PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 03.01.2025 r.

DOL.0623.18.2024

Pan
Ignacy Niemczycki
Sekretarz Stanu
Ministerstwo ds. Unii Europejskiej
Kancelaria Prezesa Rady
Ministrów

Szanowny Panie Ministrze,

w nawiązaniu do korespondencji z dnia **9 grudnia** 2024 r. dotyczącej wniosku prejudycjalnego w sprawie **C-661/24 Académie Fiscale e.a.** (DPUE.7313.454.2024.JH(1)(KWM) uprzejmie informuję, że w odniesieniu do pytania prejudycjalnego w przedstawionej sprawie, dotyczącego stosowania przepisów dyrektywy 2002/58/WE[1] **Prezes Urzędu Ochrony Danych Osobowych dostrzega zasadność udziału przedstawiciela Polski w postępowaniu przed Trybunałem Sprawiedliwości UE.**

1. Stan faktyczny i prawny sprawy

Przedmiotowa sprawa dotyczy przetwarzania danych osobowych w sektorze łączności elektronicznej. Trybunał Konstytucyjny Belgii, rozpatrując skargę o stwierdzenie nieważności belgijskiej ustawy z dnia 20 lipca 2022 r. o zbieraniu i zatrzymywaniu danych identyfikacyjnych i metadanych w sektorze łączności elektronicznej oraz o przekazywaniu tych danych organom (zwanej dalej „zaskarżoną ustawą"), nabrał wątpliwości co do zgodności przepisów ustawy z prawem UE i zwrócił się do Trybunału Sprawiedliwości z wnioskiem o interpretację art. 15 ust. 1

[1] Dyrektywa 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; Dz.U.UE.L.2002.201.37); dalej: dyrektywa o prywatności i łączności elektronicznej lub dyrektywa 2002/58/WE.

dyrektywy o prywatności i łączności elektronicznej w związku z art. 7, 8 i art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej.

Celem zaskarżonej ustawy było doprowadzenie do przestrzegania zasad ochrony danych osobowych w następstwie stwierdzenia przez Trybunał Konstytucyjny niekonstytucyjności ustaw o zbieraniu i zatrzymywaniu danych w sektorze łączności elektronicznej[2]. Co ważne, jeden z wyroków Trybunału Konstytucyjnego został wydany w następstwie skierowania do Trybunału Sprawiedliwości UE pytań prejudycjalnych zakończonych wydaniem wyroku z 6 października 2020 r., La Quadrature du Net i in. w sprawach C-511/18, C-512/18 i C-520/18.

Belgijski Trybunał Konstytucyjny sformułował zarzuty wobec zaskarżonej ustawy w odniesieniu do trzech zagadnień dotyczących zatrzymywania danych o ruchu, zatrzymywania danych dotyczących lokalizacji, oraz kompetencji funkcjonariuszy policji sądowej IBPT [(belgijskiego urzędu ds. usług pocztowych i telekomunikacji), organu regulacyjnego belgijskiego sektora poczty i telekomunikacji]. Celem zatrzymywania danych, o którym mowa w zaskarżonych przepisach (tj. art. 5 pkt 4 i 5 i art. 6 zakwestionowanej ustawy), ma być zwalczanie oszustw i wykorzystania sieci w sposób niedozwolony, a także bezpieczeństwo i prawidłowe działanie sieci. W ocenie sądu konstytucyjnego tak określony cel znajduje uzasadnienie w świetle art. 15 dyrektywy 2002/58/WE. **Wątpliwości Trybunału Konstytucyjnego odnoszą się jednak do proporcjonalności przyjętych rozwiązań.**

Jak wynika z zaskarżonego przepisu dotyczącego zatrzymywania danych o ruchu (tj. art. 5 zaskarżonej ustawy), okres zatrzymywania danych o ruchu jest różny: 4 miesiące, 12 miesięcy z możliwością wydłużania na okres niezbędny do analizy tego wykorzystania. Zaskarżone przepisy przyznają prawo operatorom do zatrzymania, w związku ze świadczeniem usługi łączności interpersonalnej, niezbędnych do tych celów danych spośród następujących danych o ruchu: identyfikator źródła połączenia; identyfikator przeznaczenia komunikatu; dokładne daty i godziny rozpoczęcia i zakończenia połączenia; lokalizacja urządzeń końcowych stron w chwili rozpoczęcia i zakończenia połączenia (okres retencji 4 m-ce). Ponadto operator zatrzymuje, w związku ze świadczeniem usługi łączności interpersonalnej, dane o ruchu dotyczące połączeń przychodzących w celu zidentyfikowania autora komunikatu: numer telefonu, z którego pochodzi połączenie przychodzące lub adres IP, z którego wysłano połączenie przychodzące, znakowanie czasowe i użyty port oraz dokładne daty i godziny rozpoczęcia i zakończenia połączenia przychodzącego (okres retencji 12 m-cy). Zaskarżone przepisy przewidują również, że operator zatrzymuje i przetwarza „dane inne, uznane za niezbędne do tych celów", a także wskazują, że zakres danych może zostać dodatkowo rozszerzony w drodze dekretu przez króla po zasięgnięciu opinii urzędu ochrony danych. Dodatkowo przewidziano możliwość zatrzymywania i przetwarzania

[2] Wyrok belgijskiego Trybunału Konstytucyjnego nr 57/2021 z dnia 22 kwietnia 2021 r., wyrok belgijskiego Trybunału Konstytucyjnego nr 158/2021 z dnia 18 listopada 2021 r.

danych o ruchu niezbędnych do zapewnienia bezpieczeństwa i prawidłowego działania sieci i usług łączności elektronicznej, w szczególności do wykrywania i analizowania potencjalnych lub rzeczywistych naruszeń tego bezpieczeństwa, w tym identyfikowania źródła tych naruszeń. Okres retencji przewidziano na 12 m-cy z możliwością wydłużenia w przypadku „szczególnego" naruszenia bezpieczeństwa sieci. Brak jednak wyjaśnienia co mieści się w hipotezie „szczególnego" naruszenia. Nie przewidziano również we wskazanych przepisach kontroli niezależnego organu nad udostępnianiem danych.

W odniesieniu do przepisu przewidującego zatrzymanie danych o lokalizacji (art. 6 zaskarżonej ustawy) sąd konstytucyjny wskazuje, że przepis ten wpisuje się w hipotezy wskazane w art. 9 ust. 1 tej dyrektywy w zakresie, w jakim przewiduje zatrzymywanie danych dotyczących lokalizacji innych niż dane o ruchu, odnoszących się do abonenta lub użytkownika końcowego w sytuacji, gdy dane te zostały poddane anonimizacji (3°) i gdy przetwarzanie odbywa się w ramach świadczenia usługi wykorzystującej dane o ruchu lub dane dotyczące lokalizacji (4°) – o ile, w tym ostatnim przypadku, abonent lub użytkownik końcowy udzielił uprzednio swojej zgody. Jednakże przepis ten dotyczy również innych sytuacji zatrzymywania danych niż te, na które zezwala dyrektywa. Jeśli chodzi o te inne stany faktyczne, należy się odnieść do art. 15 ust. 1 wspomnianej dyrektywy, który pozwala ograniczyć zakres praw ustanowionych między innymi w jej art. 9. Zgodnie z zaskarżonym przepisem operatorzy określają dane dotyczące lokalizacji inne niż dane o ruchu, które mogą być zatrzymywane i przetwarzane. W każdym przypadku oceniają oni również, czy to zatrzymanie i przetwarzanie jest niezbędne. Poza tym, przewidziane okresy zatrzymania, które wynoszą dwanaście miesięcy (gdy jest to niezbędne dla prawidłowego działania i bezpieczeństwa sieci lub usługi) i cztery miesiące (gdy jest to niezbędne do wykrywania lub analizowania oszustw lub wykorzystywania sieci w sposób niedozwolony), mogą być przedłużane odpowiednio w „szczególnych przypadk[ach] naruszeń bezpieczeństwa sieci, wymagających zatrzymania tych danych na okres dłuższy" oraz w „szczególnych przypadk[ach] oszustw lub wykorzystania sieci w sposób niedozwolony, wymagających zatrzymania tych danych na okres dłuższy".

Ponadto zarzuty dotyczą przepisów, które zezwalają funkcjonariuszom policji sądowej IBPT na dostęp do danych w dwóch sytuacjach: 1) dostęp do danych identyfikacyjnych w celu wykrywania, udowadniania lub ścigania przestępstw, o których mowa we wskazanych przepisach (dot. odpowiednio, wykonywania połączeń elektronicznych w celu uzyskania bezprawnej korzyści i wykorzystywanie komunikacji elektronicznej do nękania adresata oraz określonych w kodeksie karnym dot. przestępstw popełnianych przy pomocy sprzętu, sieci lub usług łączności elektronicznej lub radiokomunikacji), 2) dostęp do metadanych niezbędnych do wykrywania, udowadniania lub ścigania tych przestępstw na potrzeby wykonywania swoich zadań, (art. 25/1 § 1 i 2 zaskarżonej ustawy).

2. **Wątpliwości belgijskiego sądu konstytucyjnego dotyczące proporcjonalności przyjętych w zaskarżonych regulacjach przepisów odnoszących się do zatrzymywania danych o ruchu i lokalizacji w celu zwalczania oszustw i wykorzystania sieci w sposób niedozwolony.**

Mając na uwadze powyższe regulacje dotyczące zatrzymania danych o ruchu, Trybunał Konstytucyjny wyraził wątpliwości „czy 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) w związku z art. 7, 8 i art. 52 ust. 1 Karty Praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że:
a) stoi on na przeszkodzie przepisom krajowym, które nakładają na operatorów usług łączności elektronicznej obowiązek zatrzymywania i przetwarzania wskazanych w tych przepisach danych o ruchu w ramach udostępniania tej sieci lub świadczenia tej usługi, na okres wynoszący, zależnie od przypadku, od czterech do dwunastu miesięcy, aby podejmowali oni odpowiednie, proporcjonalne, **prewencyjne i naprawcze środki pozwalające unikać oszustw i wykorzystywania** ich sieci w sposób niedozwolony oraz zapobiegać ponoszeniu szkód przez użytkowników końcowych lub nękaniu ich, a także udowadniać oszustwa lub wykorzystanie sieci lub usługi w sposób niedozwolony lub identyfikować ich sprawców oraz źródło;
b) stoi on na przeszkodzie przepisom krajowym, które umożliwiają tym operatorom zatrzymywanie i przetwarzanie rozpatrywanych danych o ruchu **po upływie wskazanych wyżej terminów w przypadku zidentyfikowania szczególnego oszustwa lub szczególnego wykorzystania sieci w sposób niedozwolony**, przez czas niezbędny do jego analizy i rozstrzygnięcia sprawy albo przez czas niezbędny do analizy tego przypadku wykorzystania sieci w sposób niedozwolony?”.

Ponadto Trybunał, mając na uwadze regulacje dotyczące zatrzymania danych o lokalizacji wyraził wątpliwości, „czy art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że:
a) stoi on na przeszkodzie przepisom krajowym, które umożliwiają operatorom sieci ruchomych, w ramach udostępniania tych sieci lub świadczenia tych usług, zatrzymywanie i przetwarzanie danych dotyczących lokalizacji **bez dokładnego określenia, o jakie dane chodzi, przez okres czterech lub dwunastu miesięcy (zależnie od przypadku),** gdy jest to niezbędne do prawidłowego działania i bezpieczeństwa sieci lub usługi albo do wykrywania lub analizowania oszustw lub przypadków wykorzystania sieci w sposób niedozwolony;
b) stoi on na przeszkodzie przepisom krajowym, które umożliwiają tym operatorom zatrzymywanie i przetwarzanie danych dotyczących lokalizacji **po upływie wskazanych wyżej** terminów w przypadku zidentyfikowania szczególnego oszustwa lub szczególnego przypadku wykorzystania sieci w sposób niedozwolony?”

Odnosząc się do pytań Trybunału Konstytucyjnego, należy przypomnieć, że Trybunał Sprawiedliwości wskazał w wyroku z 8 kwietnia 2014 r. w sprawach połączonych: C-293/12 i C-594/12, Digital Rights Ireland Ltd przeciwko Minister for Communications i in., że akty prawne instytucji UE muszą być odpowiednie do realizacji uzasadnionych celów i nie mogą wykraczać poza to, co jest konieczne do ich osiągnięcia. Trybunał, stwierdzając nieważność dyrektywy retencyjnej, w szczególności wskazał, że obowiązek zatrzymania danych dotyczył wszystkich środków komunikacji elektronicznej, wszystkich abonentów i zarejestrowanych użytkowników, co wiązało się z tym, że dyrektywa ingerowała w prawa podstawowe prawie wszystkich mieszkańców UE. Jak uznał TSUE, dyrektywa nie przewidywała jakiegokolwiek zróżnicowania, ograniczenia lub wyjątków – obejmowała osoby, których dane są zatrzymywane nawet wtedy, gdy nie ma wobec nich żadnych podstaw do wszczęcia postępowania karnego oraz brakuje jakichkolwiek dowodów, nawet pośrednich, sugerujących ich związek (nawet daleki) z poważnymi przestępstwami.

W wyroku z 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, Trybunał orzekł z kolei, że art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty stoją na przeszkodzie środkom ustawodawczym przewidującym **w tych celach prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji.** Trybunał uznał, że **jeśli występują wystarczająco konkretne okoliczności, które pozwalają na uznanie, że w danym państwie członkowskim istnieje poważne zagrożenie dla bezpieczeństwa narodowego, które jest rzeczywiste i aktualne lub przewidywalne to** art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty nie stoi co do zasady na przeszkodzie środkowi ustawodawczemu, który zezwala właściwym organom na nakazanie dostawcom usług łączności elektronicznej zatrzymywania danych o ruchu i danych o lokalizacji **wszystkich użytkowników środków łączności elektronicznej w ograniczonym okresie**. Nakaz przewidujący prewencyjne zatrzymywanie danych wszystkich użytkowników środków łączności elektronicznej musi jednak być ograniczony w czasie do tego, co absolutnie niezbędne. O ile nie można wykluczyć, że skierowany do dostawców usług łączności elektronicznej nakaz zatrzymywania danych może ze względu na utrzymywanie się takiego zagrożenia zostać odnowiony, o tyle czas obowiązywania każdego nakazu nie może przekraczać dającego się przewidzieć okresu. Ponadto takie zatrzymywanie danych powinno być ograniczone i powinny mu towarzyszyć ścisłe gwarancje umożliwiające skuteczną ochronę danych osobowych osób, których dane dotyczą przed ryzykiem nadużyć. Zatrzymywanie to nie może zatem mieć charakteru systemowego.

Jeśli chodzi o cel polegający na zapobieganiu przestępstwom, ich dochodzeniu, wykrywaniu i ściganiu, Trybunał zauważył także, że zgodnie z zasadą proporcjonalności **jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego** mogą uzasadniać

poważne ingerencje w prawa podstawowe ustanowione w art. 7 i 8 Karty, takie jak te, które są związane z zatrzymywaniem danych o ruchu i danych o lokalizacji.

Jak podkreślił TSUE, **uregulowanie krajowe przewidujące uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji** w celu zwalczania poważnej przestępczości wykracza poza granice tego, co absolutnie niezbędne, i nie może być uważane za uzasadnione w społeczeństwie demokratycznym, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz 52 ust. 1 Karty (podobnie wyrok z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 107).

Ponadto w wyroku z 2 marca 2021 r., C-746/18 w sprawie Prokuratuur, Trybunał uznał, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. KPP należy interpretować w ten sposób, że **sprzeciwia się on przepisom krajowym** umożliwiającym dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, **bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego, niezależnie od długości okresu na jaki wniesiono o dostęp do takich danych oraz ilości i rodzaju danych dostępnych przez taki okres.**

Mając powyższe na uwadze należy wskazać, że z dotychczasowego orzecznictwa Trybunału wynika, że uregulowanie krajowe musi zawierać **jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka** oraz ustanawiające **minimalne wymogi** służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę ich danych przed ryzykiem nadużyć. A zatem, odpowiadając na pytania Trybunału Konstytucyjnego w pkt. 1 pkt a) i b) oraz 2 pkt a) i b), należy wskazać, że rozwiązanie krajowe, które przewidywałoby uprawnienie do dostępu do danych telekomunikacyjnych, bez precyzyjnych i jasnych warunków dostępu do danych telekomunikacyjnych, w tym bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości, bez sprecyzowania konkretnego zakresu danych i zapewnienia właściwych gwarancji dla praw osób fizycznych, takich jak co najmniej zapewnienie kontroli przez niezależny organ, należy uznać za sprzeczne z art. 15 dyrektywy w zw. z art. 1, 8 oraz 52 ust. 1 KPP.

3. **Wątpliwości belgijskiego Trybunału Konstytucyjnego dotyczące zapewnienia kontroli nad dostępem do danych telekomunikacyjnych przez niezależny organ.**

Trybunał Konstytucyjny stawiając pytanie dotyczące proporcjonalności rozwiązań przyjętych w przepisach dotyczących udostępnienia danych o ruchu – pytanie 1 c) i d) – wyraził wątpliwości, „czy 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) w związku z art. 7, 8 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że:

c) stoi on na przeszkodzie przepisom krajowym, które umożliwiają tym operatorom zatrzymywanie i przetwarzanie danych innych niż wskazane w ustawie w celu umożliwienia wykazania oszustwa lub wykorzystania sieci lub usługi w sposób niedozwolony albo zidentyfikowania sprawcy tych czynów i ich źródła, lecz **nie nakładają obowiązku uprzedniego zasięgnięcia opinii niezależnego organu lub zgłoszenia takiemu organowi;**

d) stoi on na przeszkodzie przepisom krajowym, które umożliwiają tym operatorom zatrzymywanie i przetwarzanie przez okres dwunastu miesięcy (a w przypadku szczególnego naruszenia bezpieczeństwa sieci – przez okres niezbędny do zbadania sprawy) danych o ruchu, które uznają oni za niezbędne do zapewnienia bezpieczeństwa i prawidłowego działania ich sieci i usług łączności elektronicznej, a w szczególności do wykrywania i analizowania potencjalnych lub rzeczywistych naruszeń tego bezpieczeństwa, w tym identyfikowania źródła tych naruszeń**, przy czym przepisy te nie nakładają obowiązku uprzedniego zasięgnięcia opinii niezależnego organu lub zgłoszenia takiemu organowi”.**

Odnosząc się do tych pytań belgijskiego Trybunału należy przypomnieć stanowisko TSUE, z którego wynika, że w demokratycznym państwie prawa zasadność pozyskania danych telekomunikacyjnych powinna być poddana kontroli sądu lub niezależnego organu administracyjnego. Jak wskazał Trybunał w powoływanym wyżej wyroku z 2 marca 2021 r. w sprawie Prokuratuur, C-746, w szczególności uregulowanie krajowe regulujące dostęp właściwych organów do zatrzymanych danych o ruchu i danych o lokalizacji, przyjęte na podstawie art. 15 ust. 1 dyrektywy 2002/58, nie może ograniczać się do wymagania, aby dostęp organów do danych odpowiadał celowi, do którego zmierza to uregulowanie, ale musi również przewidywać warunki materialne i proceduralne regulujące to wykorzystanie (zob. też wyroki z 6 października 2020 r.: Privacy International, C-623/17, a także La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18 i przytoczone tam orzecznictwo).

W powyższym wyroku TSUE podkreślił, że w celu zapewnienia w praktyce pełnej zgodności z tymi warunkami ważne jest, aby **dostęp właściwych organów państwowych do zatrzymanych danych był uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, a decyzja tego sądu lub organu była wydawana na uzasadniony wniosek owych organów, złożony w szczególności w ramach postępowań mających na celu zapobieganie, wykrywanie lub karanie przestępstw. W pilnych i należycie uzasadnionych przypadkach kontrola powinna nastąpić w krótkim czasie** (zob. podobnie wyrok

z 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18 i przytoczone tam orzecznictwo). 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 (zob. wyrok TSUE z 8 kwietnia 2014 r. w sprawach połączonych Digital Rights Ireland Ltd (C-293/12) i Kârntner Landesregierung (C-594/12).

Jak przypomniał Trybunał w wyroku z 5 kwietnia 2022 r. w sprawie G.D. przeciwko The Commissioner of the Garda Síochána i in, C-140/20, niezależna kontrola wymagana zgodnie z art. 15 ust. 1 dyrektywy 2002/58 powinna mieć miejsce przed uzyskaniem wszelkiego dostępu do zatrzymanych danych, z wyjątkiem pilnych i należycie uzasadnionych przypadków, w których powinna ona nastąpić w krótkim czasie**. Późniejsza kontrola nie pozwala bowiem osiągnąć celu uprzedniej kontroli, polegającego na uniemożliwieniu udzielania zezwoleń na dostęp do rozpatrywanych danych, który wykracza poza granice tego, co ściśle niezbędne** (zob. podobnie wyroki: z 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18; a także z 2 marca 2021 r., Prokuratuur C-746/18]. Jednocześnie w wyroku tym TSUE uznał, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8, 11 oraz art. 52 ust. 1 Karty należy interpretować w ten sposób, iż stoi on na przeszkodzie uregulowaniu krajowemu, na podstawie którego scentralizowane rozpatrywanie pochodzących od policji wniosków o udzielenie dostępu do danych zatrzymanych przez dostawców usług łączności elektronicznej, w ramach wykrywania i ścigania poważnych przestępstw, należy do funkcjonariusza policji, wspieranego przez jednostkę ustanowioną w obrębie policji, której przysługuje pewien stopień autonomii w wykonywaniu powierzonego jej zadania i której decyzje mogą być następnie przedmiotem kontroli sądowej (por. też wyrok TSUE wyrok z 2 marca 2021 r., Prokuratuur, C-746/18, w której TSUE uznał, że prokuratura nie może przeprowadzać uprzedniej kontroli wniosków o udzielenie dostępu do zatrzymanych danych].

W związku z powyższym, odpowiadając na pytania Trybunału Konstytucyjnego dotyczące uprzedniej kontroli nad dostępem do danych telekomunikacyjnych, należałoby wskazać, że rozwiązanie krajowe, przewidujące uprawnienie do dostępu do danych telekomunikacyjnych, powinny gwarantować zapewnienie kontroli nad takim dostępem przez niezależny organ lub sąd.

4. Pytania belgijskiego Trybunału Konstytucyjnego dotyczące skutków wyroku stwierdzającego nieważność zaskarżonych przepisów.

Jednocześnie Trybunał Konstytucyjny wyraził wątpliwości, „czy mógłby **tymczasowo utrzymać w mocy skutki zaskarżonej ustawy**, aby uniknąć niepewności prawa i zapewnić możliwość dalszego wykorzystywania uprzednio zebranych i zatrzymywanych danych do celów określonych w ustawie, jeżeli na podstawie odpowiedzi udzielonych na pierwsze lub drugie pytanie prejudycjalne

Trybunał Konstytucyjny miałby dojść do wniosku, że niektóre przepisy zaskarżonej ustawy naruszają jeden lub więcej z obowiązków wynikających z przepisów wskazanych w tych pytaniach".

Mając powyższe pytanie Trybunału Konstytucyjnego na uwadze, należy przypomnieć, że zasada pierwszeństwa prawa Unii ustanawia prymat prawa Unii nad prawem państw członkowskich. Zasada ta nakłada zatem na wszystkie organy państw członkowskich obowiązek zapewnienia pełnej skuteczności różnych norm prawa Unii, a prawo państw członkowskich nie może mieć wpływu na skuteczność przyznaną tym różnym normom na terytorium wspomnianych państw. Zgodnie z tą zasadą **w razie niemożności dokonania wykładni uregulowania krajowego w sposób zgodny z wymogami określonymi w prawie Unii sąd krajowy, do którego należy w ramach jego kompetencji stosowanie przepisów prawa Unii, jest zobowiązany zapewnić pełną ich skuteczność**, w razie potrzeby powstrzymując się od stosowania, z własnej inicjatywy, wszelkich sprzecznych z nimi przepisów prawa krajowego, także późniejszych, bez konieczności żądania uprzedniego uchylenia tych przepisów w drodze ustawodawczej lub w jakimkolwiek innym trybie konstytucyjnym ani bez konieczności oczekiwania na takie uchylenie [zob. podobnie wyroki: z 15 lipca 1964 r., Costa, 6/64,; z 19 listopada 2019 r., A.K. i in. (Niezależność Izby Dyscyplinarnej Sądu Najwyższego), C-585/18, C-624/18 i C-625/18, a także z 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18].

Jak wskazał TSUE w powołanym wyżej wyroku z 5 kwietnia 2022 r. w sprawie G.D. przeciwko The Commissioner of the Garda Síochána i in, C-140/20, **jedynie Trybunał może, w drodze wyjątku, kierując się nadrzędnymi względami pewności prawa, tymczasowo zawiesić wywierany przez prawo Unii skutek w postaci uchylenia przepisów prawa krajowego sprzecznych z prawem Unii**. Takie ograniczenie w czasie skutków wykładni prawa Unii dokonanej przez Trybunał może zostać orzeczone jedynie w samym wyroku, w którym Trybunał Sprawiedliwości rozstrzyga w przedmiocie wykładni, o którą się do niego zwrócono. Do naruszenia pierwszeństwa i jednolitego stosowania prawa Unii doszłoby, gdyby sądy krajowe były uprawnione do przyznania, choćby tymczasowo, przepisom krajowym pierwszeństwa przed prawem Unii, z którym te przepisy są sprzeczne (wyrok z 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18 i przytoczone tam orzecznictwo).

W powyższym wyroku Trybunał uznał, że prawo Unii należy interpretować w ten sposób, że **stoi ono na przeszkodzie temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego nakładającego na dostawców usług łączności elektronicznej obowiązek uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji, a to ze względu na niezgodność tego uregulowania z art. 15 ust. 1**

dyrektywy 2002/58, zmienionej dyrektywą 2009/136, w związku z Kartą Praw Podstawowych UE. Kwestia dopuszczalności dowodów uzyskanych za pomocą takiego uogólnionego i niezróżnicowanego zatrzymywania należy, zgodnie z zasadą autonomii proceduralnej państw członkowskich, do prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności. Jak wskazał Trybunał, utrzymanie w mocy skutków uregulowania krajowego oznaczałoby bowiem, że uregulowanie to w dalszym ciągu nakładałoby na dostawców usług łączności elektronicznej obowiązki, które są sprzeczne z prawem Unii i które powodują poważną ingerencję w prawa podstawowe osób, których dane są zatrzymywane (zob. analogicznie wyrok z 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18,).

W związku z powyższym należy uznać, że Trybunał Konstytucyjny nie może ograniczyć w czasie skutków stwierdzenia nieważności przepisu w związku z jego niezgodnością z prawem unijnym na podstawie prawa krajowego.

5. **Regulacje krajowe dotyczące udostępniania danych telekomunikacyjnych**.

Przekładając powyższe pytania prejudycjalne na grunt prawa polskiego, należy wskazać, że **polskie regulacje uprawniające Policję oraz określone służby do dostępu do danych telekomunikacyjnych** – które wynikają z ustawy Prawo komunikacji elektronicznej[3], tj. art. 47 oraz art. 49 PKE – **przewidują obowiązek bezwarunkowego przechowywania przez przedsiębiorców telekomunikacyjnych informacji o wszystkich klientach**.

Prezes UODO niejednokrotnie przedstawiał swoją opinię odnośnie do konieczności dokonania zmian w przepisach krajowych – w tym także przepisów ustawy o Policji (art. 19, 20c ustawy o Policji) oraz Kodeksu postępowania karnego (art. 218 § 1 k.p.k., art. 236a k.p.k.) – uprawniających określone podmioty do dostępu do danych.

Co istotne, w opinii dotyczącej ustawy Prawo komunikacji elektronicznej (druk sejmowy 423)[4] Prezes UODO zwracał uwagę, że pomimo tego, iż istniała okazja do dokonania stosownych zmian w systemie prawa, w postaci uchwalania nowego aktu prawnego, projekt ustawy powiela niezgodny z orzecznictwem TSUE model retencji i udostępniania danych telekomunikacyjnych uprawnionym podmiotom.

Uwagi Prezesa UODO odnosiły się w szczególności do art. 47 ust. 1 PKE, który nakłada na przedsiębiorców telekomunikacyjnych obowiązek przechowywania przez okres 12 miesięcy danych użytkownika końcowego, o których mowa w art. 49 ust. 1 PKE. Zgodnie z art. 49 ust. 1 PKE danymi objętymi obowiązkiem zatrzymywania, przechowywania, udostępniania i ochrony są dane niezbędne do 1) jednoznacznego zidentyfikowania zakończenia sieci, telekomunikacyjnego

[3] Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U z 2024 r. poz. 1221; dalej: PKE).
[4] Zob. opinia PUODO udostępniona na stronie UODO: https://uodo.gov.pl/pl/138/3126

urządzenia końcowego oraz użytkownika końcowego: a) inicjującego połączenie, b) do którego kierowane jest połączenie; 2) określenia: a) daty i godziny połączenia oraz czasu jego trwania, b) rodzaju połączenia, c) lokalizacji telekomunikacyjnego urządzenia końcowego. Jednocześnie art. 49 ust. 2 PKE odsyła do uregulowania szczegółowego wykazu danych użytkownika w rozporządzeniu.

W ocenie Prezesa UODO nowe regulacje PKE powielają blankietowe rozwiązania zawarte w uchylonych art. 180a oraz art. 180c Prawa telekomunikacyjnego[5], nie zapewniając zgodności z zasadami legalności, przejrzystości, ograniczonego celu oraz minimalizacji danych wynikającymi z przepisów rozporządzenia 2016/679, ani zgodności z prawem UE, w świetle powołanych powyżej wyroków Trybunału Sprawiedliwości UE[6].

Wymaga przy tym podkreślenia, że **przepisy polskiej ustawy o Policji były przedmiotem oceny Europejskiego Trybunału Praw Człowieka, który wyrokiem z 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce (skargi nr 72038/17 i 25237/18) orzekł naruszenie art. 8 EKPC**, tj. 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[7].

W powyższym wyroku Trybunał uznał, że prawo krajowe nie zapewniało wystarczających zabezpieczeń przed nadmierną ingerencją w życie prywatne jednostek, a także w odniesieniu do komunikacji objętej tajemnicą adwokacką. Brak takich gwarancji nie został dostatecznie zrównoważony przez istniejący mechanizm kontroli sądowej. Trybunał zauważył, że obowiązujące przepisy nie wymagały od sądu rozpatrującego wniosek o zezwolenie na inwigilację potwierdzenia, czy istnieje „uzasadnione podejrzenie" w odniesieniu do osoby, której dotyczy wniosek, a w szczególności zbadania, czy istnieją jakiekolwiek dowody na to, że osoba ta planuje, dokonuje lub dokonała czynów przestępczych lub jakiegokolwiek innego przestępstwa pozwalającego na zastosowanie środków tajnej inwigilacji, takich jak czyny zagrażające bezpieczeństwu narodowemu. Ponadto Trybunał uznał, że istniejąca procedura wydawania zgód powinna zostać uzupełniona o inne mechanizmy kontroli proceduralnej *post factum*. Zauważając jednocześnie, że w

---

[5] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2024, poz. 1222).

[6] Należy wskazać na takie istotne orzeczenia TSUE jak: wyrok z 4 października 2024 r. w sprawie C 548/21, CG v Bezirkshauptmannschaft Landeck, wyrok za 13 czerwca 2024 r. w sprawie C-229/23 HYA i in. II, wyrok z 30 kwietnia 2024 r. w sprawie C-470/21 La Quadrature du Net i in. przeciwko Premier ministre i Ministere de la Culture, oraz wyrok z 30 kwietnia 2024 r. w sprawie C-178/22 Procura della Repubblica presso il Tribunale di Bolzano, wyrok z 5 kwietnia 2022 r. w sprawie C-140/20, wyrok z 6 października 2020 r. w sprawie La Quadrature du Net i in. przeciwko Premier ministre i in., sprawy połączone C-511/18, C-512/18 i C-520/18, wyrok z 6 października 2020 r. Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs i in. w sprawie C-¬623/17, wyrok z 21 grudnia 2016 r. w sprawach połączonych C-203/15 i C-698/15 Tele2 Sverige AB przeciwko Post- och telestyrelsen oraz Secretary of State for the Home Department przeciwko Tom Watson, Peter Brice, Geoffrey Lewis, wyrok z 8 kwietnia 2014 r. w sprawach połączonych: C-293/12 i C-594/12, Digital Rights Ireland Ltd przeciwko Minister for Communications i in.

[7] Zob. też inne np. wyrok ETPC z 12.01.2023 w sprawie Potoczká i Adamčo przeciwko Słowacji, skarga nr 7286/16.

obecnym stanie prawnym, nie przewidziano obowiązku informowania osoby objętej środkiem kontroli, nawet po upływie określonego czasu i nawet w przypadku, gdy nie zagrażałoby to celowi, dla którego zastosowano ww. środek. ETPC wskazał przy tym, że prawo nie przewidywało skutecznego środka odwoławczego dla osób, które uważały, że zostały poddane tajnej inwigilacji.

W związku z powyższym, w szczególności zważywszy na wyrok ETPC, potwierdzający, że polskie przepisy prowadzą do naruszenia prawa do prywatności należy wskazać, że choć nie zawierają one tożsamych unormowań dotyczących dostępu do danych o ruchu czy lokalizacji w celu zwalczania oszustw i wykorzystania sieci w sposób niedozwolony, to przewidują bardzo ogólne, niedookreślone regulacje, które nie zapewniają właściwych gwarancji dla praw osób fizycznych.

Ewentualne rozstrzygnięcie Trybunału w przedmiotowej sprawie będzie więc miało wpływ również na aktualnie obowiązujące polskie przepisy.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/