FUNDACJA PANOPTYKON

Warszawa, 7 marca 2024 r.

Stanowisko Fundacji Panoptykon[1] w sprawie projektu ustawy – Prawo Komunikacji Elektronicznej[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 skupiamy się jedynie na obowiązku przedsiębiorców telekomunikacyjnych, o którym mowa w art. 47 projektu, czyli retencji danych wskazanych w art. 49.

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

Trybunał Sprawiedliwości UE sformułował konkretne 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.

[1] Stanowisko przygotowane przez Wojciecha Klickiego i Mateusza Wrotnego.
[2] Projekt z dnia 22 lutego 2024 r.

Zgodnie z wyrokiem 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 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.

Na marginesie należy przywołać opinię[3] Ministerstwa do Spraw Unii Europejskiej z 15 grudnia 2022 r. o zgodności z prawem UE projektu ustawy – Prawo komunikacji elektronicznej z 17 listopada 2022 r. (druk sejmowy nr 2861), które powielało treść art. 47 PKE w zakresie obowiązków retencyjnych przedsiębiorców. 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 projektu ustawy z 17 listopada 2022 r.), 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 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, aby zapewnić zgodność zarówno z prawem unijnym, jak i Konstytucją RP, niezbędna jest zmiana art. 47 PKE i uwzględnienie w nim wymogów wynikających z wyroków TSUE.

***

Podsumowując, w naszej ocenie przepisy związane z przechowywaniem i udostępnianiem policji i służbom specjalnych danych telekomunikacyjnych wymagają systemowej, głębokiej zmiany. Jest ona niezbędna do przestrzegania przez Polskę prawa unijnego. Dane o aktywności każdego klienta przedsiębiorstw telekomunikacyjnych, a więc w praktyce każdego z nas, nie powinny być

[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

przechowywane „na wszelki wypadek", a jedynie w ściśle określonych warunkach wskazanych w orzecznictwie TSUE.

Ignorowanie orzeczeń Trybunału, wraz z brakiem szerszych zmian związanych z informowaniem jednostek o fakcie bycia przedmiotem zainteresowania ze strony policji czy służb specjalnych, utrzymuje wysokie ryzyko nadużyć i bezpodstawnej inwigilacji, której ekstremalnym przykładem było ujawnione stosowanie oprogramowania szpiegującego Pegasus.