



**KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ**

Kozminski University, Poland

*ORCID iD: 0000-0003-0188-5704*

## **PRAWNE ASPEKTY ZWALCZANIA TREŚCI NIELEGALNYCH I SZKODLIWYCH W CYBERPRZESTRZENI. ANALIZA PORÓWNAWCZA: FRANCJA, NIEMCY, POLSKA**

**LEGAL ASPECTS OF COMBATING ILLEGAL  
AND HARMFUL CONTENT IN CYBERSPACE:  
A COMPARATIVE ANALYSIS: FRANCE,  
GERMANY, AND POLAND**

**ABSTRACT**

**Objectives:** *This article provides an overview of regulations related to the process of combating illegal and harmful content, in force in selected European Union countries. Coordination in defining illegal content and digital content in the context of cross-border digital services is becoming particularly important following the entry into force of the Digital Services Act*

**Material and methods:** *Comparative method – EU countries: Germany, France, Poland*

**Results:** *Differences in the understanding of the definition of illegal content may negatively impact the coordination of combating it, not only at the level of relations between the EU and platforms and social media (BIG TECHY) but also at the level of EU Member States.*

**Conclusions:** *Taking into account the cross-border nature of digital services and combating illegal or harmful content in these services becomes problematic given the fundamental differences in the definitional approaches in the various legislations of EU Member States, not just in the regulatory framework of relations between the EU and BIG TECHY. These differences may pose a fundamental challenge to building a unified and secure digital services market.*

**KEYWORDS:** *media, digital services, illegal content, digital services act, harmful content*

**ABSTRAKT**

**Cel pracy:** *Artykuł stanowi przegląd regulacji związanych z procesem zwalczania treści nielegalnych i szkodliwych, obowiązujących w wybranych krajach Unii Europejskiej. Koordynacja w definiowaniu treści nielegalnych oraz treści cyfrowych w warunkach transgraniczności usług cyfrowych w związku z wejściem życie rozporządzenia Digital Services Act nabiera szczególnego znaczenia*

**Materiał i metody:** *Metoda porównawcza – kraje UE: Niemcy, Francja, Polska*

**Wyniki:** *Różnice w pojmowaniu przede wszystkim definicji treści nielegalnych mogą wpływać negatywnie na koordynację ich zwalczania nie tylko na poziomie relacji UE a platformy i media społecznościowe ( BIG TECHY) ale także na poziomie państw członkowskich UE*

**Wnioski:** *Problematyczne staje się uwzględnienie aspektu transgraniczności usług cyfrowych i zwalczanie treści nielegalnych czy szkodliwych*

*w tych usługach w sytuacji zasadniczych różnic w podejście definicyjnym w różnych ustawodawstwach samych państw członkowskich UE a nie tylko w uwarunkowaniach regulacyjnych w relacjach UE I BIG Techy. Te różnice mogą stanowić zasadniczy problem budowania jednolitego i bezpiecznego rynku usług cyfrowych.*

**SŁOWA KLUCZOWE:** *media, usługi cyfrowe, treści nielegalne, akt o usługach cyfrowych, treści szkodliwe*

Procesy konwergencji różnych obszarów naszego funkcjonowania przyczyniły się do powstania szczególnego rodzaju konfliktu w obszarze ustaleń co do zakresu i poziomu nowych regulacji, zwłaszcza w odniesieniu do treści cyfrowych, gdzie najczęściej zagadnień dotyka kwestii nowych mediów i nowych technologii, również w sferze odpowiedzialności dostawców usług cyfrowych. Pojawiają się nowe modele zarządzania treściami, wspomagane przez nowe zasady wirtualnej organizacji rynku cyfrowego. Zmiana technologii komunikowania zasadniczo zmieniła zasady funkcjonowania jednostek i całych społeczności. Z jednej strony otwarta i wolna cyberprzestrzeń pozwala na wymianę kultur i doświadczeń między państwami, społecznościami i obywatelami, umożliwiając interakcję oraz wymianę treści, a w konsekwencji wiedzy, doświadczeń i technologii. Z drugiej strony otwartość ta wyzwała aktywność wkraczającą w obszar praw i wolności jednostki – użytkownika sieci. W szczególności dotyczy to zawartości sieci – treści cyfrowych. Artykuł stanowi przegląd regulacji związanych z procesem zwalczania treści nielegalnych i szkodliwych, obowiązujących w wybranych krajach Unii Europejskiej. Koordynacja w definiowaniu treści nielegalnych oraz treści cyfrowych w warunkach transgraniczności usług cyfrowych w związku z wejściem życie rozporządzenia Digital Services Act w 2024 r. (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (ustawa o usługach cyfrowych) (Tekst mający znaczenie dla EOG) PE/30/2022/REV/1 Dz.U. L 277 z 27.10.2022, s. 1–102, DSA) obecnie nabiera szczególnego znaczenia.

## WPROWADZENIE

Jednym z kluczowych celów w egzekwowaniu przepisów prawa i zwalczania cyberzagrożeń stała się regulacja dotycząca kwestii odpowiedzialności za działania w sieci. Nowe sposoby świadczenia usług w sieci spowodowały powstanie zupełnie nowych rodzajów podmiotów świadczących te usługi: dostawców internetu, dostawców hostingu, operatorów platform internetowych, w tym dostawców treści cyfrowych, którzy na gruncie nowych regulacji stają się odpowiedzialni za działania w sieci, także w kontekście zwalczania treści nielegalnych czy szkodliwych. W nowym ekosystemie regulacji świadczenia usług w obszarze e-commerce pojawił się także problem ustalenia działań operacyjnych i odpowiednich procedur oraz koordynacji w zakresie odpowiedzialności.

Nowy ład technologiczny stanowi przesłankę i zarazem przedmiot omawianych zmian, które wpływają zasadniczo na bardzo ważny obszar, jakim jest cyberprzestrzeń oraz media cyfrowe, których podstawą funkcjonowania jest wolność słowa. Trzeba tu jednak podkreślić, że kwestia ograniczeń w obszarze wolności słowa to w warunkach demokratycznych decyzje o ingerencji w treści organizacji religijnych, właścicieli mediów, ugrupowań politycznych i różnych grup społecznych, które przyjmują ściśle określony sposób myślenia, co media cyfrowe wspomagają, zamykając użytkownika sieci w tzw. bańce ideowej. Problem ograniczeń regulacyjnych dotyczy nie tylko dostarczania określonych treści użytkownikom sieci, lecz także udostępniania treści cyfrowych przez samych użytkowników. Należy mieć tu na uwadze słowa filozofki Onory O'Neill, iż *nasze media powinny być nie tylko dostępne (accessible), ale i możliwe do oceniania (assessable)* (Garton, 2018, s. 301). *Chociaż, jak podkreśla T. Garton Ash, „Bogiem a prawdą, najbardziej skutecznym ograniczeniem mediów powinniśmy być my sami – czytelnicy, widzowie i użytkownicy* (Garton, 2018, s. 379). Nakazy blokujące, wynikające z DSA, pozwalają zmniejszyć skalę nielegalnej działalności w sieci. Wykorzystują one fakt, że dostawcy usług cyfrowych – pośrednicy mają praktyczne narzędzia do uniemożliwienia dalszego naruszenia przepisów prawa (por. Savin, 2021). Nowy system *notice and take action* wprowadza wymóg proaktywności ze strony dostawców usług cyfrowych w zakresie identyfikacji treści nielegalnych i szkodliwych, w tym automatycznego ich wykrywania. Mówimy o tzw. moderowaniu treści.

W tych warunkach kluczowe staje się ustalenie, czym jest treść nielegalna czy też szkodliwa. W konsekwencji zmian zaproponowanych w DSA niezbędne stały się zmiany związane z procesem wdrażania procedur, w szczególności dotyczących zwalczania nielegalnych treści w sieci, co odnosi się bezpośrednio do kwestii definiowania samej treści nielegalnej, ale także ustalenia systemu organizatorskiego instytucji odpowiedzialnych za egzekwowanie prawa.

## TREŚCI NIELEGALNE

Rozporządzenie DSA bazuje na zaleceniu z 2018 r. dotyczącym nielegalnych treści (Zalecenie Komisji z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (C(2018) 1177 final). W rozporządzeniu uwzględnia się doświadczenia zdobyte w ramach działań samoregulacyjnych prowadzonych przy wsparciu Komisji Europejskiej, takich jak system dobrowolnych zobowiązań do zapewnienia bezpieczeństwa produktów (Product Safety Pledge), protokół ustaleń w sprawie sprzedaży podróżniczych towarów w internecie, decyzji ramowej Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych, kodeks postępowania dotyczący nielegalnego nawoływania do nienawiści w internecie oraz Forum UE ds. Internetu w odniesieniu do treści o charakterze terrorystycznym. W samym tekście DSA nie zdefiniowano szczegółowo, czym jest *treść nielegalna*. Zgodnie z art. 3 lit. h tego rozporządzenia *nielegalne treści* oznaczają informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa. To oznacza, że ustalenie, czy dana treść jest nielegalna, ma być determinowane przez przyjęty w danym państwie członkowskim system rozwiązań prawnych podyktowanych także wspólnymi zakresami takiego definiowania, które zostało przeprowadzone np. na gruncie przepisów dyrektywy o audiowizualnych usługach medialnych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1808 z dnia 14 listopada 2018 r. zmieniająca dyrektywę 2010/13/UE w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw

członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) w związku ze zmieniającą się sytuacją rynkową, Dz.U. L 303 z 28.11.2018, s. 69–92 oraz dyrektywy o prawie autorskim i prawach pokrewnych na jednolitym rynku cyfrowym (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie praw autorskich i praw pokrewnych na jednolitym rynku cyfrowym, Dz.U. L 130 z 17.05.2019, s. 92–125).

## FRANCJA

Francuski ustawodawca przekazał ocenę przestrzegania obowiązków i elementów je warunkujących, takich jak m.in. dostępność środków blokowania, o których mowa w DSA, niezależnemu organowi publicznemu. Wdrożenie DSA nadzoruje francuski Urząd Regulacji Komunikacji Audiowizualnej i Cyfrowej (Autorité de Régulation de la Communication Audiovisuelle et Numérique ARCOM). Dodatkowo w dniu 3 stycznia 2025 r. Francuski Urząd ds. Konkurencji i Konsumentów (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes, DGCCRF) został oficjalnie wyznaczony na organ odpowiedzialny za nadzór i egzekwowanie DSA, a francuskiemu koordynatorowi ds. usług cyfrowych (ARCOM) przyznano uprawnienia dochodzeniowe. W dniu 1 stycznia 2025 r. weszła w życie ustawa z 21 maja 2024 r. o zabezpieczeniu i regulacji przestrzeni cyfrowej (Loi nr 2024-449 (SREN). Journal Officiel de la République Française (JORF nr 0117 z dnia 22 maja 2024 r.). Celem ustawy jest transpozycja obowiązków określonych w DSA i w ustawie o rynkach cyfrowych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie konkurencyjnych i uczciwych rynków w sektorze cyfrowym oraz zmieniające dyrektywy (UE) 2019/1937 i (UE) 2020/1828 PE/17/2022/REV/1 Dz.U. L 265 z 12.10.2022, s. 1–66 (DMA)) w celu dostosowania przepisów krajowych do tych regulacji. Ustawa SREN ma na celu wzmocnienie ochrony obywateli, a w szczególności nieletnich, przed zagrożeniami online. Jej główne środki obejmują ochronę dzieci przed pornografią i cyberprzemocą, utworzenie filtra antyscam, zaostrezenie kar dla cyberprzemocowców. Zgodnie z ustawą ma zostać utworzony filtr cyberbezpieczeństwa poprzez zaprojektowanie bazy

danych zawierającej zgłoszone złośliwe strony internetowe zidentyfikowane przez ofiary i zgłoszone organom administracyjnym. Strony, których dotyczy skarga, będą miały pięciodniowy okres karencji na zakwestionowanie ich klasyfikacji jako złośliwej, pod warunkiem że możliwe będzie skontaktowanie się z właścicielem strony. Obywatele Francji próbujący uzyskać dostęp do takich złośliwych stron internetowych otrzymają komunikat ostrzegawczy. Ponadto ustawa nakłada na dostawców usług hostingowych obowiązek usuwania wszelkich niezgodnych z prawem treści pornograficznych, w szczególności pornografii dziecięcej, w ciągu 24 godzin od powiadomienia przez francuskie organy policji ( art. 3-I SREN).

Artykuł 10 ustawy z dnia 21 czerwca 2004 r. o zaufaniu do gospodarki cyfrowej (Loi nr 2004-575 LCENJORF z dnia 22 czerwca 2004 r.) – ustawa ustanawia wymogi prawne dotyczące przejrzystości, moderowania treści, odpowiedzialności dostawców usług oraz obowiązku ujawniania informacji przez operatorów stron internetowych. Głównym celem jest pomoc użytkownikom internetu w identyfikacji i dotarciu do wydawcy strony internetowej, zwłaszcza gdy strona służy celom komercyjnym) – brzmi następująco: *Urząd Regulacji Komunikacji Audiowizualnej i Cyfrowej zapewnia, że treści pornograficzne udostępniane publicznie przez dostawcę usług komunikacji publicznej online, na jego odpowiedzialność redakcyjną, lub dostarczane za pośrednictwem platformy udostępniania wideo, zgodnie z definicją zawartą w artykule 2 ustawy z dnia 30 września 1986 r. o wolności komunikacji, nie są dostępne dla osób nieletnich (Loi nr 86-1067 z dnia 30 września 1986 Loi LéotardJORF z dnia 1 października 1986).* Zgodnie z art. 6-2-1.-I. *Nieusunięcie przez dostawców usług hostingowych obrazów lub wizerunków osób nieletnich o charakterze pornograficznym, w rozumieniu art. 227-23 Kodeksu karnego, w ciągu dwudziestu czterech godzin od otrzymania żądania usunięcia, o którym mowa w art. 6-1 niniejszej ustawy, podlega karze jednego roku pozbawienia wolności i grzywny w wysokości 250 000 euro.*

Zgodnie z ustawą SREN zmienia się postanowienia Kodeksu karnego, przyjmując, iż sąd może orzec, jako karę dodatkową, zawieszenie kont dostępu do usług online, które posłużyły do popełnienia przestępstwa. Regulacja ta ma zastosowanie do kont dostępu do usług platformy online, zgodnie z definicją zawartą w par. 4 pkt I art. 6 ustawy o zaufaniu do gospodarki cyfrowej.

Zawieszenie stosuje się na okres maksymalnie sześciu miesięcy; okres ten ulega przedłużeniu do jednego roku w przypadku recydywy.

W systemie prawa francuskiego przewiduje się rozszerzenia uprawnień Centralnego Biura ds. Zwalczania Przeszłości Związanej z Technologiami Informacyjno-Komunikacyjnymi, zgodnie z procedurą przewidzianą w art. 6-1 ustawy o zaufaniu do gospodarki cyfrowej, w zakresie usuwania treści przedstawiających niehumanitarne i poniżające traktowanie, gwałt i sytuacje kazirodztwa.

Treść uznaje się za nielegalną, jeżeli można ją porównać z jednym z następujących przestępstw: terroryzm, pornografia dziecięca (przemoc seksualna wobec nieletnich), handel narkotykami, dyskryminacja, podżeganie do przestępstwa (przykład: podżeganie do popełnienia morderstwa, kradzieży lub napaści seksualnej), propaganda, radykalizacja, groźby lub nawoływanie do przemocy, rozpowszechnianie obrazów przedstawiających tortury i akty barbarzyństwa, pedofilia, pornografia dziecięca, składanie propozycji seksualnej osobie nieletniej przez internet, podżeganie do nienawiści, nawoływanie do nienawiści ze względu na pochodzenie, płeć, orientację seksualną lub niepełnosprawność, handel ludźmi, wykorzystywanie w celach seksualnych, ekonomicznych, akty okrucieństwa wobec zwierząt, nękanie w internecie, narażanie ludzi na niebezpieczeństwo, bezpośrednie ryzyko utraty życia, treści związane z samobójstwem.

Kwestie treści nielegalnych reguluje francuski Kodeks karny (Code penal, [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006070719/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/)). Sprawcą może być jedna z następujących osób: twórca stron internetowych, twórca bloga, reżyser wideo, fotograf, autor komentarza, autor prywatnej wiadomości. Autorowi nielegalnych treści publikowanych w internecie grozi dodatkowa kara w postaci zakazu korzystania z platformy internetowej. Natychmiast po otrzymaniu informacji o zakazie, dostawcy usług internetowych (np. Orange, SFR itp.) muszą zablokować konta sprawcy i uniemożliwić mu tworzenie nowych. Blokada obowiązuje maksymalnie przez sześć miesięcy. Okres ten może zostać przedłużony do roku w przypadku recydywy. Dodatkowo osoba mająca dostęp do usług komunikacji publicznej online ma obowiązek zapewnić, że dostęp ten nie będzie wykorzystywany w celu reprodukcji, przedstawiania, udostępniania lub komunikowania publicznie utworów lub innych przedmiotów chronionych prawem autorskim lub prawami pokrewnymi bez

zezwoleń posiadaczy praw. Warto podkreślić, że ujawnienie opinii publicznej lub osobom trzecim, w jakikolwiek sposób, montażu o charakterze seksualnym, stworzonego z wykorzystaniem słów lub wizerunku osoby bez jej zgody, podlega karze dwóch lat pozbawienia wolności i grzywnie w wysokości 60 000 euro. Ujawnienie opinii publicznej lub osobom trzecim, w jakikolwiek sposób, treści wizualnych lub dźwiękowych o charakterze seksualnym, wygenerowanych w wyniku przetwarzania algorytmicznego, oraz powielających wizerunek lub słowa osoby bez jej zgody, jest równoznaczne z przestępstwem i podlega takim samym karom. Jeżeli przestępstwo zostało popełnione za pośrednictwem mediów drukowanych lub nadawczych, do ustalenia osób odpowiedzialnych stosuje się przepisy szczególne regulujące te kwestie. Kary ulegają podwyższeniu do trzech lat pozbawienia wolności i grzywny w wysokości 75 000 euro, jeżeli publikacja zmontowanego filmu lub treści wygenerowanych w wyniku przetwarzania algorytmicznego została dokonana za pośrednictwem internetowej usługi komunikacji publicznej.

Ustawa z dnia 7 lipca 2023 r. mająca na celu ustanowienie większości cyfrowej i zwalczanie nienawiści w internecie (Loi nr 2023-566, JORF z dnia 8 lipca 2023 r.) ustanawia pełnoletność cyfrową i nakłada na dostawców usług mediów społecznościowych, wszelkich platform umożliwiających użytkownikom końcowym łączenie się i komunikację ze sobą, udostępnianie treści oraz odkrywanie innych użytkowników i treści na wielu urządzeniach, w szczególności poprzez rozmowy online, posty, filmy i rekomendacje, obowiązek weryfikacji wieku każdego nowego użytkownika zakładającego konto w ich serwisach, jak również wieku użytkowników już istniejących. Dostęp do serwisu mediów społecznościowych jest zabroniony osobom poniżej 15. roku życia, chyba że dostawca uzyskał wyraźną zgodę jednego z opiekunów prawnych osoby małoletniej. Chociaż ustawa ta została uchwalona przez parlament francuski, jej wejście w życie było uzależnione od wydania dekretu wykonawczego, który nigdy nie został opublikowany. W rezultacie obowiązki te nie są obecnie egzekwowane we Francji. Nieprzestrzeganie przepisów może skutkować grzywną w wysokości do 1% globalnego rocznego obrotu. Wejście w życie ustawy nastąpi na podstawie dekretu prezydenckiego.

Z kolei ustawa SREN wymaga od dostawców platform udostępniających filmy pornograficzne i wydawców stron internetowych z pornografią wdrożenia

systemu weryfikacji wieku zgodnego z ramami technicznymi określonymi przez ARCOM, którego celem jest uniemożliwienie osobom nieletnim dostępu do takich treści. Już przed 2024 r. francuski kodeks karny zabraniał rozpowszechniania treści pornograficznych, jeśli istniało prawdopodobieństwo, że będą one widoczne lub oglądane przez osoby nieletnie. Ustawa stanowiła, że samo oświadczenie o wieku użytkownika jest niewystarczające, co w praktyce nakładało na każdą osobę rozpowszechniającą treści pornograficzne obowiązek wdrożenia mechanizmu weryfikacji wieku. Ustawa SREN wymaga, aby mechanizmy weryfikacji wieku spełniały minimalne standardy techniczne określone przez ARCOM. Obecnie ARCOM ma możliwość wydawania formalnych wezwań i nakładania sankcji na dostawców usług niespełniających wymogów (do 150 000 EUR lub 2% globalnego rocznego obrotu oraz 300 000 EUR lub 4% w przypadku powtarzających się naruszeń). ARCOM może również żądać zablokowania lub usunięcia z listy stron internetowych i platform niespełniających wymogów przez dostawców usług pośredniczących, takich jak dostawcy usług internetowych, dostawcy rozwiązań nazw domen lub wyszukiwarki.

Obowiązki weryfikacji wieku wynikające z ustawy SREN mają zastosowanie do dostawców z siedzibą we Francji lub poza Unią Europejską. Rozporządzenie wykonawcze z 26 lutego 2025 r. wskazuje 17 stron internetowych z pornografią i platform do udostępniania takich treści. Niektórzy dostawcy wnieśli odwołania od tego rozporządzenia. Niektóre platformy wycofały się z rynku francuskiego, protestując przeciwko nieskuteczności systemu i naruszaniu prywatności użytkowników.

Jednym z innowacyjnych aspektów SREN jest regulacja gier z obiektami cyfrowymi podlegającymi monetyzacji. Gry te, często nazywane grami typu *play-to-earn* lub *blockchain games* pozwalają m.in. kupować obiekty cyfrowe, które można wymienić na prawdziwe pieniądze. Ustawa o SREN wprowadza surowe przepisy regulujące te praktyki, mające na celu zapobieganie ryzyku oszustw, prania pieniędzy i wykorzystywania graczy. Twórcy gier muszą wdrożyć przejrzyste mechanizmy zarządzania i wymiany tych obiektów cyfrowych, zapewnić ochronę danych użytkowników oraz przestrzegać standardów przejrzystości finansowej.

W konsekwencji uchwalenie SREN doprowadziło do eskalacji napięć między rządem francuskim a Komisją Europejską. Konflikt ten osiągnął punkt

kulminacyjny wraz ze szczegółową opinią Komisji wydaną 25 października 2023 r. (w ramach procedury na podstawie: Akcepta (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udostępniania informacji w przepisach technicznych oraz zasadach dotyczących usług informacyjnych (tekst jednolity) (Tekst mający znaczenie dla EOG) Dz.U. L 241 z 17.09.2015, s. 1).

Po pierwsze, Komisja podkreśliła, że DSA ma bezpośrednie zastosowanie i nie wymaga uchwalania transpozycji ani dostosowania przepisów. Po drugie, Komisja zidentyfikowała niespójności między przepisami francuskimi a DSA. Jeśli chodzi o przepisy mające zastosowanie do wszystkich przedsiębiorstw społeczeństwa informacyjnego, Komisja podkreśliła, że art. 3 ust. 1 i 2 DMA wprowadza *zasadę kontroli w państwie członkowskim macierzystym*. Zasada ta nakazuje, aby regulacja usług społeczeństwa informacyjnego podlegała jurysdykcji kraju, w którym dostawcy usług mają siedzibę, a zatem podlegała ramom prawnym tego państwa członkowskiego. Jednakże uprawnienie przyznane ARCOM na mocy ustawy SREN do wydawania nakazów przeciwko wszelkim podmiotom świadczącym usługi we Francji stoi w sprzeczności z tą zasadą. Komisja Europejska podkreśliła również, że rząd francuski jest uprawniony do wydawania nakazów podmiotom z siedzibą poza Francją, zgodnie z art. 3 ust. 4 DMA. Przepis ten pozwala państwom członkowskim na podejmowanie działań przeciwko podmiotom z siedzibą w innym państwie członkowskim, pod warunkiem spełnienia trzech określonych warunków: środki te muszą być niezbędne do realizacji celów polityki publicznej, ochrony zdrowia publicznego, zapewnienia bezpieczeństwa publicznego lub ochrony konsumentów. Podmiot taki musi naruszyć cele określone w DMA lub stwarzać znaczne i poważne ryzyko naruszenia tych celów, przy czym podejmowane działania muszą być odpowiednie do osiągnięcia zamierzonego celu. Francuskie przepisy wykraczają poza obowiązki wskazane zarówno w DSA, jak i DMA, w szczególności w przypadku określania tożsamości cyfrowej we Francji. Jean Noël Barrot, były minister ds. cyfryzacji we Francji, scharakteryzował ustawę SREN jako próbę *pójścia o krok dalej* niż DSA, a nie jedynie jako środek wdrażania i egzekwowania unijnego rozporządzenia.

## NIEMCY

Niemiecka ustawa *Netzwerkdurchsetzungsgesetz (NetzDG)* o egzekwowaniu prawa w sieciach społecznościowych z dnia 1 października 2017 r. (BGBl, 2017, s. 3352), ostatnio zmieniona art.29 ustawy z dnia 6 maja 2024 r. (BGBl, 2024 I, s. 149) jako pierwsza miała na celu zwalczanie mowy nienawiści i fałszywych wiadomości. W szczególności katalog zawarty w art. 1 (3) nadał nowy system zwalczania przestępstw, które dotyczą wolności słowa, sztuki i nauki, wolności osobistych i godności ludzkiej oraz wolności wyznania i sumienia. W rezultacie prywatni dostawcy mediów społecznościowych zostali obarczeni odpowiedzialnością za naruszenia praw człowieka i podstawowych wolności, stając się strażnikami świata cyfrowego. Podobne cele określały nowelizacje: ustawa o zwalczaniu ekstremizmu prawicowego i przestępstw z nienawiści z dnia 30 marca 2021 r., (BGBl.I, s. 441, nr 13); ostatnio zmieniona art. 3 ustawy z dnia 3 czerwca 2021 r. (ReHaKrBG) oraz ustawa o zmianie ustawy o egzekwowaniu prawa w sieciach społecznościowych *Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes* z dnia 3 czerwca 2021 r. (BGBl. I, s. 1436); *Geltung* z dnia 28 czerwca 2021 r., (*NetzDGÄndG*).

Ustawa *NetzDG* odwołuje się, podobnie jak francuska *SREN* do definicji treści nielegalnych, do Kodeksu karnego. W rozumieniu tej ustawy jest to treść, która wypełnia znamiona przestępstwa określonego w art. 86, 86a, 89a, 91, 100a, 111, 126, 129–129b, 130, 131, 140, 166, 184b, 185–187, 189, 201a, 241 lub 269 Kodeksu karnego i nie jest usprawiedliwiona. Ustawę stosuje się do dostawców usług cyfrowych, którzy prowadzą w internecie platformy w celach zarobkowych, umożliwiające użytkownikom dzielenie się treściami z innymi użytkownikami lub ich publiczne udostępnianie (obejmuje to także sieci społecznościowe). Platformy zawierające treści dziennikarskie lub redakcyjne, za które odpowiedzialność ponosi dostawca usługi, nie są uważane za sieci społecznościowe w rozumieniu tej ustawy. To samo dotyczy platform przeznaczonych do indywidualnej komunikacji. Na temat nowych obowiązków platform (por. Kraski, 2017; Guggenberger, 2017; Liesching, 2018; Kalscheuer, Hornung, 2017; Löber, Roßnagel, 2019).

W Niemczech DSA został wdrożony za pośrednictwem ustawy o usługach cyfrowych z dnia 6 maja 2024 r. (BGBl. 2024 I, poz. 149) (*Digitale Dienste*

Gesetz (DDG), która powołuje Federalną Agencję Sieci (Bundesnetzagentur /BNetzA). Niemcy wprowadziły ustawę, gdzie organ nadzoru w usługach cyfrowych BNetzA współpracuje z naukowcami, branżą i organizacjami społecznymi, co przekłada się na konsensualne podejście do egzekwowania prawa oraz poprawę procedur zgłaszania nielegalnych treści. Niemieckie Centrum Informacji i Wolności Informacji (DSC). Federalna Agencja Sieci (DSC) jest centralnym organem koordynującym egzekwowanie ustawy DSA w Niemczech. DSC monitoruje dostawców usług i platformy internetowe pod kątem przestrzegania ich obowiązków, pełni funkcję centralnego punktu rozpatrywania skarg użytkowników w przypadku naruszenia ustawy DSA oraz koordynuje współpracę między właściwymi organami w Niemczech i UE. DSC certyfikuje pozasądowe organy rozstrzygania sporów oraz zaufane podmioty zgłaszające. Na żądanie DSC może udzielić zweryfikowanym badaczom dostępu do danych bardzo dużych platform internetowych i wyszukiwarek. Pracę DSC wspierają Federalna Agencja ds. Ochrony Dzieci i Młodzieży w Mediach (BzKJ) (Struckmeyer, 2025), Urząd ds. Mediów Nadrenii Północnej-Westfalii koordynujący działania organów odpowiedzialnych za monitorowanie mediów oraz Federalny Komisarz ds. Ochrony Danych i Wolności Informacji (BfDI). Zgodnie z § 1 (2) DDG wymagania dotyczące treści i różnorodności usług cyfrowych oraz właściwe organy nadzoru określają przepisy prawa medialnego krajów związkowych.

Agencje rządowe, takie jak Federalny Departament ds. Mediów Szkodliwych dla Młodzieży oraz Federalny Komisarz ds. Ochrony Danych i Wolności Informacji, ściśle współpracują z BNetzA. Jedną z kluczowych innowacji w niemieckim systemie jest Rada Doradcza, niezależny organ ekspertów, który wspiera BNetzA w realizacji jej zadań i służy jako forum dyskusji ze środowiskiem akademickim, stowarzyszeniami branżowymi i społeczeństwem obywatelskim. Rada Doradcza Koordynatora ds. Usług Cyfrowych to niezależny organ ekspertów, który wspiera DSC w realizacji jego zadań i pełni funkcję łącznika między DSC a środowiskiem akademickim i rynkiem. Członkowie Rady Doradczej zostali nominowani przez niemiecki Bundestag i powołani do grona ekspertów przez Federalne Ministerstwo Gospodarki i Działań na rzecz Klimatu, w porozumieniu z Federalnym Ministerstwem Cyfryzacji i Transportu. Rada Doradcza składa się z przedstawicieli środowiska

akademickiego, stowarzyszeń branżowych i organizacji społeczeństwa obywatelskiego. Formułuje ogólne zalecenia dotyczące skutecznego i jednolitego wdrażania DSA oraz przedstawia DSC i innym właściwym organom kwestie naukowe, w szczególności dotyczące przetwarzania danych. Rada Doradcza co roku składa Bundestagowi sprawozdanie ze swojej działalności i współpracy z DSC i innymi właściwymi organami.

Istotny dla ustalenia nielegalności treści jest także Federalny Urząd Policji Kryminalnej (BKA), który otrzymuje zgłoszenia o podejrzeniach popełnienia przestępstw online i bada nielegalność treści. Centralne Biuro Zgłaszania Treści Kryminalnych w Internecie (ZMI BKA) rozpoczęło działalność 1 lutego 2022 r. Współpraca ta ma na celu przeciwdziałanie rosnącej wulgarności komunikacji w mediach społecznościowych oraz umożliwienie skutecznego ścigania popełnianych tam przestępstw, takich jak przestępstwa propagandowe, podżeganie do nienawiści i groźby. W tym celu połączono centralnie części zdecentralizowanych struktur zgłoszeniowych, które już istniały w krajach związkowych, powołane w celu zwalczania mowy nienawiści i podżegania do nienawiści w internecie. Kluczowa debata koncentrowała się na tym, czy zaufani sygnaliści powinni mieć prawo do zgłaszania treści wykraczających poza to, co jest uznawane za *nielegalne* w świetle prawa krajowego. Na przykład jeśli przepisy danego kraju dotyczące mowy nienawiści nie uwzględniają kwestii płci jako kategorii chronionej, zaufani sygnaliści mogą nie mieć możliwości zgłaszania takich treści.

Zgodnie z § 8 (1) DDG, jeżeli usługa cyfrowa polegająca na przesyłaniu informacji dostarczonych przez użytkownika za pośrednictwem sieci komunikacyjnej lub zapewnianiu dostępu do sieci komunikacyjnej została wykorzystana przez użytkownika do naruszenia praw własności intelektualnej innej osoby, a właściciel prawa nie dysponuje innymi środkami zaradczymi w związku z naruszeniem, może on żądać od właściwego dostawcy usług zablokowania korzystania z informacji w celu zapobieżenia powtórzeniu się naruszenia. Procedurę stosuje się również w przypadku, gdy usługa jest świadczona bezpłatnie lub przez podmioty publiczne. Obowiązki usuwania informacji lub blokowania korzystania z informacji wynikające z przepisów prawa powszechnego na podstawie nakazów sądowych lub administracyjnych pozostają nienaruszone nawet w przypadku ograniczonej odpowiedzialności usługodawcy zgodnie z art. 4–6 rozporządzenia DSA.

Obowiązki sieci społecznościowych wynikające z ustawy NetzDG, jeśli chodzi o określoną procedurę składania skarg, odnoszą się wyłącznie do treści niezgodnych z prawem. Obejmuje to treści podlegające zaskarżeniu na podstawie określonych przepisów wymienionych w niemieckim kodeksie karnym, np. używanie symboli organizacji niekonstytucyjnych, tworzenie organizacji terrorystycznych, podżeganie mas, w tym negowanie Holokaustu, pornografia dziecięca, zniewaga, złośliwe plotki, zniesławienie, naruszenie intymnej prywatności poprzez robienie zdjęć lub innych obrazów oraz groźenie popełnieniem poważnego przestępstwa. Jak wskazuje Patrick Zurth (Zurth, 2021), nie wszystko, co można by nazwać mową nienawiści lub fake newsami, mieści się w zakresie ustawy NetzDG. W związku z tym, szczególnie w walce z fake newsami, od samego początku było jasne, że ustawa NetzDG może wnieść jedynie ograniczoną regulację. W przypadku fałszywego stwierdzenia faktu nie jest karalne ono samo w sobie, ale podlega oskarżeniu jedynie w bardzo szczególnych okolicznościach. Co więcej, autor podkreśla, iż obowiązki platform w zakresie usuwania i blokowania treści wynikają z ogólnych zasad prawnych, a ustawa NetzDG ma jedynie regulować praktyczne egzekwowanie (tj. samą procedurę). Zatem ustawa NetzDG „nie wprowadza nowego systemu odpowiedzialności ani nie czyni nielegalnym wcześniej już ustalonych jako nielegalne wypowiedzi. W konsekwencji, w przypadku przestępstw bez naruszenia dóbr osobistych (np. używanie symboli organizacji niekonstytucyjnych), nie ma roszczenia o usunięcie lub zablokowanie treści. Jednak w przypadku nieusunięcia nielegalnych treści mogą także nastąpić potencjalne konsekwencje prawne w postaci grzywnien.

Z kolei Federalna Agencja ds. Ochrony Dzieci i Młodzieży w Mediach jest właściwym organem do egzekwowania strukturalnych środków ostrożności zgodnie z art. 28 ust. 1 DSA, o ile nie dotyczą one środków przewidzianych w porozumieniu międzykrajowym o ochronie młodzieży w mediach w brzmieniu z dnia 14 grudnia 2021 r. Właściwymi organami w tym zakresie pozostają organy wyznaczone na mocy przepisów prawa medialnego krajów związkowych. W celu egzekwowania i monitorowania rozporządzenia DSA w ramach Federalnej Agencji ds. Ochrony Dzieci i Młodzieży w Mediach utworzono jednostkę ds. egzekwowania praw dziecka w usługach cyfrowych z siedzibą w Bonn. W Niemczech do najważniejszych regulacji normatywnych mających

na celu ochronę małoletnich przed nielegalnymi i szkodliwymi dla rozwoju treściami należy zaliczyć ustawę o ochronie małoletnich (Jugendschutzgesetz) z dnia 23 lipca 2002 r. (BGBl. 2002 I, s. 2730) oraz traktat między krajami związkowymi dotyczący ochrony godności ludzkiej i ochrony małoletniego w radiu, telewizji oraz telemediach (Jugendmedienschutz-Staatsvertrag – JMStV). Regulacje te stanowią podstawę niemieckiego systemu ochrony młodzieży w internecie i uzupełniają przepisy o ochronie małoletnich (JuSchG), które regulują kwestie związane także z gramami i filmami online. Ustawa JMStV chroni osoby niepełnoletnie przed szkodliwymi treściami online poprzez ograniczenia treści, techniczne środki ochrony, oznakowanie i przepisy dotyczące reklam (Siwicki, 2011, s. 80–129), (Struckmeyer, 2024).

Jak zauważa Kate Klonick (Klonick, 2020), każda proponowana regulacja powinna działać ze zrozumieniem skomplikowanej struktury samoregulacyjnej, która już istnieje, aby być skuteczniejszą dla użytkowników i zachować demokratyzującą moc funkcjonowania platform internetowych.

## POLSKA

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2024. 1513 z późn. zm. USUDE) stała się właściwym aktem, w ramach którego powinna zostać wdrożona część (podlegających transpozycji) przepisów DSA. Jest to ustawa, która implementuje do krajowego porządku prawnego dyrektywę 2000/31/WE (Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w wydaniu prawnym usług informacyjnych, w wydaniu elektronicznym w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) Dz.U. L 178 z 17.07.2000, s. 1–16), zmienianą i uzupełnianą poprzez przedmiotowe rozporządzenie. Zgodnie z projektem ustawy nowelizującej USUDE kompetencje w zakresie koordynacji, o której mowa w przepisach DSA mają zostać przekazane Prezesowi Urzędu Komunikacji Elektronicznej (UKE). Tym samym to Prezes UKE jako organ podległy administracji rządowej – bezpośrednio – ma pełnić funkcję koordynatora do spraw usług cyfrowych. Wskazanie Prezesa UKE jako właściwego organu sprawującego nadzór nad stosowaniem przepisów DSA wraz z wejściem w życie ustawy nowelizującej rozszerza obowiązki koordynatora

ds. usług cyfrowych wskazane w rozporządzeniu DSA m.in. o konieczność prowadzenia nadzoru nad treściami nielegalnymi w mediach społecznościowych, nakładanie administracyjnych kar pieniężnych, współpracę z koordynatorami innych państw członkowskich oraz z Radą Usług Cyfrowych i Komisją Europejską. Kluczowa jest zmiana dotycząca organów właściwych, tzn. wskazanie Prezesa Urzędu Ochrony Konkurencji i Konsumentów oraz Krajowej Rady Radiofonii i Telewizji (KRRiT) konstytucyjnego organu kontroli Państwa jako organów właściwych, sprawujących nadzór nad stosowaniem przepisów DSA w zakresie swojej właściwości, określonej przepisami projektu ustawy. Kwestia ww. nadzoru budzi pewne zastrzeżenia w świetle motywu 112 DSA, zgodnie z którym *właściwe organy wyznaczone na podstawie niniejszego rozporządzenia powinny również działać w pełni niezależnie od podmiotów prywatnych i publicznych, bez obowiązku lub możliwości zwracania się, między innymi do rządu, o instrukcje, lub ich otrzymywania oraz bez uszczerbku dla szczególnych obowiązków w zakresie współpracy z innymi właściwymi organami, koordynatorami ds. usług cyfrowych, Radą Usług Cyfrowych i Komisją.*

Projekt ustawy uprawnia prokuratora, policję, usługobiorcę oraz zaufany podmiot sygnalizujący do złożenia wniosku o wydanie nakazu podjęcia działań przeciwko nielegalnym treściom polegającego na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich. Zmiana polityki regulacyjnej w przedmiotowym zakresie daje możliwości koordynacji działań związanych ze zwalczaniem treści nielegalnych, które wynikają z innych ustaw – w przypadku KRRiT ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji (Dz.U.2022.1722 z późn. zm.). Podział obowiązków pomiędzy wyznaczone organy powinien być jasno wskazany i opisany w przepisach znowelizowanej USUDE, co pozwoliłoby uniknąć wątpliwości interpretacyjnych, ewentualnych sporów kompetencyjnych pomiędzy organami oraz ograniczyć ryzyka dla uczestników rynku. Zgodnie z art. 11 a prokurator, policja, usługobiorca lub zaufany podmiot sygnalizujący może złożyć wniosek o wydanie nakazu podjęcia działań przeciwko nielegalnym treściom, polegającego na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich, których rozpowszechnianie może wyczerpywać znamiona czynu zabronionego lub pochwalających lub nawołujących do popełnienia czynu zabronionego

określonego w polskim Kodeksie karnym (Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U.2025.383 z późn. zm.). Podobnie odwołanie w obszarze definicji treści nielegalnych istnieje w systemie niemieckim i francuskim.

Procedury wnioskowej nie stosuje się do: treści o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym. W projekcie ustalono, iż definicja treści nielegalnych jest określona poprzez odwołanie do definicji zawartej w DSA. Nie ustalono także kwestii zastosowania przepisów projektowanej ustawy do treści szkodliwych (dezinformacja). To oznacza definiowanie treści nielegalnych w zawężonym zakresie czynów, o których mowa w wymienionych przepisach. Dotyczy to odpowiednio takich czynów jak:

- **Dyskryminacja** – Kto stosuje przemoc lub groźbę bezprawną wobec grupy osób lub poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, politycznej, wyznaniowej lub z powodu jej bezwyznaniowości.

Zakres treści nielegalnej zdefiniowanej na gruncie ustawy o radiofonii i telewizji jest szerszy, bowiem nie odnosi się jedynie do przemocy czy groźby, ale w ogóle czynów zawierających także nawoływanie do przemocy lub nienawiści wobec grupy osób ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność państwową, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną. Chodzi tu o tzw. mowę nienawiści, która powinna być uwzględniona jako czyn zabroniony. Treścią nielegalną są także treści nawołujące do znieważania grupy ludności albo poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości. Zasady oceny, czym jest treść nielegalna w kontekście dyskryminacji oraz mowy nienawiści, powinny być skoordynowane z przepisami stosowanymi zarówno do platform udostępniania wideo działających zgodnie z wykazem na rynku polskim, jak i wobec platform transgranicznych i mediów społecznościowych.

- **Nakłanianie lub zmuszanie innej osoby do spowodowania u niej ciężkiego uszczerbku na zdrowiu** – zdaniem projektodawczyń termin ten może obejmować cyberbullying, namawianie do samobójstwa w ramach platform społecznościowych, co jest szczególnie niebezpieczne w odniesieniu do młodych użytkowników sieci.
- **Groźba karalna** – dotyczy stosowania groźby karalnej, tj. popełnienia przestępstwa na szkodę osoby lub jej bliskich. W kontekście możliwości popełnienia tego przestępstwa online będzie to obejmowało wiadomości umieszczane w ramach portali społecznościowych – podobnie jak w przypadku cyberbullyingu można odnieść zastosowanie tego przepisu do materiałów wideo rozpowszechnianych przez platformy udostępniania wideo.
- **Elektroniczna korupcja seksualna małoletniego** – w tym kontekście za treść nielegalną URTV określa treści zagrażające prawidłowemu fizycznemu, psychicznemu lub moralnemu rozwojowi małoletnich, w szczególności zawierające treści pornograficzne lub w sposób nieuzasadniony eksponujące przemoc, bez stosowania skutecznych zabezpieczeń technicznych, o których mowa w art. 47p ust. 1 URTV. Ten zakres cyberzagrożeń także powinien być uwzględniony w procedurze nakazowej.
- **Publiczne prezentowanie treści pornograficznych** – zakres tego czynu jest szerszy niż zakres ustalony na gruncie URTV. W świetle przepisów tej ustawy treściami nielegalnymi są treści pornograficzne z udziałem małoletniego. Artykuł 202 kodeksu karnego ma szersze zastosowanie.
- **Fałszywy alarm** – zdaniem projektodawcy dotyczy zawiadomienia o nieistniejącym zagrożeniu, wywołującego działania instytucji publicznych. Obejmuje on rozsyłanie fałszywych alarmów bombowych przez media społecznościowe.
- **Propagowanie nazizmu, komunizmu, faszyzmu lub innego ustroju totalitarnego** – przepis ten odnosi się do publicznego propagowania nazistowskiego, komunistycznego, faszystowskiego lub innego totalitarnego ustroju państwa lub nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość – jest to regulacja zbliżona do zakresu regulacji mowy nienawiści w URTV – jednak w zawężonym zakresie.

Zdaniem projektodawcy przepis ten obejmuje mowę nienawiści w mediach społecznościowych. Ze względu na fakt, iż obecna definicja platformy udostępniania wideo w URTV nie obejmuje mediów społecznościowych, pojawia się pytanie, czy organem właściwym w przypadku treści nielegalnych występujących w mediach społecznościowych będzie Prezes UKE czy powinna być KRRiT.

- **Napaść z powodu ksenofobii, rasizmu lub nietolerancji religijnej** – kto publicznie znieważa grupę ludności albo poszczególną osobę z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości lub z takich powodów narusza nieetykalność cielesną innej osoby – jest to regulacja zbliżona do zakresu regulacji mowy nienawiści w URTV, jednak w zawężonym zakresie.
- **Rozpowszechnianie utworu bez pozwolenia** – treścią nielegalną jest naruszenie majątkowych praw autorskich, natomiast nie będzie nią już naruszenie osobistych praw autorskich w postaci plagiatu, ponieważ projekt nie wymienia przywłaszczenia autorstwa, rozpowszechniania utworu bez podania nazwiska lub pseudonimu twórcy, zniekształcenia utworu, które są czynami niedozwolonymi na gruncie przepisów prawa autorskiego.

W przypadku braku innych skutecznych środków, które mogą doprowadzić do wykonania decyzji nakazującej uniemożliwienie dostępu do nielegalnych treści, w stosunku do nielegalnych treści występujących w usłudze, o której mowa w art. 4 DSA, organ właściwy do rozpatrzenia wniosku może zgłosić domenę internetową na listę ostrzeżeń, o której mowa w art. 20 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U.2024.1803) – takie rozwiązanie dotyczy tych stron internetowych, których mechanizm działania jest oparty na publikacji treści naruszających cudze prawa, w szczególności poprzez publikację bez uprawnień cudzych utworów. Rozwiązanie zawarte w projektowanym ust. 20 art. 11a dotyczy sytuacji, w których mamy do czynienia z rozszerzoną odpowiedzialnością dostawców usług pośrednich, o której mowa w art. 222 ust. 1 pkt 3 ustawy z dnia z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U.2025.24) – dostawca ma obowiązek dołożenia należytej staranności, aby uniemożliwić w przyszłości

dostęp do zgłoszonych wcześniej nielegalnych treści. Aby zapewnić stronom postępowania ścieżkę odwoławczą, wprowadzona została możliwość wniesienia sprzeciwu do sądu powszechnego, który rozpatrzy go w trybie nieprocesowym.

Projektując regulacje dotyczące postępowania nakazowego, projektodawca kierował się realną potrzebą wprowadzenia w polskim systemie prawnym przystających do funkcjonujących obecnie w sieci form komunikacji, środków prawnych zapewniających jak najszybszą ochronę prawną. Z kolei nieco inne zasady, chociażby blokowania dostępu do treści, określają przepisy URTV oraz przepisy ustawy o prawie autorskim i prawach pokrewnych. Procedury te powinny być skoordynowane.

Obecna definicja dotycząca treści nielegalnych, której zastosowanie ma mieć transgraniczny charakter, wydaje się niekonsekwentna wobec regulacji warunkujących prawidłowe funkcjonowanie krajowego rynku mediów cyfrowych. Należy zauważyć, że 53% respondentów we wspólnym badaniu KIGEIT i ALK na temat treści nielegalnych w internecie (zob. Dot.pl NASK PIB Wydanie specjalne nr 2 <https://www.journaldot.pl/Archiwum>) uważa, że kontrowersyjne treści (np. opinie polityczne, religijne, filozoficzne, sztuka krytyczna) powinny pozostać legalne, jeśli są zgodne z zasadami wolności słowa. Najczęściej pogląd ten podzielają mężczyźni (57%) oraz osoby z wyższym wykształceniem (59%). 17% badanych jest przeciwnych takiej wolności słowa, podczas gdy 30% respondentów nie ma w tej kwestii zdania. Wyniki te pokazują, że większość badanych popiera prawo do publikowania treści kontrowersyjnych, ale niewykraczających poza normy prawne. Co warto uwagi, polskie społeczeństwo nie jest też przekonane o skuteczności działań przeciwko nielegalnym treściom w internecie – jedynie 20% uważa, że przepisy prawa w tym zakresie są skuteczne, a niewiele więcej (26%) uważa, że platformy społecznościowe sprawnie usuwają nielegalne treści. Ogólnie dominuje przekonanie (44%), że zarówno usuwanie treści nielegalnych, jak i blokowanie dostępu do konta jej autorowi to równie skuteczne metody zwalczania nielegalnych treści w internecie. Jak wskazują Turillazzi, Mariarosaria, Floridi, Casolari (2023) należy definiować solidniejsze ramy dla dobra wszystkich interesariuszy rynku cyfrowego. Chociaż podkreślenia wymaga proaktywna postawa UE w dostosowywaniu swoich struktur prawnych do wyzwań ery cyfrowej, co daje wrażenie, iż otoczenie regulacyjne nadaża za postępem technologicznym (Gongeta, 2024).

## PODSUMOWANIE

Zmiany technologiczne w funkcjonowaniu rynku mediów cyfrowych, zwłaszcza rozwój internetu i mediów społecznościowych, wymagają nowego spojrzenia na kwestie związane z zapewnieniem ochrony celów interesu publicznego. W trakcie diagnozy, jakie nowe kierunki pojawiły się w realizacji interesu publicznego w mediach cyfrowych, może okazać się, iż wymagana tu będzie zupełnie nowe podejście do wolności rządzących światem cyfrowym. Pojawiają się wtedy zupełnie nowe zadania dla ustawodawcy, uwzględniające przesłanki takie jak moralność publiczna, bezpieczeństwo publiczne, porządek publiczny oraz prawa i wolności innych osób, na co zwracają uwagę wszystkie trzy systemy opisane w niniejszym artykule. Problematyczne jednak staje się uwzględnienie aspektu transgraniczności usług cyfrowych i zwalczanie treści nielegalnych czy szkodliwych w sytuacji zasadniczych różnic w podejściu definicyjnym treści nielegalnych czy szkodliwych, ale także różnic organizatorskich w różnych ustawodawstwach samych państw członkowskich UE (a zjawisko takie jest oczywiste i wynika z różnic kulturowych, związanych z organizacją samego państwa, również tych związanych z samą kulturą prawną). Nie jest to tylko problem różnie pojmowanych koncepcji wolności słowa i środków społecznego przekazu na świecie. Nie jest to kwestia warunkowań regulacyjnych w relacjach prawo UE – regulaminy big techów. Te różnice, wynikające z tak szanowanego i pożądanego pluralizmu w podejściu do regulacji zawartości sieci, mogą stanowić zasadniczy problem w budowaniu jednolitego i bezpiecznego rynku usług cyfrowych.

## REFERENCES

- Ash, T.G. (2018). *Wolne słowo. Dziesięć zasad dla połączonego świata*. Znak, s. 301.
- Conseil d'État, 4ème chambre, Conclusions de M. Boutron, Rapporteur public sur les Affaires N° 453763 Coyotte system N°s 461193 i 461195 Société Webgroup Czech Republic et autre, 3.06.2024, [https://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2024-03-06/453763?download\\_pdf](https://www.conseil-etat.fr/fr/arianeweb/CRP/conclusion/2024-03-06/453763?download_pdf) (dostęp: 20.12.2025).
- Gongeta, S. (2024). *Revolucja cyfrowa i wyzwania dla prawodawstwa europejskiego. Zatrudnienie, edukacja i przedsiębiorczość*, 2024, <https://api.semanticscholar.org/CorpusID:275026072> (dostęp: 2.02.2026).
- Guggenberger, N. Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht. *Zeitschrift für Rechtspolitik [ZRP]*, s.98, 100.
- Kalscheuer, F., Hornung, Ch. Das Netzwerkdurchsetzungsgesetz – Ein verfassungswidriger Schnellschuss. *Neue Zeitschrift für Verwaltungsrecht [NVwZ]*, s.1721, 1724.
- Klonick, K. (2020). The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *The Yale Law Journal*, 129, s. 2418, 2437 (dostęp: 2.02.2026).
- Kraski, R. (2017). The German Right of Personality, Combating Fake News in Social Media: U.S. and German Legal Approaches. , 91,s. 923, 930–935.
- Liesching, M. (2018). Die Durchsetzung von Verfassungs – und Europarecht gegen das NetzDG. Überblick über die wesentlichen Kritikpunkte. *Multimedia und Recht [MMR]*, 21, s. 26, 27–28.
- Löber, L.L., Roßnagel, A. (2019). Das Netzwerkdurchsetzungsgesetz in der Umsetzung. Bilanz nach den ersten Transparenzberichten. *Multimedia und Recht [MMR]*, 22, s. 71.
- Savin, A. (2021). Ustawa o usługach cyfrowych UE: w kierunku bardziej odpowiedzialnego internetu. Copenhagen Business School [wp]. Dokument badawczy CBS LAW nr 21-04, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3786792](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786792) (dostęp: 2.02.2026).
- Siwicki, M. (2011). *Nielegalna i szkodliwa treść w Internecie*. Warszawa; s. 80–129.
- Struckmeyer, K. (2024). Słowo kluczowe: Ustawa o usługach cyfrowych. *Merz, Media, Edukacja*, 68(4), s. 4. <https://doi.org/10.21240/merz/2024.4.3>.
- Struckmeyer, K. (2025). Dzieci – mniejszość bez ochrony: El-Mafaalani, A., Kurtenbach, S., Strohmeier, K.P. (2025). Dzieci – mniejszość bez ochrony: dorastanie w starzejącym się społeczeństwie. Kolonia: Kiepenheuer und Witsch. Merz, median + erziehung, 69(3), s. 91–92, <https://doi.org/10.21240/merz/2025.03.25>
- Turillazzi, A., Taddeo, M., Floridi, L., Casolari, F. (2023). The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15, s. 1–24, <https://doi.org/10.1080/17579961.2023.2184136>
- Zurth, P. (2021). Niemiecka ustawa NetzDG jako wzór do naśladowania czy przestroga? Implikacje dla debaty na temat odpowiedzialności w mediach społecznościowych. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 1084, 31, <https://ir.lawnet.fordham.edu/iplj/vol31/iss4/4> (dostęp: 2.02.2026).