

Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215339



Security in the digital age. The role of DSA and TCO in limiting the spread of illegal content on the Internet

Bezpieczeństwo w erze cyfrowej. Rola DSA i TCO w ograniczaniu rozpowszechniania nielegalnych treści w Internecie

Karolina MIKUSEK

Akademia Sztuki Wojennej

ORCID: 0009-0006-1645-7605

E-mail: k.mikusek@doktorant.akademia.mil.pl

Abstract

The article analyzes the Digital Services Act (DSA) and the Regulation on terrorist content online (TCO) as key instruments for combating illegal content in the European Union. The main objective of the text is to analyze how these regulations strengthen digital security while increasing the responsibility of online platforms and protecting users from threats such as radicalization, terrorism, crime, and disinformation.

The study uses qualitative analysis based on legal provisions, European Union documents, and media reports. In order to assess the scope, mechanisms, and obligations imposed on both digital service providers and member states, these were discussed. The methodology combines source research and textual analysis, enabling an interdisciplinary assessment of the effectiveness of the regulations and the challenges associated with their implementation.

The results indicate that the DSA and TCO together form a comprehensive regulatory framework for combating illegal content on the Internet. The TCO introduces a rapid response mechanism, while the DSA provides broader systemic safeguards. Both pieces of legislation significantly strengthen user protection and platform responsibility, although some inconsistencies remain.

The analysis shows that the combined regulatory framework is an important milestone in the European Union's digital policy. However, its long-term success depends on consistent enforcement across all Member States, adequate institutional capacity, and maintaining a balance between security objectives and fundamental rights.

Keywords

DSA, TCO, digital security, cyber threats, terrorist content

Streszczenie

W artykule przeprowadzono analizę przepisów Aktu o usługach cyfrowych (DSA) oraz Rozporządzenia w sprawie treści terrorystycznych w internecie (TCO), jako kluczowych instrumentów służących zwalczaniu nielegalnych treści w Unii Europejskiej. Głównym celem artykułu jest analiza sposobu, w jaki wskazane przepisy wzmacniają bezpieczeństwo cyfrowe, przy jednoczesnym zwiększeniu odpowiedzialności platform internetowych oraz ochronie użytkowników przed zagrożeniami, takimi jak radykalizacja, terroryzm, przestępczość oraz dezinformacja.

W badaniu zastosowano analizę jakościową opartą na zapisach prawnych, dokumentach Unii Europejskiej oraz doniesieniach medialnych. W celu oceny zakresu, mechanizmów i obowiązków nałożonych zarówno na podmioty świadczące usługi cyfrowe, jak również państwa członkowskie dokonano ich omówienia. Metodologia łączy badania źródłowe i analizę tekstową, umożliwiając interdyscyplinarną ocenę skuteczności rozporządzeń i wyzwań związanych z ich wdrażaniem.

Wyniki wskazują, że DSA i TCO tworzą razem kompleksową strukturę regulacyjną służącą zwalczaniu nielegalnych treści w Internecie. TCO wprowadza mechanizm szybkiego reagowania, natomiast DSA zapewnia szersze zabezpieczenia systemowe. Oba akty prawne znacznie wzmacniają ochronę użytkowników i odpowiedzialność platform, chociaż nadal pozostają pewne nieścisłości.

Analiza pokazuje, że połączone ramy regulacyjne stanowią ważny kamień milowy w polityce cyfrowej Unii Europejskiej. Ich długoterminowy sukces zależy jednak od spójnego egzekwowania przepisów we wszystkich państwach członkowskich, odpowiednich zdolności instytucjonalnych oraz utrzymania równowagi między celami w zakresie bezpieczeństwa a prawami podstawowymi.

Słowa kluczowe

DSA, TCO, bezpieczeństwo cyfrowe, zagrożenia cybernetyczne, treści terrorystyczne

Wprowadzenie

W dzisiejszym świecie przestrzeń cyfrowa stanowi ważny element codziennego funkcjonowania społeczeństwa informacyjnego. Nie ulega wątpliwości, że w obecnych czasach coraz częściej i szerzej mówi się o licznych zagrożeniach, które w bezpośredni sposób oddziałują na poczucie bezpieczeństwa użytkowników Internetu. Ich zakres dotyczy licznych przestrzeni, zarówno tych wojskowych, jak i cywilnych¹. Organy ścigania oraz wymiar sprawiedliwości napotyka szereg luk prawnych, których obecność uniemożliwia postawienie zarzutów oraz egzekwowanie zapisów prawnych w stosunku do przestępców cyfrowych oraz cyberterrorystów. W związku z tym coraz częściej organizacje międzynarodowe oraz regionalne podejmują się próby stworzenia ram regulacyjnych, umożliwiających wspieranie wskazanych procesów. W tym aspekcie Unia Europejska podjęła szereg aktywności, które pomagają państwom członkowskim w walce z nielegalną działalnością na platformach cyfrowych.

Wskazana sytuacja problemowa stanowiła o podjęciu badań, za cel których przyjęto przedstawienie Aktu o usługach cyfrowych oraz Rozporządzenia w sprawie przeciwdziałania rozpowszechnianiu treści terrorystycznych w Internecie, jako rozwiązań prawnych wspierających działania na rzecz ograniczania rozpowszechniania nielegalnych treści w Internecie. Problem główny sformułowano w postaci następującego pytania badawczego: W jaki

¹ G. Pilarski, T. Zawadzki, Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, „Wiedza Obronna” 2025, t. 292, nr 3, s. 131.

sposób wskazane regulacje wspierają aktywności na rzecz ograniczania rozpowszechniania nielegalnych treści w Internecie? W celu rozwinięcia wskazanego głównego problemu badawczego sformułowano szczegółowe problemy badawcze określone w postaci poniższych pytań: w jaki sposób Akt o usługach cyfrowych jako narzędzie prawne wspiera walkę z nielegalnymi treściami?; w jakim zakresie Rozporządzenie w sprawie przeciwdziałania rozpowszechnianiu treści terrorystycznych w Internecie zwalcza materiały o charakterze terrorystycznym?; jakie znaczenie mają opisane regulacje dla bezpieczeństwa społeczeństwa w Internecie?

Cel badawczy został pomyślnie osiągnięty dzięki zastosowaniu metody jakościowej do przeglądu istniejącej literatury². Przyjęta metodologia pozwoliła na wszechstronne przeanalizowanie treści aktów prawnych, jak i aktualnych źródeł internetowych, w tym oficjalnych stron instytucji unijnych oraz treści publikowane na platformach cyfrowych. Dzięki tak szerokiemu zakresowi danych możliwe było uzyskanie rzetelnej, opartej na dowodach wiedzy dotyczącej DSA i TCO, a także poznanie zróżnicowanych perspektyw, interpretacji i doświadczeń podmiotów zajmujących się problematyką bezpieczeństwa cyfrowego.

Akt o usługach cyfrowych jako narzędzie prawne do walki z nielegalnymi treściami

Wiele zjawisk zachodzących w przestrzeni cyfrowej stanowi szeroki wektor oddziaływania grup przestępczych na platformach internetowych. Należy w tym zakresie wskazać zarówno wszelkiego rodzaju próby oszustwa, wykorzystujących przestrzeń socjotechnik, takich jak manipulacja lub dezinformacja, jak również formy podszywania się pod inne, dobrze znane użytkownikom pomioty jak ma to miejsce w przypadku phishingu. Nie zależnie jednak od profilu oraz rodzaju działalności przestępczej, cel zazwyczaj jest ten sam – wprowadzenie użytkownika w błąd po to, aby osiągnąć zamierzony cel, zarówno finansowy, jak również informacyjny. W związku z tym konieczne było podjęcie kroków prawnych, które w znaczący sposób wspomogą walkę z tymi zjawiskami, chroniąc użytkowników Internetu, jednocześnie angażując tym samym poszczególne platformy hostingowe³.

W tym zakresie nie sposób nie wspomnieć o Akcie o usługach cyfrowych (ang. Digital Services Act – DSA). Samo rozporządzenie zostało uchwalone w 2022 r., jednak implementacja wskazanych w nim rozwiązań miała rozpocząć się w państwach członkowskich dopiero w 2024 r.⁴. Jak wskazuje sama regulacja, istnieje wiele przesłanek, które spowodowały powstanie tego prawnego rozwiązania. Po pierwsze państwa członkowskie nie były w stanie samodzielnie stworzyć jednolitego systemu odpowiedzialnego za zarządzanie usługami cyfrowymi. Biorąc pod uwagę funkcjonującą w Unii Europejskiej zasadę

² Zob. szerzej: K. Chałubińska-Jentkiewicz, *Prawna ochrona treści cyfrowych*, Warszawa 2021; M. Gumularz, *Przedmowa* [w:] M. Gumularz (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa 2024, s. 41; W. Wiewiórowski, *Słowo wstępne* [w:] D. Lubasz, M. Namysłowska (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa 2024, s. 23–24.

³ M. Nowikowska, *Hate speech as an example of illegal content on the internet under the provisions of the Digital Services Act – Definitional Issues*, [w:] Żylińska, K. Huczek (eds.), *Multidimensionality of cybersecurity. Hate speech in the cyberworld*, Wydawnictwo: Uczelnia Techniczno-Handlowa im. H. Chodkowskiej w Warszawie, Warszawa 2025, s. 91 i n.

⁴ A. Szczęsna, *Wdrożenie DSA w Polsce*. https://cyberpolicy.nask.pl/wdrozenie-dsa-w-polsce/#_ftn1 [dostęp: 26.11.2025].

pomocniczości, tylko dzięki podjęciu wspólnych wysiłków można zapewnić jednolite ramy działania dla platform⁵. Dodatkowo wskazano na brak skuteczności krajowych przepisów w stosunku do usług cyfrowych, które stały się transgraniczne⁶. Ważnym aspektem określonym w dokumencie jest konieczność zwiększenia bezpieczeństwa i zaufania użytkowników Internetu pochodzących z państw członkowskich Unii Europejskiej ze względu na generowanie przez duże platformy internetowe zagrożeń społecznych. Co za tym idzie niezbędne jest podjęcie pilnych działań na rzecz przeciwdziałania negatywnym skutkom ich występowania⁷.

Głównym założeniem dokumentu było stworzenie spójnej, unijnej regulacji dotyczące usług pośrednich takich jak hosting, czy obsługa platform internetowych. Dzięki temu możliwe byłoby uniknięcie chaosu regulacyjnego i fragmentacji rynku wynikającej z różnych przepisów krajowych w przyszłości⁸. Istnieje szereg zmian, jakie wraz z przyjęciem rozporządzenia zaakceptowały państwa członkowskie. Do jednego z nich należy chociażby ujednolicenie zasad odpowiedzialności i obowiązków internetowych platform. We wcześniejszych regulacjach nie uwzględniano zmieniających się warunków świata cyfrowego, a co za tym idzie, szerokiego zakresu zagrożeń związanych z tą tematyką⁹. W związku z tym akt prawny zastępuje kluczowe przepisy dyrektywy o handlu elektronicznym (ang. e-commerce directive)¹⁰, ale również stwarza na nowo ramy obowiązków dostawców usług pośrednich¹¹.

DSA wprowadza zupełnie nowy, znacznie bardziej rygorystyczny reżim prawny dla bardzo dużych platform internetowych (VLOPs), czyli takich, które mają co najmniej 45 mln aktywnych użytkowników miesięcznie w Unii Europejskiej¹². Wynika to z faktu, że platformy te mają ogromny wpływ na społeczeństwo, gospodarkę, debatę publiczną i przepływ informacji, a ze względu na swoje rozmiary generują także ryzyka systemowe¹³. Wśród nowych obowiązków należy wskazać m.in.: ocenę ryzyka systemowego wraz z podejmowaniem środków ograniczających je, prowadzenie corocznych, obowiązkowych audytów, zwiększenie transparentności algorytmów rekomendacji oraz udostępnianie danych badaczom i organom nadzoru¹⁴.

Kolejna zmiana dotyczy wprowadzenia jednolitego systemu nadzoru. Dotychczas każde państwo członkowskie miało własne przepisy prawne oraz organy odpowiedzialne za zakres egzekwowania poszczególnych zapisów, co przyczyniało się do chaosu regulacyjnego¹⁵. Przy obecnym rozwiązaniu istnieje możliwość utworzenia jednolitego systemu z koordynatorem ds. usług cyfrowych

⁵ Pkt. 155 Rozporządzenia 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 (akt o usługach cyfrowych) (Dz.Urz. UE L 277/1 z 27.10.2022).

⁶ Ibidem, pkt. 110.

⁷ Ibidem, pkt 154.

⁸ Ibidem, art. 1.

⁹ Ibidem, pkt. 16.

¹⁰ Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego, w ramach rynku wewnętrznego (Dz.Urz. UE L 178 z 17.07.2000).

¹¹ Pkt. 34-35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065.

¹² Ibidem, Art. 33.

¹³ Ibidem, pkt. 75-76.

¹⁴ Ibidem, art. 34-40.

¹⁵ Zob. szerzej: M. Nowikowska, Zasada rozliczalności i przejrzystości – rozwiązania w zakresie niezależnego audytu w świetle postanowień aktu o usługach cyfrowych, „Europejski Przegląd Sądowy” 2025, nr 3, s. 37.

w każdym państwie¹⁶. Istotnym również aspektem jest wzmocnienie ochrony podstawowych praw użytkowników, szczególnie w odniesieniu do wolności wypowiedzi oraz możliwości uzyskiwania informacji¹⁷.

Rozporządzenie nakłada w pewnym stopniu konkretne wymagania wobec państw członkowskich Unii Europejskiej. W tym zakresie warto wspomnieć o kilku istotnych aspektach. Pierwszym z nich jest konieczność wyznaczenia właściwych organów ds. nadzorowania działań platform cyfrowych i wdrażania określonych w regulacji przepisów. Dodatkowo każde z państwo powinno powołać koordynatora ds. usług cyfrowych, którego wybiera się z pośród właściwych organów. Czas na wyznaczenie powyższego stanowiska upłynął 17 lutego 2024 r¹⁸. Co równie istotne, państwa członkowskie muszą zapewnić niezależność koordynatorów od wpływów politycznych, dostęp do zasobów technicznych, finansowych oraz kadrowych, a także zdolność podejmowania działań nadzorczych nad platformami działającymi na terenie kraju¹⁹. Warto również odnieść się do zapewnienia współpracy między organami krajowymi oraz instytucjami Unii Europejskiej. Konieczne w tym zakresie jest nawiązanie ścisłych relacji pomiędzy koordynatorem i organami państwowymi, a także utrzymanie transgranicznych kontaktów z innymi przedstawicielami państw członkowskich. Dodatkowo wskazano na udział wspomnianego podmiotu w Radzie Usług Cyfrowych (ang. Digital Services Board)²⁰.

Państwa członkowskie muszą również umożliwić swoim organom stosowanie narzędzi nadzoru i egzekwowania prawa. W tym zakresie wyszczególnia się takie uprawnienia jak: nakazania zaprzestania naruszeń, nakładania kar pieniężnych, prowadzenie czynności kontrolnych oraz żądanie informacji od platform²¹. Dodatkowo istnieje obowiązek sporządzania przez koordynatora corocznych sprawozdań w zakresie swojej działalności²². Wreszcie państwa członkowskie muszą umożliwić współdziałanie z Komisją Europejską w sytuacjach zagrożenia bezpieczeństwa lub zdrowia publicznego²³.

Jak można zauważyć, Akt o usługach cyfrowych stanowi istotną zmianę w dotychczasowym podejściu do treści zawartych na stronach oraz platformach internetowych, a także zwiększenie odpowiedzialności podmiotów cyfrowych w kontekście nielegalnych materiałów. Funkcjonowanie w każdym państwie właściwych organów ds. egzekwowania prawa stanowi element wspierający wprowadzanie odpowiednich zmian.

Rozporządzenie w sprawie przeciwdziałania rozpowszechnianiu treści terrorystycznych w Internecie

Działalność terrorystyczna stanowi jedną z głównych zagrożeń XXI wieku. Pomimo zmieniających się trendów oraz sposobów osiągania przez organizacje terrorystyczne głównych celów, potrzeba rozgłosu, wzbudzenia paniki, lęku oraz zmiany decyzji wśród decydentów stanowią ważny element ich działalności. Przy obecnym rozwoju technologicznym, konieczności przeniesienia prawie każdej

¹⁶ Ibidem, art. 49-50.

¹⁷ Ibidem, pkt. 150.

¹⁸ Ibidem, pkt 109 oraz art. 49.

¹⁹ Ibidem, art. 50 ust. 1 oraz pkt. 112.

²⁰ Ibidem, pkt. 110, 129-130.

²¹ Ibidem, pkt. 114 oraz art. 56.

²² Ibidem, art. 55.

²³ Ibidem, pkt. 82.

dziedziny naszego życia do sfery cyfrowej oraz ogromnych zasięgach platform internetowych nie należy się dziwić, że coraz częściej w przestrzeni nowoczesnych mediów można odnaleźć treści nawiązujące do postulatów grup terrorystycznych lub tworzonych przez nich materiałów promocyjnych.

W związku z przedstawionym zakresem tematycznym podjęto próbę utworzenia regulacji prawnej, która ograniczałaby rozpowszechnianie treści o charakterze terrorystycznym. Parlament Europejski oraz Rada Europy podjęły się tego trudu, który przyczynił się do powstania Rozporządzenia w sprawie przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym (ang. Terrorist Content Online Regulation - TCO). Oprócz wskazanego wyżej aspektu przeniesienia części działalności terrorystycznej do przestrzeni online warto również wskazać inne przesłanki wskazujące na zasadność opracowania aktu prawnego. Warto wspomnieć o tym, że treści terrorystyczne szybko rozprzestrzeniają się online i stanowią realne zagrożenie bezpieczeństwa publicznego, procesów demokratycznych i ochrony obywateli Unii Europejskiej. Co równie ważne wskazany zakres tematyczny może stać się katalizatorem procesu radykalizacji²⁴. Jak przedstawiono w rozporządzaniu brakuje skutecznych narzędzi prawnych w państwach członkowskich, ponieważ dotychczasowe prawo Unii Europejskiej nie przewidywało jednolitego modelu szybkiego usuwania treści o charakterze terrorystycznym²⁵. Niespójność i różnice w krajowych modelach walki z treściami terrorystycznymi również stanowią ważny aspekt omawianej tematyki. Celem powstania regulacji jest ujednolicenie systemu oraz unikanie rozbieżności regulacyjnych między państwami Unii Europejskiej²⁶. Co równie ważne stworzenie możliwości błyskawicznej reakcji, aby uniemożliwić rozprzestrzenianie się niebezpiecznych treści stanowi istotny element omawianego zagadnienia²⁷.

Rozporządzenie wprowadza zmiany w dotychczasowym systemie podejścia do tematyki treści o charakterze terrorystycznym. Pierwszym ze znaczących przełomów jest wprowadzenie niespotykanego wcześniej w Unii Europejskiej obowiązku usunięcia treści przez dostawców usług hostingowych, w ciągu 1 godziny od otrzymania nakazu usunięcia²⁸. Dodatkowo utworzono jednolity system obsługujący wyżej wymienione nakazy (ang. Removal Orders) w całej wspólnotie. Dotychczasowe każde działania państw członkowskich były wewnętrzne, bez możliwości egzekwowania tego prawa poza swoim terytorium. Dokument wprowadza obowiązek transgraniczny, co oznacza, że nakaz z jednego państwa obowiązuje usługodawcę w całej Unii Europejskiej²⁹. Warto również odnieść się do wprowadzenia obowiązku aktywnych środków (ang. proactive measures) opartych na tym, że dostawcy usług muszą podejmować działania zapobiegające ponownemu przesyłaniu treści terrorystycznych. To pierwszy przypadek w prawie organizacji, w którym dopuszcza się prewencyjne środki bez obowiązku ogólnego monitorowania treści³⁰. Dodatkowo

²⁴ Pkt. 1,4-5,9-10 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym (Dz.Urz. UE L 172/79 z 17.05.2021).

²⁵ Ibidem, pkt 50, 3.

²⁶ Ibidem, pkt. 3,6,50.

²⁷ Ibidem, art. 3.

²⁸ Ibidem, art. 3, ust. 3.

²⁹ Ibidem, art. 3, ust. 1-2.

³⁰ Ibidem, art. 5, ust. 2, 6.

wprowadzono wysokie kary za brak reakcji nawet do 4 % całkowitych obrotów usługodawców w poprzednim roku³¹.

Warto również wspomnieć o obowiązkach, jakie zostały nałożone na państwa członkowskie Unii Europejskiej. Pierwszą kwestią jest wyznaczenie właściwego organu (ang. Competent Authority) odpowiedzialny za wydawanie nakazów usunięcia treści. Podmiot ten musi wykazywać się niezależnością, a jego działania powinny być z poszanowaniem praw podstawowych³². Co równie ważne ma on uprawnienia do kontroli i wydawania nakazów³³. W dalszej kolejności należy wskazać zapewnienie mechanizmów nadzoru i kontroli usługodawców. Każdy kraj musi zapewnić możliwość wysyłania nakazów, żądania informacji, prowadzenia postępowania oraz nakładania sankcji³⁴. Odnosząc się do wcześniej wspomnianej transgranicznej kooperacji administracyjnej TCO wprowadza system współpracy między państwami (ang. cross-border cooperation). Dotyczy to w szczególności wymiany informacji i nawiązywania kontaktów w zakresie np. powiadamiania innych państw i Komisji Europejskiej³⁵. Istotnym aspektem jest również zapewnienie prawnej możliwości odwołania i kontroli sądowej. W tym zakresie państwa są zobowiązane do zagwarantowania mechanizmów odwoławczych. Przewidziane są chociażby środki prawne dla usługodawców oraz użytkowników³⁶.

Jak zostało wskazane w analizowanym akcie prawnym, kwestie obowiązków wiążą się również z zobowiązaniami dostawców usług hostingowych. Oprócz wyszczególnionego wcześniej obowiązku usunięcia treści terrorystycznych w ciągu 1 godziny, kolejnym istotnym elementem jest ustanowienie punktu kontaktowego działającego całodobowo. W ten sposób usługodawcy muszą zapewnić mechanizm stałego kontaktu dla organów krajowych³⁷. Warto również odnieść się do obowiązku zachowania danych związanych z usuniętą treścią. Wymagane jest przechowywanie danych dowodowych przez 6 miesięcy³⁸. W odniesieniu do środków proaktywnych platformy cyfrowe muszą podejmować działania ograniczające ponowne udostępnianie treści terrorystycznych w zgodzie z zapisami Karty Praw Podstawowych³⁹. Warto również wspomnieć o obowiązku publikacji sprawozdań przejrzystości. Wskazane dokumenty dotyczą działań podejmowanych przeciw treściom terrorystycznym⁴⁰.

Biorąc pod uwagę zaprezentowane aspekty należy wskazać na zasadność wprowadzenia zmian zaproponowanych w rozporządzeniu. W związku z brakiem usystematyzowanego podejścia co do monitorowania oraz zapobiegania rozpowszechniania się treści o charakterze terrorystycznym, istotnym jest wprowadzenie w obecnym prawie Unii Europejskiej możliwości zapewnienia wsparcia w wyżej wymienionych kwestiach. Dodatkowo określenie

³¹ Ibidem, art. 18.

³² W odniesieniu do Rzeczypospolitej Polskiej rolę takiego organu pełni Agencja Bezpieczeństwa Wewnętrznego. Zob. art. 26a, 26b Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U.2025.194 t.j.).

³³ Art. 12, ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784.

³⁴ Ibidem, art. 12-17.

³⁵ Ibidem, art. 13.

³⁶ Ibidem, art. 17.

³⁷ Ibidem, art. 3, ust. 6.

³⁸ Ibidem, art. 7, ust. 2.

³⁹ Ibidem, art. 5, ust 2, 6 oraz art. 6, ust. 2.

⁴⁰ Ibidem, art. 8.

obowiązków dla dostawców usług cyfrowych powoduje zwiększenie ich odpowiedzialności za negatywnie oddziałujące materiały.

Znaczenie regulacji dla bezpieczeństwa społeczeństwa w Internecie

Zasadnym byłoby odniesienie się do istoty omawianych regulacji w kontekście kluczowego znaczenia dla bezpieczeństwa społeczeństwa w Internecie. Pierwszą ważną kwestią jest wzmocnienie ochrony przed nielegalnymi treściami. W odniesieniu do TCO wymagana jest natychmiastowa reakcja na treści o charakterze terrorystycznym, a co za tym idzie ograniczenie rozpowszechniania propagandy, a także materiałów wpływających na proces radykalizacji oraz rekrutacji do struktur terrorystycznych. Z kolei DSA nakłada obowiązek szybkiego reagowania na szeroką kategorię nielegalnych treści, w tym przestępczych, nawołujących do przemocy. W ten sposób społeczeństwo jest mniej narażone na zagrożenia w postaci ruchów ekstremistycznych, oszustw, dezinformacji i przemocy. Warto również wspomnieć o zwiększonej przejrzystości działań platform świadczących usługi cyfrowe. Akt o usługach cyfrowych wymaga ujawniania zasad moderacji, działania algorytmów oraz możliwości wyłączenia profilowania. Z kolei rozporządzenie dot. treści o charakterze terrorystycznym wymaga pełnej przejrzystości działań platform związanych z usuwaniem omawianych materiałów. W ten sposób dochodzi do ograniczenia występowania manipulacji zarówno informacyjnej, jak i sprzedażowej (tzw. dark patterns), a także ukrytych mechanizmów wpływu. Ważnym aspektem jest również ograniczenie ryzyka systemowego ze strony VLOP. W odniesieniu do DSA regulacja nakłada na platformy cyfrowe obowiązek analizy wpływu ich działań na prawa obywatelskie, bezpieczeństwo i debatę publiczną. Jest to istotne ze względu na fakt, że największe platformy wywierają znaczącą presję na procesy społeczne. Wreszcie oba akty prawne wzmacniają zaufanie użytkowników do środowiska online. W ten sposób uregulowane są mechanizmy przewidywania działalności platform cyfrowych. Co równie istotne zapewniona jest możliwość odwołania, uzasadnienia decyzji moderacyjnych, oraz dostęp do danych o zmianach. Buduje to większą odporność społeczeństwa na manipulacje i zwiększa poczucie bezpieczeństwa.

Ważnym aspektem, który również odnosi się do zapewnienia odpowiedniego poziomu bezpieczeństwa, stanowi swoista synergia regulacyjna, jaka zachodzi pomiędzy tymi aktami prawnymi. W pierwszej kolejności warto wspomnieć o funkcjonowaniu jednolitego systemu moderacji treści w całej Unii Europejskiej. Dotychczas nie działało podobne rozwiązanie, które wpierałoby państwa członkowskie w walce z nielegalnymi treściami online. Dzięki funkcjonowaniu obu aktów prawnych razem możliwe jest zmniejszenie ryzyka powstania szarych stref dla działalności przestępczej oraz terrorystycznej. Co równie istotne wspomniane rozwiązania umożliwiają osiągnięcie holistycznej ochrony społeczeństwa. Każda z regulacji dotyczy szerokiego zakresu tematycznego, nie mniej jednak podejmowanie aktywności w aspekcie zapobiegania radykalizacji oraz rozpowszechniania zagrożeń społecznych, w tym dezinformacji, stanowi wartość dodaną do ochrony społeczeństwa informacyjnego. Warto również odnieść się do wielopoziomowego systemu nadzoru, zarówno w obrębie działań krajowych, jak również w odniesieniu do aktywności instytucji unijnych. W odniesieniu do TCO większy nacisk jest położony na działalność operacyjną, podczas gdy DSA wskazuje na podejście

strukturalne i algorytmiczne. Oba akty nakładają obowiązek raportowania i dokumentowania działań. W ten sposób możliwe jest osiągnięcie wspólnych standardów przejrzystości i odpowiedzialności platform. Dodatkowo obie regulacje wzmacniają prawa użytkowników oraz zapewniają im możliwości odwoławcze.

Implementacja obu regulacji stanowi ważną kwestię, w szczególności w odniesieniu do szeregu szans i wyzwań, jakie wiążą się z ich funkcjonowaniem w systemach prawnych państw członkowskich Unii Europejskiej. Biorąc pod uwagę szanse, jakie oba dokumenty tworzą należy odnieść się na pewno do stworzenia kompleksowej tarczy, zapewniającej bezpieczeństwo cyfrowe wspólnoty. Jak wskazano wcześniej oba dokumenty uzupełniają się co do kwestii zagrożeń oraz form reagowania na nie, co powoduje, że akty prawne tworzą spójną ramę⁴¹. W latach poprzednich brakowało jednolitego podejścia do wskazanej tematyki, co było wielokrotnie podkreślane jako konieczne działanie⁴². Ochronna funkcja tychże regulacji odnosi się zarówno do ochrony użytkowników, kontroli działania platform świadczących usługi cyfrowe, a także monitorowania przepływu informacji. Warto również wskazać w tym zakresie na fakt, że TCO przeciwdziała zagrożeniom natychmiastowo, a DSA dokonuje to w formie strukturalnej. Istotnym aspektem jest również to, że regulacje poprawiają jakość debaty publicznej. Akt o usługach cyfrowych zwiększa przejrzystość reklam politycznych i treści sponsorowanych, a co za tym idzie ma to ogromne znaczenie dla uczciwości dyskursu publicznego⁴³. Funkcjonowanie obowiązku ujawnienia zasad działania algorytmów ogranicza promowanie wybranych treści bez wiedzy użytkowników. Ograniczenia mowy nienawiści i treści terrorystycznych zmniejszają polaryzację przestrzeni publicznej⁴⁴. Kolejnym ważnym aspektem jest przeciwdziałanie zagrożeniom skrajnym, jak również i codziennych. W odniesieniu do Rozporządzenia o rozpowszechnieniu treści o charakterze terrorystycznym online mamy jednoznaczny system reakcji w określonym czasie⁴⁵. Z kolei DSA reguluje przestępstwa dotyczące mowy nienawiści, manipulacji informacyjnej, oszustw oraz treści nielegalnych (sprzedaż broni, narkotyków, materiałów pedofilskich)⁴⁶. W tym zakresie warto wskazać na odniesienie się regulacji zarówno do negatywnych aktywności na poziomie makro (terroryzm, radykalizacja, propaganda), ale również mikro (codzienne naruszenia, toksyczne treści, kradzieże danych, fake newsy). Kompleksowe podejście do wskazanej tematyki jest tylko potwierdzenie jak bardzo potrzebne jest ograniczenie ryzyka społecznego w postaci polaryzacji, radykalizacji oraz zastraszanie.

Warto odnieść się również do wyzwań związanych z implementacją wskazanych rozwiązań. Pierwszą z kluczowych kwestii jest trudność z wprowadzeniem rozwiązań prawnych w państwach członkowskich. Tylko część państw zdążyła utworzyć właściwe instytucje będące koordynatorami ds. usług

⁴¹ Zob. pkt 155 oraz art. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 oraz art. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784.

⁴² Zob. R. Gorwa, The platform governance triangle: conceptualising the informal regulation of online content, [w:] J. van Dijck, B. Rieder (red.) „Internet Policy Review”. T. 8, no. 2, s. 14-15.

⁴³ Pkt. 153 oraz art. 39, 27, 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065.

⁴⁴ Pkt 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784.

⁴⁵ Ibidem, art. 1–3 oraz pkt. 1-6, 50.

⁴⁶ Pkt. 81–84, 34-35 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065.

cyfrowych⁴⁷, czy też podmiotów odpowiedzialnych za zgłaszanie treści o charakterze terrorystycznym⁴⁸. Wynika to z faktu, że kraje różnią się zasobami, procedurami oraz kulturą prawną, obowiązującą na ich terenie. Dodatkowym wyzwaniem jest zachowanie balansu pomiędzy bezpieczeństwem a możliwością wypowiedzenia się. Regulacje mają chronić społeczeństwo, ale jednocześnie nie mogą nadmiernie ograniczać wolności słowa. Zarówno DSA, jak i TCO zawierają środki potencjalnie ingerujące w swobodę wypowiedzi. W TCO problem jest szczególnie silny przez jedno godzinny obowiązek usuwania treści. W ten sposób istnieje duże ryzyko podejmowania błędnych decyzji. W odniesieniu do DSA wyzwanie dotyczy oceny ryzyka systemowego. Unia Europejska podkreśla konieczność proporcjonalności działań, jednak istnieje ciekna linia co do uznania konkretnych treści za realnie szkodliwe, a dokonywania subiektywnych sądów i stosowania mechanizmów cenzury. Warto równie odnieść się do obciążeń technicznych, prawnych i finansowych platform świadczących usługi cyfrowe. Wdrożenie obu regulacji wymaga szeregu działań związanych m.in. z zatrudnieniem wykwalifikowanego personelu, stworzenia systemów audytów, prowadzenia rejestrów, a także integracji dobowych punktów kontaktowych oraz wdrożenia procedur odwoławczych. W perspektywie rozwiniętych gigantów usługodawczych istnieje realna możliwość zrealizowania wszelkich wymagań uwzględnionych powyżej. Nie mniej stanowi to jednak znaczący problem w odniesieniu do małych platform, które mogą nie mieć środków.

Podsumowanie

Przeprowadzone rozważania pozwalają stwierdzić, że obie regulacje stanowią ambitny plan zwiększenia bezpieczeństwa cyfrowego społeczeństwa, poprzez wyznaczenie nowych standardów globalnych. Sposób ich wdrożenia w państwach członkowskich oraz współpraca pomiędzy platformami świadczącymi usługi cyfrowe oraz państwowymi koordynatorami będzie wyznacznikiem ich skuteczności w przyszłości. Dynamiczny rozwój zagrożeń w przestrzeni cyfrowej oraz zmieniające się warunki funkcjonowania usługodawców cyfrowych wskazują na bezwzględną konieczność wprowadzenia regulacji w życie.

⁴⁷ Większość państw wyznaczyła organy egzekwowania Aktu o usługach cyfrowych. Jednak Komisja Europejska wszczęła postępowanie przeciwko co najmniej 6 państwom i prowadziła dalsze działania egzekucyjne w 2024–2025. Zob. C. Kroet, European Commission sues five countries for not applying digital platform rules. <https://www.euronews.com/next/2025/05/07/european-commission-sues-five-countries-for-not-applying-digital-platform-rules> [dostęp: 24.11.2025]; Reuters, EU sues several countries for not properly implementing Digital Services Act. <https://www.reuters.com/technology/eu-sues-several-countries-not-properly-implementing-digital-services-act-2025-05-07> [dostęp: 24.11.2025].

⁴⁸ W odniesieniu do TCO z 27 państw członkowskich 23 z nich wyznaczyło kompetentne organy (stan na 31.12.2023 r.). Zob. Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady Europejskiej w sprawie wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu treści terrorystycznych w Internecie.

Bibliografia

- Chałubińska-Jentkiewicz K., Prawna ochrona treści cyfrowych, Warszawa 2021.
- Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego, w ramach rynku wewnętrznego (Dz.Urz. UE L 178 z 17.07.2000).
- Gorwa R., The platform governance triangle: conceptualising the informal regulation of online content, [w:] van Dijck J., Rieder B. (ed.) „Internet Policy Review”, t. 8, no. 2.
- Gumularz M., Przedmowa [w:] M. Gumularz (red.), Akt o usługach cyfrowych. Komentarz, Warszawa 2024.
- Kroet C., European Commission sues five countries for not applying digital platform rules, <https://www.euronews.com/next/2025/05/07/european-commission-sues-five-countries-for-not-applying-digital-platform-rules>.
- Nowikowska M., Hate speech as an example of illegal content on the internet under the provisions of the Digital Services Act – Definitional Issues, [w:] Żylińska, K. Huczek (eds.), Multidimensionality of cybersecurity. Hate speech in the cyberworld, Wydawnictwo: Uczelnia Techniczno-Handlowa im. H. Chodkowskiej w Warszawie, Warszawa 2025.
- Nowikowska M., Zasada rozliczalności i przejrzystości – rozwiązania w zakresie niezależnego audytu w świetle postanowień aktu o usługach cyfrowych, „Europejski Przegląd Sądowy” 2025, nr 3.
- Pilarski G., Zawadzki T., Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, „Wiedza Obronna” 2025, tom 292, nr 3.
- Reuters, EU sues several countries for not properly implementing Digital Services Act. <https://www.reuters.com/technology/eu-sues-several-countries-not-properly-implementing-digital-services-act-2025-05-07>.
- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym (Dz.Urz. UE L 172/79 z 17.05.2021).
- 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 (akt o usługach cyfrowych) (Dz.Urz. UE L. 277/1 z 27.10.2022).
- Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady Europejskiej w sprawie wykonania rozporządzenia (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu treści terrorystycznych w Internecie.
- Szczęsna A., Wdrożenie DSA w Polsce, https://cyberpolicy.nask.pl/wdrozenie-dsa-w-polsce/#_ftn1.
- Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. j.t. z 2025 poz. 194).
- Wiewiórowski W., Słowo wstępne [w:] D. Lubasz, M. Namysłowska (red.), Akt o usługach cyfrowych. Komentarz, Warszawa 2024.