

Projekt ustawy o wolności słowa w internetowych serwisach społecznościowych – remedium na walkę z bezprawnymi treściami?

Kamila Brylak-Hudyma¹

Walka z nielegalnymi treściami udostępnianymi na platformach internetowych jest aktualnym i palącym tematem, z którym ustawodawstwa krajowe, jak też europejskie próbują się zmierzyć. Dotychczasową i podstawową regulacją w przedmiocie platform internetowych była dyrektywa e-Commerce, a w polskim porządku prawnym dodatkowo ustawa o świadczeniu usług drogą elektroniczną. W ostatnich miesiącach nader często dochodziło do usuwania, blokowania nie tylko publikowanych na portalach społecznościowych treści, ale także kont użytkowników tychże portali. W ocenie niektórych środowisk takie arbitralne działania i decyzje platform społecznościowych stanowią zagrożenie dla wolności słowa gwarantowanej w Konstytucji RP oraz Europejskiej Konwencji Praw Człowieka. Na szczeblu unijnym trwają prace nad rozporządzeniem w przedmiocie określenia zasad przejrzystości decyzji dotyczących moderacji treści (Digital Service Act). Niemniej po ogłoszeniu projektu rozporządzenia Digital Service Act Ministerstwo Sprawiedliwości złożyło projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych mającej na celu walkę z bezprawnymi treściami na platformach społecznościowych. Niniejszy artykuł ma na celu przedstawienie i omówienie najważniejszych regulacji dotyczących tej ustawy wraz z uwzględnieniem ryzyk i wątpliwości wiążących się z ewentualnym przyjęciem ustawy.

Uwagi wstępne

Podkreślanie roli, jaką platformy społecznościowe odgrywają w obecnych czasach, wydaje się truizmem. Świadczą o tym chociażby dane przedstawione w raporcie Hootsuite „Digital 2022”. W Polsce z Internetu korzysta 32,86 mln, co stanowi niemal 87% całkowitej populacji. W styczniu 2022 r. odnotowano 27,20 mln użytkowników social mediów, co stanowiło blisko 72% całkowitej populacji. Wskazano także, że liczba użytkowników social mediów w porównaniu do 2021 r. wzrosła o 1,3 mln². Używanie social mediów należy już raczej do monotonii dnia. Często zaraz po przebudzeniu niemal nałogowo sprawdza się powiadomienia, wiadomości i aktualności na serwisach społecznościowych. Co więcej, trudno wyobrazić sobie codzienne funkcjonowanie bez tego medium. Świadczyć może o tym chociażby sytuacja, która zdarzyła się 4.10.2021 r. Nastąpiła wówczas tzw. wielka awaria Facebooka (obecnie Mety), a za nim także Instagrama, Whats Appa, Messengera, w trakcie której kilka miliardów użytkowników straciło na kilkanaście godzin dostęp do swoich kont³. Co ciekawe, za utratę dostępu do kont obwinił sam Internet (dostawców Internetu), a nie błąd czy problemy techniczne po stronie platform. Oznacza to, że dla wielu platformy są „trwalsze” niż sam Internet. Poza tym nie można zapomnieć, jak ważne są te platformy dla biznesu. Każda chwila uniemożliwiająca dostęp do Facebooka (Mety) czy Instagrama stanowi wymierne straty⁴. Niemniej oprócz zapewne wielu pozytywnych aspektów funkcjonowania social mediów nie można zapomnieć o zagrożeniach z nimi

związanych. W ostatnich latach szczególnie podkreśla się negatywny wpływ platform na zdrowie psychiczne, zwłaszcza młodych ludzi, którzy nieustannie porównują się do zakłamanej w social mediach rzeczywistości i sztucznych ideałów⁵, a wiele osób powtarza niezwyfikowane informacje, przez co w społeczeństwie rozwija się dezinformacja. Było to silnie widoczne w czasie pandemii COVID-19, kiedy w Internecie pojawiały się zagrażające zdrowiu sposoby na walkę z wirusem, np. „picie wybielaczy lub czystego alkoholu może wyleczyć zakażenie koronawirusem”, „instalacje sieci 5G sprzyjają rozprzestrzenianiu się wirusa”⁶. Zgodnie z wynikami raportu pt. Dezinformacja w sieci, według analizy wiarygodności kanałów informacyjnych przygotowanej przez IAB Polska, opublikowanej w lipcu 2018 r., ponad połowa internautów zapytanych, gdzie najczęściej zdarzało im się natrafić na nieprawdziwe informacje, wskazywała media społecznościowe.

¹ Doktorantka w jednostce naukowo-badawczej Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE) działającej w ramach Uniwersytetu Wrocławskiego. ORCID: 0000-0002-2631-7159.

² Zob. <https://datareportal.com/reports/digital-2022-poland> (dostęp z 6.6.2022 r.).

³ Zob. <https://polskatimes.pl/awaria-facebook-co-sie-stalo-nie-dzialaly-tez-instagram-messenger-i-whatsapp/ar/c1-15835813> (dostęp z 6.6.2022 r.).

⁴ Zob. <https://spidersweb.pl/2021/10/awaria-facebook-nie-dziala-paraliz.html> (dostęp z 6.1.2022 r.).

⁵ Zob. <https://cyberdefence24.pl/bezpieczenstwo-informacyjne/facebook-od-dawna-wie-ze-instagram-jest-toksyczny-dla-nastolatkow> (dostęp z 6.6.2022 r.).

⁶ Zob. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_pl#przyklady-dezinformacji (dostęp z 26.6.2022 r.).

Media społecznościowe są zatem głównym źródłem nieprawdziwych informacji z kraju i ze świata⁷. Były one wskazywane przez 58% pytanym, drugie miejsce (39%) zajęły portale informacyjne. Co więcej, serwisy społecznościowe umożliwiają szerzenie treści nielegalnych i tych uznanych za szkodliwe, ponieważ ich bieżące usuwanie czy blokowanie z uwagi na ich ilość zdaje się zgoła niemożliwa, a algorytmy nie są w stanie zweryfikować wszystkich naruszeń. Ponadto pojawiła się obawa, że monopolistyczne platformy staną się zagrożeniem dla podstawowych praw i wolności obywatelskich, jak swoboda i wolność wypowiedzi czy swoboda prowadzenia działalności gospodarczej. Nic więc dziwnego, że poszczególne państwa⁸ postanowiły wprowadzić własne regulacje w przedmiocie uregulowania serwisów społecznościowych. W ślad za nimi poszło polskie Ministerstwo Sprawiedliwości, które chwilę po ogłoszeniu przez KE – w grudniu 2020 r. – projektu rozporządzenia Digital Service Act⁹ (DSA) przedstawiło pierwszą wersję swojej propozycji, mającej na celu uregulowanie rynku usług cyfrowych¹⁰.

Dlaczego temat regulacji platform stał się istotny?

Rola platform społecznościowych znacząco ewoluowała. Początkowo miały głównie pełnić funkcję komunikatora dla osób, które na co dzień nie mają ze sobą kontaktu i nie mogą utrzymywać relacji. Poprzez umożliwienie tworzenia kont, a następnie udostępnianie na nich zdjęć, filmów, relacji użytkownicy portali mogą natychmiast dzielić się ze światem swoją prywatnością. Jednakże obecnie poprzez platformy społecznościowe publikowane są nie tylko zdjęcia czy nagrania z wakacji, z rodzinnych wyjazdów, imprez okolicznościowych. Platformy te są teraz miejscem do wyrażania opinii, recenzji, poglądów, a także do przekazywania i rozpowszechniania informacji o aktualnych wydarzeniach z kraju i świata. Jeśli przekazywane informacje byłyby wiarygodne i rzetelne, a wyrażane w komentarzach opinie nie szerzyłyby mowy nienawiści, treści o charakterze terrorystycznym, stanowiąc forum do dyskusji, wówczas wirtualny świat tworzony przez platformy społecznościowe przypominałby idyllę. Niestety, rzeczywistość jest zgoła inna.

Aktualny stan prawny w zakresie świadczenia usług drogą elektroniczną, w tym w szczególności udostępnianiu internetowych serwisów społecznościowych, reguluje przede wszystkim ustawa z 18.7.2002 r. o świadczeniu usług elektronicznych¹¹, wdrażająca dyrektywę 2000/31/WE z 8.6.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym („dyrektywa o handlu elektronicznym”)¹². Mając na uwadze rozwój Internetu, a przy tym platform społecznościowych, których rola w globalnym

i industrialnym społeczeństwie znacząco wzrosła, wydaje się, że obowiązujące regulacje (zarówno unijne, jak i krajowe) zdają się przestarzałe i nie odpowiadać na aktualne problemy w sieci. Z jednej strony istnieje zagrożenie, że nielegalne treści nie będą niezwłocznie usuwane z platformy, ale z drugiej strony jest obawa, że prywatna platforma będzie usuwała treści arbitralnie, naruszając tym samym prawo do wolności słowa zagwarantowane chociażby w art. 54 Konstytucji RP oraz w art. 10 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Pojawia się więc pytanie, kto, w jaki sposób powołany, za pomocą jakich mechanizmów powinien stać na straży wolności słowa, a jednocześnie bezpieczeństwa udostępnianych w Internecie treści.

Prace nad projektem

Podczas konferencji prasowych, mających miejsce 17.12.2020 r. oraz 15.1.2021 r., Minister Sprawiedliwości zapowiedział projekt ustawy mającej na celu ochronę wolności słowa na internetowych serwisach społecznościowych. Informacja ta stała się medialną sensacją i rzekomo m.in. ze względu na liczne zapytania ze strony prasy i innych zainteresowanych stron, w lutym 2021 r. na stronie rządowej Ministerstwa Sprawiedliwości został opublikowany tekst projektu ustawy pt. Ustawa o ochronie wolności użytkowników serwisów społecznościowych¹³. Po wielu tygodniach oczekiwania, tj. 27.9.2021 r., projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych został wpisany do wykazu prac Rady Ministrów pod numerem UD293¹⁴, wywołując tym samym ponowne poruszenie opinii publicznej. Niemniej 10.1.2022 r. opublikowano nową

⁷ Krajowa Rada Radiofonii i Telewizji: „Fake news – dezinformacja online próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski”, Warszawa 2018.

⁸ Tak np. niemiecka ustawa NetzDG – Network Enforcement Act (dalej jako: niemiecka ustawa lub NetzDG), <https://www.gesetze-im-internet.de/netzdg/BjNR335210017.html> (dostęp z 6.1.2022 r.); Francja – ustawa o zwalczaniu manipulowania informacją z 22.12.2018 r. (dalej jako: francuska ustawa), <https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte> (dostęp z 26.6.2022 r.).

⁹ Pl.: „Akt o usługach cyfrowych”.

¹⁰ Z uwagi na ramy niniejszego artykułu i w celu zachowania przejrzystości, autorka nie będzie odnosiła się do treści o charakterze przestępnym, zdefiniowanych w art. 3 ust. 1 pkt 6.

¹¹ T.j. Dz.U. z 2020 r. poz. 344 ze zm.; dalej jako: ŚwUsłElekU. Istotną rolę w tym zakresie odgrywa również Kodeks cywilny, ustawa z 16.7.2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648 ze zm.; dalej jako: PrTelU) oraz ustawa z 10.5.2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781 ze zm.).

¹² Dz.Urz. WE L Nr 178, s. 1; dalej jako: dyrektywa E-commerce.

¹³ Zob. <https://www.gov.pl/web/sprawiedliwosc/zachecamy-do-zapoznania-sie-z-projektem-ustawy-o-ochronie-wolnosci-uzytownikow-serwisow-spoecznościowych> (dalej jako: projekt UWSł albo projekt), (dostęp z 22.5.2022 r.).

¹⁴ Zob. <https://legislacja.rcl.gov.pl/projekt/12351757/katalog/12819479#12819479> (dostęp z 22.5.2022 r.).

wersję projektu ustawy z 3.1.2022 r. wraz ze zmodyfikowanym uzasadnieniem projektu¹⁵. Żadnych uwag do projektu nie złożył KRS, NSA oraz PK, natomiast RPD zadeklarował, iż przedmiot projektowanej regulacji pozostaje poza zakresem jego właściwości. Natomiast uwagi zostały zgłoszone przez KRRIT, RMIŚP, RPO, SN, UKE, UODO, UOKiK.

Uzasadnienie projektu

W uzasadnieniu projektu (zarówno do wersji projektu z 2021 r., jak i 2022 r.) podkreślono, że prawda jest fundamentalnym prawem człowieka stanowiącym o godności człowieczeństwa i chronionym przez wiele dokumentów, a zjawisko masowego blokowania treści w przestrzeni internetowej wymaga wprowadzenia narzędzi, które zapewnią ochronę wyrażonej w art. 54 Konstytucji RP zasady wolności wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. Podkreślono, iż mimo że w doktrynie prawa konstytucyjnego wolność wypowiedzi gwarantowana w art. 54 Konstytucji RP jest wartością fundamentalną dla państwa prawa, nie jest wartością absolutną¹⁶. Ograniczenia wolności wypowiedzi mogą pochodzić z instrumentów prawnych przewidzianych w zakresie zarówno prawa prywatnego, jak i prawa karnego¹⁷. Wszelka ingerencja w upowszechnione treści, będąca niewątpliwie formą ograniczenia konstytucyjnych wolności, może zostać wprowadzona pod warunkami określonymi w art. 31 ust. 3 Konstytucji RP. Zgodnie z treścią tej regulacji ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób. Co istotne, ograniczenia te nie mogą naruszać istoty wolności i praw. Niemniej w uzasadnieniu projektu nie odniesiono się do art. 10 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności¹⁸ (EKPC). Wnioskodawca podkreśla, że informacje umieszczane przez użytkowników portali społecznościowych są często uważane za najważniejsze źródło wiedzy w przedmiocie aktualnych wydarzeń dla szerokiej części społeczeństwa. Ponadto stanowią relevantne miejsce, w którym może się odbywać debata dotycząca aktualnych zagadnień społecznych i politycznych. Dlatego też wnioskodawca wskazuje, że „kluczowe znaczenie ma zatem przeciwdziałanie arbitralnemu oraz bezpodstawnemu izolowaniu określonych podmiotów od podstawowych źródeł informacji, funkcjonujących szeroko w obecnym życiu publicznym”¹⁹. Głównym celem projektu UWSł jest zapewnienie warunków dla zagwarantowania wolności wypowiedzi, zapewnienie prawa do prawdziwej informacji, poprawa ochrony wolności i praw człowieka w udostępnianych w Polsce internetowych serwisach społecznościowych oraz przestrzeganie przez nie wolności do wyrażania poglądów,

opinii, pozyskiwania informacji, rozpowszechniania informacji, wyrażania przekonań religijnych, światopoglądowych i filozoficznych oraz wolności komunikowania się²⁰. Według wnioskodawcy portale społecznościowe notorycznie usuwają arbitralnie treści publikowane przez ich użytkowników, które nie powinny zostać usunięte. Takie postępowanie portali ma stanowić przykład naruszania konstytucyjnie gwarantowanych wolności i praw innych osób. Stąd też relevantnym celem projektu UWSł jest zapewnienie użytkownikom portali ochrony przed wymierzonymi w nich „bezpawnymi działaniami, które nie mieszczą się w realizacji wolności wyrażania opinii, a tym samym nie mogą korzystać z ochrony prawnej”²¹. Sposobem urzeczywistnienia ww. celów mają być przede wszystkim przewidziane w projekcie UWSł regulacje dot. Rady Wolności Słowa, instytucja zaufanych podmiotów sygnalizujących nowe obowiązki dla platform, w tym m.in. obowiązek sprawozdawczy, kary pieniężne oraz instytucja tzw. ślepego pozwu.

Rada Wolności Słowa

Rada Wolności Słowa (RWS), zgodnie z art. 4 projektu, ma być organem administracji publicznej stojącym na straży przestrzegania przez usługodawców²² wolności do wyrażania poglądów, pozyskiwania informacji, rozpowszechniania informacji, wyrażania przekonań religijnych, światopoglądowych i filozoficznych oraz wolności komunikowania się. Ma ona być organem objętym sześcioletnią kadencją i składać się z Przewodniczącego i czterech członków, wobec których projekt przewiduje pewne wymagania, jak: wyłącznie polskie obywatelstwo, korzystanie z pełni praw publicznych, pełną zdolność do czynności prawnych, niekaralność, brak powiązań z organami bezpieczeństwa państwa w rozumieniu art. 2 ustawy z 18.10.2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów²³ w okresie od 22.7.1944 r. do 31.7.1990 r.; nieposzlakowaną opinię, wyższe wykształcenie prawnicze lub niezbędną wiedzę w zakresie językoznawstwa

¹⁵ Zob. <https://legislacja.rcl.gov.pl/projekt/12351757/katalog/12819479#12819479> (dostęp z 22.5.2022 r.).

¹⁶ L. Garlicki, Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2016.

¹⁷ Uzasadnienie projektu UWSł z 3.1.2022 r., s. 1–2, [za:] wyrok TK z 11.10.2006 r., P 3/06, Legalis.

¹⁸ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami Nr 3, 5 i 8 oraz uzupełniona Protokołem Nr 2 (Dz.U. z 1993 r. Nr 61 poz. 284).

¹⁹ Uzasadnienie projektu UWSł z 3.1.2022 r., s. 4.

²⁰ Art. 1 projektu.

²¹ Zob. uzasadnienie projektu z 3.1.2022 r., s. 7.

²² Osoby fizyczne, osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, które świadczą usługę internetowego serwisu społecznościowego (art. 3 pkt 1 projektu).

²³ T.j. Dz.U. z 2021 r. poz. 1633 ze zm.

lub nowych technologii. Zgodnie z uzasadnieniem projektu UWSł wszystkie ww. wymagania muszą zostać spełnione kumulatywnie. Niemniej członkiem RWS nie może być minister, sekretarz stanu, podsekretarz stanu, poseł, senator, poseł do PE, a także radny, wójt (burmistrz, prezydent miasta), zastępca wójta (burmistrza, prezydenta miasta), sekretarz gminy, skarbnik gminy, członek zarządu powiatu, sekretarz powiatu, skarbnik powiatu, członek zarządu województwa, skarbnik województwa, sekretarz województwa oraz osoba należąca do partii politycznej lub osoba, której interesy mogą pozostawać w konflikcie z pełnieniem funkcji członka RWS (zob. art. 6). Według założeń projektu członkowie RWS mają być powoływani przez Sejm RP większością 3/5 głosów w obecności co najmniej połowy ustawowej liczby posłów na wspólną kadencję. Natomiast jeśli w pierwszym głosowaniu kandydat na członka RWS nie uzyskał większości 3/5 głosów albo zgłoszono więcej niż jednego kandydata na członka Rady, a żaden z kandydatów nie uzyskał większości 3/5 głosów, wówczas głosowanie przeprowadza się ponownie, ale Sejm RP powołuje członka RWS już zwykłą większością głosów. Kandydaci na członka RWS zgłaszani są Marszałkowi Sejmu, który najpóźniej na dwa miesiące przed końcem kadencji członków RWS obwieszcza o możliwości składania przez kandydatów zgłoszeń o powołanie do Rady. Do zgłoszenia kandydatów uprawniona jest grupa co najmniej 2000 obywateli RP, którzy ukończyli osiemnaście lat, mają pełną zdolność do czynności prawnych i korzystają z pełni praw publicznych. W tym przypadku nie ma już wymagania, aby w skład grupy wchodziły jednostki, które mają wyłącznie polskie obywatelstwo, ale z brzmienia regulacji wynika, że zagraniczne podmioty, zamieszkujące na terenie Polski, nie będą uprawnione do zgłaszania kandydatów na członków RWS. Projekt przewiduje zamknięty katalog sytuacji, w jakich może dojść do wygaśnięcia członkostwa w RWS – analogicznie ma to miejsce, w sytuacji gdy choć jedna z ww. kryteriów przewidzianych dla kandydatów na członka RWS zostanie naruszona, np. członek nabędzie obywatelstwo innego państwa. Ponadto członkostwo w RWS wygasa z upływem 30 dni od dnia złożenia rezygnacji. Wygaśnięcie członkostwa w RWS niezwłocznie stwierdza postanowieniem Marszałek Sejmu RP. W przypadku wygaśnięcia członkostwa w RWS powołuje się nowego członka na okres, jaki pozostaje do dnia upływu trwającej kadencji członków RWS.

Co istotne, w art. 4 wskazano, iż Przewodniczący prowadzi listę ekspertów RWS, do których RWS może się zwrócić o sporządzenie opinii, gdy na potrzeby postępowania potrzebuje wiadomości specjalnych. Ekspert ma siedem dni na wydanie decyzji²⁴. Ekspertem RWS może być osoba, która korzysta z pełni praw publicznych, ukończyła 25 lat, posiada teoretyczne i praktyczne wiadomości specjalne, w szczególności z zakresu medycyny, prawa, praw człowieka, językoznawstwa, rynku finansowego, bezpieczeństwa publicznego,

informatyki i telekomunikacji²⁵, daje rękojmię należytego wykonywania obowiązków eksperta Rady oraz wyrazi pisemną zgodę na sprawowanie tej funkcji. W ust. 4 art. 14 projektodawca wskazał podmioty, które mogą zgłaszać kandydatów na ekspertów²⁶.

Nie można także pominąć regulacji dotyczących postępowania przed RWS, które zostały umieszczone w rozdziale 6 projektu. Niemniej, w celu zachowania przejrzystości niniejszego artykułu, postępowanie to zostanie przybliżone w dalszej części artykułu.

Zaufane podmioty sygnalizujące

Instytucja zaufanych podmiotów sygnalizujących ma działać w interesie publicznym w celu przeciwdziałania dezinformacji rozpowszechnianej za pośrednictwem internetowych serwisów społecznościowych. W celu dokładniejszej analizy roli zaufanych podmiotów sygnalizujących w walce o bezpieczne portale społecznościowe autor przybliży ustaloną w projekcie UWSł definicję „dezinformacji”. Z brzmienia ww. przepisu wynika, iż podmioty będą mogły zgłaszać tylko treści dot. dezinformacji. Takie założenie potwierdza także treść art. 25 ust. 1²⁷ oraz uzasadnienia projektu²⁸. Należy więc uznać, iż „oddelegowanie” zaufanych podmiotów sygnalizujących do monitorowania jedynie dezinformacji było zabiegiem celowym. Niemniej, dezinformacja wg projektodawców jest klasyfikowana jako treść o charakterze bezprawnym. Zgodnie z definicją treści o charakterze bezprawnym są to treści naruszające dobra osobiste, o charakterze przestępnym, treści, które naruszają dobre obyczaje²⁹, w szczególności rozpowszechniają lub pochwalają przemoc, cierpienie lub poniżenie oraz właśnie dezinformacja. Takie ujęcie dezinformacji stoi w sprzeczności z poglądami unijnymi. W raporcie opracowanym przez niezależną Grupę Wysokiego Szczebla ds.

²⁴ Art. 29 ust. 2 projektu.

²⁵ Posiadanie wiadomości specjalnych ma być udowodnienie poprzez przedłożenie dokumentów lub ew. innych dowodów (projekt nie uściśla, o jakich „innych dowodach” mowa. Natomiast, ocena dostatecznego wykazania posiadania wiadomości specjalnych należy do Przewodniczącego RWS.

²⁶ Do tych podmiotów należą: NIL, NIA, GIF, GIS, GIOŚ, NRA, KIRP, RPP, KRS, Pierwszy Prezes SN; RPO, RPD, KNE, Rzecznik Finansowy, Prezes UOKiK, Prezes UKE, Szef ABW, rektorzy uczelni publicznych oraz ministrowie kierujący działami administracji rządowej.

²⁷ Art. 25. 1. „(...) zaufany podmiot sygnalizujący niezadowolony ze sposobu rozpatrzenia w wewnętrznym postępowaniu kontrolnym reklamacji w przedmiocie rozpowszechniania dezinformacji (...)”.

²⁸ „Oprócz zdefiniowania pojęcia dezinformacji, podmiotom powołanym do jej zwalczania w interesie publicznym, tj. zaufanym podmiotom sygnalizującym, które będą certyfikowane przez fachowe organy państwowe, przyznano szczególne uprawnienia” – zob. uzasadnienie, s. 5.

²⁹ Uwagi do definicji treści bezprawnych zgłosił także Prezes UOKiK, który zwraca uwagę na potencjalne problemy związane z brakiem rozgraniczenia kompetencji pomiędzy Prezesem UOKiK a Radą Wolności Słowa, które mogą odmiennie ocenić naruszenie przez opublikowaną treść dobrych obyczajów z obszaru ochrony konsumentów.

falszywych wiadomości i dezinformacji w Internecie (ang. *independent High level Group on fake news and online disinformation*) pt. *A multi-dimensional approach to disinformation* z 2018 r. przedstawiono i omówiono problematykę zjawiska dezinformacji, jego definicje, skalę zagrożenia, którą za sobą niesienie, oraz przedstawiono sposoby, które dotychczas zostały podjęte do zwalczania dezinformacji, jak też te, które mogłyby zostać wprowadzone. W Raporcie podkreślono, iż pomiędzy dezinformacją a fake newsami nie może zostać postawiony znak równości. Autorzy raportu wskazują, że obecne debaty na temat fake newsów obejmują spektrum rodzajów informacji; są to zarówno treści o stosunkowo niskim ryzyku, takie jak pomyłki reporterów, stroniczy dyskurs polityczny, jak i treści o wysokim ryzyku, jak np. działania obcych państw lub grup krajowych, które próbują osłabić proces polityczny w państwach członkowskich UE i w UE, wykorzystując różne formy złośliwych fabrykacji, infiltracji. Raport koncentrował się przede wszystkim na dezinformacji, która niesie za sobą ryzyko szkód obejmujących zagrożenia dla demokratycznych procesów politycznych i wartości, które mogą dotyczyć różnych sektorów, takich jak zdrowie, nauka, edukacja, finanse i inne. Ryzyko to wynika z produkcji i promocji dezinformacji dla korzyści ekonomicznych lub celów politycznych czy ideologicznych, ale może być także zaostreżone przez sposób, w jaki różni odbiorcy przekazują informacje³⁰. Dezinformacja jest definiowana w raporcie jako fałszywa, niedokładna lub błędna informacja zaprojektowana, prezentowana i promowana w celu wyrządzenia szkody społeczeństwu lub dla zysku³¹. Dezinformacja, zgodnie z ww. definicją, obejmuje formy wypowiedzi, które nie są już nielegalne, ale mimo to mogą być szkodliwe. W ujęciu unijnym więc dezinformacja nie stanowi (lub nie musi stanowić) treści nielegalnej. Natomiast w polskim projekcie dezinformacja, zgodnie z literalnym brzmieniem art. 3 ust. 1 pkt 1, powinna stanowić treść o charakterze nielegalnym, co stanowi znaczące ograniczenie dla monitorowania treści na portalach społecznościowych przez zaufane podmioty sygnalizujące. Zwłaszcza że jak zostało ujęte w raporcie, nie tylko nielegalne treści mogą być szkodliwe. Warto zwrócić uwagę, że projektodawca wskazał w uzasadnieniu, iż definicja dezinformacji została skonstruowana na podstawie Unijnego kodeksu postępowania w zakresie zwalczania dezinformacji z 2018 r.³². Niemniej w Kodeksie tym również nie sklasyfikowano dezinformacji jako treści o charakterze bezprawnym.

Podsumowując, mimo twierdzeń projektodawców co do tego, iż polska propozycja definicji dezinformacji jest węższa i precyzyjniejsza od unijnych uregulowań, wydaje się ona nie brać pod uwagę będących dezinformacją treści, które nie są jednocześnie bezprawne. Niemniej te treści (pomimo braku charakteru bezprawności), jeśli niosą za sobą szkodę i krzywdę, również powinny być poddane kontroli i ew. zablokowane, usunięte. Oczywiście wciąż mając na uwadze „konstytucyjne

wymogi, zezwalające na ingerowanie w rozpowszechnianie jakichkolwiek informacji, jedynie wtedy, gdy jest to niezbędne w demokratycznym państwie prawnym i nie narusza istoty prawa do wolności słowa”³³.

Wracając do regulacji *strictae* dot. instytucji zaufanych podmiotów sygnalizujących, w pierwszej kolejności należy wspomnieć, iż pierwszy projekt ustawy, tj. z grudnia 2021 r., nie przewidywał takiej instytucji. Została ona wprowadzona w drugiej wersji projektu z 2022 r. i zgodnie z tą wersją zaufanym podmiotem sygnalizującym może zostać osoba fizyczna, która posiada specjalistyczną wiedzę, w szczególności z zakresu medycyny, prawa, praw człowieka, rynku finansowego lub bezpieczeństwa publicznego, ale także organizacja społeczna, do której statutowych celów należy zwalczanie dezinformacji w przestrzeni publicznej³⁴. Projektodawca przedstawił zamknięty katalog podmiotów (tzw. podmiotów certyfikujących), które mogą wyznaczyć zaufane podmioty sygnalizujące i jest to FGIF, GIS, GIOŚ, RPP, RPO, RPP, KNF, Prezes UOKiK, Szef ABW, ministrowie kierujący działami administracji rządowej. Podmioty te zgłaszają RWS wybrane zaufane podmioty sygnalizujące po wyrażeniu przez nie

³⁰ W raporcie termin „fake news” został pominięty celowo z dwóch powodów. Po pierwsze, termin ten jest nieodpowiedni do uchwycenia złożonego problemu dezinformacji, który obejmuje treści, które nie są w rzeczywistości lub całkowicie „fałszywe”, lecz stanowią sfabrykowane informacje zmieszane z faktami, a także praktyki, które wykraczają daleko poza wszystko, co przypomina „wiadomości”, i obejmują pewne formy automatycznych kont, które mogą być wykorzystane np. do zorganizowanego trollingu. Może również obejmować cały wachlarz zachowań cyfrowych, które w większym stopniu polegają na rozpowszechnianiu dezinformacji niż na jej wytwarzaniu, począwszy od zamieszczania postów, komentowania, udostępniania, tweetowania i re-tweetowania itp (za: C. Wardle, H. Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Report to the Council of Europe 2017, <https://shorensteincenter.org/information-disorder-framework-for-research-and-policy-making/> (dostęp z 19.6.2022 r.)). Po drugie, termin „fake news” jest nie tylko nieadekwatny, lecz także mylący, ponieważ został zawłaszczony przez niektórych polityków i ich zwolenników, którzy używają go do odrzucania informacji, z którymi się nie zgadzają, i stał się w ten sposób bronią, za pomocą której wpływowe podmioty mogą ingerować w obieg informacji oraz atakować i osłabiać niezależne media informacyjne. Badania wykazały, że obywatele kojarzą termin „fake news” z partyzancką debatą polityczną i słabym dziennikarstwem, a nie z bardziej szkodliwymi i precyzyjnie zdefiniowanymi formami dezinformacji (R.K. Nielsen, L. Graves, *News You Don't Believe: Audience Perspectives on Fake News*, Oxford 2017).

³¹ Zob. Raport, s. 10.

³² Code of Practice on Disinformation 2018, <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation> (dostęp z 19.6.2022 r.); dalej jako: Kodeks. Definicja dezinformacji zawarta w Kodeksie natomiast w głównej mierze odnosi się do komunikatu Komisji Europejskiej „Zwalczanie dezinformacji w internecie: podejście europejskie” z 2018 r. <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018DC0236&qid=1556211423628&from=PL> (dostęp z 19.6.2022 r.). Kodeks odnosi się także do rekomendacji Komisji zawartych w ww. komunikacie, że sygnatariusze mają świadomość podstawowego prawa do wolności wypowiedzi i otwartego internetu, a także delikatnej równowagi, którą należy zachować przy podejmowaniu starań na rzecz ograniczenia rozpowszechniania i wpływu treści, które są zgodne z prawem (zob. Kodeks, s. 1).

³³ Zob. Uzasadnienie, s. 16.

³⁴ Zob. art. 15 projektu.

zgody, z urzędu. Lista zaufanych podmiotów sygnalizacyjnych ma być publikowana w BIP. Co istotne, podmiotom certyfikującym przysługują uprawnienia zaufanego podmiotu sygnalizującego³⁵. Mówiąc o „uprawnieniach”, projektodawca proponuje regulację, zgodnie z którą, jeśli zaufane podmioty sygnalizujące zgłoszą daną treść do usługodawcy, wówczas zarówno ich zgłoszenia, jak i ew. reklamacje powinny być traktowane jako te „zaufane”, ponieważ od wykwalifikowanych, wyspecjalizowanych podmiotów, i przez to priorytetowe (a więc przed zgłoszeniami np. użytkowników ów portalu społecznościowego). Jeśli więc ww. podmiotom certyfikującym mają zostać przyznane uprawnienia zaufanych podmiotów sygnalizujących, które to, jak zostało wyżej wspomniane, mogą zgłaszać jedynie bezprawną dezinformację, to należy domniemać, iż podmioty certyfikujące będą mogły zgłaszać analogicznie takie same treści. Ponadto projekt nie precyzuje, czy zaufany podmiot sygnalizujący będzie uprawniony do zgłaszania wszystkich treści czy też tylko tych, w których się specjalizuje. Idąc dalej, zastanawiające jest, czy KNF jako podmiot certyfikujący posiadający uprawnienia zaufanego podmiotu sygnalizującego będzie mogła zgłaszać tylko treści z obszaru rynku finansowego, czy też będzie mogła także (korzystając z przywilejów zaufanego podmiotu zgłaszającego) zgłosić treści z zakresu prawa autorskiego. Ponadto zaufane podmioty sygnalizujące będą uprawnione do wnoszenia do RWS skarg na rozstrzygnięcia usługodawców w sprawie rozpowszechniania dezinformacji. Usługodawcy są również zobowiązani do wprowadzenia niezbędnych środków technicznych i organizacyjnych, aby zapewnić priorytetowe i niezwłoczne rozpatrywanie zgłoszeń oraz reklamacji zaufanych podmiotów sygnalizujących (art. 22 ust. 6).

Należy również wspomnieć, iż instytucja dot. zaufanych podmiotów sygnalizujących (ang. *trusted flaggers*) nie jest *novum*, na szczeblu unijnym bowiem została ona przewidziana w Digital Service Act (DSA)³⁶, a wcześniej także chociażby w Zaleceniach Komisji (UE) 2018/334 z 1.3.2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie³⁷. Ponadto portale społecznościowe jak np. YouTube już w 2012 r. zaczęły prowadzić swój własny program pt. Heroes trusted flagger³⁸. Brak w projekcie w wersji z 2021 r. regulacji w przedmiocie „zaufanych podmiotów sygnalizujących” podkreślił RPO w swojej opinii do projektu UWSł z 26.10.2021 r.³⁹.

W art. 19 ust. 1 DSA, w wersji z czerwca 2022 r.⁴⁰, wskazuje, iż dostawcy platform internetowych (ang. „*providers of online platform*”) powinni podjąć niezbędne środki techniczne i organizacyjne w celu zapewnienia, aby zawiadomienia składane przez zaufane podmioty sygnalizujące (ang. „*trusted flaggers*”), działające w ramach wyznaczonego obszaru wiedzy specjalistycznej, za pośrednictwem mechanizmów, o których mowa w art. 14, były przetwarzane i rozpatrywane w sposób priorytetowy i bez zbędnej zwłoki. W ww. art. 14

wspomniana jest procedura *notice and action*, stąd też przyjęto, iż *trusted flaggers* mają stanowić „przedłużenie” tej procedury. Niemniej takie brzmienie art. 19 ust. 1 nie było zaproponowane w pierwotnej wersji projektu z grudnia 2020 r.⁴¹. Po pierwsze, art. 19 odnosił się bezpośrednio do platform internetowych, a nie do dostawców platform internetowych jak obecnie. Po drugie, ustalono, iż *trusted flaggers* mogą działać, a dokładniej mieć uprawnienia, tylko w relacji do branży, która została im wyznaczona (np. tylko odnośnie do treści o charakterze terrorystycznym). Po trzecie, sprecyzowano, iż zawiadomienia zgłaszane przez *trusted flaggers* mają być rozpatrywane bez zbędnej zwłoki (wcześniej było jedynie wskazane, iż mają być rozpatrywane bez zwłoki). Status *trusted flagger* w świetle DSA przyznaje, na wniosek dowolnego podmiotu, Koordynator ds. usług cyfrowych w państwie członkowskim, w którym wnioskodawca ma siedzibę. Nie ma więc, tak jak w polskim projekcie UWSł, zamkniętego katalogu podmiotów mogących zgłaszać zaufane podmioty sygnalizujące. DSA nakłada również na *trusted flaggers* obowiązek publikacji, co najmniej raz w roku sprawozdania dotyczące zawiadomień złożonych zgodnie z art. 14 (a więc w trybie procedury *notice and action*). W sprawozdaniu podaje się co najmniej liczbę powiadomień skategoryzowanych według: (a) tożsamości podmiotu świadczącego usługi hostingowe; (b) rodzaju rzekomo nielegalnej treści, której dotyczy powiadomienie; (c) działań podjętych przez usługodawcę. Sprawozdania te zawierają wyjaśnienie procedur stosowanych w celu zagwarantowania, że *trusted flagger* zachowuje swoją niezależność. Istotne jest także, że w omawianym art. 19 DSA przewidziano także procedurę kontrolowania działań *trusted*

³⁵ Zob. art. 16 projektu.

³⁶ Projekt rozporządzenia DSA z grudnia 2020 r.

³⁷ „W uzupełnieniu odpowiednich organów również określone osoby fizyczne lub podmioty, w tym organizacje pozarządowe i stowarzyszenia handlowe, mogą posiadać szczególną wiedzę fachową i być gotowe do przejścia, na zasadach dobrowolności, określonej odpowiedzialności związanej ze zwalczaniem nielegalnych treści w internecie. W świetle wnoszonej przez te podmioty wartości dodanej i czasami wysokiej liczby przedmiotowych zawiadomień należy zachęcać do współpracy między takimi zaufanymi podmiotami sygnalizującymi i dostawcami usług hostingowych, zwłaszcza poprzez traktowanie realizowanych przez nich zgłoszeń w sposób priorytetowy i z odpowiednim stopniem zaufania, jeżeli chodzi o dokładność tych zgłoszeń. Jednak w związku z ich szczególnym statusem współpraca taka powinna być otwarta jedynie dla osób fizycznych i podmiotów przestrzegających wartości, na których opiera się Unia i które określono w art. 2 TUE, spełniających pewne odpowiednie warunki, które z kolei powinny być dostępne publicznie w sposób wyraźny i obiektywny” – pkt 28 Zaleceń Komisji (UE) 2018/334 z 1.3.2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie.

³⁸ Zob. <https://blog.youtube/news-and-events/growing-our-trusted-flagger-program/> (dostęp z 20.6.2022 r.).

³⁹ Stanowisko RPO w przedmiocie uwag do projektu UWSł z 26.10.2021 r., s. 11.

⁴⁰ Zob. <https://www.consilium.europa.eu/pl/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/> (dostęp z 20.6.2022 r.).

⁴¹ Zob. <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:825:FIN> (dostęp z 20.6.2022 r.).

flaggers oraz określono warunki i procedurę odebrania im statusu *trusted flagger*. W przypadku gdy dostawca platform internetowych posiada informacje wskazujące na to, że *trusted flagger* złożył znaczną liczbę nieprecyzyjnych, niedokładnych lub nieodpowiednio uzasadnionych zawiadomień w trybie art. 14, przekazuje te informacje koordynatorowi ds. usług cyfrowych, który przyznał danemu podmiotowi status *trusted flagger*. Na czas trwania postępowania status zaufanego podmiotu oflagowującego zostaje zawieszony na czas dochodzenia, które powinno zostać przeprowadzone bez zbędnej zwłoki. Natomiast projektowane polskie regulacje w przedmiocie zaufanych podmiotów sygnalizujących nie przewidują podobnych mechanizmów kontroli jak w przypadku DSA. W przeciwieństwie do polskiego projektu, w świetle DSA, status *trusted flagger* nie może zostać przyznany osobie fizycznej. Zarówno DSA, jak i projekt UWSł nie przewidują, by status ten miał charakter kadencyjny

Obowiązki usługodawców

Przez „usługodawcę” rozumie się osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę internetowego serwisu społecznościowego⁴². Natomiast przez „internetowy serwis społecznościowy” rozumie się usługę świadczoną drogą elektroniczną w rozumieniu ustawy o świadczeniu usług drogą elektroniczną, która umożliwia udostępnianie przez użytkowników dowolnych treści innym użytkownikom lub ogółowi, z której korzysta na terytorium RP co najmniej jeden milion użytkowników, którzy założyli profil użytkownika, chyba że usługa jest wyłącznie funkcją innej usługi, stanowiącej usługę główną, a ze względów obiektywnych lub technicznych nie można jej wykorzystać bez usługi głównej lub ma charakter wyłącznie wspierający funkcjonalność usługi głównej⁴³. Ta wersja definicji różni się od tej z projektu z 2020 r. Poprzednia nie zawierała w sobie żadnego wyłączenia, na co zwrócił uwagę RPO w swojej opinii do projektu z 2020 r. RPO wskazał, że zgodnie z definicją serwisu społecznościowego w wersji projektu UWSł zakresem ustawy objęte zostaną nie tylko portale społecznościowe, takie jak Facebook czy Twitter, ale również portale informacyjne umożliwiające komentowanie publikowanych artykułów czy komunikatory internetowe.

Projektodawca w art. 18 nakłada na usługodawców, którzy otrzymują w roku kalendarzowym ponad 100 zgłoszeń dotyczących rozpowszechniania treści o charakterze bezprawnym, obowiązek sporządzenia w języku polskim, co pół roku, sprawozdania w przedmiocie sposobu rozstrzygnięcia zgłoszeń i reklamacji w danym półroczu. Sprawozdanie to ma również zostać opublikowane w tymże internetowym serwisie społecznościowym. W ust. 2 art. 18 wskazane są elementy, które muszą znaleźć się w owym sprawozdaniu, przy czym są to elementy jedynie podstawowe i usługodawca może upublicz-

nić więcej danych⁴⁴. Ponadto w art. 19 ust. 1 przewidziano, że usługodawca jest obowiązany do udzielania odpowiedzi i wszelkich informacji organom państwowym uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań. Niemniej przepis nie precyzuje, jakiego obszaru miałyby dot. zapytania i czy usługodawca będzie mógł odmówić przedłożenia odpowiedzi z uwagi na nadzwyczajne okoliczności lub swój interes biznesowy.

Kolejnym obowiązkiem, uregulowanym w rozdziale 5, jest zobowiązanie usługodawcy do ustanowienia w języku polskim skutecznego, zrozumiałego, tzw. wewnętrznego postępowania kontrolnego, pozwalającego na elektroniczne przysyłanie użytkownikom ów portali społecznościowych zgłoszeń⁴⁵ oraz reklamacji⁴⁶. Jeśli zgłoszenie albo reklamacja zawiera adres poczty elektronicznej, usługodawca ma niezwłocznie przesłać na ten adres potwierdzenie ich otrzymania. Niezwłocznie, czyli nie później niż w ciągu 48 godzin od dnia otrzymania zgłoszenia czy reklamacji, ponieważ usługodawca ma 48 godzin na rozpatrzenie zgłoszenia i reklamacji od chwili ich wniesienia. W tym samym czasie usługodawca ma przesłać drogą elektroniczną informację o sposobie ich rozpatrzenia, w tym na adres poczty elektronicznej, o ile został wskazany przez użytkownika. Niemniej w opinii autora przepis ten nie przesądza, czy termin 48 godzin obowiązuje także w przedmiocie obowiązku informacyjnego nałożonego na usługodawcę. Jeśli usługodawca miałby także informować, jaka decyzja zapadła do zgłoszonej treści, wówczas powinno to zostać uściślone⁴⁷. O sposobie rozpatrzenia zgłoszenia albo reklamacji usługodawca w każdym przypadku ma także informować użytkownika, który udostępnił treść lub założył profil użytkownika będące przedmiotem wewnętrznego postępowania kontrolnego. Z literalnego brzmienia regulacji nie wynika jednak, by usługodawca informował podmiot, który opublikował zgłoszoną treść, o danych zgłaszającego.

Informacja o sposobie rozpatrzenia zgłoszenia albo reklamacji powinna zawierać przyczyny rozstrzygnięcia wskazujące w szczególności podstawy prawne z odwołaniem się do regulaminu internetowego serwisu społecznościowego oraz podstawy faktyczne rozstrzygnięcia wraz z uzasadnieniem (art. 22 ust. 5). W niemieckiej ustawie natomiast serwisy mają obowią-

⁴² Art. 3 ust. 1 pkt 2 projektu.

⁴³ Art. 3 ust. 1 pkt 1 projektu.

⁴⁴ Przykładowo sprawozdanie ma zawierać co najmniej ogólne informacje dotyczące działań podjętych przez usługodawcę w zakresie zapobiegania udostępnianiu treści o charakterze bezprawnym; łączną liczbę zgłoszeń i łączną liczbę reklamacji, które wpłynęły w okresie sprawozdawczym – zob. art. 18 ust. 2 projektu UWSł.

⁴⁵ Przedmiotem zgłoszenia jest rozpowszechnianie treści o charakterze bezprawnym (art. 23).

⁴⁶ Od rozstrzygnięcia wydanego w wyniku zgłoszenia użytkownikowi, który dokonał zgłoszenia albo udostępnił treść lub założył profil użytkownika będące przedmiotem zgłoszenia, przysługuje reklamacja.

⁴⁷ Przykładowo usługodawca rozpatruje zgłoszenia w terminie 48 godzin od ich wniesienia i w tym czasie przysyła także drogą elektroniczną informację o sposobie rozpatrzenia zgłoszenia.

zek usuwania treści (np. filmów i komentarzy), które są „w sposób oczywisty niezgodne z prawem”, w ciągu 24 godzin od powiadomienia. Jeśli legalność (lub jej brak) nie jest oczywista, dostawca ma maksymalnie siedem dni na podjęcie decyzji dotyczącej postępowania w danym przypadku. W wyjątkowych sytuacjach czas na podjęcie decyzji może być dłuższy – jeśli użytkownicy przesyłający treści, czyli użytkownicy, których filmy lub komentarze są zapisywane w YouTube (przesyłający), zostaną poproszeni o odniesienie się do uwag lub gdy decyzja jest przekazywana organizacji branżowej akredytowanej jako instytucja regulowania wewnętrznego⁴⁸.

W przypadku gdy użytkownik nie jest usatysfakcjonowany z wyniku wniesionej w wewnętrznym postępowaniu kontrolnym reklamacji czy też zaufany podmiot sygnalizujący nie jest zadowolony ze sposobu rozpatrzenia reklamacji, ale już tylko w przedmiocie rozpowszechniania dezinformacji mogą wnieść skargę do RWS w terminie siedmiu dni od otrzymania informacji o sposobie rozpatrzenia reklamacji⁴⁹. Użytkownik wnosi skargę do Rady na piśmie utrwalonym w postaci elektronicznej na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z 18.11.2020 r. o doręczeniach elektronicznych⁵⁰. Skargę opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym⁵¹. Skarga ma zawierać: imię i nazwisko, nazwę lub firmę użytkownika oraz jego przedstawiciela ustawowego lub ew. pełnomocnika, oznaczenie usługodawcy i pełnomocnika do doręczeń w kraju, opis naruszenia, wskazanie żądania, podpis i ew. wymienienie załączników. RWS jest uprawniona do pominięcia dowodów, które prowadziłyby do przedłużenia postępowania. Niemniej nie jest wskazane w projekcie, o jakiego rodzaju dowodach mowa, ani czy RWS będzie zobowiązana wyjaśnić, z jakich przyczyn uważała, że ów dowód może przedłużyć postępowanie; uzasadnienie projektu również nie rozwija regulacji (art. 29 ust. 3). Warto zwrócić uwagę, że projektodawca wskazał ścisły krąg podmiotów, którym przysługuje status strony postępowania przed RWS. Jest nią (1) użytkownik, któremu ograniczono dostęp do treści, albo (2) któremu ograniczono dostęp do profilu użytkownika, albo (3) zaufany podmiot sygnalizujący i (4) usługodawca⁵². Taki katalog podmiotów nie uwzględnia jednak samego zgłaszającego daną treść. O wniesionej skardze niezwłocznie zawiadamiany jest usługodawca⁵³, który ma 24 godziny na przekazanie RWS materiałów zgromadzonych w wewnętrznym postępowaniu kontrolnym, w tym reklamacji. Ustawa nie precyzuje, w jaki sposób te dane miałyby zostać przekazane.

Zgodnie z art. 30 postępowanie prowadzone przed RWS może zakończyć się decyzją w przedmiocie (1) nakazania zniesienia ograniczenia dostępu do treści albo (2) odmowy nakazania zniesienia tego ograniczenia; albo w przedmiocie (3) nakazania zniesienia ograniczenia dostępu do profilu użytkownika albo odmowy nakazania zniesienia tego ograni-

czenia. Jeśli natomiast zaufane podmioty sygnalizujące mogą zgłaszać jedynie dezinformację, to projektodawca wykluczył tę instytucję także ze zgłaszania danych profili użytkowników. Dlatego też decyzje RWS w przedmiocie zgłoszeń pochodzących od zaufanych podmiotów sygnalizujących mogą dotyczyć nakazania uniemożliwienia rozpowszechniania treści albo odmowy nakazania uniemożliwienia rozpowszechniania treści. Niemniej, jeśli na danym profilu użytkownika notorycznie są udostępniane treści dezinformacyjne, to nieekonomiczne i nieefektywne wydaje się zgłaszanie przez zaufany podmiot sygnalizujący każdej z tych treści. W takim przypadku zaufany podmiot sygnalizujący (którego kompetencje w walce z bezprawnymi treściami i tak zostały przez projekt znacznie ograniczone) mógłby zgłosić cały profil użytkownika, który szerzy dezinformację w sieci.

Projektodawca zobowiązał także usługodawcę do zapewnienia, aby reklamacje nie były rozpatrywane wyłącznie z wykorzystaniem zautomatyzowanych środków (art. 24 ust. 4). Z literalnego brzmienia regulacji wynika zatem, że automatyczne rozpatrywanie części reklamacji nie jest całkowicie wykluczone, niemniej nie uściślono, jaka część może być rozpatrywana w trybie zautomatyzowanym. Ponadto, zgodnie z art. 33, jeśli dana treść była już przedmiotem badań przed RWS, usługodawca nie może ponownie ograniczyć dostępu do tej treści. Niemniej można sobie wyobrazić sytuację, w której przedmiotem zgłoszenia jest treść, która narusza prawo do znaku towarowego, a zgłoszenia dokonuje użytkownik, który nie jest właścicielem tego znaku i nie ma do niego praw. Ostatecznie RWS stwierdza, iż ta treść nie narusza prawa, ale informacja o niej dochodzi do rzeczywistego właściciela znaku. Pytanie, czy w takim przypadku treść ponownie nie będzie mogła być zgłoszona. Wątpliwości budzi również zmiana okoliczności sprawy, aktualnej sytuacji na świecie czy też właśnie zmiana podmiotu zgłaszającego udostępnioną treść. Dlatego też przepis powinien precyzować, w jakich okolicznościach, w zależności od tego, jaki podmiot zgłasza treść, kolejne postępowanie w przedmiocie tożsamej treści przed RWS byłoby bądź nie byłoby dozwolone.

Rada ma doręczyć decyzję stronom⁵⁴ postępowania niezwłocznie, ale nie później niż w terminie 24 godzin od jej

⁴⁸ Zob. <https://transparencyreport.google.com/netzdg/youtube?hl=pl> (dostęp z 28.6.2022 r.).

⁴⁹ Art. 25 projektu.

⁵⁰ T.j. Dz.U. z 2022 r. poz. 569 ze zm.

⁵¹ Do skargi użytkownik obowiązany jest dołączyć informację o sposobie rozpatrzenia reklamacji, chyba że wnosi skargę, bo nie uzyskał na czas informacji w zakresie sposobu rozstrzygnięcia wniesionej reklamacji (zob. art. 25–26 projektu).

⁵² Art. 27 projektu.

⁵³ Jeżeli skarga została wniesiona przez zaufany podmiot sygnalizujący, wówczas usługodawca jest o tym informowany. Projekt nie precyzuje jednak, czy usługodawca jest informowany bezpośrednio o imieniu i nazwisku/nazwie zaufanego podmiotu sygnalizującego czy tylko generalnie o tym, że skargę wniosła ta instytucja.

⁵⁴ Taka regulacja art. 32 oznacza, że zgłaszający treść nie otrzyma informacji o finalnej decyzji RWS.

wydania. Usługodawca również zobowiązany jest wykonać decyzję RWS niezwłocznie, nie później niż w terminie 24 godzin od jej doręczenia. Ponadto usługodawca w terminie 24 godzin od upływu terminu do wykonania decyzji, o którym ma poinformować RWS o sposobie jej wykonania (art. 32 projektu)⁵⁵. W ocenie projektodawcy termin 24 godzin na wykonanie przez usługodawcę decyzji RWS będzie całkowicie wystarczający, gdyż „w tym terminie nie będzie podejmował dodatkowych czynności analitycznych, a jedynie, zgodnie z decyzją Rady, przywracał wcześniej ograniczony dostęp do treści lub ograniczony dostęp do profilu użytkownika”⁵⁶. Termin wprowadzenia 24 godzin uzasadniony został również tym, aby czas ograniczenia wolności słowa trwał jak najkrócej⁵⁷. Za brak subordynacji z przepisami projektu na usługodawców mogą zostać nałożone, na podstawie Kodeksu postępowania karnego, grzywny w wysokości od 50 000 zł do 50 000 000 zł i będą podlegały egzekucji administracyjnej na podstawie art. 2 § 1 pkt 2 ustawy z 17.6.1966 r. o postępowaniu egzekucyjnym w administracji⁵⁸. W sprawach nieuregulowanych w rozdziale dotyczącym postępowania przed RWS mają być stosowane przepisy Kodeksu postępowania administracyjnego ze wskazanymi wyłączeniami⁵⁹.

Strona niezadowolona z decyzji Rady będzie uprawniona do złożenia skargi do sądu administracyjnego⁶⁰. Natomiast, z uwagi na fakt, że zgłaszającemu daną treść nie został przyznany status strony, nie będzie mógł on złożyć skargi do WSA.

Ślepy pozew

Powództwo nie zostanie zainicjowane, jeżeli powód nie oznaczy prawidłowo pozwanego⁶¹. Dlatego też dochodzenie swoich praw przeciwko użytkownikom portali społecznościowych, którzy przez swoją aktywność naruszają prawa innych i szerzą treści bezprawne, często nie jest możliwe; wynika to bowiem z faktu, że powód nie jest w stanie dowiedzieć się albo zweryfikować danych potencjalnego pozwanego. Rozwiązaniem tego patu ma być instytucja pozwu ślepego, która miałaby zostać dodana do Kodeksu postępowania cywilnego w drodze art. 38 pkt 1 projektu, w części pierwszej, w księdze pierwszej Kodeksu postępowania cywilnego jako rozdział IX.

Pomysł wprowadzenia instytucji pozwu ślepego do polskiej procedury cywilnej nie stanowi *novum*. W dniu 17.5.2016 r. RPO wystąpił do Ministra Sprawiedliwości z inicjatywą podjęcia prac legislacyjnych w przedmiocie umożliwienia wprowadzenia instytucji ślepego pozwu⁶². Rzecznik podkreślił, że instytucja ta mogłaby się przyczynić do zminimalizowania ilości wszczynanych postępowań karnych, administracyjnych i sądowoadministracyjnych tylko w jednym celu – uzyskania w nich danych osobowych, które mogłyby zostać wykorzystywane w kolejnym postępowaniu⁶³. Wprowadzenie instytucji „ślepego pozwu” było także postulowane przez posłów „Nowoczesnej” w czerwcu 2017 r. w projekcie ustawy o zmianie ustawy – Kodeks postępowania

cywilnego oraz ustawy – Prawo telekomunikacyjne (druk Nr 1715)⁶⁴. Należy również przywołać uzasadnienie uchwały SN z 20.8.2020 r.⁶⁵, zgodnie z którym w obecnym stanie prawnym „powód dochodzący roszczeń o ochronę dóbr osobistych musi zidentyfikować osobę, której zarzuca czyn będący formą takiego naruszenia i wykazać, że pozwany dopuścił się zarzucanego mu czynu. Ustawodawca nie przewidział odmiennych zasad dochodzenia tego rodzaju roszczeń, gdy czyn naruszający dobra osobiste miał miejsce w sieci Internet. Także w takim przypadku powód musi zatem oznaczyć pozwanego już na etapie wniesienia pozwu”. W orzeczeniu tym SN przyjął dopuszczalność żądania od podmiotu związanego tajemnicą telekomunikacyjną informacji pozwalających zweryfikować twierdzenie powoda, że czynu naruszającego dobra osobiste dopuścił się pozwany w sprawie, na podstawie art. 159 ust. 2 pkt 4 PrTelU⁶⁶. Niemniej powód wciąż jest zobowiązany oznaczyć pozwanego w pozwie. Dlatego też jedynym remedium na zapewnienie możliwości wszczęcia postępowania przeciwko nieznanemu „hejterowi” ma być właśnie instytucja ślepego pozwu.

W świetle projektu regulacje w przedmiocie ślepego pozwu będą aplikowały wyłącznie do spraw o ochronę dóbr osobistych, które naruszono za pośrednictwem usługi świadczonej drogą elektroniczną i będą należały do właściwości sądów

⁵⁵ W zakresie nieuregulowanym w Rozdziale 6 (Postępowanie przed RWS) stosuje się odpowiednio przepisy Kodeksu postępowania administracyjnego – zob. art. 34 projektu.

⁵⁶ Zob. uzasadnienie, s. 37.

⁵⁷ *Ibidem*.

⁵⁸ T.j. Dz.U. z 2022 r. poz. 479 ze zm.

⁵⁹ Art. 8 § 2, art. 10, art. 28, art. 31, art. 36, art. 38, art. 77 § 1, art. 79, art. 89–98, art. 114–122h., art. 217–220. Do decyzji RWS nie stosuje się art. 61 i art. 152 § 1 ustawy z 30.8.2002 r. Prawo o postępowaniu przed sądami administracyjnymi, t.j. Dz.U. z 2022 r. poz. 329 ze zm.; dalej jako: PrPostSądAdmU – zob. art. 34 projektu.

⁶⁰ Na podstawie art. 3 § 2 PrPostSądAdmU.

⁶¹ Art. 187 w zw. z 126 § 1 pkt 1 KPC.

⁶² Funkcjonującej w systemie anglosaskim instytucji tzw. ślepego pozwu (*John Doe lawsuit*).

⁶³ W mniemaniu RPO kluczowym problemem jest zwykle anonimowość osoby, która złamała prawo: ofiara nie wie i nie jest w stanie samodzielnie ustalić, kto dokonał obraźliwego bądź zniesławiającego ją wpisu. Rzecznik w swoim wystąpieniu nawiązał także do koncepcji ślepego pozwu, funkcjonującej z powodzeniem od wielu lat (w najbardziej klasycznej formie) w procesie anglosaskim – *John Doe lawsuit*. „Tożsamość pozwanego jest nieznaną we wstępnej fazie procesu, dopiero w trakcie postępowania sąd ustala wszelkie potrzebne dane osoby pozwanej. Instytucja ta zapewnia możliwość uzyskania danych anonimowego sprawcy szkody, jednak równocześnie chroni prywatność potencjalnego pozwanego – wykluczony jest wszelki automatyzm w korzystaniu z tego narzędzia prawnego” – wystąpienie RPO do Ministra Sprawiedliwości ws. zwalczania mowy nienawiści w Internecie z 17.5.2016 r., <https://bip.brpo.gov.pl/sites/default/files/Wystapienie%20do%20Ministra%20Sprawiedliwosci%20ws%20zwalczania%20mowy%20nienawisci%20w%20internecie%2017.05.2016.pdf> (dostęp z 20.6.2022 r.), [za:] M. Mazzotta, Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers, 51 Boston College Law Rev. 833 (2010), s. 845 i n., <http://lawdigitalcommons.bc.edu/bclr/vol51/iss3/6> (dostęp z 20.6.2022 r.).

⁶⁴ Projekt ten został odrzucony w pierwszym czytaniu na 48. posiedzeniu Sejmu VIII kadencji 29.9.2017 r.

⁶⁵ III CZP 78/19, OSNC 2021, Nr 2, poz. 7.

⁶⁶ Zob. przypis Nr 11.

okręgowych. W pozwie zamiast imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego powód podaje informacje pozwalające ustalić osobę, która dopuściła się naruszenia, w szczególności nazwę profilu lub login użytkownika. Pozew powinien zawierać również (1) wniosek o zobowiązanie usługodawcy do wskazania (a) danych pozwanego określonych w art. 18 ust. 1 ŚwUsłElekU, (b) danych eksploatacyjnych określonych w art. 18 ust. 5 ŚwUsłElekU – w oparciu o podane przez powoda informacje⁶⁷; (2) oznaczenie usługodawcy świadczącego usługę drogą elektroniczną w sposób umożliwiający doręczenie zobowiązania do nadesłania danych pozwanego; (3) wskazanie publikacji naruszających dobra osobiste powoda, z podaniem adresu identyfikującego treść w zasobach danych internetowych, w których zostały opublikowane; (4) datę i godzinę publikacji, o której mowa w pkt (3), oraz nazwę profilu lub loginu użytkownika, jeśli wskazanie tych danych jest możliwe. Zgodnie z proponowanym brzmieniem nowego art. 755(5) KPC, w sprawach o ochronę dóbr osobistych, naruszonych za pośrednictwem usługi⁶⁸ świadczonej drogą elektroniczną, sąd może udzielić zabezpieczenia również poprzez: (1) nakazanie uniemożliwienia dostępu do publikacji, (2) nakazanie umieszczenia oświadczenia uprawnionego odnoszącego się do publikacji, (3) nakazanie umieszczenia oznaczenia informującego o spornym charakterze publikacji. Mając na uwadze powyższe, sąd zobowiąże więc usługodawcę świadczącego usługę drogą elektroniczną do wskazania danych, o których mowa w art. 505⁴¹ § 1 pkt 1⁶⁹, i zagrozi mu grzywną na wypadek, gdyby w wyznaczonym terminie ich nie wskazał. Po bezskutecznym upływie terminu wyznaczonego usługodawcy do wskazania danych sąd nałoży grzywnę i jednocześnie wyznaczy nowy termin do wskazania danych, z zagrożeniem surowszą grzywną. Jeśli ustawodawca nie wskazałby tych danych, wówczas, w wersji art. 505⁴³ § 2 z projektu z 2021 r., postępowanie miałyby podlegać umorzeniu. Nie było natomiast jasne, czy do umorzenia postępowania musiałoby dojść, nawet w przypadku gdy usługodawca podał tylko niektóre wymagane dane pozwanego. Sąd Najwyższy postulował, że w razie uznania, iż podanie niewystarczających danych prowadzi do umorzenia postępowania, należałoby rozważyć wprowadzenie mechanizmu przekazywania tych niekompletnych danych powodowi, co mogłoby mu ułatwić wytoczenie powództwa na zasadach ogólnych⁷⁰. Niemniej projektodawca, w wersji projektu z 2022 r., wskazał w art. 505⁴³ § 3 pkt 2, że sąd umarza postępowanie, jeżeli usługodawca świadczący usługę drogą elektroniczną nie wskazał wystarczających danych identyfikujących pozwanego, ich pozyskanie nie jest możliwe lub byłoby połączone z nadmiernymi trudnościami.

Projekt ma również nowelizować ustawę z 28.7.2005 r. o kosztach sądowych w sprawach cywilnych⁷¹. Zgodnie z proponowaną treścią art. 13f KosztSądSpCywU w sprawach dochodzonych w postępowaniu o ochronę dóbr osobistych przeciwko osobom o nieustalonej tożsamości, o którym mowa w części pierwszej w księdze pierwszej w tytule VII

w dziale VIII, rozdziale 2 KPC pobiera się opłatę stałą w kwocie 1000 zł. Projektodawca wyjaśnia, że określając wysokość opłaty, kierował się art. 26 ust. 1 pkt 3 KosztSądSpCywU. Przepis ten wskazuje, że opłata stała od pozwu o ochronę dóbr osobistych wynosi 600 zł, ale w tym przypadku sąd nie jest już zobligowany do dokonania dodatkowych czynności mających na celu ustalenia danych pozwanego (tj. osoby, która naruszyła dobra osobiste powoda na portalu)⁷².

Nie można również zapomnieć, że często konta tworzone na portalach i serwisach społecznościowych tworzone są przy użyciu fałszywych danych, a usługodawcy nie weryfikują ich, nie prowadzą rejestru danych używanych do założenia konta i analogicznie nie aktualizują go. Obowiązek takiej weryfikacji nie wynika także z przepisów prawa. Uwaga ta jest istotna z tego powodu, iż liczba profili, które zostały utworzone przy użyciu nieprawdziwych danych osobowych, jest znacząca. Dla przykładu w pierwszym kwartale 2021 r. Facebook na całym świecie dezaktywował 1,3 miliarda fałszywych kont, a w drugim już 1,7 miliarda⁷³. Istnieje więc prawdopodobieństwo, że pomimo uzyskania danych potencjalnego pozwanego nie będą one przydatne, ponieważ okażą się fałszywe, co prowadzi do błędnego koła. Niemniej trudno oczekiwać,

⁶⁷ Sąd zobowiąże usługodawcę do wskazania tych danych i zagrozi grzywną na wypadek, gdyby w wyznaczonym terminie ich nie wskazał. Po bezskutecznym upływie terminu wyznaczonego usługodawcy do wskazania danych sąd nałoży grzywnę i jednocześnie wyznaczy nowy termin do wskazania danych, z zagrożeniem surowszą grzywną. Grzywna jest powtarzana, jeżeli pomimo wyznaczenia nowego terminu usługodawca świadczący usługę drogą elektroniczną nadal bez usprawiedliwienia nie wskazał danych. Ogólna suma grzywien w tej samej sprawie nie może przewyższać 2 milionów zł. Natomiast w razie wskazania danych przez usługodawcę lub usprawiedliwienia powodów, dla których ich pozyskanie nie jest możliwe lub byłoby połączone z nadmiernymi trudnościami, grzywny niezapłacone do tego czasu ulegają umorzeniu [art. 505(43) § 1–2].

⁶⁸ W poprzedniej wersji projektu, zamiast pojęcia „usługi” w sformułowaniu z art. 505(40) § 1: „naruszenia dóbr osobistych za pośrednictwem usługi świadczonej drogą elektroniczną w rozumieniu ustawy o świadczeniu usług drogą elektroniczną”, użyto pojęcia „usługodawca w UośuDE”. W poprzednim sformułowaniu 505(40) § 1, wątpliwości praktyczne mogła budzić kwestia tego, czy zobowiązanie do podania danych pozwanego będzie mogło być skierowane do podmiotów, które jedynie umożliwiają dostęp do sieci Internet, nie świadcząc żadnych usług „drogą elektroniczną”. Na gruncie ustawy o świadczeniu usług drogą elektroniczną to właśnie podmioty zapewniające dostęp do sieci mogą dysponować wiarygodnymi danymi użytkowników Internetu (w szczególności ukrywających się pod określonym adresem IP), tj. nie tylko imieniem i nazwiskiem, tak jak sam usługodawca – zob. Uwagi SN do projektu ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych z 27.10.2021 r.

⁶⁹ Tj. tych wskazanych w art. 18 ust. 1 i 2 ŚwUsłElekU. W poprzedniej wersji projektu mowa była o danych od ust. 1 do ust. 5, co oznaczało, że projekt znacząco wykraczał poza te dane, które są niezbędne do wytoczenia powództwa. Niemniej projektodawca ograniczył w wersji projektu z 2022 r. dane, które usługodawca miałby udostępnić już tylko do tych wskazanych w ust. 1–2 art. 18 ŚwUsłElekU (nazwisko i imiona usługobiorcy; PESEL a przy jego braku numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość).

⁷⁰ Uwagi Sądu Najwyższego do projektu ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych z 27.10.2021 r., s. 15.

⁷¹ Tj. Dz.U. z 2022 r. poz. 1125) ze zm.; dalej jako: KosztSądSpCywU.

⁷² Uzasadnienie, s. 54.

⁷³ Zob. <https://transparency.fb.com/data/community-standards-enforcement/> (dostęp z 26.6.2022 r.).

że przy zakładaniu konta na portalu społecznościowym weryfikacja będzie przypominała tę, która jest wymagana np. w procedurze rejestracji na platformę ePUAP. Do tworzenia konta na portalu społecznościowym, najczęściej, wymagane jest wskazanie adresu e-mail, a tych można tworzyć wiele. Ponadto samej idei tworzenia kont społecznościowych towarzyszyły względy rozrywkowe i z pewnością mało kto mógł się spodziewać, jak rewolucyjna okaże się rola portali społecznościowych, w szczególności w zakresie dostępu do informacji i możliwości wyrażania swoich opinii.

Podsumowanie

Nie ulega wątpliwości, że aktualnie obowiązujące regulacje w przedmiocie dostawców usług hostingowych, tj. przede wszystkim platform społecznościowych, nie przystają do obowiązujących realiów. W szczególności mowa tu o monopolistycznych platformach, które nader często arbitralnie ograniczają bądź usuwają treści, które mimo że naruszają ich politykę i regulamin, obiektywnie nie powinny zostać uznane za bezprawne.

Pozycja tych platform sprawia, że nie wahają się one usunąć nie tylko treści, ale także konta osób globalnie znanych, chociażby ze świata polityki. Mowa oczywiście o incydencie związanym z usunięciem konta *D. Trumpa* z Twittera⁷⁴. W ostatnim czasie także profil polskiej partii – Konfederacji został zablokowany przez Facebooka. Z jednej strony można oceniać, że każdy użytkownik platform – bez względu na status społeczny czy pełniącą funkcję, jest traktowany przez te platformy w sposób równy, z drugiej jednak istnieje obawa, by platformy nie ograniczały tematów nie tyle bezprawnych, ile kontrowersyjnych i przez to mogących pozornie naruszać jej regulamin i politykę. Jak powszechnie wiadomo, granica pomiędzy wolnością słowa a szerzeniem treści bezprawnych jest niezwykle cienka i wciąż trudna do jednoznacznego zdefiniowania. Należy także mieć na względzie, że platformy społecznościowe to wciąż prywatne platformy. ETPCz orzekł⁷⁵, że art. 10 EKPC nie zapewnia żadnej „swobody wyboru forum” dla korzystania z prawa do wolności wypowiedzi, co oznacza, że art. 10 EKPC nie gwarantuje żadnego prawa do nadawania swoich treści na jakimkolwiek konkretnym forum prywatnym. Prywatne platformy nie mogą być zatem zmuszane do rozpowszechniania treści osób trzecich, nawet jeśli treści te nie są w rzeczywistości nielegalne, co jest logiczne⁷⁶.

Poszczególne usługodawcy, w zależności od własnego profilu światopoglądowego i promowanych przez siebie wartości, mogą w zasadniczych kwestiach często różnić się w diametralny sposób w odbiorze publikowanych przez ich użytkowników treści. Przez co dane treści, choć kontrowersyjne dla danej platformy, a obiektywnie legalne i rzeczywistnie art. 10 EKPC, mogą zostać usunięte przez platformę. Jakikolwiek usunięcie czy zablokowanie konta lub treści na danej platformie społecznościowej momentalnie wywołuje

falę spekulacji i dyskusji, która dość często szerzy bezprawne treści, np. mowę nienawiści. Dlatego też tak newralgiczne jest wprowadzenie środków prawnych pozwalających z jednej strony na monitorowanie, a wręcz nadzorowanie treści udostępnianych online, ale z drugiej strony takich, które będą respektowały zasadę wolności słowa i prawa do swobody wypowiedzi. Z tego też względu należy docenić inicjatywę ustawodawczą Ministerstwa Sprawiedliwości w przedmiocie regulacji portali społecznościowych. Niemniej wersja regulacji przedstawiona przez Ministerstwo jest w wielu aspektach niespójna i niejednoznaczna, co zostało podniesione we wcześniejszej części artykułu. Wątpliwości budzi także pominięcie w regulacji projektu osoby zgłaszającego daną treść, ponieważ jego rola zaczyna i kończy się na etapie zgłoszenia danej treści. Nie jest on także uznany za stronę postępowania przed RWS, co, jak wskazano, blokuje go przed złożeniem skargi do WSA na decyzje RWS. Z drugiej strony, projekt nie reguluje odpowiedzialności zgłaszającego, w przypadku gdyby okazało się, że zgłoszona treść nie jest bezprawna. Może się jednak okazać, że zgłoszenia dokonał konkurent autora publikacji czy właściciela zakwestionowanego konta społecznościowego. Brak dostępu do opublikowanej treści czy też konta może wywołać katastrofalne skutki, nie tylko w sferze finansowej, ale również wizerunkowej. Co prawda można próbować dochodzić roszczeń na podstawie przepisów Kodeksu cywilnego czy ustawy z 16.4.1993 r. o zwalczaniu nieuczciwej konkurencji⁷⁷.

Pojawiają się także wątpliwości dotyczące sposobu wyegzekwowania od zagranicznych platform podporządkowania się pod krajowe regulacje. Wydaje się, że przymus zapłaty kwoty 50 mln zł dla takich gigantów jak Facebook (obecnie Meta) nie stanowiłby większego problemu, biorąc pod uwagę dochody firmy. W 2020 r. Facebook (Meta) odnotował przychód w wysokości 85 mld dolarów i zysk w wysokości 29 mld dolarów⁷⁸. Pytanie więc, jak zmusić platformy do respektowania krajowych rozwiązań. Niemniej, skoro platformy respektują obowiązki nałożone przez niemiecką ustawę, dlaczego miałyby

⁷⁴ Zgodnie z amerykańskim prawem działanie Twittera nie stanowiło naruszenia Pierwszej Poprawki, ponieważ nie było to działanie państwa <https://www.techdirt.com/2021/01/08/not-easy-not-unreasonable-not-censorship-decision-to-ban-trump-twitter/> (dostęp z 28.6.2022 r.).

⁷⁵ Appleby and Others v. the United Kingdom, no. 44306/98, ECHR 2003-V, I https://www.echr.coe.int/documents/research_report_article_10_eng.pdf (dostęp z 28.6.2022 r.).

⁷⁶ Trudno sobie wyobrazić, by platforma dla właścicieli psów była zmuszana do udostępniania zdjęć kotów, <https://verfassungsblog.de/twitter-trump-trump/> (dostęp z 28.6.2022 r.).

⁷⁷ T.j. Dz.U. z 2022 r. poz. 1233 ze zm.; zob. M. Mielniczuk-Skibicka, R. Skibicki, Jak nie wpaść w Kanał (Sportowy), czyli o odpowiedzialności za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat – cz. I, PME 2021, Nr 1, *passim*; M. Mielniczuk-Skibicka, R. Skibicki, Jak nie wpaść w Kanał (Sportowy), czyli o odpowiedzialności za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat – cz. II, PME 2021, Nr 2, *passim*.

⁷⁸ Zob. <https://businessinsider.com.pl wiadomosci/facebook-ile-zarabia-ile-placi-podatkow-w-polsce-dane-za-2019-r> (dostęp z 22.1.2022 r.).

nie podporządkować się pod polskie standardy, dla przykładu, YouTube publikuje raporty w przedmiocie przejrzystości co dwa lata. Raporty mają zawierać dane na temat organizacji i przyjętych procedur oraz ilości otrzymanych skarg i usuniętych treści oraz ogólne informacje o praktykach obowiązujących u usługodawcy oraz zasadach w zakresie usuwania treści⁷⁹. Polski projekt natomiast wymaga od usługodawcy, otrzymującego w roku kalendarzowym ponad 100 zgłoszeń w przedmiocie rozpowszechniania treści o charakterze bezprawnym, sporządzania sprawozdania w języku polskim, już co pół roku. Nie jest również wiadome, w jaki sposób weryfikować liczbę zgłoszeń, tj. czy przekroczy ona pułap 100 zgłoszeń.

Ponadto, w uproszczeniu, w przypadku niemieckiej ustawy obowiązki są nałożone na sieci społecznościowe liczące ponad dwa miliony zarejestrowanych użytkowników, a jeśli mowa o projekcie UWSł wiele obowiązków jest nałożonych na usługodawców posiadających już co najmniej jeden milion użytkowników, którzy założyli profil użytkownika, korzystając z usługi na terytorium Polski.

Mając na uwadze powyższe, wiele środowisk, począwszy od przedstawicieli różnych gałęzi biznesu, jak np. wydawcy prasowi, branża usług cyfrowych, organizacje przedsiębiorców, aż po organizacje zajmujące się ochroną praw człowieka apelują o zaniechanie prac nad projektem UWSł. Z takim apelem 24.1.2022 r. wystąpiła do Ministra Sprawiedliwości Krajowa Izba Gospodarcza, wskazując, że „projekt ustawy, wbrew deklaracjom projektodawców, nie doprowadzi do wzmocnienia praw użytkowników serwisów społecznościowych względem wielkich korporacji internetowych. Z dużym prawdopodobieństwem przyczyni się natomiast do wprowadzenia arbitralnej kontroli politycznej nad swobodą

wypowiedzi w Internecie oraz wprowadzenia rozwiązań niezgodnych z prawem UE”⁸⁰.

Podsumowując, najlepszym rozwiązaniem wydaje się porzucenie, a przynajmniej zawieszenie prac nad projektem do czasu przyjęcia ostatecznej wersji rozporządzenia DSA. Dzięki temu regulacje w przedmiocie platform społecznościowych byłyby spójne na szczeblu unijnym. Co więcej, platformom po pierwsze, łatwiej byłoby „podporządkować” się pod regionalną regulację aniżeli krajową, a po drugie, platformy chociażby ze względów wizerunkowych, ale i finansowych poczuwałyby się do działania zgodnie z rozporządzeniem unijnym i są podstawy, by takiego podejścia od nich oczekiwać. Platformy społecznościowe jak np. Facebook, Twitter, Instagram, już podejmowały współpracę mającą na celu walkę z dezinformacją czy mową nienawiści. Świadczy o tym odpowiednio, Kodeks postępowania w zakresie dezinformacji z 2018 r., znowelizowany w 2022 r.⁸¹ oraz Unijny kodeks postępowania dotyczący zwalczania niezgodnego z prawem nawoływania do nienawiści w Internecie⁸². Mając na uwadze powyższe, niewykluczone, że rozporządzenie DSA, jeśli zostanie przyjęte, przyczyni się do zwiększenia bezpieczeństwa i świadomości użytkowników platform społecznościowych.

⁷⁹ Zob. <https://transparencyreport.google.com/netzdg/youtube?hl=pl> (dostęp z 22.6.2022 r.).

⁸⁰ Zob. <https://kig.pl/apel-o-zaniechanie-prac-nad-projektem-transparencyreport.google.com/netzdg/youtube?hl=pl> - ustawy-o-wolnoscislo-wa-w-serwisach-spoecznoosciowych/ (dostęp z 28.6.2022 r.).

⁸¹ Zob. <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> (dostęp z 28.6.2022 r.).

⁸² Zob. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_pl (dostęp z 28.6.2022 r.).

Słowa kluczowe: wolność słowa, Akt o usługach cyfrowych, platformy społecznościowe, treści nielegalne, zaufane podmioty zgłaszające.

Draft law on the freedom of speech in social media – remedy for combating unlawful content?

The fight against illegal content provided on online platforms is a current and pressing topic that the national as well as European legislation is trying to tackle. The previous and basic regulation on the subject of Internet platforms has been the e-Commerce Directive and, in the Polish legal system, additionally the Act on the Provision of Electronic Services. In recent months, it has been all too common to remove or block not only the content published on social networks, but also the accounts of users of these portals. In the opinion of some circles, such arbitrary actions and decisions of social media platforms pose a threat to freedom of speech guaranteed by the Polish Constitution and the European Convention on Human Rights. At the EU level, work is underway on a regulation on defining the principles of transparency of decisions regarding content moderation (Digital Service Act). However, after the announcement of the Digital Service Act regulation draft, the Ministry of Justice submitted a draft law on the protection of freedom of expression in social network websites aimed at combating unlawful content on social media platforms. This article aims to present and discuss the most important regulations of this act along with the risks and uncertainties associated with the possible adoption of this act.

Key words: freedom of speech, Digital Service Act, social media platforms, illegal content, trusted flaggers.