar trebui să desemneze puncte de contact pentru aspectele legate de conținutul ilegal online.

23. Ar trebui prevăzute proceduri accelerate pentru prelucrarea notificărilor transmise de autoritățile competente.

24. Statele membre sunt încurajate să impună furnizorilor de servicii de găzduire obligația legală de a informa cu promptitudine autoritățile de aplicare a legii, în scopul prevenirii, al depistării, al investigării sau al urmăririi penale a infracțiunilor, cu privire la orice dovadă a unei presupuse infracțiuni grave care implică o amenințare la adresa vieții sau a siguranței persoanelor, dovadă obținută în cadrul activităților lor de eliminare a conținutului ilegal sau de blocare a accesului la acesta, în conformitate cu cerințele legislative aplicabile, în special cele referitoare la protecția datelor cu caracter personal, inclusiv cu Regulamentul (UE) 2016/679.

Cooperarea dintre furnizorii de servicii de găzduire și notificatorii de încredere

25. Ar trebui încurajată cooperarea dintre furnizorii de servicii de găzduire și notificatorii de încredere. Mai exact, ar trebui prevăzute proceduri accelerate pentru prelucrarea notificărilor transmise de notificatorii de încredere.

26. Furnizorii de servicii de găzduire ar trebui încurajați să publice condiții clare și obiective pentru stabilirea persoanelor și a entităților pe care le consideră notificatori de încredere.

27. Scopul acestor condiții ar trebui să fie acela de a asigura faptul că persoanele sau entitățile în cauză au competențele necesare și își desfășoară activitatea ca notificatori de încredere cu diligență și obiectivitate, respectând valorile pe care este întemeiată Uniunea.

Cooperarea dintre furnizorii de servicii de găzduire

28. Furnizorii de servicii de găzduire ar trebui, dacă este cazul, să facă între ei schimb de experiență, soluții tehnologice și cele mai bune practici identificate pentru a combate conținutul ilegal online, mai ales cu furnizorii de servicii de găzduire care, date fiind dimensiunile sau anvergura activităților lor, dispun de resurse și competențe limitate, inclusiv în contextul cooperării permanente dintre furnizorii de servicii de găzduire prin intermediul codurilor de conduită, al memorandumurilor de înțelegere și al altor acorduri voluntare.

CAPITOLUL III

Recomandări specifice referitoare la conținutul cu caracter terorist

Aspecte generale

29. Recomandările specifice referitoare la conținutul cu caracter terorist descrise în prezentul capitol se aplică în plus față de recomandările generale din capitolul II.

30. Furnizorii de servicii de găzduire ar trebui să declare în mod explicit în condițiile de utilizare a serviciilor lor că nu vor stoca niciun conținut cu caracter terorist.

31. Furnizorii de servicii de găzduire ar trebui să ia măsuri astfel încât să nu stocheze conținut cu caracter terorist, în special în ceea ce privește semnalările, măsurile proactive și cooperarea, în conformitate cu punctele 32-40.

Transmiterea și prelucrarea semnalărilor

32. Statele membre ar trebui să se asigure că autoritățile lor competente au capacitatea și suficiente resurse pentru a detecta și a identifica în mod eficace conținutul cu caracter terorist și a transmite semnalări furnizorilor de servicii de găzduire în cauză, în special prin intermediul unităților lor naționale de semnalare a conținutului online și în cooperare cu Unitatea UE de semnalare a conținutului online din cadrul Europol.

33. Ar trebui să se prevadă mecanisme care să permită transmiterea semnalărilor. Ar trebui să se prevadă proceduri accelerate pentru prelucrarea semnalărilor, în special a celor transmise de către unitățile naționale de semnalare a conținutului online și de către Unitatea UE de semnalare a conținutului online din cadrul Europol.

34. Furnizorii de servicii de găzduire ar trebui, fără întârzieri nejustificate, să transmită confirmări ale primirii semnalărilor și să informeze autoritatea competentă sau Europol despre deciziile luate cu privire la conținutul la care se referă semnalările, indicând, după caz, când a fost eliminat conținutul sau a fost blocat accesul la acesta sau de ce au hotărât să nu elimine conținutul respectiv ori să nu blocheze accesul la acesta.

35. În general, furnizorii de servicii de găzduire ar trebui să evalueze și, dacă este cazul, să elimine conținutul identificat în semnalări sau să blocheze accesul la acesta în termen de o oră din momentul în care au primit semnalarea.

Măsuri proactive

36. Furnizorii de servicii de găzduire ar trebui să ia măsuri proactive proporționale și specifice, inclusiv utilizând mijloace automatizate, pentru a detecta, a identifica și a elimina cu promptitudine conținutul cu caracter terorist sau a bloca accesul la acesta.

37. Furnizorii de servicii de găzduire ar trebui să ia măsuri proactive proporționale și specifice, inclusiv utilizând mijloace automatizate, pentru a-i împiedica imediat pe furnizorii de conținut să redifuzeze un conținut care a fost deja eliminat sau la care a fost deja blocat accesul din cauză că este considerat conținut cu caracter terorist.

Cooperare

38. Pentru a preveni difuzarea conținutului cu caracter terorist între diferitele servicii de găzduire, furnizorii de servicii de găzduire ar trebui să fie încurajați să coopereze între ei prin partajarea și optimizarea unor instrumente tehnologice eficace, adecvate și proporționale, inclusiv instrumente care să permită detectarea automată a conținutului. În cazul în care acest lucru este posibil din punct de vedere tehnologic, ar trebui acoperite toate formatele relevante prin care se difuzează conținut cu caracter terorist. Această cooperare ar trebui să-i includă în special pe furnizorii de servicii de găzduire care, date fiind dimensiunile și anvergura activității lor, dispun de resurse și competențe limitate.

39. Furnizorii de servicii de găzduire ar trebui încurajați să ia măsurile necesare pentru a asigura funcționarea corespunzătoare și îmbunătățirea instrumentelor menționate la punctul 38, în special prin furnizarea de identificatori pentru conținutul considerat ca având caracter terorist și prin valorificarea deplină a tuturor posibilităților oferite de aceste instrumente.

40. Autoritățile competente și furnizorii de servicii de găzduire ar trebui să încheie acorduri de lucru, dacă este cazul inclusiv cu Europol, privind chestiunile legate de conținutul online cu caracter terorist, inclusiv pentru a asigura o mai bună înțelegere a activităților teroriste online, a îmbunătăți mecanismele de semnalare a conținutului, a preveni suprapunerea inutilă a eforturilor și a facilita soluționarea solicitărilor venite din partea autorităților de aplicare a legii în scopul derulării investigațiilor penale legate de terorism.

CAPITOLUL IV

Furnizarea de informații

41. Statele membre ar trebui, la intervale regulate și preferabil o dată la trei luni, să informeze Comisia cu privire la semnalările transmise de autoritățile lor competente și cu privire la deciziile luate de furnizorii de servicii de găzduire în urma primirii semnalărilor respective, precum și cu privire la cooperarea lor cu furnizorii de servicii de găzduire în vederea combaterii conținutului cu caracter terorist.

42. Pentru a permite monitorizarea acțiunilor întreprinse în ceea ce privește conținutul cu caracter terorist ca urmare a prezentei recomandări, în termen de cel mult trei luni de la data publicării sale, furnizorii de servicii de găzduire ar trebui să transmită Comisiei, la solicitarea acesteia, toate informațiile relevante necesare pentru a permite o astfel de monitorizare. Informațiile respective pot include în special informațiile privind volumul de conținut care a fost eliminat sau la care a fost blocat accesul, fie în urma semnalărilor sau a notificărilor, fie ca urmare a măsurilor proactive luate și a utilizării mijloacelor automatizate. Acest informații pot include, totodată, numărul de semnalări primite și intervalul de timp necesar pentru luarea de măsuri, precum și volumul de conținut a cărui difuzare sau redifuzare a fost împiedicată prin utilizarea instrumentelor de detectare automată a conținutului și prin alte instrumente tehnologice.

43. Pentru a permite monitorizarea acțiunilor întreprinse în ceea ce privește conținutul ilegal, altul decât conținutul cu caracter terorist, ca urmare a prezentei recomandări, în termen de cel mult șase luni de la data publicării sale, statele membre și furnizorii de servicii de găzduire ar trebui să transmită Comisiei, la solicitarea acesteia, toate informațiile relevante necesare pentru a permite o astfel de monitorizare.

Adoptată la Bruxelles, 1 martie 2018.

Pentru Comisie
Andrus ANSIP
Vicepreședinte