

IX Traktat Państwowy zmieniający traktaty państwowe dotyczące prawa medialnego

Przedmiot: Wykorzystanie środków technicznych w nadzorze mediów

Wniosek dotyczący ustanowienia normy w Traktacie międzykrajowym w sprawie mediów

§ 109a Wykorzystanie środków technicznych w nadzorze	Uwagi
(1) Państwowe organy ds. mediów mogą wykorzystywać środki techniczne do badania naruszeń prawa, określonych w § 109 niniejszego traktatu państwowego i § 20 JMStV, które obejmują treści tekstowe, obrazowe, audio i automatyczne porównywanie treści wideo z nadawanych programów i teledzienników pod kątem potencjalnych naruszeń. Zdanie pierwsze obejmuje również treści w radiofonii i telewizji oraz teledziennikach, które podlegają ograniczeniom dostępu.	Ustęp 1 przewiduje zasadniczą dopuszczalność automatycznego wyszukiwania i badania treści pod kątem potencjalnych naruszeń prawa. Automatyczne porównanie obejmuje również wykorzystanie systemów opartych na sztucznej inteligencji, do których mają zastosowanie wymogi rozporządzenia w sprawie sztucznej inteligencji, oprócz wymogów dotyczących ochrony danych określonych w ust. 2 i następnych. Możliwość wykorzystania środków technicznych zapewnia skuteczny i wydajny niezależny nadzór nad mediami, a także może przyczynić się do wyższego poziomu ochrony pracowników w zakresie postępowania z materiałami wrażliwymi. Naruszenia prawa są ograniczone w zakresie zezwolenia na stosowanie takich środków technicznych do tych środków, które podlegają również środkom nadzoru przez państwowe organy ds. mediów zgodnie z § 109 MStV lub § 20 JMStV. Automatyczne porównanie będzie również ograniczone do treści nadawanych i teledzienników. Jedynie te usługi wchodzą w zakres Międzypaństwowego traktatu o mediach oraz Międzypaństwowego traktatu o ochronie małoletnich w mediach i jako takie podlegają nadzorowi państwowych organów ds. mediów. Jednocześnie ogranicza to porównanie z treściami, które dostawca udostępnia „publicznie”, ponieważ zarówno nadawanie programów, jak i teledzienniki są ofertami dziennikarskimi, które w przeciwieństwie do komunikacji indywidualnej są skierowane do nieokreślonej liczby użytkowników. Ograniczenia dostępu, o których mowa w zdaniu drugim, w zakresie, w jakim podlegają one kwalifikacji jako usługi nadawcze lub teledzienniki, są dostępne wyłącznie po zastosowaniu systemu weryfikacji wieku lub za zaporą płatniczą, po uprzedniej rejestracji lub utworzeniu konta użytkownika (na przykład).
(2) Informacje, o których mowa w treściach tekstowych, obrazowych, dźwiękowych i wideo, w tym szczególne kategorie danych osobowych określone w art. 9 ust. 1 rozporządzenia (UE) 2016/679, mogą być przetwarzane w ramach zautomatyzowanego porównania zgodnie z ust. 1 w zakresie, w jakim jest to konieczne do dokonania ostatecznej oceny treści. Automatyczne porównywanie na podstawie konkretnych danych osobowych jest niedozwolone.	Naruszenia prawa określone w § 1 dotyczą ogólnych elementów przestępstwa, a nie konkretnych osób, w związku z czym gromadzenie danych osobowych nie jest i nie powinno być celem. Niemniej jednak porównywane treści mogą w sposób nieunikniony i konieczny zawierać dane osobowe. Takie dane osobowe mogą również stanowić szczególne kategorie danych osobowych. W szczególności materiały wizualne mogą na przykład zawierać informacje dotyczące pochodzenia rasowego i

	etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych lub przynależności do związków zawodowych, a także dane dotyczące zdrowia lub życia seksualnego lub orientacji seksualnej osoby fizycznej. Przetwarzanie tych danych jest zatem dozwolone wyłącznie w ograniczonym zakresie. Przetwarzanie, a w szczególności gromadzenie danych, jest dopuszczalne tylko wtedy, gdy wynika to z samej porównywanej treści i jest konieczne do przetwarzania treści zgodnie z przepisami prawa nadzorczego. Takie przetwarzanie danych jest dopuszczalne na podstawie art. 9 ust. 2 lit. e) RODO, jeżeli dane zostały „w sposób oczywisty podane do wiadomości publicznej” przez samą osobę, której dane dotyczą. Jeżeli jednak chodzi o opublikowane dane osób trzecich, wyważenie wymagane na podstawie art. 9 ust. 2 lit. g) RODO („istotny interes publiczny”) zależy w dużej mierze od ścisłego nierozzerwalnego związku z treścią podlegającą przeglądowi i wchodzącymi w grę chronionymi interesami wysokiego szczebla. Ponieważ ocena treści bez jej ogólnego kontekstu nie jest możliwa, nie można stwierdzić tutaj naruszenia. Nawet w szczególnie delikatnych przypadkach, np. czynności seksualnych, środki, w szczególności zakazy, nakazy usunięcia i zablokowania wydane przez państwowe organy ds. mediów, służą również interesom tych osób trzecich. O ile możliwe jest oddzielenie danych osobowych, a tym samym unikanie konieczności ich gromadzenia, nie wolno przechowywać danych szczególnie wrażliwych. „Profilowanie” nie jest częścią procesu porównawczego przewidzianego w ust. 1 i byłoby niedopuszczalne. Ponadto wyraźnie określono wyłączenie porównania na podstawie konkretnych danych osobowych, tj. danych dotyczących konkretnej osoby.
(3) W przypadku gdy potencjalne naruszenie przepisów prawa, o którym mowa w ust. 1, zostanie wykryte przy użyciu środków technicznych, przy wykorzystaniu tych środków technicznych mogą być przetwarzane następujące dodatkowe dane osobowe dotyczące treści mogących stanowić naruszenie, pod warunkiem że dane te są niezbędne do celów określonych w ust. 4: Dane dostawcy, w tym informacje, o których mowa w § 18, adres strony internetowej treści, data publikacji i czas gromadzenia danych, położenie geograficzne, powiązania i interakcje z treścią.	W przypadku wykrycia przez narzędzie potencjalnego naruszenia prawa, które podlega środkom nadzorczym na mocy § 109 MStV lub § 20 JMStV, oprócz samej treści można gromadzić i przetwarzać dalsze dane osobowe, pod warunkiem że jest to konieczne do podjęcia dalszych środków nadzorczych.
(4) Jeżeli środki techniczne wykryją potencjalne naruszenie prawa w rozumieniu § 1, osoba fizyczna musi niezwłocznie sprawdzić, czy można to potwierdzić; jeżeli tak nie jest, przetwarzane dane osobowe muszą zostać niezwłocznie usunięte. Usunięcie zgodnie z zdaniem 1 musi nastąpić nie	Zebrane dane muszą zostać poddane niezwłocznemu przeglądowi przez człowieka. W przypadku braku konkretnego podejrzenia naruszenia prawa dane muszą zostać niezwłocznie usunięte. Jeśli nie przeprowadza się przeglądu, dane muszą zostać usunięte po maksymalnie 30 dniach.

później niż w ciągu 30 dni, nawet jeśli do tego czasu nie będzie można przeprowadzić przeglądu.	
(5) Osoby zaangażowane w przetwarzanie szczególnych kategorii danych osobowych muszą być świadome szczególnej potrzeby ochrony takich danych. Należy podjąć odpowiednie środki techniczne i organizacyjne, aby zapewnić możliwość późniejszej weryfikacji, czy i przez kogo dane osobowe określone w ustępach 2 i 3 zostały wprowadzone, zmienione lub usunięte. Ogólne przepisy dotyczące ochrony danych, w szczególności dotyczące bezpieczeństwa danych osobowych, pozostają bez zmian.	Określono wytyczne dotyczące bezpieczeństwa danych. Pozostałe przepisy dotyczące ochrony danych (np. kwestie przekazywania danych do państw trzecich, bezpieczeństwo danych osobowych itp.) pozostają bez zmian.
(6) Jeżeli po przeprowadzeniu kontroli zgodnie z § 4 zachodzi konkretne podejrzenie naruszenia prawa, dane osobowe mogą być przetwarzane do celów stosowania środków nadzoru zgodnie z § 109 niniejszej umowy państwowej i § 20 JMStV, a także do celów ścigania przestępstw administracyjnych zgodnie z § 115 ust. 1 niniejszej umowy państwowej oraz § 24 ust. 1 i 2 JMStV. Jeżeli istnieje podejrzenie popełnienia przestępstwa związanego z elementami przestępstwa, o którym mowa w § 4 ust. 1 lub § 4 ust. 2 pkt 1 JMStV, lub przestępstwa, o którym mowa w § 23 JMStV, dane osobowe można również przekazać innym właściwym organom, jeżeli jest to niezbędne do prowadzenia postępowań przygotowawczych w sprawie tych przestępstw i ich ścigania. Wykorzystywanie do innych celów nie jest dozwolone. Dane osobowe należy natychmiast usunąć, jeżeli nie są już potrzebne do wdrożenia środków nadzorczych lub do ścigania przestępstw administracyjnych, najpóźniej po upływie 6 miesięcy, pod warunkiem, że do tego czasu nie toczy się żadne postępowanie nadzorcze.	W przypadku konkretnego podejrzenia naruszenia prawa dane osobowe mogą być wykorzystywane do celów środków nadzorczych oraz ścigania przestępstw administracyjnych. Przedawnienie karalności przestępstw administracyjnych stanowi ograniczenie dozwolonego przechowywania danych. Ponadto przewidziano również obowiązek usunięcia przechowywanych danych, w odniesieniu do których nie wszczęto żadnego postępowania. Jeżeli istnieje podejrzenie popełnienia przestępstwa na podstawie znamion przestępstwa określonych w § 4 ust. 1 lub § 4 ust. 2 pkt 1 lub § 23 JMStV, wymagane dane mogą zostać przekazane organom ścigania.
(7) Środki techniczne określone w ust. 1 opierają się na odpowiednich algorytmach, modelach i danych treningowych. Środki techniczne muszą zostać zatwierdzone przed użyciem, a następnie regularnie poddawane kontroli. Dozwolone jest szkolenie z wykorzystaniem zanonimizowanych danych. Wykorzystywanie danych osobowych do celów szkolenia środków technicznych, stosowanych zgodnie z ust. 1, jest niedopuszczalne; wyjątek stanowią dane osobowe wymagane na podstawie ust. 2 pkt 1, dotyczące osób pełniących funkcje publiczne, o ile pseudonimizacja nie jest skuteczna lub byłaby nieproporcjonalna. Anonimizacja lub pseudonimizacja danych osobowych przed ich usunięciem zgodnie z § 4 zdanie 1 pkt 2. Stosowanie klauzuli w celu szkolenia środków technicznych jest dopuszczalne pod warunkiem, że dane te są niezbędne do zbadania naruszeń prawa określonych w § 1. Przed użyciem narzędzi technicznych należy przeprowadzić ocenę skutków dla ochrony danych zgodnie z § 35 rozporządzenia (UE) 2016/679.	Wymagania dotyczące środków technicznych i ich weryfikacji zostały określone bardziej szczegółowo. W szczególności przewidziano regularną walidację i określono specyfikacje dla danych dotyczących szkoleń. Szkolenie z wykorzystaniem danych osobowych jest zatem ogólnie zabronione. Aby jednak zapewnić funkcjonalność i dokładność takiego narzędzia przy jednoczesnym zminimalizowaniu wykorzystania danych, w razie potrzeby musi istnieć możliwość wykorzystywania danych osobowych do celów szkoleniowych. Zdanie trzecie przewiduje odpowiedni wyjątek. Dotyczy to również wymaganych danych dotyczących osób publicznych, które ze względu na odniesienia historyczne mogą stanowić istotne punkty odniesienia dla wyszukiwania. Przed usunięciem danych osobowych zgodnie z ust. 4 zdanie 1 2. Klauzula stanowi, że anonimizacja danych osobowych w celu szkolenia narzędzi technicznych jest dopuszczalna. Warunkiem jest jednak, aby dane były niezbędne do korzystania z narzędzia, tj. wykrywania naruszeń prawa zgodnie z ust. 1. Procesy

	anonimizacji muszą być zgodne z obowiązującymi normami.
(8) Szczegóły dotyczące rodzaju, przeznaczenia i wykorzystania środków technicznych zgodnie z ust. 1 zostaną uregulowane przez państwowe organy ds. mediów w drodze wspólnego statutu. Wykorzystanie środków technicznych musi być udokumentowane, a kluczowe wyniki tego wykorzystania muszą być publikowane corocznie w raporcie. W ramach środków nadzorczych informacje o zastosowaniu środków technicznych muszą zostać ujawnione zainteresowanemu dostawcy.	Na mocy upoważnienia ustawowego komisje są zaangażowane w podstawowe kwestie związane z projektowaniem i wykorzystaniem środków technicznych; statuty mogą w szczególności określać obszary zastosowania, godziny pracy lub bardziej szczegółowo definiować cykle, funkcjonalność i kategorie kryteriów wyszukiwania. Wspólny zbiór przepisów gwarantuje, że państwowe organy ds. mediów działają zgodnie z jednolitymi standardami.
(9) Dostawcy platform internetowych w rozumieniu rozporządzenia (UE) 2022/2065 zapewniają, na wniosek właściwego państwowego organu ds. mediów, odpowiednie interfejsy do korzystania ze środków technicznych, o których mowa w ust. 1, o ile jest to technicznie i ekonomicznie wykonalne. Za pośrednictwem interfejsu można udostępniać wyłącznie dane określone w ustępach 2 i 3. Zastosowanie mają odpowiednio § 109 ust. 4 i § 21 ust. 3 Międzypaństwowego traktatu o ochronie małoletnich w mediach.	Oprócz spoczywającego na dostawcach obowiązku umożliwienia nadzoru nad ich usługami, jak określono w § 109 ust. 4 MStV i § 21 ust. 3 JMStV, wprowadza się szczególny obowiązek dotyczący interfejsu w odniesieniu do korzystania ze środków technicznych. Obowiązek ten dotyczy platform internetowych, a tym samym usług telemedialnych, które – w przeciwieństwie do dostawców treści i platform medialnych – nie oferują treści ani ogólnych usług, za które ponoszą wyłączną odpowiedzialność. Są to przede wszystkim pośrednicy medialni. Usługi telemediów podlegają przepisom dotyczącym odpowiedzialności zawartym w rozporządzeniu (UE) 2022/2065 i w związku z tym są regularnie zwolnione z odpowiedzialności za informacje dostarczane przez ich użytkowników. Wytyczne te pozostają niezmienione. Nakładając na organy regulacyjne ds. mediów wymóg zapewnienia wymaganego interfejsu, zapewnia się dostęp do treści, za które odpowiedzialne są osoby trzecie, a tym samym nadzór nad tymi treściami lub dostawcami treści. Za pośrednictwem interfejsu mogą być udostępniane wyłącznie odpowiednie, publicznie dostępne dane, o których mowa w ust. 2 i 3, z wyłączeniem danych umownych oraz danych przechowywanych za kontami użytkowników. Dostęp musi być udzielany bezpłatnie, tak jak w przypadkach określonych w § 109 ust. 4 MStV oraz § 21 ust. 3 JMStV.