Warszawa, 20-07-2022 r.

RZECZNIK PRAW OBYWATELSKICH

VII.564.4.2022.DZ

Pan

Janusz Cieszyński

sekretarz stanu,
pełnomocnik Rządu do
Spraw Cyberbezpieczeństwa

Kancelaria Prezesa Rady
Ministrów

ePUAP

Szanowny Panie Ministrze,

w odpowiedzi na pismo Pana Ministra w sprawie przedstawienia opinii Rzecznika Praw Obywatelskich na temat usunięcia na początku 2022 r. profilu partii Konfederacja z portalu społecznościowego Facebook, uprzejmie proszę o przyjęcie następujących informacji.

Do Rzecznika Praw Obywatelskich wpływają liczne skargi dotyczące blokowania lub usuwania profili w serwisach społecznościowych takich jak Facebook, a także ograniczenia możliwości publikowania treści przez użytkowników portali internetowych. Skarżący wskazują, że konta oraz wpisy są blokowane lub usuwane ze

względu na ich przekonania bądź określone wypowiedzi. Mając jednak na uwadze fakt, że zgłaszane Rzecznikowi sprawy dotyczą podmiotów prywatnych, niefinansowanych ze środków publicznych ani niewykonujących zadań publicznych, Rzecznik nie ma kompetencji do interwencji w tych indywidualnych sprawach. Należy bowiem podkreślić, że ustrojowe wyodrębnienie instytucji Rzecznika miało na celu stworzenie instytucji zajmującej się badaniem przejawów działalności organów władzy publicznej, prowadzących, czy też mogących prowadzić, do naruszeń praw i wolności (art. 80 oraz 208 Konstytucji RP). W konsekwencji prawodawca nie przewidział możliwości podejmowania przez Rzecznika działań względem podmiotów prywatnych, jakimi są działające w Polsce portale społecznościowe.

Niezależnie od powyższego, Rzecznik Praw Obywatelskich, stojąc na straży praw i wolności człowieka i obywatela określonych w Konstytucji RP oraz innych aktach normatywnych, z uwagą i troską analizuje wszelkie sygnały dotyczące problematyki zapewnienia przestrzegania wolności wyrażania poglądów oraz pozyskiwania i rozpowszechniania informacji w Internecie. Rzecznik nie pozostaje również obojętny na problem odnoszący się do blokowania profili, czy usuwania komentarzy w serwisach społecznościowych, w tym na Facebooku.

Przykładem zaangażowania Rzecznika Praw Obywatelskich, zmierzającym do rozwiązania wskazanych wyżej problemów, było m. in. zorganizowanie w dniu 18 listopada 2016 r. w Biurze Rzecznika Praw Obywatelskich debaty zatytułowanej „Facebook – mowa nienawiści – wolność słowa. Wyzwanie cywilizacyjne i prawnicze czy kryzys wartości?”[1] . W debacie tej udział wzięli, na zaproszenie Rzecznika Praw Obywatelskich, przedstawiciele administracji publicznej, naukowcy, aktywiści na rzecz wolności w Internecie, działacze organizacji praw człowieka, zabiegających o wolność słowa i reprezentujących prawa mniejszości, a także ruchów nacjonalistycznych, których profile w serwisie społecznościowych Facebook zostały skasowane. Mimo odmiennych poglądów dyskutanci zgodzili się, że procedury usuwania treści z serwisu społecznościowego Facebook, czy blokowania lub usuwania kont są niewystarczające.

[1] https://bip.brpo.gov.pl/pl/content/stenogram-z-debaty-u-RPO-facebook-mowa-nienawisci-wolnosc-slowa-18-11-2016, dostęp: marzec 2022 r.

W związku z tym rozważali m. in. stosowanie ostrzeżeń, trybu odwoławczego i włączenia w procedurę wymiaru sprawiedliwości, w tym stosowanie przepisów karnych. Debata potwierdziła zatem, że problem związany z blokowaniem lub usuwaniem kont na Facebook'u istnieje i że dotyczy on różnych opcji ideowych i światopoglądowych.

Na podstawie wniosków z debaty dnia 7 marca 2018 roku w wystąpieniu, skierowanym do Ministra Cyfryzacji[2] , RPO wskazał na potrzebę zapewnienia większej przejrzystości funkcjonowania portali społecznościowych. Dotychczasowa praktyka wskazywała bowiem, że filtrowanie napastliwych treści na serwisach społecznościowych jest nieskuteczne, kryteria kasowania profili są niejasne, można również zakładać, że jest to proces w większości zautomatyzowany. W ocenie Rzecznika tego typu działania mogą zostać uznane za ograniczenie, a nawet naruszenie, konstytucyjnie chronionej wolności słowa (art. 54 Konstytucji RP) i wymaga to podjęcia odpowiednich działań przez władze państwa. Pomimo kilkukrotnie ponawianej korespondencji Rzecznik Praw Obywatelskich nie otrzymał żadnej odpowiedzi w tej sprawie.

Warto też zauważyć, że problematyka poszanowania praw użytkowników platform internetowych była przedmiotem analizy RPO w trakcie opiniowania projektu ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych z dnia 28 września 2021 r. W tej częściowo krytycznej opinii RPO, z jednej strony, zwrócił uwagę na znaczenie swobodnego obiegu wiedzy, opinii i poglądów w demokratycznym państwie prawa i stworzenia adekwatnych mechanizmów gwarantujących poszanowanie tych wartości, z drugiej strony podkreślił konieczność wprowadzenia rozwiązań umożliwiających usuwanie czy blokowania treści niezgodnych z prawem[3].

Choć możliwość debaty publicznej, także anonimowej, na forach internetowych jest fundamentem współczesnej demokracji, należy wyraźnie dodać, że wolność słowa nie jest nieograniczona. Co więcej, skutki wypowiedzi zamieszczonych w Internecie,

---

[2] https://bip.brpo.gov.pl/pl/content/blokowanie-kont-przez-portale-spolecznosciowe-moze-naruszac-wolnosc-slowaocenia-rpo,%20dost%C4%99p:%2010.01.2022%20r, dostęp: marzec 2022 r.
[3] https://bip.brpo.gov.pl/pl/content/rpo-ms-uwagi-projekt-wolnosci-slowa-internet, dostęp: marzec 2022 r.

stanowiących mowę nienawiści, mogą wykroczyć poza krzywdę samej jednostki. Międzynarodowe organy, odpowiedzialne za zapobieganie konfliktom na tle narodowym i rasowym, zwracają uwagę na to, że „rasistowskie, ksenofobiczne, antysemickie oraz innego rodzaju nienawistne treści, obecne w Internecie, mogą stanowić pożywkę dla poważnych zbrodni nienawiści”[4]. Z kolei Specjalna Sprawozdawczyni Rady Praw Człowieka Narodów Zjednoczonych do spraw mniejszości już w styczniu 2015 r. informowała o stale rosnącej liczbie skarg, kierowanych do tego organu, a dotyczących wypowiedzi – także zamieszczonych online – podżegających do nienawiści, rozniecających napięcia, skutkujących często poważnymi przestępstwami. W raporcie podkreślono także, że o ile nie każda wypowiedź o charakterze mowy nienawiści prowadzi do poważnych zbrodni, to w zasadzie prawie każda zbrodnia nienawiści poprzedzona jest wcześniejszą stygmatyzacją i dehumanizacją określonych osób i podżeganiem do przestępstw na tle religijnym czy rasowym – czyli jest następstwem mowy nienawiści[5]. W dokumencie wskazano na ogromną rolę Internetu w rozprzestrzenianiu wypowiedzi nienawistnych i dyskryminujących: treść zamieszczona np. w mediach społecznościowych może być rozpowszechniona w skali niespotykanej w przypadku mediów tradycyjnych[6].

Nie można też zapomnieć, że zjawisko mowy nienawiści w sferze cyfrowej, jak wskazano w opracowaniu sporządzonym na potrzeby działalności UNESCO, wyróżnia specyfika miejsca publikowania treści. W odróżnieniu od podobnych wypowiedzi funkcjonujących poza Internetem, treści zamieszczane online są bardzo trwałe (zlikwidowanie takiej wypowiedzi oznacza zwykle wyłącznie zmianę jej lokalizacji internetowej), często mają charakter transgraniczny (*cross-jurisdictional*) i –

[4] Stanowisko ekspertów Biura Instytucji Demokratycznych i Praw Człowieka OBWE: Incitement to Hatred vs. Freedom of Expression: Challenges of combating hate crimes motivated by hate on the Internet - Report of the OSCE-ODIHR Expert Meeting, marzec 2010 r., http://www.osce.org/odihr/68750?download=true, dostęp: marzec 2022 r.
[5] *Report of the Special Rapporteur on minority issues*, Rita Izsák, January 2015, Human Rights Council, 28 Session, s. 25, 26, 42.
[6] ibidem, s. 74 – 79.

anonimowy. To właśnie te okoliczności powodują, że mowa nienawiści, obecna w Internecie, jest zjawiskiem wyjątkowo trudnym do zwalczenia[7].

Konstytucyjnie gwarantowana wolność wypowiedzi podlega ograniczeniom na zasadach określonych w art. 31 ust. 3 Konstytucji RP. W tym kontekście zasadne jest też odwołanie się do art. 10 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (dalej jako: EKPC). Przepis te stanowi o prawie do wolności wyrażania opinii, które obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Jednakże ustęp 2 art. 10 EKPC określa przesłanki, które mogą być powodem ograniczenia wolności słowa. Są to: bezpieczeństwo państwa, integralność terytorialna lub bezpieczeństwo publiczne, zapobieganie zakłóceniu porządku lub przestępstwu, ochrona zdrowia i moralności, ochrona dobrego imienia i praw innych osób oraz zapobieganie ujawnieniu informacji poufnych lub zagwarantowanie powagi i bezstronności władzy sądowej. Każdorazowo ingerencja państwa musi być proporcjonalna i niezbędna.

Na mocy wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 3 października 2019 r. w sprawie C-18/18, *Eva Glawischnig-Piesczek przeciwko Facebook Ireland Limited*, administratorzy portali internetowych zostali zobowiązani do usuwania treści nielegalnych, w tym przejawów mowy nienawiści, treści zniesławiających czy naruszających dobra osobiste[8]. Trybunał stwierdził, że sądy mogą nakazać dostawcy usług hostingowych usuwanie nielegalnych treści i dopuścił nakazanie kasowania pojawiających się wpisów identycznych i równoznacznych z tymi, które sąd uzna za bezprawne (np. zniesławiające). Podczas, gdy nakaz usuwania treści identycznych nie budzi wątpliwości, rozszerzająca interpretacja pojęcia „treści równoznacznych" może w efekcie prowadzić do nadmiernej moderacji portali internetowych. Dlatego niezbędnym jest, by stosowane regulacje były proporcjonalne i w odpowiedni sposób równoważyły obowiązki nakładane na dostawców usług, interes społeczny oraz prawa i wolności obywatelskie.

[7] I. Gagliardone, D. Gal, T. Alves, G. Martinez*, Countering online hate speech*, UNESCO 2015, s. 13.
[8] Wyrok TSUE z 3.10.2019 r., C-18/18, Eva Glawischnig-Piesczek p. Facebook Ireland Limited., LEX nr 2723800.

Jednakże praktyka wdrażania tych rozwiązań jest problematyczna. Obecnie stosowane algorytmy nie są doskonałe i mogą prowadzić do nadmiernego, a w niektórych przypadkach niewystarczającego, usuwania komentarzy i blokowania profili. Większość treści udostępnianych w Internecie powinna podlegać weryfikacji kontekstowej, a nie automatycznej. Technicznie jednak oznaczałoby to konieczność zatrudnienia setek specjalistów, którzy ręcznie weryfikowaliby treści – z powodów technicznych i ekonomicznych byłoby to bardzo trudne pod wieloma względami dla właścicieli szczególnie niewielkich forów internetowych (zwłaszcza tych specjalistycznych, np. dotyczących literatury, wędkarstwa, etc.), można jednak oczekiwać takich działań od wiodących platform społecznościowych.

Na użytkowników Internetu czekają także inne związane z rozwojem nowych technologii zagrożenia, takie jak rozprzestrzenianie się *fake newsów* i dezinformacja, kradzież danych osobowych czy ataki, uszkodzenia bądź nieautoryzowany dostęp do urządzeń, programów i chronionych danych. Zgodnie z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369 ze zm.), implementującej do polskiego prawa dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywa NIS) w Polsce funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT – Computer Security Incident Response Team). Na mocy ustawy role CSIRT poziomu krajowego przyjęły na siebie Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), NASK – Państwowy Instytut Badawczy (CSIRT NASK) oraz resort obrony narodowej (CSIRT MON). Organy te współpracują one ze sobą oraz z organami właściwymi do spraw cyberbezpieczeństwa, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów. Podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa tworzą system pozwalający na podejmowanie różnorodnych i skutecznych działań zarówno przeciwdziałających

zagrożeniom, jak i zapewniających skuteczne reagowanie w przypadku pojawienia się takich zagrożeń.

Najwięcej kompetencji w tym zakresie ustawodawca powierzył CSIRT NASK – prowadzonemu przez Naukową i Akademicką Sieć Komputerową Państwowemu Instytutowi Badawczemu. Do głównych zadań zespołu CSIRT NASK należy: rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci; aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników; współpraca z innymi zespołami CERT/CSIRT w Polsce i na świecie; udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego; działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach; rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń; regularne publikowanie Raportu CSIRT NASK o bezpieczeństwie polskich zasobów Internetu; działania informacyjno-edukacyjne, zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego.

W dorocznym raporcie „Krajobraz bezpieczeństwa polskiego internetu. Raport z działalności CERT Polska 2020", opracowanym przez NASK, wskazano, że w 2020 r. liczba incydentów cyberbezpieczeństwa wzrosła o 60,7 % w porównaniu do roku poprzedniego[9]. Zaobserwowano także liczne akcje dezinformacyjne związane z włamaniami na portale informacyjne i konta polskich polityków. W celu zapobiegania kolejnym incydentom w marcu 2020 r. uruchomiono "Listę Ostrzeżeń CERT Polska", czyli publiczną i dostępną nieodpłatnie bazę domen wykorzystywanych do nadużyć.

Jednocześnie warto przypomnieć, że na przełomie 2018 i 2019 roku na podstawie porozumienia Ministerstwa Cyfryzacji z przedstawicielami Facebooka uruchomiony został tzw. punkt kontaktowy[10]. Platforma ta miała służyć polskim użytkownikom Facebooka, których treści, konta lub profile zostały usunięte lub zablokowane. Dzięki usłudze użytkownicy otrzymali możliwość składania wniosku o przeprowadzenie dodatkowej kontroli czy blokada nastąpiła słusznie.

[9] https://www.nask.pl/pl/raporty/raporty/4289,RAPORT-CERT-2020.html, dostęp: marzec 2022 r.
[10] https://www.nask.pl/pl/aktualnosci/2385,Pierwsze-tego-typu-porozumienie-Ministerstwo-Cyfryzacji-i-Facebook.html, dostęp: marzec 2022 r.

Prace mające na celu zwiększenia ochrony konsumentów oraz ich praw podstawowych w Internecie prowadzone są także na szczeblu unijnym. W grudniu 2020 roku Komisja Europejska przedstawiła projekt aktu o usługach cyfrowych (DSA – Digital Services Act), w którym określono m. in. obowiązki i odpowiedzialność platform internetowych. Od czasu przyjęcia dyrektywy 2000/31/WE1 („dyrektywa o handlu elektronicznym") pojawiły się bowiem nowe i innowacyjne cyfrowe usługi społeczeństwa informacyjnego, które zmieniły codzienne życie obywateli Unii, modyfikując dotychczasowe sposoby komunikacji, łączności, konsumpcji i prowadzenia działalności gospodarczej przez obywateli[11].

Akt o usługach cyfrowych znacznie usprawnia mechanizmy usuwania nielegalnych treści oraz skutecznej ochrony praw podstawowych użytkowników w Internecie, w tym swobody wypowiedzi. Zwiększa też poziom kontroli publicznej nad działalnością platform internetowych. W projekcie zaproponowano m. in.:

1. Wprowadzenie środków służących zwalczaniu nielegalnych towarów, usług lub treści w Internecie, takich jak mechanizm sygnalizowania takich treści przez użytkowników, a w przypadku platform – mechanizm współpracy z „zaufanymi podmiotami sygnalizującymi";
2. Nałożenie nowych obowiązków dotyczących identyfikowalności użytkowników biznesowych na internetowych platformach handlowych, aby pomóc w identyfikowaniu sprzedawców nielegalnych towarów;
3. Wdrożenie skutecznych zabezpieczeń dla użytkowników, w tym możliwość zakwestionowania decyzji platform w zakresie moderowania treści;
4. Uruchomienie szeroko zakrojonych środków na rzecz przejrzystości funkcjonowania platform internetowych, w tym w sprawie algorytmów stosowanych w podpowiedziach;
5. Zwiększenie obowiązków bardzo dużych platform w zakresie zapobiegania niewłaściwemu wykorzystywaniu ich systemów poprzez podejmowanie działań

[11] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020PC0825&from=en, dostęp: marzec 2022 r.

opartych na ocenie ryzyka oraz poprzez przeprowadzanie niezależnych kontroli zarządzania ryzykiem związanym z tymi systemami;

6. Udostępnianie naukowcom najważniejszych danych przez największe platformy, aby mogli oni badać, jak ewoluują zagrożenia w sieci;
7. Utworzenie struktury nadzorczej odpowiadającej złożoności przestrzeni internetowej: kraje Unii Europejskiej będą odgrywać główną rolę, przy wsparciu nowej Europejskiej Rady ds. Usług Cyfrowych, w przypadku bardzo dużych platform – wzmocniony nadzór i egzekwowanie przepisów przez Komisję Europejską.

Pomimo wdrożenia mechanizmów mających na celu zapewnienie bezpieczeństwa w cyberprzestrzeni oraz zapobiegania ograniczania wolności słowa problem blokowania kont i usuwania komentarzy w mediach społecznościowych nadal jest aktualny. Co więcej, opinii publicznej nieznana jest efektywność poszczególnych narzędzi.

Niezależnie od zalet swobodnego obiegu wiedzy, opinii i poglądów, konieczne jest znalezienie sposobu na powstrzymanie bądź przynajmniej znaczne zmniejszenie skali negatywnych zjawisk w internecie takich dezinformacja, czy mowa nienawiści, choć przy jednoczesnym poszanowaniu proporcjonalności ingerencji w swobodę i wolność wypowiedzi. W opinii Rzecznika znaczną zmianę w tym zakresie może przynieść zakończenie procesu legislacyjnego i implementacja do porządku krajowego unijnego aktu o usługach cyfrowych.

Mam nadzieję, że powyższe informacje okażą się dla Pana Ministra pomocne.

Z wyrazami poważania

Stanisław Trociuk
Zastępca Rzecznika Praw Obywatelskich
/-podpisano elektronicznie/