PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa,

DOL.0623.15.2021

Pan
Adam Szłapka
Minister ds. Unii Europejskiej
Kancelaria Prezesa Rady Ministrów

Al. Ujazdowskie 1/3
00-583 Warszawa

Szanowny Panie Ministrze,

w odpowiedzi na korespondencję z dnia 6 maja 2024 r. w sprawie wyroku Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE) z dnia 30 kwietnia 2024 r. w sprawie **C-470/21** ***La Quadrature du Net*** uprzejmie informuję, że w ocenie organu nadzorczego do spraw ochrony danych osobowych **powoduje on konieczność rozważenia wprowadzenia zmian w przepisach polskiego prawa**.

W wyroku tym TSUE (w pełnym składzie) orzekł, że „Artykuł 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 (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że:
- nie stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala organowi publicznemu odpowiedzialnemu za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw, do których dochodzi w Internecie, na dostęp do przechowywanych przez dostawców publicznie dostępnych usług łączności elektronicznej danych dotyczących tożsamości cywilnej odpowiadających adresom IP zbieranym wcześniej przez organizacje zrzeszające uprawnionych, aby ów organ

mógł zidentyfikować posiadaczy tych adresów wykorzystywanych do aktywności mogącej stanowić takie naruszenia i aby mógł on w razie potrzeby zastosować wobec nich środki, pod warunkiem że na mocy tego uregulowania:
- dane te przechowywane są w warunkach i zgodnie z zasadami technicznymi, które gwarantują, że wykluczone jest, by ich przechowywanie mogło pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego tych posiadaczy, na przykład poprzez ustalenie ich szczegółowego profilu, co można osiągnąć w szczególności poprzez nałożenie na dostawców usług łączności elektronicznej obowiązku przechowywania poszczególnych kategorii danych osobowych, takich jak dane dotyczące tożsamości cywilnej, adresy IP oraz dane o ruchu i dane dotyczące lokalizacji, gwarantującego rzeczywiście szczelne odseparowanie tych poszczególnych kategorii danych, które uniemożliwia na etapie przechowywania wszelkie powiązanie tych poszczególnych kategorii danych, przez okres nieprzekraczający tego, co ściśle niezbędne;
- dostęp tego organu publicznego do takich danych przechowywanych w sposób odseparowany i rzeczywiście szczelny służy wyłącznie zidentyfikowaniu osoby podejrzewanej o dopuszczenie się czynu zabronionego i towarzyszą mu gwarancje niezbędne do wykluczenia, by, poza sytuacjami nietypowymi, dostęp ten mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego posiadaczy adresów IP, na przykład poprzez ustalenie ich szczegółowego profilu, co wymaga w szczególności, by upoważnionych do posiadania takiego dostępu urzędników owego organu obowiązywał zakaz ujawniania w jakiejkolwiek formie informacji na temat zawartości plików przeglądanych przez tych posiadaczy, z jedynym wyjątkiem wiążącym się z ujawnieniem ich w celu zawiadomienia prokuratury, zakaz śledzenia historii treści przeglądanych przez owych posiadaczy oraz, ogólniej, zakaz wykorzystywania tych adresów IP do celów innych niż zidentyfikowanie ich posiadaczy, aby zastosować wobec nich ewentualne środki;
- możliwość powiązania przez osoby odpowiedzialne w ramach wspomnianego organu publicznego za analizę zdarzeń takich danych z plikami zawierającymi elementy umożliwiające poznanie tytułów utworów chronionych, których udostępnienie w Internecie uzasadniało zebranie adresów IP przez organizacje zrzeszające uprawnionych, jest uzależniona – w przypadkach kolejnego ponowienia aktywności naruszającej prawa autorskie lub prawa pokrewne przez tę samą osobę – od dokonania przez sąd lub niezależny organ administracyjny kontroli, która nie może być w pełni zautomatyzowana i powinna mieć miejsce przed dokonaniem takiego powiązania, ponieważ powiązanie to może w takich przypadkach pozwolić na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego wspomnianej osoby, której adres IP wykorzystano do aktywności mogącej naruszać prawa autorskie lub prawa pokrewne;
- system przetwarzania danych wykorzystywany przez organ publiczny podlega w regularnych odstępach czasu kontroli niezależnego organu mającego status strony trzeciej w stosunku do tego organu publicznego, mającej na celu weryfikację integralności systemu, w tym skutecznych gwarancji chroniących przed ryzykiem takiego dostępu do tych danych lub takiego ich wykorzystywania, które nosiłyby

znamiona nadużycia lub byłyby niezgodne z prawem, oraz jego skuteczności i niezawodności w wykrywaniu ewentualnych uchybień".

Odnosząc się do ww. wyroku TSUE, należy zauważyć, że w prawie polskim nie ma odpowiednika francuskiego Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie (Hadopi)], o którym mowa w orzeczeniu jako organie publicznym odpowiedzialnym za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw. Niemniej – jak to zostało opisane w wyroku – Hadopi posiada również kompetencję do ścigania przestępstw przeciwko prawom własności intelektualnej i jest organem publicznym w rozumieniu art. 3 dyrektywy 2016/680[1]. Ma to znaczenie z punktu widzenia oceny wpływu wyroku na prawo polskie ze względu na to, że w świetle przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[2] organami publicznymi powołanymi do ścigania przestępstw stypizowanych w art. 115 i n. tej ustawy są organy ścigania. W konsekwencji do ich działania w tym zakresie zastosowanie znajdują wskazania płynące z tego wyroku. Organy prowadzące postępowania karne z tego zakresu nie są zatem objęte przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej: RODO lub rozporządzenie 2016/679)[3], a podlegają przepisom ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[4]. Przesłanka legalności ich działania wynika z art. 13 ust. 1 tej ustawy, zgodnie z którym właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Jednocześnie uczestnikom postępowania przysługują prawa wynikające z ww. ustawy wdrażającej dyrektywę 2016/680.

Zgodnie z orzecznictwem Trybunału, jak też i utrwalonym stanowiskiem sądów polskich, adres IP uznawany jest za daną osobową w rozumieniu RODO, jak i daną o ruchu w rozumieniu dyrektywy 2002/58[5] (podobnie np. wyrok z dnia 17 czerwca

---

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE. L 119 z 4.5.2016, str. 89 ze zm.).

[2] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509).

[3] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).

[4] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).

[5] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. U. UE. L 201 z 31.7.2002, str. 37 ze zm.).

2021 r. w sprawie C-597/19[6], czy wyrok TSUE z dnia 7 marca 2024 r. w sprawie C-604/22[7]).

Jak wskazał TSUE w przytoczonym wyroku w sprawie C-604/22, powiązanie identyfikatora jakim jest np. adres IP urządzenia użytkownika z innymi informacjami o użytkowniku (np. dotyczącymi płatności przy użyciu karty kredytowej) pozwala na faktyczną identyfikację osoby (także przy dynamicznym adresie IP) oraz na stworzenie profilu użytkownika. Stworzenie takiego profilu skutkować może dostępem do informacji o różnego rodzaju aktywnościach użytkownika w Internecie, z których pośrednio wynikać mogą dane dotyczące tego użytkownika, w tym dane szczególnych kategorii.

Na gruncie prawa polskiego organ mający informację o uzasadnionym podejrzeniu popełnienia przestępstwa przeciwko prawom własności intelektualnej popełnionego przez użytkownika posługującego się określonym numerem IP może wystąpić do operatora telekomunikacyjnego o udostępnienie danych pozwalających ustalić jego tożsamość. Dane dotyczące podmiotu korzystającego z publicznie dostępnej sieci telekomunikacyjnej (użytkownika) objęte są tajemnicą telekomunikacyjną na podstawie art. 159 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[8]. Zasady przetwarzania takich danych i dostępu do nich określone zostały w dziale VII tej ustawy, która zasadniczo implementowała przepisy dyrektywy 2002/58. Na gruncie tych przepisów przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom, w tym sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 3-5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych (art. 180d ustawy Prawo telekomunikacyjne). Analizując treść tych przepisów przez pryzmat wyroku TSUE z dnia 30 kwietnia 2024 r. stwierdzić należy, że nie odpowiadają one standardom wynikającym z art. 7, 8, 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej i ograniczenie tajemnicy telekomunikacyjnej nie spełnia warunku wynikającego z art. 15 ust. 1 dyrektywy 2002/58 w postaci niezbędności i proporcjonalności w społeczeństwie demokratycznym.

Zgodnie z wyrokiem TSUE przepisy krajowe zezwalające organowi publicznemu na dostęp do przechowywanych przez operatora telekomunikacyjnego danych dotyczących tożsamości użytkownika posługującego się określonym numerem IP, co do którego organ posiada uzasadnione podejrzenie popełnienia przestępstwa przeciwko prawom własności intelektualnej, powinny określać, aby dane te przechowywane były w warunkach i zgodnie z zasadami technicznymi, które wykluczają możliwość uzyskania informacji pozwalających na wyciągnięcie na ich podstawie precyzyjnych wniosków na temat życia prywatnego tej osoby. Osiągnięcie tego celu jest możliwe w szczególności poprzez nałożenie na dostawców usług

---

[6] Wyrok TSUE z dnia 17 czerwca 2021 r. w sprawie C-597/19, Mircom International Content Management & Consulting (M.I.C.M.) Limited Przeciwko Telenet Bvba.
[7] Wyrok TSUE z dnia 7 marca 2024 r. w sprawie C-604/22, IAB EUROPE.
[8] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34 ze zm.).

łączności elektronicznej obowiązku przechowywania poszczególnych kategorii danych osobowych w sposób gwarantujący faktyczne odseparowanie poszczególnych kategorii danych i uniemożliwienie powiązania ich przez okres niezbędny. **Wyżej wskazane przepisy ustawy Prawo telekomunikacyjne nie zawierają gwarancji, na które wskazał Trybunał.** Brak jest w nich gwarancji technicznych, które uniemożliwiałyby uzyskanie danych w zakresie szerszym niż tylko dla ustalenia tożsamości użytkownika, jak też operatorzy telekomunikacyjni nie mają obowiązku gromadzenia danych w sposób zapewniający odseparowanie poszczególnych kategorii danych, tak aby nie było możliwe ich łączenie i tworzenie profilu aktywności użytkownika. Nawiązując do treści wyroku, stwierdzić należy, że brak jest przepisów gwarantujących, że dane przechowywane będą w „sposób odseparowany i rzeczywiście szczelny", i że służyć będą wyłącznie zidentyfikowaniu osoby podejrzewanej o dopuszczenie się czynu zabronionego, a przetwarzaniu towarzyszyć będą gwarancje niezbędne do wykluczenia „by, poza sytuacjami nietypowymi, dostęp ten mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego posiadaczy adresów IP".

Ponadto Trybunał wskazał w wyroku, że aby można było uznać dostęp do danych objętych tajemnicą telekomunikacyjną za niezbędny i adekwatny powinny istnieć w prawie krajowym gwarancje w postaci kontroli niezależnego organu mającego status osoby trzeciej w stosunku do organu ubiegającego się o dane osobowe.

Zgodnie z art. 180d Prawa telekomunikacyjnego przedsiębiorcy telekomunikacyjni obligatoryjnie udostępniają dane uprawnionym podmiotom, a także sądowi i prokuratorowi. W kontekście tego przepisu oraz analizowanego wyroku istnieją podstawy do przyjęcia wniosku, że właściwe jest udostępnienie danych objętych tajemnicą telekomunikacyjną sądowi i niezależnemu organowi, natomiast wątpliwe wydaje się udostępnianie tych danych innym podmiotom. W demokratycznym państwie prawa zasadność pozyskania danych telekomunikacyjnych powinna być poddana kontroli sądu lub niezależnego organu administracyjnego. Kontrola przeprowadzona przez te podmioty nie naruszałaby zasady zaufania obywateli do państwa, gdyż eliminowałaby ryzyko nieproporcjonalnej ingerencji w prawa podstawowe i gwarantowałaby z drugiej strony pewność stosowania prawa (na co wskazywał TSUE w wyroku z dnia 8 kwietnia 2014 r. w sprawach połączonych Digital Rights Ireland Ltd (C-293/12) i Kärntner Landesregierung (C-594/12)). **Zmianie powinny więc ulec przepisy ustawy Prawo telekomunikacyjne w zakresie zasad dostępu organów ścigania do danych objętych tajemnicą telekomunikacyjną.** Jednocześnie sama kontrola przeprowadzana przez sąd lub niezależny organ administracyjny powinna być konieczna i adekwatna w demokratycznym porządku, a także przeprowadzona zgodnie z zasadą proporcjonalności (zgodnie z wyrokiem TSUE z dnia 2 marca 2021 r. w sprawie C-746/18 Prokuratuur) oraz dotyczyć powinna wyłącznie przypadków wskazanych w art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej.

W kontekście kontroli sądowej należy wspomnieć także o niedawnym wyroku Europejskiego Trybunału Praw Człowieka (dalej: ETPCz) z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce (skargi nr 72038/17 i 25237/18). Sprawa dotyczyła ustawodawstwa polskiego, pozwalającego służbom na zbieranie informacji o obywatelach pod pretekstem walki z przestępczością i zagrożeniami dla bezpieczeństwa publicznego. ETPCz stwierdził, że w wyniku braku realnej kontroli nad prowadzeniem kontroli operacyjnej w ramach czynności operacyjno-rozpoznawczych oraz zbyt ogólnie sformułowanych przesłanek umożliwiających prowadzenie tej kontroli, doszło do trzech naruszeń art. 8 EKPC[9] – prawa do poszanowania życia prywatnego, rodzinnego oraz korespondencji – w odniesieniu do skarg dotyczących m.in. zatrzymywania danych komunikacyjnych do potencjalnego wykorzystania przez właściwe organy lub władze krajowe.

Wnioski

Trybunał Sprawiedliwości UE w omawianym wyroku w kontekście art. 15 ust. 1 dyrektywy 2002/58/WE dopuścił możliwość uregulowania krajowego, które zezwala organowi publicznemu odpowiedzialnemu za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw na dostęp do przechowywanych przez dostawców publicznie dostępnych usług łączności elektronicznej danych dotyczących ustalenia tożsamości cywilnej osoby podejrzewanej o dopuszczenie się naruszenia. Wskazał przy tym na konkretne warunki, jakie tego rodzaju uregulowanie krajowe musi spełniać, aby należycie chronić dane osobowe przetwarzane przez przedsiębiorców telekomunikacyjnych. **Na gruncie prawa polskiego brak jest jednak przepisów, które gwarantowałyby zachowanie wskazanych przez TSUE warunków udostępniania danych osobowych chronionych tajemnicą telekomunikacyjną. W związku z tym wyrok w sprawie C-470/21 powoduje konieczność rozważenia zmiany przepisów prawa.**

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

[9] Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.).