FUNDACJA PANOPTYKON

Warszawa, 8 września 2017 r.

Uwagi Fundacji Panoptykon[1] w sprawie projektu ustawy o zmianie ustawy o nadzorze nad rynkiem finansowym oraz niektórych innych ustaw[2]

Przedstawiony przez Ministra Rozwoju i Finansów projekt ustawy o zmianie ustawy o nadzorze nad rynkiem finansowym oraz niektórych innych ustaw (dalej: **projekt ustawy**) przewiduje, że Komisja Nadzoru Finansowego (dalej: **KNF**) uzyska uprawnienie do zamieszczania na Liście ostrzeżeń publicznych nazw domen internetowych wykorzystywanych do świadczenia usług finansowych niezgodnie z prawem, co do których dopiero złożono zawiadomienie o podejrzeniu popełnienia przestępstwa, a nawet w sytuacji, gdy zawiadomienie nie zostało jeszcze złożone, ale w uznaniu KNF wymaga tego ochrona interesów uczestników rynku finansowego. Wpis domeny na Listę ostrzeżeń publicznych ma następować w drodze uchwały KNF. Konsekwencją wpisu domeny na Listę ostrzeżeń publicznych będzie automatyczne zamieszczenie jej w odrębnym rejestrze domen zastrzeżonych, do których dostęp będzie musiał zostać obligatoryjnie zablokowany w ciągu 48 godzin przez przedsiębiorców telekomunikacyjnych świadczących usługi dostępu do Internetu. Zablokowane mogą zostać m.in. strony podmiotów, które przy użyciu Internetu bez zezwolenia gromadzą środki pieniężne innych osób w celu udzielania pożyczek lub kredytów czy też strony podmiotów, które bez upoważnienie prowadzą działalność pośrednictwa ubezpieczeniowego.

Projekt przewiduje ponadto wprowadzenie w ustawie o nadzorze nad rynkiem finansowym art. 18a ust. 1c, którego brzmienie odpowiada uchylanemu art. 38 ust. 5 ustawy o nadzorze nad rynkiem kapitałowym. Przepis ten uprawnia Przewodniczącego KNF do pozyskiwania od podmiotów świadczących usługi telekomunikacyjne danych dotyczących wykazu połączeń telefonicznych lub innych przekazów informacji, jak również umożliwia mu zwrócenie się do podmiotów związanych z funkcjonowaniem funduszy inwestycyjnych otwartych o udostępnienie nagrań rozmów telefonicznych i innych informacji zarejestrowanych przez urządzenia i systemy teleinformatyczne. Projekt reguluje również sprawowanie kontroli nad pozyskiwaniem danych telekomunikacyjnych przez Sąd Okręgowy w Warszawie, przy czym kontrola ta ma mieć następczy charakter i polegać na analizie sprawozdań przedstawianych sądowi przez Przewodniczącego KNF w okresach półrocznych.

I. Wprowadzenie rejestru domen zastrzeżonych

Zaproponowane rozwiązanie, wzorowane na przepisach ustawy hazardowej (w brzmieniu nadanym nowelizacją z 15 grudnia 2016 r.), budzi nasze poważne wątpliwości. **W naszej opinii jest ono sprzeczne z podstawowymi zasadami obowiązującymi w państwie prawa oraz chronionymi przez Konstytucję RP prawami i wolnościami, w szczególności wolnością**

[1] Opinia przygotowana przez Karolinę Iwańską oraz Wojciecha Klickiego.
[2] Projekt z 10 lipca 2017 r.

słowa i prawem dostępu do informacji, o których mowa w art. 54 Konstytucji RP oraz prawem do sprawiedliwego i jawnego rozpatrzenia sprawy przez niezależny, bezstronny i niezawisły sąd (art. 45 Konstytucji RP).

Wprowadzenie mechanizmu blokowania stron budzi poważne ryzyko dla wolności słowa, która obejmuje nie tylko możliwość swobodnego otrzymywania i przekazywania informacji, ale także jej aktywne poszukiwanie i zdobywanie[3]. Ponadto, Konstytucja RP wprowadza w art. 54 ust. 2 zakaz cenzury prewencyjnej. Trybunał Konstytucyjny w uchwale z 2 marca 1994 r. stwierdził, że „jednym z elementów istoty wolności słowa jest wolność od cenzury prewencyjnej, rozumianej jako przyznanie organom państwowym kompetencji do kontrolowania treści wypowiedzi przed ich przekazaniem odbiorcy, a także do uzależniania przekazania wypowiedzi odbiorcom od uprzedniej zgody organu państwowego. Państwo może ustanawiać mechanizmy następczej odpowiedzialności za nadużycie wolności słowa, natomiast ingerencja uprzednia może być dopuszczona tylko wyjątkowo, jako uboczny efekt innych, legitymowanych konstytucyjnie działań państwa np. ścigania przestępstw czy zapewnienia prawidłowego działania wymiaru sprawiedliwości”[4].

Dopuszczalność wprowadzenia ograniczeń dla wolności słowa powinna być także oceniana przez pryzmat art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, którego ust. 2 określa dopuszczalny zakres ograniczeń. Orzecznictwo Europejskiego Trybunału Praw Człowieka (dalej: **ETPCz**) wskazuje, że stosowanie środków prewencyjnych polegających na blokowaniu stron internetowych jest dopuszczalne jedynie wyjątkowo, ponieważ zagrożenia z nimi związane są na tyle poważne, że działania władz krajowych wymagają wyjątkowo restrykcyjnej kontroli[5], a blokada stron internetowych musi być stosowana z rozwagą[6]. ETPCz podkreślił również, że wszelkie ograniczenia wolności słowa muszą być oparte na określonej podstawie prawnej, jasno regulującej zakres tych ograniczeń, jak i podlegać muszą kontroli sądowej w celu ochrony przed nadużyciami[7].

Tym samym, zarówno na gruncie Konstytucji RP, jak i Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności istnieje możliwość ograniczenia wolności słowa poprzez blokowanie stron internetowych. **Ograniczenia te muszą być jednak stosowanie absolutnie wyjątkowo oraz muszą być niezbędne do osiągnięcia celu, który uzasadnia ograniczenie praw podstawowych.**

W naszej ocenie, zaproponowane rozwiązania są niezgodne z opisanymi wyżej zasadami.

---

[3] R. Wieruszewski (red.), Międzynarodowy Pakt Praw Obywatelskich (Osobistych) i Politycznych. Komentarz, Warszawa 2012, s. 468.

[4] Uchwała Trybunału Konstytucyjnego z dnia 2 marca 1994 r. dotycząca ustalenia powszechnie obowiązującej wykładni przepisów art. 21 ust. 2 pkt 6 w związku z art. 18 ust. 1 i 2 oraz art. 6 ust. 1, art. 14 ust. 1 i art. 22 ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji.

[5] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 26 listopada 1991 r. w sprawie Observer i Guardian przeciwko Wielkiej Brytanii, skarga 13585/88 i 13166/87.

[6] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 19 stycznia 2016 r. w sprawie Kalda przeciwko Estonii, skarga 17429/10.

[7] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 18 grudnia 2012 r. w sprawie Yildirim przeciwko Turcji, skarga 3111/10; Wyrok Europejskiego Trybunału Praw Człowieka z dnia 1 grudnia 2015 r. w sprawie Cengiz i in. Przeciwko Turcji, skarga 48226/10 i 14027/11.

1. Skuteczność mechanizmu blokowania stron

W uzasadnieniu projektodawca wskazuje, że celem komentowanego rozwiązania jest podniesienie poziomu bezpieczeństwa uczestników rynku finansowego korzystających z usług finansowych świadczonych za pośrednictwem platform internetowych. Wprowadzenie rejestru ma zminimalizować ryzyko korzystania przez nieprofesjonalnych uczestników rynku z usług podmiotów nieuprawnionych do wykonywania takiej działalności. Jakkolwiek walka z nadużyciami na rynku finansowym jest istotna, to wątpliwym jest, że do realizacji tego celu przyczyni się blokowanie stron internetowych. Jak wspomniano wyżej, aby ograniczenie wolności słowa rozumianej także jako poszukiwanie dostępu do informacji było dopuszczalne, musi ono być niezbędne i proporcjonalne. W związku z tym, aby stanowić zgodne z prawem ograniczenie konstytucyjnej wolności, mechanizm blokowania stron musiałby charakteryzować się wyjątkową skutecznością. Brak jest jednak rzetelnych badań i analiz potwierdzających skuteczność blokowania stron w systemowym zwalczaniu nadużyć. Również projektodawca w ocenie skutków planowanej regulacji nie wskazuje żadnych danych potwierdzających zawartą w uzasadnieniu tezę, zgodnie z którą „należy oczekiwać, że takie rozwiązanie także na rynku finansowym zapewni dużą skuteczność działań prewencyjnych”[8].

Projekt ustawy przewiduje, że blokowanie stron internetowych odbywać się będzie na poziomie adresów DNS. Takie rozwiązanie wymaga sprawdzenia każdego zapytania, jakie przekazuje operator. Należy zauważyć, że blokowanie na poziomie DNS może być skuteczne tylko wtedy, gdy operator ma pełną kontrolę nad połączeniem sieciowym użytkownika końcowego, co często nie ma miejsca. Ponadto, blokowanie takie łatwo jest ominąć, tak przez użytkownika końcowego (zmiana serwera DNS, użycie sieci Tor lub połączenia VPN), jak i przez dostawcę treści (zmiana adresu DNS).

Blokowanie stron internetowych nie jest więc skutecznym remedium na problem nadużyć finansowych dokonywanych za pomocą Internetu. W kontekście przedstawionych we wstępie uwag dotyczących konstytucyjnych wymogów ograniczania wolności słowa i prawa dostępu do informacji, stosowane mechanizmy powinny charakteryzować się wyjątkową skutecznością i nie stwarzać ryzyka blokowania treści zgodnych z prawem.

2. Alternatywne środki prawne

Projektodawca w uzasadnieniu nie wskazuje, dlaczego mechanizm blokowania stron jest rozwiązaniem lepszym z punktu widzenia ochrony konstytucyjnych praw i wolności z jednej strony i zwalczania nadużyć z drugiej, niż istniejące już mechanizmy prawne. W kontekście uniemożliwiania dostępu do bezprawnych treści zastosowanie mogłaby znaleźć regulacja art. 14 ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, która przewiduje możliwość wystąpienia do usługodawcy z żądaniem usunięcia danych o bezprawnym charakterze. Projektodawca zdecydował się zamiast tego wprowadzić rozwiązanie dużo bardziej restrykcyjne. Istnienie możliwości osiągnięcia przewidywanego celu za pomocą środków mniej dotkliwie ograniczających wolność słowa nie spełnia warunku proporcjonalności przewidzianego w art. 31 ust. 3 Konstytucji RP.

[8] Por. s. 1 uzasadnienia projektu.

3. Zagrożenia związane z obowiązkami nałożonymi na operatorów

Art. 3 pkt 2 projektu ustawy przewiduje, że przedsiębiorca telekomunikacyjny, który nie dopełni obowiązku zablokowania określonych stron, może podlegać karze pieniężnej w wysokości do 250 tys. zł. Zagrożenie taką sankcją może powodować, że dostawcy usług, chcąc zabezpieczyć się przed zarzutem niepodejmowania wymaganych działań, będą w celach dowodowych gromadzili nadmierne ilości danych o zachowaniu konkretnych użytkowników w Internecie dotyczące historii połączeń użytkownika z konkretnymi adresami stron. Jak bowiem wspomniano wyżej, blokowanie stron internetowych na poziomie DNS wymaga sprawdzenia każdego zapytania kierowanego do operatora. Gromadzenie przez operatorów tych danych jest tym bardziej niebezpieczne, że dostęp do nich na potrzeby działań operacyjnych mogą uzyskać Policja i inne służby.

4. Arbitralność decyzji. Blokowanie treści zgodnych z prawem

W naszej ocenie, jeśli projektodawca utrzyma plan przyznania KNF uprawnienia do prowadzenia rejestru domen zastrzeżonych, powinien zminimalizować ryzyko arbitralności decyzji o wpisie. Zgodnie z projektem ustawy, wpis domeny na Listę ostrzeżeń publicznych skutkujący jej wpisem do rejestru ma następować w drodze uchwały KNF. Naszym zdaniem takie rozwiązanie jest niedopuszczalne. Sytuacja, w której taka decyzja podejmowana jest przez organ administracyjny, rodzi wysokie ryzyko arbitralności. Przy tak daleko idącym ograniczeniu wolności słowa, jaki proponuje regulacja, **każdorazowa decyzja o wpisie danej domeny na Listę ostrzeżeń publicznych powinna być oceniana merytorycznie przez niezawisły sąd**. Jest to tym istotniejsze, że wpisowi na Listę ostrzeżeń publicznych mają podlegać domeny wykorzystywane do prowadzenia działalności, co do legalności której nie wypowiedział się jeszcze sąd. KNF uzyska bowiem uprawnienie do wpisu na Listę ostrzeżeń publicznych domen prowadzonych przez podmioty, w stosunku do których dopiero złożone zostało zawiadomienie o podejrzeniu popełnienia przestępstwa, a nawet – zgodnie z proponowanym art. 6b ust. 4a – w stosunku do których takie zawiadomienie nie zostało złożone, ale podania strony internetowej do publicznej wiadomości wymaga ochrona interesów użytkowników rynku finansowego. Tak arbitralnie ukształtowana procedura wpisu stwarza ryzyko zablokowania strony internetowej podmiotu, który nie naruszył prawa. O ile zrozumiały jest prewencyjny cel Listy ostrzeżeń publicznych, o tyle w celu zapobiegania potencjalnym nadużyciom nad wpisem domeny na listę powinien czuwać sąd. Kwestią otwartą jest takie skonstruowanie zasad podejmowania tej decyzji przez sąd, by jednocześnie zapewnić niezależność podejmowanej decyzji oraz jej szybkość.

Poważne wątpliwości budzi również proponowana procedura sprzeciwu. Zgodnie z projektem, wpis na Listę ostrzeżeń publicznych nie będzie miał charakteru decyzji administracyjnej. Przysługiwał będzie od niego sprzeciw do Komisji Nadzoru Finansowego, która tym samym stanie się sędzią we własnej sprawie. Na rozpatrzenie sprzeciwu KNF będzie miała 60 dni, a rozstrzygnięcie przybierze formę decyzji administracyjnej. W naszej opinii termin 60 dni na ustosunkowanie się do sprzeciwu jest zdecydowanie za długi. W przewidującej podobny mechanizm ustawie o grach hazardowych, na której – zgodnie z treścią uzasadnienia opiniowanego projektu – wzorowano proponowane rozwiązania, termin na rozpatrzenie sprzeciwu wynosi 7 dni. **Wprowadzenie 60-dniowego terminu na rozpatrzenie sprzeciwu może powodować, że podmioty prowadzące strony internetowe omyłkowo wpisane na listę poniosą znaczne straty, jak również w sposób nieuprawniony ograniczeniu ulegnie**

wolność prowadzenia przez nich działalności gospodarczej oraz wolność słowa. Co więcej, w wyniku błędnego wpisu domeny na listę znaczne straty ponieść mogą również sami klienci usług oferowanych przez te podmioty. Dodatkowo, blokada strony internetowej może doprowadzić do tego, że rezygnacja z usług danego podmiotu będzie znacznie utrudniona. Problem ten jest tym istotniejszy, że w projekcie ustawy nie znalazły się żadne zapisy dotyczące roszczeń odszkodowawczych, z którymi dany usługodawca lub klient mógłby wystąpić w razie niezasadnej blokady strony. Również uzasadnienie ani ocena skutków regulacji nie podnoszą tej kwestii. Wreszcie, tak zbudowany mechanizm odwołań od decyzji Komisji stwarza poważne ryzyko nadużyć – umożliwia bowiem *de facto* zablokowanie dowolnej strony internetowej na okres dwóch miesięcy. Uniknięciu tego niebezpieczeństwa służyłoby wprowadzenie merytorycznej kontroli sądowej nad każdym wpisem domeny na Listę lub znaczne skrócenie terminu na rozpatrzenie sprzeciwu.

Podkreślić trzeba także niebezpieczeństwo blokowania w pełni legalnych treści – blokowaniu, zgodnie z projektem ustawy, poddana będzie bowiem cała domena. Oznacza to, że jeśli niezgodna z prawem działalność prowadzona jest przy wykorzystaniu wyłącznie podstrony danej domeny, wpisanie domeny do rejestru spowoduje zablokowanie treści, które nie naruszają prawa, a tym samym rażącą ingerencję w wolność słowa w Internecie.

II. Uprawnienia Przewodniczącego KNF i nadzór nad pozyskiwaniem danych

Jak wskazano we wstępie,, Przewodniczący KNF zachowa uprawnienie do pozyskiwania od podmiotów świadczących usługi telekomunikacyjne wykazu połączeń telefonicznych i innych danych niestanowiących treści przekazu, jak również – w przypadku wskazanych w ustawie przestępstw lub postępowań związanych z działalnością funduszy inwestycyjnych – do uzyskiwania od określonych podmiotów nie tylko danych niestanowiących treści przekazu, ale także nagrań rozmów telefonicznych oraz innych informacji zarejestrowanych za pośrednictwem urządzeń i systemów teleinformatycznych. Udostępnienie takich informacji nie stanowi naruszenia obowiązku zachowania tajemnicy komunikacji.

Przy tak daleko ingerującym w prawo do prywatności zakresie danych, do których dostęp może uzyskać Przewodniczący Komisji Nadzoru Finansowego, niezwykle istotne jest zapewnienie efektywnej kontroli sądowej nad ich pozyskiwaniem. Pragniemy zauważyć, że komentowany przepis projektowanego art. 18a ust. 1c pkt 2 stanowi szczególny przypadek dostępu organów państwa do nagrań rozmów w miejscu pracy. Uzyskiwanie tak wrażliwych danych – zakładając nawet, że wszelkie rozmowy dotyczyć będą spraw zawodowych – wymaga realnej kontroli sądu. Tymczasem, projektowany art. 18aa ustawy o nadzorze nad rynkiem finansowym budzi poważne wątpliwości. W szczególności, z komentowanego przepisu – z uwagi na użycie wyrażenia „dane, o których mowa w art. 18a ust. 1c" – nie wynika wystarczająco jasno, że kontroli podlegać będzie nie tylko pozyskiwanie danych telekomunikacyjnych niestanowiących treści przekazu (o czym mówi art. 18a ust. 1c pkt 1), ale także nagrań rozmów telefonicznych lub innych informacji zarejestrowanych przez urządzenia i systemy teleinformatyczne. Ponadto, wprowadzana kontrola posiada charakter następczy i polegać będzie na analizie zbiorczych sprawozdań przedstawianych Sądowi Okręgowemu w Warszawie przez Przewodniczącego KNF w okresach półrocznych.

W naszej opinii, **takie ukształtowanie systemu kontroli nad pozyskiwaniem przez Przewodniczącego Komisji określonych w projekcie danych, narusza konstytucyjne prawo**

do ochrony prywatności (art. 47 Konstytucji RP) i tajemnicy komunikowania się (art. 49 Konstytucji RP). Jakkolwiek sama ingerencja w te prawa jest dopuszczalna w celu walki z przestępczością, to – zgodnie z orzecznictwem Trybunału Konstytucyjnego – powinna ona być efektywnie kontrolowana przez niezależny sąd. Według Trybunału, „skoro pozyskiwanie tych danych dokonuje się w sposób niejawny, bez wiedzy i woli podmiotów, o których informacje są przez Policję gromadzone, a zarazem przy ograniczonej kontroli społeczeństwa, brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć. Może to nie tylko przyczynić się do nieuzasadnionej ingerencji w wolności lub prawa człowieka, ale i stanowić zagrożenie demokratycznych mechanizmów sprawowania władzy”[9]. Ponadto, w sytuacji, gdy Przewodniczący KNF dysponuje wyżej opisanymi uprawnieniami już na etapie postępowania wyjaśniającego, czy istnieją podstawy do złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa lub wszczęcia postępowania administracyjnego, ingerencja w tajemnicę komunikowania się następuje niezwykle wcześnie. I co więcej – wbrew wytycznym płynącym z orzecznictwa TK – możliwa jest nie tylko w celu przeciwdziałania przestępczości. Zakres uprawnień Przewodniczącego KNF jest zatem rażąco szeroki i stanowi nieproporcjonalne ograniczenie tajemnicy komunikowania się.

Ponadto, przewidziana w projekcie ustawy kontrola ma charakter iluzoryczny. Kontrola prowadzona po 6 miesiącach od uzyskania danych będzie nieefektywna, a jednocześnie bardziej czasochłonna niż kontrola przeprowadzana przy każdorazowym wystąpieniu o udostępnienie danych. Podobne rozwiązanie przewidziane zostało m.in. w ustawie o Policji. Jak stwierdził Sąd Okręgowy w Gdańsku przy ocenie sprawozdania Policji z przeprowadzonych działań operacyjnych, następcza kontrola sądu nad dostępem do danych „nie stwarza możliwości zweryfikowania, czy sięgnięcie po informacje było niezbędne, celowe i należycie uzasadnione (…), a więc nie daje podstawy do przeprowadzenia realnej – spełniającej standardy ochrony praw człowieka – kontroli uzyskiwania przez Policję danych”[10]. Ponadto, Sąd Okręgowy w Gdańsku stwierdził szereg nieprawidłowości popełnionych przez funkcjonariuszy Policji, m.in. przy kwalifikacji prawnej czynów, co uniemożliwiałoby nawet uprzednią kontrolę uzyskania danych pod kątem kryterium proporcjonalności. Kontrola następcza nie daje zatem żadnych gwarancji ochronnych wymaganych w tak poważnym przypadku jakim jest pozyskiwanie danych telekomunikacyjnych obejmujących treść przekazu.

***

Mając na uwadze powyższe, Fundacja Panoptykon uznaje, że proponowane rozwiązania nie przyczynią się do realizacji celów określonych przez projektodawcę a jednocześnie istnieje realne ryzyko naruszenia podstawowym praw i wolności obywatelskich. **Uważamy, że blokowanie treści w Internecie jest środkiem niebezpiecznym i nieskutecznym, a w konsekwencji niedopuszczalnym w demokratycznym państwie prawa. Z kolei dostęp Przewodniczącego KNF do danych telekomunikacyjnych oraz nagrań rozmów telefonicznych i innych informacji stanowiących treść przekazu bez uprzedniej realnej kontroli sądu tworzy ogromne zagrożenie dla gwarantowanego konstytucją prawa do prywatności.**

[9] Wyrok Trybunału Konstytucyjnego z 30 lipca 2014 r., sygn. K 23/11, pkt 10.4.4 uzasadnienia.
[10] Odpowiedź Sądu Okręgowego w Gdańsku na wniosek Fundacji Panoptykon o udostępnienie informacji publicznej:
https://panoptykon.org/sites/default/files/so_gdansk_wyniki_kontroli_sprawozdania_31.05.2017.pdf.