FUNDACJA PANOPTYKON

Warszawa, 2 stycznia 2023 r.

Stanowisko Fundacji Panoptykon[1]

w sprawie projektu ustawy – Prawo Komunikacji Elektronicznej (druk sejmowy: 2861)[2]

Fundacja Panoptykon jest organizacją pozarządową, której celem jest ochrona praw człowieka, w szczególności prawa do prywatności. W naszej działalności zajmujemy się m.in. kwestią uprawnień policji i służb specjalnych, a także innymi formami nadzoru, jakie państwo sprawuje nad obywatelami.

W niniejszym stanowisku nie odnosimy się do całości przepisów ustawy – Prawo Komunikacji Elektronicznej (**dalej: PKE, projekt**), a jedynie skupiamy się na obowiązkach przedsiębiorców komunikacji elektronicznej w zakresie współpracy z Policją i innymi służbami.

1. Retencja danych (art. 47 PKE)

Art. 47 PKE nakłada na przedsiębiorców komunikacji elektronicznej obowiązek zatrzymywania i przechowywania wskazanych w projekcie danych przez okres 12 miesięcy, a także udostępniania ich uprawnionym podmiotom (m.in. policji i służbom specjalnym).

Poza wskazanymi w dalszej części opinii zmianami, jest to przeniesienie na grunt PKE obowiązujących przepisów ustawy – Prawo telekomunikacyjne (art. 180a i następne), która także nakładała na przedsiębiorców telekomunikacyjnych obowiązek retencji danych.

Zarówno obowiązujące dotychczas przepisy, jak i projektowany art. 47 PKE – poprzez nałożenie na przedsiębiorców bezwarunkowego obowiązku przechowywania informacji o wszystkich klientach – są niezgodne z prawem UE, co potwierdzają liczne wyroki Trybunału Sprawiedliwości UE.

W swoim orzecznictwie Trybunał Sprawiedliwości UE sformułował precyzyjne wytyczne, jakie ustawodawca krajowy musi spełnić, aby umożliwić policji i służbom specjalnym dostęp np. do lokalizacji telefonów komórkowych czy wykazu połączeń. Są to m.in. obowiązek informowania post-factum osób, których dane pozyskano o tym fakcie oraz skuteczna kontrola sądu lub niezależnego organu administracyjnego nad tym działaniem.

Jednocześnie TSUE jednoznacznie przesądził, że nałożenie na firmy telekomunikacyjne obowiązku przechowywania i udostępniania służbom wszystkich danych o użytkownikach narusza Kartę Praw Podstawowych UE.

> ***Wyrok Trybunału Sprawiedliwości z dnia 6 października 2020 r. C-511/18 C-512/18 C-520/18 (La Quadrature du Net and Others)***: „art. 52 ust. 1 Karty Praw

[1] Stanowisko przygotowane przez Rozalię Bielińską i Wojciecha Klickiego
[2] Projekt z dnia 17 listopada 2022 r.

Podstawowych należy interpretować w ten sposób, że nie stoi on na przeszkodzie uregulowaniu krajowemu zobowiązującemu dostawców usług łączności elektronicznej, po pierwsze, do posłużenia się zautomatyzowaną analizą oraz do gromadzenia w czasie rzeczywistym w szczególności danych o ruchu i danych o lokalizacji, a po drugie, do gromadzenia w czasie rzeczywistym danych technicznych o lokalizacji wykorzystywanych urządzeń końcowych, jeśli:

- posłużenie się zautomatyzowaną analizą ogranicza się do sytuacji, w których państwo członkowskie napotyka na poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub przewidywalne, przy czym posłużenie się tą analizą może podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja ma wiążący skutek, mającej na celu sprawdzenie, czy wystąpiła sytuacja uzasadniająca wspomniany środek, jak również weryfikację poszanowania warunków i gwarancji, które powinny zostać przewidziane, oraz
- korzystanie z gromadzenia w czasie rzeczywistym danych o ruchu i danych o lokalizacji jest ograniczone do osób, wobec których istnieje uzasadniony powód, by podejrzewać, że są one zaangażowane w taki lub inny sposób w działalność terrorystyczną, i podlega uprzedniej kontroli dokonywanej albo przez sąd, albo przez niezależny organ administracyjny, którego decyzja ma wiążący skutek, w celu zapewnienia, że takie gromadzenie w czasie rzeczywistym jest dozwolone jedynie w granicach tego, co jest ściśle niezbędne. W należycie uzasadnionych pilnych przypadkach kontrola powinna nastąpić w krótkim czasie".

***Wyrok Trybunału Sprawiedliwości z dnia 6 października 2020 r. C-623/17 (Privacy International)*: „**art. 7, 8 i 11 oraz 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej, należy interpretować w ten sposób, że **stoi on na przeszkodzie** uregulowaniu krajowemu umożliwiającemu organowi państwa nałożenie na dostawców usług łączności elektronicznej **obowiązku uogólnionego i niezróżnicowanego transmitowania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego."**

TSUE zdecydował, że **retencja danych powinna być stosowana w wyjątkowych sytuacjach** kiedy istnieje **poważne zagrożenie dla bezpieczeństwa narodowego**, a posłużenie się analizą tych danych musi podlegać **skutecznej kontroli sądu lub niezależnego organu administracyjnego**. Ponadto, **gromadzenie danych powinno być ograniczone do osób** wobec których istnieje **uzasadniony powód,** by podejrzewać **zaangażowanie w działalność terrorystyczną**, tylko kiedy jest to **ściśle niezbędne**. Zgodnie ze stanowiskiem TSUE, **państwo członkowskie nie może** nałożyć obowiązku **uogólnionego i niezróżnicowanego transmitowania danych służbom w celu ochrony bezpieczeństwa narodowego czy porządku i bezpieczeństwa publicznego.**

W projekcie brakuje zatem elementów wskazanych w powyższych wyrokach, które pozwalałyby na zgodną z prawem UE retencję danych.

W opinii[3] z 15 grudnia 2022 r. o zgodności projektu z prawem UE podobne stanowisko wyraziło Ministerstwo do Spraw Unii Europejskiej. Zgodnie z opinią: „projektowane przepisy utrzymują obowiązujący obecnie powszechny i niezróżnicowany (pod względem geograficznym i podmiotowym) obowiązek zatrzymywania szerokiego katalogu danych telekomunikacyjnych (art. 47 ust. 1 pkt. 1 projektowanej ustawy), który zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej jest niezgodny z art. 15 ust. 1 dyrektywy 2002/58/WE”[4].

Podsumowując, ustawa mająca implementować prawo unijne, zawiera naszym zdaniem (oraz w ocenie Ministerstwa do Spraw Unii Europejskiej) rozwiązania jednoznacznie z tym prawem niezgodne.

Nie można też zapominać, że kwestia retencji danych i zasad dostępu policji i innych służb do danych telekomunikacyjnych były przedmiotem zainteresowania Trybunału Konstytucyjnego, który w wyroku z 30 lipca 2014 r. (sygn. K 23/11) wskazał, że niezbędna jest uprzednia, niezależna kontrola nad tym procesem. Wyrok ten nie został nigdy prawidłowo wykonany.

W związku z tym apelujemy do autorów projektu o zmianę art. 47 PKE uwzględniając warunki retencji wskazane w wyrokach TSUE, aby zapewnić zgodność zarówno z prawem unijnym, jak i Konstytucją RP.

2. Poszerzenie katalogu podmiotów zobowiązanych do retencji danych. (art. 47 PKE c.d.)

Zgodnie z art. 47 PKE przechowywanie danych na temat swoich użytkowników będzie obowiązkiem **przedsiębiorców komunikacji elektronicznej**. Na tę grupę składają się:

- przedsiębiorcy telekomunikacyjni, którzy już dziś (na podstawie przepisów Prawa telekomunikacyjnego) zobowiązani są do retencji danych
- **podmioty świadczące usługi komunikacji interpersonalnej niewykorzystującej numerów**. Do tego typu usług zaliczamy[5] np. połączenia głosowe, pocztę elektroniczną, usługi przekazywania wiadomości, czaty grupowe, komunikatory internetowe[6].

Oznacza to w praktyce znaczne poszerzenie katalogu podmiotów zobowiązanych do retencji danych, które później będą udostępniane policji i innym uprawnionym podmiotom.

---

[3] https://orka.sejm.gov.pl/Druki9ka.nsf/0/82DB9792FD296E51C125891A0043E0EC/%24File/2861-001.pdf

[4] Art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), zgodnie z którym państwa członkowskie mogą uchwalić przepisy ograniczające poufność komunikacji pod warunkiem, że przewidziane w nich środki są niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (np. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych

[5] https://www.parp.gov.pl/component/content/article/71124:nowa-ustawa-prawo-komunikacji-elektronicznej-obowiazki-dostawcow-uslug-komunikacji-interpersonalnej-niewykorzystujacych-numerow

[6] Usługi, których **nie zaliczymy** do komunikacji interpersonalnej niewykorzystującej numerów to: strony internetowe, serwisy społecznościowe, blogi, usługa dostarczania wideo na żądanie oraz czaty w grach internetowych (ponieważ usługa komunikacji interpersonalnej jest podrzędna i nie istnieje bez głównej usługi jaką jest rozgrywka)

Zgodnie z projektem obowiązkowi rocznej retencji podlegać będą np. dane kto (z jakiego komputera, numeru IP) korzystał z usługi oraz w jaki sposób to robił (o której się zalogował i jak długo pozostawał zalogowany). Dodatkowo retencji podlegać mają dane „jednoznacznie identyfikujące użytkownika w sieci, co w praktyce oznaczać może po prostu wszystkie dane, jakie na temat użytkownika mają podmioty świadczące usługi interpersonalne niewykorzystujące numerów (lokalizacja urządzenia, ustawienia przeglądarki etc.)

W uzasadnieniu projektu wskazano, że rozszerzenie katalogu podmiotów, na których są nakładane obowiązki w art. 43–53, z przedsiębiorców telekomunikacyjnych na przedsiębiorców komunikacji elektronicznej, nastąpiło na żądanie ministra obrony narodowej oraz ministra koordynatora służb specjalnych. Jako uzasadnienie tej decyzji wskazano możliwość przeniesienia działalności przedsiębiorców telekomunikacyjnych do segmentu usług interpersonalnych niewykorzystujących numerów w niedalekiej przyszłości, a co za tym idzie uniknięcie obowiązków związanych z bezpieczeństwem państwa oraz bezpieczeństwem i porządkiem publicznym.

Autorzy projektu abstrahują jednak od trudności z egzekwowaniem nowego obowiązku względem podmiotów, które nie mają siedziby na terenie Polski oraz podmiotów, których usługa komunikacji interpersonalnej skonstruowana jest w taki sposób, że jej dostawca nie ma dostępu do informacji, które mają podlegać retencji.

Zwracamy ponadto uwagę, że dotychczas niezgodny z prawem UE standard retencji danych telekomunikacyjnych dotyczył tylko przedsiębiorców telekomunikacyjnych. Zatem **poszerzenie katalogu podmiotów zobowiązanych do przechowywania danych i udostępniania ich podmiotom uprawnionym pogłębi dotychczasowy problem: w 2021 r. uprawnione podmioty sięgały po dane telekomunikacyjne (objęte obowiązkiem retencji) 1 820 630 razy[7]. Po wejściu w życie projektu ta liczba znacząco wzrośnie. Oznacza to, że PKE zamiast rozwiązywać problem niezgodności przepisów dotyczących retencji danych z prawem UE, pogłębia go.**

Podobne stanowisko przedstawiło Ministerstwo do Spraw Unii Europejskiej, które w przywołanej wyżej opinii wskazało, że zwiększenie liczby podmiotów zobowiązanych do retencji danych „**pogłębiło zakres niezgodności projektowanych przepisów z prawem UE”**.

3. Poszerzenie katalogu danych podlegających retencji (art. 49 ust. 1 pkt. 2 PKE)

W art. 49 ust. 1 pkt 2 PKE dodano nową kategorię danych podlegających retencji – **„dane jednoznacznie identyfikujące użytkownika w sieci”**. Nie jest jasne, jakie dane można do niej zakwalifikować. Zgodnie z art. 49 ust. 2 pkt 1 PKE szczegółowy wykaz danych ma zostać określony w rozporządzeniu przez Ministra właściwego do spraw informatyzacji (w porozumieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii Ministra – Koordynatora Służb Specjalnych). Jednakże to ustawa, a nie rozporządzenie powinna szczegółowo określać rodzaje danych zbieranych o obywatelach przez państwo zgodnie z art. 51 Konstytucji RP.

Podobne stanowisko wyraził Trybunał Konstytucyjny w wyroku z dnia 18 grudnia 2014 r. (sygn. K 33/13) dotyczącym rejestrów medycznych.

[7] Źródło: druk senacki 769 (https://www.senat.gov.pl/download/gfx/senat/pl/senatdruki/12301/druk/769.pdf?r12301)

Zdaniem TK art. 20 ust. 1 pkt. 5 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, w części, w jakiej przewiduje, że w rozporządzeniu minister określa zakres i rodzaj przetwarzanych danych w rejestrze spośród danych określonych w art. 19 ust. 6 tej ustawy, jest niezgodny z art. 47 oraz art. 51 ust. 1, 2 i 5 w związku z art. 31 ust. 3 Konstytucji. TK wystąpił do Generalnego Inspektora Ochrony Danych Osobowych z pismem o zajęcie stanowiska w sprawie. GIODO zwrócił uwagę, że tworzenie przez ministra rejestrów medycznych zawierających dane o stanie zdrowia, czyli dane podlegające szczególnej ochronie będzie następować w drodze aktów wykonawczych, budziło zasadnicze wątpliwości w trakcie całego procesu legislacyjnego ustawy o systemie informacji. GIODO podzielił też wątpliwości zgłoszone przez Rzecznika Praw Obywatelskich. Przekazanie pewnych spraw do uregulowania w rozporządzeniu nie powinno doprowadzić do nadania ustawie charakteru blankietowego, tj. pozostawienia organowi władzy wykonawczej możliwości samodzielnego uregulowania całego kompleksu zagadnień. TK stwierdził, że art. 20 ust. 1 pkt. 5, w części, w jakiej upoważnia ministra do określenia w rozporządzeniu, że przetwarzaniu w rejestrze będą podlegać niesprecyzowane „inne dane", o których mowa w art. 19 ust. 6 ustawy, nie odpowiada konstytucyjnemu wymaganiu normowania ograniczeń autonomii informacyjnej w ustawie. Regulacja ustawowa dotycząca „innych danych" jest w pełni blankietowa.

Pojęcie „dane jednoznacznie identyfikujące użytkownika w sieci" z art. 49 ust. 2 pkt 2 PKE jest nieprecyzyjne i pozostawia właściwemu ministrowi, który będzie wydawał rozporządzenie nadmierną dyskrecjonalność. Sporządzenie wykazu tych danych w rozporządzeniu pozostawia dowolność organowi władzy wykonawczej oraz nadaje ustawie charakter blankietowy. Apelujemy zatem o doprecyzowanie w projekcie tej kategorii danych, które mają podlegać retencji.

4. **Blokowanie: brak obowiązku informowania dostawców treści o blokowaniu połączeń lub komunikatów elektronicznych (art. 53 PKE)**

W art. 53 PKE dokonano zmiany w dobrym kierunku względem art. 180 Prawa telekomunikacyjnego (dalej: PT), ponieważ Prezes UKE otrzymał kompetencję do nałożenia obowiązku blokowania połączeń lub komunikatów elektronicznych, w drodze decyzji, na żądanie uprawnionych podmiotów, jeżeli mogą one zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu. Dotychczas, na podstawie art. 180 Prawa telekomunikacyjnego uprawnione podmioty (np. ABW) mogły bezpośrednio żądać od przedsiębiorców telekomunikacyjnych blokowania danych treści, dlatego zaangażowanie Prezesa UKE i dodanie formy decyzji dla takiego nakazu uważamy za krok w dobrą stronę. Decyzja ma nadany rygor natychmiastowej wykonalności, a przedsiębiorca komunikacji elektronicznej ma 6 godzin na zablokowanie danych treści.

W przepisie **zabrakło** jednak **obowiązku informowania o decyzji (a tym samym – zakwestionowania decyzji Prezesa UKE) dostawców treści.**

Zgodnie z aktualną propozycją jedynie przedsiębiorcy komunikacji elektronicznej mogą odwołać się od decyzji Prezesa UKE. Natomiast dostawcy komunikatów elektronicznych (np. autorzy stron internetowych) nie będą informowani o blokowaniu treści ich autorstwa oraz nie będą mieli możliwości odwołania się od tej decyzji. Odbiera to tym podmiotom możliwość skorzystania z prawa do skutecznego środka odwoławczego, które wynika zarówno z

Konstytucji (art. 45 i 78), jak i Europejskiej Konwencji Praw Człowieka (art. 13) oraz Karty Praw Podstawowych UE (art. 47).

Jest to dla nas tym bardziej niezrozumiałe, że zgodnie z art. 11 rozporządzenia 2021/784[8] w przypadku, gdy dostawca usług hostingowych usuwa treści o charakterze terrorystycznym lub uniemożliwia dostęp do nich, udostępnia on dostawcy treści informacje na temat takiego usunięcia lub uniemożliwienia dostępu. Na wniosek dostawcy treści dostawca usług hostingowych informuje go o powodach usunięcia lub uniemożliwienia dostępu oraz o jego prawach do zaskarżenia nakazu usunięcia albo udostępnia dostawcy treści kopię nakazu usunięcia.

Oznacza to, że w przypadku usunięcia treści o charakterze terrorystycznym, dostawcy treści będą o tym informowani, a w sytuacji blokowania treści ze względu na zagrożenie obronności, bezpieczeństwo państwa oraz porządek publiczny (co wydaje się mniej groźne) dostawcy treści notyfikacji nie otrzymają.

W naszej ocenie nie ma powodów, aby w projekcie nie wprowadzić rozwiązań analogicznych do przewidzianych rozporządzeniem 2021/784.

***

Podsumowując, w naszej ocenie przepisy związane z przechowywaniem i udostępnianiem policji i służbom specjalnych danych telekomunikacyjnych wymagają systemowej zmiany. Jest ona do przestrzegania przez Polskę prawa unijnego. Jednak wynikająca z orzecznictwa TSUE konieczność wprowadzenia obowiązku informowania post factum osób inwigilowanych o tym fakcie oraz stworzenia silnej niezależnej kontroli nad służbami zmniejszy ryzyko nadużyć i zapobiegnie bezpodstawnej inwigilacji, której ekstremalnym przykładem było ujawnione w minionym roku stosowanie oprogramowania szpiegującego Pegasus. Niestety projekt PKE zamiast rozwiązywać powyższe problemy, zwiększa uprawnienia służb, a tym samym prowadzi do zwiększenia ryzyka nadużyć.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania w internecie treści o charakterze terrorystycznym