

Al nouălea Tratat de stat de modificare a tratatelor de stat referitoare la legislația privind mass-media

Obiectul: Utilizarea mijloacelor tehnice în supravegherea mass-media

Propunere de stabilire a unui standard în Tratatul interstatal privind mass-media

Articolul 109a Utilizarea mijloacelor tehnice în supraveghere	Observații
(1) Autoritățile de stat în domeniul mass-media pot utiliza mijloace tehnice pentru a investiga încălcările legii, astfel cum sunt definite la articolul 109 din prezentul tratat de stat și la articolul 20 din JMStV, care includ compararea automată a conținutului text, imagine, audio și video din emisiunile de radiodifuziune și teledifuziune pentru potențiale încălcări. Prima teză include, de asemenea, conținutul din domeniul radiodifuziunii și teledifuziunii care face obiectul restricțiilor de acces.	Alineatul (1) prevede admisibilitatea fundamentală a cercetării și examinării automate a conținutului în vederea identificării potențialelor încălcări ale legii. O comparație automată include, de asemenea, utilizarea sistemelor bazate pe IA, cărora li se aplică cerințele Regulamentului privind IA, pe lângă cerințele de protecție a datelor de la articolul 2 și următoarele. Posibilitatea de a utiliza mijloace tehnice prevede o supraveghere independentă eficientă și eficace a mass-media și poate contribui, de asemenea, la un nivel mai ridicat de protecție a angajaților în manipularea materialelor sensibile. Încălcările legii sunt limitate, în cadrul domeniului de aplicare al autorizației de utilizare a unor astfel de mijloace tehnice, la cele care fac, de asemenea, obiectul unor măsuri de supraveghere din partea autorităților de stat în domeniul mass-media în temeiul articolului 109 din MStV sau al articolului 20 din JMStV. Comparația automată va fi limitată, de asemenea, la conținutul difuzat și la conținutul teledifuziunii. Numai aceste servicii intră în domeniul de aplicare al Tratatului interstatal privind mass-media și al Tratatului interstatal privind protecția minorilor în mass-media și, ca atare, sunt supuse supravegherii autorităților de stat în domeniul mass-media. În același timp, acest lucru limitează comparația cu conținutul care este făcut „public” de către un furnizor, întrucât atât radiodifuziunea, cât și teledifuziunea sunt oferte jurnalistice care, spre deosebire de comunicarea individuală, se adresează unui număr nedeterminat de utilizatori. Restricțiile de acces definite la a doua teză sunt, în măsura în care sunt considerate difuzare sau teledifuziune, accesibile numai în urma verificării vârstei sau a plății unei taxe, după înregistrarea sau crearea unui cont de utilizator (de exemplu).
(2) Informațiile menționate în conținutul text, imagine, audio și video, inclusiv categoriile speciale de date cu caracter personal definite la articolul 9 alineatul (1) din Regulamentul (UE) 2016/679, pot fi prelucrate în cadrul comparării automate în conformitate cu alineatul (1), în măsura în care acest lucru este necesar pentru a putea efectua o evaluare finală a conținutului. Nu este permisă compararea automată pe baza datelor cu caracter personal	Încălcările legii, astfel cum sunt definite la articolul 1, vizează elemente generale ale infracțiunii, nu persoane specifice, astfel încât colectarea datelor cu caracter personal nu constituie, în general, și nici nu ar trebui să constituie obiectul acesteia. Cu toate acestea, conținutul comparat poate conține în mod inevitabil și necesar date cu caracter personal. Aceste date cu caracter personal pot constitui, de asemenea, categorii speciale de date cu caracter personal. În

specifice.	special, materialele vizuale pot, de exemplu, să furnizeze informații despre originea rasială și etnică, opiniile politice, convingerile religioase sau filozofice sau apartenența la sindicate, sau pot conține date privind sănătatea sau date referitoare la viața sexuală sau orientarea sexuală a unei persoane fizice. Prin urmare, prelucrarea acestor date este permisă numai în limite restrânse. Prelucrarea și, în special, colectarea datelor sunt permise numai dacă rezultă chiar din conținutul comparat și sunt necesare pentru prelucrarea conținutului în temeiul legislației în materie de supraveghere. O astfel de prelucrare a datelor este permisă în temeiul articolului 9 alineatul (2) litera (e) din RGPD, dacă datele au fost făcute „în mod evident publice” de către persoana vizată. Cu toate acestea, în ceea ce privește datele publicate de terți, echilibrul impus de articolul 9 alineatul (2) litera (g) din RGPD („interes public semnificativ”) este determinat în mare măsură de legătura strânsă și indisolubilă cu conținutul care urmează să fie revizuit și de interesele protejate la nivel înalt care sunt în joc. Deoarece nu este posibilă evaluarea conținutului fără contextul său general, nu se poate stabili dacă există o încălcare. Chiar și în special în cazuri deosebit de sensibile, de exemplu acte sexuale, măsurile, în special interdicțiile, ordinele de ștergere și blocare emise de autoritățile de stat în domeniul mass-media, servesc, de asemenea, intereselor acestor terțe părți. În măsura în care este posibil să se separe datele cu caracter personal și, astfel, să se evite colectarea acestora, datele deosebit de sensibile nu trebuie stocate. „Crearea de profiluri” nu face parte din procesul de comparare prevăzut la alineatul (1) și ar fi inadmisibilă. În plus, excluderea unei comparații bazate pe date cu caracter personal specifice, și anume date referitoare la o anumită persoană, este menționată în mod explicit.
(3) În cazul în care se constată o potențială încălcare a legii, astfel cum este definită la alineatul (1), prin mijloace tehnice, următoarele date cu caracter personal suplimentare referitoare la conținutul potențial ilicit pot fi prelucrate prin intermediul mijloacelor tehnice respective, cu condiția ca aceste date să fie necesare în sensul alineatului (4): datele furnizorului, inclusiv informațiile în conformitate cu articolul 18, adresa web a conținutului, data publicării și ora colectării datelor, localizarea geografică, legăturile și interacțiunile cu conținutul.	În cazul în care instrumentul detectează o posibilă încălcare a legii, care face obiectul unor măsuri de supraveghere în temeiul articolului 109 din MStV și/sau al articolului 20 din JMStV, pot fi colectate și prelucrate date cu caracter personal suplimentare, pe lângă conținutul în sine, cu condiția ca acest lucru să fie necesar pentru măsuri de supraveghere ulterioare.
(4) În cazul în care mijlocul tehnic detectează o posibilă încălcare a legii, astfel cum este definită la alineatul (1), trebuie să se verifice fără întârziere de către o persoană fizică dacă acest lucru poate fi confirmat; în caz contrar, datele cu caracter personal prelucrate trebuie șterse fără întârziere. O ștergere în conformitate cu prima teză trebuie să aibă loc în	Datele colectate trebuie să facă obiectul unei examinări umane imediate. În absența unei suspiciuni concrete de încălcare a legii, datele trebuie șterse imediat. Dacă nu are loc nicio revizuire, datele trebuie șterse după maximum 30 de zile.

termen de cel mult 30 de zile, chiar dacă până la acea dată nu s-a putut efectua nicio verificare.	
(5) Persoanele implicate în prelucrarea categoriilor speciale de date cu caracter personal trebuie să fie informate cu privire la nevoia specială de protecție a acestor date. Trebuie luate măsuri tehnice și organizatorice adecvate pentru a se asigura că se poate verifica ulterior dacă și de către cine au fost introduse, modificate sau șterse datele cu caracter personal, astfel cum sunt definite la alineatele (2) și (3). Reglementările generale privind protecția datelor, în special cele referitoare la securitatea datelor cu caracter personal, rămân neafectate.	Sunt definite liniile directoare pentru securitatea datelor. Alte reglementări privind protecția datelor (de exemplu, aspectele legate de transferul către țări terțe, securitatea datelor cu caracter personal etc.) rămân neschimbate.
(6) Dacă, după examinarea în conformitate cu alineatul (4), există o suspiciune concretă de încălcare a legii, datele cu caracter personal pot fi prelucrate în scopul aplicării măsurilor de supraveghere în conformitate cu articolul 109 din prezentul tratat de stat și articolul 20 din JMStV, precum și în scopul urmăririi penale a contravențiilor administrative în conformitate cu articolul 115 alineatul (1) din prezentul tratat de stat și articolul 24 alineatele (1) și (2) din JMStV. În cazul în care există suspiciunea unei infracțiuni legate de elementele infracțiunii în temeiul articolului 4 alineatul (1) sau (2) punctul 1 din JMStV sau a unei infracțiuni în temeiul articolului 23 din JMStV, datele cu caracter personal pot fi, de asemenea, transmise altor autorități competente, dacă acest lucru este necesar pentru investigarea și urmărirea penală a acestor infracțiuni. Nu este permisă utilizarea în alte scopuri. Datele cu caracter personal trebuie șterse imediat în cazul în care nu mai sunt necesare pentru punerea în aplicare a măsurilor de supraveghere sau pentru urmărirea penală a infracțiunilor administrative, în termen de cel mult șase luni, cu condiția ca nicio procedură de supraveghere să nu fie în curs de desfășurare până la momentul respectiv.	În cazurile în care există suspiciuni concrete de încălcare a legii, datele cu caracter personal pot fi utilizate pentru măsuri de supraveghere și urmărirea penală a contravențiilor administrative. Termenul de prescripție pentru contravenții constituie limita permisă de stocare a datelor. În plus, sunt prevăzute obligații de ștergere și pentru datele stocate pentru care nu a fost inițiată nicio procedură. În cazul în care există suspiciunea unei infracțiuni pe baza elementelor infracțiunii în temeiul articolului 4 alineatul (1) sau (2) punctul 1 sau al articolului 23 din JMStV, datele necesare pot fi transmise autorităților de aplicare a legii.
(7) Mijloacele tehnice definite la alineatul (1) se bazează pe algoritmi, modele și date de instruire adecvate. Mijloacele tehnice trebuie validate înainte de utilizare și în mod regulat ulterior. Este permisă efectuarea unui antrenament cu date anonimizate. Utilizarea datelor cu caracter personal în scopul pregătirii mijloacelor tehnice de utilizare în conformitate cu articolul 1 nu este permisă; se aplică excepții în cazul datelor cu caracter personal solicitate în temeiul articolului 2 alineatul (1) și care se referă la personalități din ochiul public, în măsura în care pseudonimizarea nu este eficace sau este disproporționată. Anonimizarea sau pseudonimizarea datelor cu caracter personal înainte de ștergerea acestora în temeiul alineatului (4) prima teză punctul 2; Utilizarea unei clauze în scopul instruirii mijloacelor tehnice este permisă, cu condiția ca datele să fie	Cerințele privind mijloacele tehnice și verificarea acestora sunt specificate mai detaliat. În special, este prevăzută o validare periodică și sunt definite specificații pentru datele de antrenament. Instruirea cu date cu caracter personal este, prin urmare, în general interzisă. Cu toate acestea, pentru a asigura funcționalitatea și acuratețea unui astfel de instrument, reducând în același timp la minimum utilizarea datelor, datele cu caracter personal trebuie să poată fi utilizate în scopuri de formare, dacă este necesar. Alineatul (3) prevede o excepție corespunzătoare. Acest lucru se extinde și la datele necesare privind personalitățile publice care, în special datorită referințelor istorice, pot constitui puncte de referință relevante pentru căutare. Înainte de ștergerea datelor cu caracter personal în conformitate cu alineatul (4) prima teză punctul 2.

necesare pentru investigarea încălcărilor legii, astfel cum sunt definite la alineatul (1). Înainte de utilizarea instrumentelor tehnice, trebuie efectuată o evaluare a impactului asupra protecției datelor în conformitate cu articolul 35 din Regulamentul (UE) 2016/679.	Clauza prevede că anonimizarea datelor cu caracter personal în scopul instruirii instrumentelor tehnice este permisă. Cu toate acestea, acest lucru este supus condiției ca datele să fie necesare pentru utilizarea instrumentului, și anume detectarea încălcărilor legii în temeiul alineatului (1). Procesele de anonimizare trebuie să respecte standardele actuale.
(8) Detaliile privind tipul, scopul și utilizarea mijloacelor tehnice în conformitate cu alineatul (1) vor fi reglementate de autoritățile de stat în domeniul mass-media printr-un statut comun. Utilizarea mijloacelor tehnice trebuie documentată; principalele rezultate ale utilizării trebuie publicate anual într-un raport. Ca parte a măsurilor de supraveghere, utilizarea mijloacelor tehnice trebuie comunicată furnizorului în cauză.	Prin intermediul unei autorizații statutare, comitetele sunt implicate în aspectele fundamentale ale proiectării și utilizării mijloacelor tehnice; statutele pot specifica, în special, domeniile de utilizare, orele de funcționare sau pot defini mai detaliat ciclurile, funcționalitatea și categoriile criteriilor de căutare. Un set comun de reglementări asigură faptul că autoritățile de stat în domeniul mass-media funcționează în conformitate cu standarde uniforme.
(9) Furnizorii de platforme online, astfel cum sunt definiți în Regulamentul (UE) 2022/2065, furnizează, la cererea autorității de stat în domeniul mass-media competente, interfețe adecvate pentru utilizarea mijloacelor tehnice menționate la alineatul (1), în măsura în care acest lucru este fezabil din punct de vedere tehnic și economic. Numai datele definite la alineatele (2) și (3) pot fi puse la dispoziție prin intermediul interfeței. Articolul 109 alineatul (4) și articolul 21 alineatul (3) din Tratatul interstatal privind protecția minorilor în mass-media se aplică în mod corespunzător.	Pe lângă obligația furnizorilor de a permite supravegherea serviciilor lor, astfel cum se prevede la articolul 109 alineatul (4) din MStV și la articolul 21 alineatul (3) din JMStV, se introduce o obligație specifică privind interfața pentru utilizarea mijloacelor tehnice. Această obligație se adresează platformelor online și, prin urmare, serviciilor de telemedia care, spre deosebire de furnizorii de conținut și platformele media, nu oferă conținut sau servicii globale pentru care sunt singurii responsabili. Aceștia sunt, în esență, intermediari mass-media. Aceste servicii de telemedia sunt supuse regimului de răspundere prevăzut în Regulamentul (UE) 2022/2065 și, prin urmare, sunt în mod regulat exonerate de răspundere pentru informațiile furnizate de utilizatorii lor. Aceste orientări rămân neschimbate. Prin obligarea autorităților de reglementare din domeniul mass-media să furnizeze o interfață necesară, se asigură accesul la conținutul pentru care sunt responsabile terțe părți și, prin urmare, supravegherea acestui conținut sau a furnizorilor de conținut. Numai datele relevante, accesibile publicului, menționate la alineatele (2) și (3), dar nu și datele contractuale sau datele stocate în conturi, pot fi puse la dispoziție prin intermediul interfeței. Accesul trebuie acordat gratuit, la fel ca în cazurile prevăzute la articolul 109 alineatul (4) din MStV și la articolul 21 alineatul (3) din JMStV.