RZECZNIK PRAW OBYWATELSKICH
Marcin Wiącek

Warszawa, 17.07.24

VII.501.114.2024.KSZ

Pani
Małgorzata Kidawa-Błońska
Marszałek Senatu
Kancelaria Senatu
e-PUAP

Szanowna Pani Marszałek,

na podstawie art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2023 r. poz. 1058), przedkładam moją opinię do uchwalonej przez Sejm RP w dniu 12 lipca 2024 r. ustawy – Prawo komunikacji elektronicznej, z uprzejmą prośbą o uwzględnienie jej w pracach Senatu RP.

Z poważaniem

Marcin Wiącek
(podpis na oryginale)

Do wiadomości:
Pan Mirosław Wróblewski – Prezes Urzędu Ochrony Danych Osobowych
Urząd Ochrony Danych Osobowych – e-PUAP

Opinia Rzecznika Praw Obywatelskich do ustawy – Prawo komunikacji elektronicznej uchwalonej przez Sejm RP w dniu 12 lipca 2024 r.

I. Uwagi wprowadzające

1. Zakres przedmiotowy projektu

Uchwalone przepisy ustawy – Prawo komunikacji elektronicznej (PKE) – jak wynika z uzasadnienia projektu złożonego do laski marszałkowskiej – mają za zadanie kompleksowo uregulować między innymi kwestie wykonywania działalności polegającej na zapewnieniu komunikacji elektronicznej, regulowania rynków komunikacji elektronicznej, warunki gospodarowania częstotliwościami, zasobami orbitalnymi oraz zasobami numeracji, a także prawa i obowiązki użytkowników, zasady przetwarzania danych telekomunikacyjnych i ochrony tajemnicy komunikacji elektronicznej. Materia ta jest obecnie regulowana ustawą z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34).

Konieczność opracowania nowej ustawy, w ocenie wnioskodawców, wynika z obowiązku wdrożenia do polskiego porządku prawnego przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Zastąpienie obecnie obowiązującej ustawy (Prawa telekomunikacyjnego) nowym aktem prawnym uzasadnione jest – w ocenie wnioskodawców projektu – zakresem i liczbą zmian oraz koniecznością uporządkowania, przeredagowania i niejednokrotnie uproszczenia dotychczas funkcjonujących przepisów.

2. Zakres uwag Rzecznika Praw Obywatelskich

Dla Rzecznika Praw Obywatelskich szczególnie istotnym wątkiem w uchwalonych przepisach są kwestie związane z retencją danych telekomunikacyjnych oraz ochroną praw użytkowników. Ocena proponowanych przez wnioskodawcę rozwiązań prawnych, w szczególności konstytucyjnych praw i wolności użytkowników, wymaga odwołania się do wzorców prawnych w postaci postanowień dotyczących **ochrony godności człowieka** (art. 30 Konstytucji RP), **wolności człowieka** (art. 31 ust. 1 i 2 Konstytucji RP), **ochrony życia prywatnego** (art. 47 Konstytucji RP), **wolności i ochrony tajemnicy komunikowania się** (art. 49 Konstytucji RP) oraz **ochrony autonomii informacyjnej jednostek** (art. 51 Konstytucji RP).

3. Standard konstytucyjny

Status człowieka w demokratycznym państwie prawa opiera się na poszanowaniu jego przyrodzonej i niezbywalnej godności (art. 30 Konstytucji RP), a także wynikającej z niej swobody decydowania o swym postępowaniu, zgodnie z własną wolą (art. 31 ust. 1 i 2 Konstytucji RP). Godność człowieka, zgodnie z art. 30 Konstytucji RP, jest nienaruszalna i nie może podlegać żadnym ograniczeniom. Ustawodawca może jednak ingerować w wolność człowieka, na zasadach uregulowanych w art. 31 ust. 3 Konstytucji RP.

Konstytucyjna ochrona wolności człowieka odnosi się przede wszystkim do sfery jego prywatności. Ustrojodawca statuuje prywatność jednostki jako wolność konstytucyjnie chronioną, co oznacza swobodę działania jednostek aż do granic ustanowionych w ustawie. Wyłącznie jednoznaczna regulacja ustawowa może nakładać ograniczenia w zakresie określonych zachowań mieszczących się w ramach konkretnej wolności[1]. Państwo ma obowiązek prawnego poszanowania i ochrony konstytucyjnych wolności człowieka, a także powstrzymania się od ingerowania w wolności zarówno przez państwo, jak i podmioty prywatne. Standard ten

[1] Wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11.

odnosi się w szczególności do wolności osobistych, do których – obok wyrażonej w art. 47 Konstytucji RP prywatności – zaliczają się również wolność komunikowania się (art. 49 Konstytucji RP), czy szeroko rozumiana autonomia informacyjna (art. 51 Konstytucji RP). Ochrona prywatności i autonomii informacyjnej jest konsekwencją ochrony przyrodzonej i niezbywalnej godności człowieka[2].

Jak przyjmuje się w orzecznictwie, art. 47 i 51 Konstytucji RP chronią tę samą wartość konstytucyjną – sferę prywatności. **Autonomia informacyjna stanowi istotny element składowy prawa do ochrony prywatności, a polega na samodzielnym decydowaniu o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także na sprawowaniu kontroli nad tymi informacjami, nawet jeśli znajdują się w posiadaniu innych osób**[3]. W swoim orzecznictwie Trybunał Konstytucyjny podkreślał, że art. 51 Konstytucji RP ustanawia szczególny środek poszanowania tych samych wartości, które chronione są za pośrednictwem art. 47 Konstytucji RP[4].

Z ochroną prywatności i autonomii informacyjnej koresponduje też **prawo do ochrony tajemnicy komunikowania się**, ustanowione w art. 49 Konstytucji RP. Zdaniem Trybunału Konstytucyjnego, konstytucyjnymi gwarancjami wynikającymi z art. 49 Konstytucji RP objęta jest treść komunikowana bezpośrednio, jak i za pomocą środków komunikowania na odległość[5].

Trybunał Konstytucyjny wyraźnie podkreślił, że konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji RP objęte są „wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. **rozmowy osobiste i telefoniczne**, korespondencja pisemna,

---

[2] Wyrok TK z 12 grudnia 2005 r. o sygn. akt K 32/04.
[3] Wyroki TK: z 19 lutego 2002 r., o sygn. akt U 3/01; z 30 listopada 2002 r. o sygn. akt K 41/02 czy też z 13 grudnia 2011 r. o sygn. akt K 33/08.
[4] Wyrok TK z 12 listopada 2002 r. o sygn. akt SK 40/01.
[5] Wyroki TK: z 20 czerwca 2005 r. o akt sygn. K 4/04 oraz z 2 lipca 2007 r. o sygn. akt K 41/05.

faks, **wiadomości tekstowe i multimedialne, poczta elektroniczna**). **Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń, czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI"**[6]. W tym samym wyroku Trybunał Konstytucyjny podkreślił również wyraźnie, że w ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się również ochrona przed niejawnym monitorowaniem jednostki.

II. Retencja danych telekomunikacyjnych

1. Standard europejski

1.1. Rzecznik Praw Obywatelskich dostrzega potrzebę właściwego uregulowania kwestii retencji danych telekomunikacyjnych. Należy bowiem przypomnieć, że w 2014 r. Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał orzeczenie w połączonych sprawach C293/12 i C-594/12 Digital Rights Ireland[7], w którym stwierdził nieważność dyrektywy 2006/24[8]. Przyczyną nieważności nie była jednak istota rozwiązań prawnych zastosowanych w dyrektywie, gdyż co do zasady konieczność przechwytywania określonych danych telekomunikacyjnych jest konieczna dla zapewnienia bezpieczeństwa. Stwierdzenie nieważności wiązało się z brakiem proporcjonalności wynikającej z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej (KPP), a także z

[6] Wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11.

[7] Wyrok TSUE z 8.04.2014 r. w sprawach połączonych: C-293/12, Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General i C-594/12, Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, ECLI:EU:C:2014:238.

[8] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15.03.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 2006 r., s. 54).

niezgodnością z art. 7 i 8 KPP. **TSUE uznał, że nie wystarczy samo odniesienie się do „poważnych przestępstw", by uznać przesłanki wskazane w art. 52 ust. 1 Karty Praw Podstawowych UE (KPP) za spełnione i uzasadniające ingerencję w prawa podstawowe.** TSUE wskazał także, że dyrektywa retencyjna wykraczała poza to, co jest ściśle niezbędne dla osiągnięcia założonego celu. Nie przewidując jakiegokolwiek rozróżniania, ograniczania czy wyjątków, postanowienia dyrektywy obejmowały osoby, których dane zatrzymywane były nawet wtedy, gdy nie było wobec nich żadnych podstaw do wszczęcia postępowania karnego oraz brakowało jakichkolwiek dowodów wskazujących na ich związek z poważnymi przestępstwami.

1.2. Powyżej przywołany wyrok był szeroko komentowany **w kontekście konieczności zapewnienia zgodności z prawem europejskim polskiego ustawodawstwa**[9]. TSUE wskazał bowiem na szereg istotnych czynników niezbędnych dla prawidłowych regulacji dotyczących zbierania danych:

1) konieczność rozróżnienia zbierania danych osób podejrzewanych czy powiązanych z działalnością przestępczą i wszelkich innych;
2) wprowadzany okres i typ przechowywanych danych w poszczególnych sprawach musi mieć wyraźny związek z konkretnym celem ich zbierania;
3) niezbędne są prawne gwarancje przed nadużyciem danych, czy też nieuprawnionym do nich dostępem;
4) dostęp do danych musi być przedmiotem kontroli sądowej lub kontroli niezależnego organu administracyjnego

- które w polskim porządku prawnym nie były, a także - jak wynika z analizy projektowanych przepisów - w dalszym ciągu nie zostały uwzględnione.

[9] Zob. np. A. Grzelak, *Granica między skuteczną walką z przestępczością a prawem do prywatności i do ochrony danych osobowych – glosa do wyroku TS z 8.04.2014 r. w sprawach połączonych C-293/12 i C-594/12 Digital Rights Ireland*, Europejski Przegląd Sądowy, 07/2014, s. 45-52.

1.3. W wyroku sprawie C-623/17, Privacy International[10], Trybunał Sprawiedliwości orzekł, że – po pierwsze – zakresem stosowania dyrektywy 2002/58/WE objęte jest uregulowanie krajowe umożliwiające organowi państwa zobowiązanie dostawców usług łączności elektronicznej do przekazywania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego, a – po drugie – art. 15 ust. 1 dyrektywy 2002/58/WE w zw. z art. 4 ust. 2 TUE, a także art. 7, 8 i 11 oraz art. 52 ust. 1 KPP 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 przekazywania służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego.**

W ocenie Trybunału Sprawiedliwości UE, art. 15 ust. 1 dyrektywy 2002/58/WE nie stoi jednak na przeszkodzie przepisom krajowym, które umożliwiają, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji w sytuacjach, gdy dane państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia. Decyzja o wydaniu takiego nakazu powinna być przy tym przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego, wywierającej wiążący skutek, mającej na celu weryfikację występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, które powinny zostać przewidziane. Wspomniany nakaz można zaś wydać jedynie na określony czas ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia. Dopuszczalne jest

[10] Wyrok TSUE z 6.10.2020 r. w sprawie C-623/17, Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service, EU:C:2020:790.

również, zdaniem Trybunału, w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego ukierunkowane zatrzymywanie danych o ruchu i danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego, na okres ograniczony do tego, co ściśle niezbędne, ale odnawialny. Dopuszczalne jest także – w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego:

- **uogólnione i niezróżnicowane zatrzymywanie adresów IP** przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne.
- przyjęcie przepisów regulujących **uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej** oraz umożliwiających posłużenie się nakazem skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, **szybkiego zatrzymywania przez określony czas danych o ruchu i danych o lokalizacji,** którymi dysponują ci dostawcy usług.

Warunkiem legalności takich przepisów krajowych jest jednak to, by zawierały one jasne i precyzyjne gwarancje zapewniające, że **zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych warunków oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.**

Trybunał Sprawiedliwości dopuścił również uregulowania krajowe zobowiązujące 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, przy czym określił wymogi i wskazał, że jest to dopuszczalne, 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 powinno 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.

Ponadto Trybunał wskazał, że art. 23 ust. 1 rozporządzenia 2016/679[11] w zw. z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP należy interpretować w ten sposób, że **stoi on na przeszkodzie przepisom krajowym nakładającym na dostawców dostępu do usług internetowej komunikacji publicznej i na dostawców usług hostingowych obowiązek uogólnionego i niezróżnicowanego zatrzymywania m.in. danych osobowych dotyczących tych usług.**

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektyw 95/46/WE (ogólne rozporządzenie o ochronie danych).

1.4. W swojej dotychczasowej działalności Rzecznik Praw Obywatelskich wielokrotnie sygnalizował[12] również potrzebę przeanalizowania i uwzględnienia kolejnego wyroku retencyjnego[13]. TSUE wskazał w nim, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP należy interpretować w ten sposób, iż stoi on na przeszkodzie środkom ustawodawczym przewidującym, w celach, o których mowa w tym art. 15 ust. 1, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji. Natomiast wspomniany art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP nie stoi na przeszkodzie przepisom ustawodawczym:

- umożliwiającym, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji w sytuacjach, gdy dane państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa narodowego, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia, przy czym decyzja o wydaniu takiego nakazu powinno być przedmiotem skutecznej kontroli sądu lub niezależnego organu administracyjnego, którego decyzja wywiera wiążący skutek, mającej na celu weryfikację występowania jednej z takich sytuacji oraz poszanowania warunków i gwarancji, które powinny zostać przewidziane, zaś wspomniany nakaz można wydać jedynie na określony czas ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia;
- przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego ukierunkowane zatrzymywanie danych o ruchu i

[12] Wystąpienia Rzecznika Praw Obywatelskich: do Prezesa Rady Ministrów z 13.01.2022 r., do Prezesa Rady Ministrów z 13.07.2022 r., do Ministra Spraw Wewnętrznych i Administracji z 6.01.2023 r., do Ministra Spraw Wewnętrznych i Administracji z 7.04.2023 r.

[13] Wyrok TS z 5.04.2022 r., C-140/20, G.D. przeciwko The Commissioner of the Garda Síochána i in., EU:C:2022:258.

danych o lokalizacji, którego granice zostają wyznaczone na podstawie obiektywnych i niedyskryminacyjnych przesłanek w zależności od kręgu osób, których dane dotyczą, lub kryterium geograficznego, na okres ograniczony do tego, co ściśle niezbędne, ale odnawialny;

- przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego uogólnione i niezróżnicowane zatrzymywanie adresów IP przydzielonych źródłu połączenia, w okresie ograniczonym do tego, co ściśle niezbędne;
- przewidującym w celu ochrony bezpieczeństwa narodowego, zwalczania przestępczości i ochrony bezpieczeństwa publicznego, uogólnione i niezróżnicowane zatrzymywanie danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej; oraz
- umożliwiającym, w celu zwalczania poważnej przestępczości oraz, *a fortiori*, ochrony bezpieczeństwa narodowego, posłużenie się nakazem skierowanym do dostawców usług łączności elektronicznej, w drodze decyzji właściwego organu poddanej skutecznej kontroli sądowej, szybkiego zatrzymywania przez określony czas danych o ruchu i danych o lokalizacji, którymi dysponują ci dostawcy usług

- jeśli środki te zawierają jasne i precyzyjne przepisy zapewniające, że rozpatrywane **zatrzymywanie danych jest uzależnione od spełnienia związanych z nim materialnych i proceduralnych warunków oraz że osoby, których dane dotyczą, dysponują skutecznymi gwarancjami chroniącymi przed ryzykiem nadużyć.**

1.5. Ponadto należy podkreślić, że w wyroku w sprawach połączonych C-793/19 i C-794/19[14] TSUE orzekł analogicznie do powyższego rozstrzygnięcia – potwierdzając dotychczasową linię orzeczniczą – wskazując na to, w jaki sposób interpretować art. 15

[14] Wyrok TS z 20.09.2022 r. sprawy połączone C-793/19 i C-794/19, Bundesrepublik Deutschland przeciwko SpaceNet AG, Telekom Deutschland GmbH, ECLI:EU:C:2022:702.

ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP, a także jakie krajowe środki ustawodawcze są sprzeczne z przywołanymi przepisami, a jakie pozostają z nimi w zgodności.

1.6. W wyroku w sprawach połączonych C-339/20 i C-397/20[15] TSUE orzekł natomiast, że art. 12 ust. 2 lit. a i d dyrektywy 2003/6/WE[16] w związku z art. 15 ust. 1 dyrektywy 2002/58/WE oraz w świetle art. 7, 8, 11 i art. 52 ust. 1 KPP należy interpretować w ten sposób, że:

1) sprzeciwiają się one środkom ustawodawczym przewidującym zapobiegawczo w celu zwalczania przestępstw polegających na nadużyciach na rynku, do których zalicza się wykorzystywanie informacji poufnych, **ogólne i niezróżnicowane zatrzymywanie danych o ruchu przez rok od dnia ich zapisu;**

2) prawo Unii należy interpretować w ten sposób, że sprzeciwia się ono temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego na mocy prawa krajowego ma on dokonać w odniesieniu do przepisów krajowych, które z jednej strony nakładają na operatorów świadczących usługi łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, a z drugiej strony pozwalają na przekazywanie tych danych organowi właściwemu w sprawach finansowych bez uprzedniego zezwolenia sądu lub niezależnego organu administracyjnego, ze względu na niezgodność tych przepisów z art. 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, interpretowanym w świetle Karty praw podstawowych Unii Europejskiej. Dopuszczalność dowodów uzyskanych na podstawie krajowych przepisów ustawowych niezgodnych z prawem Unii podlega, zgodnie z zasadą autonomii

[15] Wyrok TS z 20.09.2022 r., sprawy połączone C-339/20 i C-397/20, VD i SR, ECLI:EU:C:2022:703.

[16] Dyrektywa 2003/6/WE Parlamentu Europejskiego i Rady z dnia 28 stycznia 2003 r. w sprawie wykorzystywania poufnych informacji i manipulacji na rynku (nadużyć na rynku) oraz art. 23 ust. 2 lit. g) i h) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenia w sprawie nadużyć na rynku) i uchylającego dyrektywę 2003/6 i dyrektywy Komisji 2003/124/WE, 2003/125/WE, 2004/72/WE.

proceduralnej państw członkowskich, prawu krajowemu, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

1.7. Kolejne wyroki z 30.04.2024 r. potwierdziły dotychczasową linię orzeczniczą Trybunału Sprawiedliwości, przy czym w wyroku w sprawie C-470/21[17] Trybunał rozstrzygnął, że art. 15 ust. 1 dyrektywy 2002/58/WE w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 KPP 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

[17] Wyrok TS z 30.04.2024 r. , w sprawie C-470/21, La Quadrature du Net,, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network przeciwko Premier ministre, Ministre de la Culture, ECLI:EU:C:2024:370.

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 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.

1.8. Możliwość natomiast głębszej ingerencji w prawo do prywatności określił Trybunał Sprawiedliwości w wyroku w sprawie C-178/22[18], którą rozpatrywał analizując przepisy karne, a także możliwość ingerencji w prawo do prywatności w związku podejrzeniem popełnienia przestępstwa zagrożonego określoną sankcją. W tym wyroku Trybunał orzekł, że art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP należy interpretować w ten sposób, że nie stoi on na przeszkodzie przepisowi krajowemu zobowiązującemu sąd krajowy orzekający w ramach uprzedniej kontroli dokonywanej po przedstawieniu przez właściwy organ krajowy w ramach karnego postępowania przygotowawczego uzasadnionego **wniosku o dostęp do zbioru danych o ruchu lub danych o lokalizacji mogących pozwolić na wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego użytkownika środka łączności elektronicznej, które to dane są zatrzymywane przez dostawców usług łączności elektronicznej, do wydania zgody na udzielenie tego dostępu, jeżeli zażądano go do celów dochodzenia przestępstw zagrożonych w prawie krajowym karą pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata**, z zastrzeżeniem, że **istnieją wystarczające przesłanki popełnienia takich przestępstw i że dane te są istotne dla ustalenia okoliczności faktycznych, pod warunkiem jednak, iż ów sąd jest**

[18] Wyrok TS z dnia 30.04.2024 r., w sprawie C-178/22, Procura della Repubblica presso il Tribunale di Bolzano, ECLI:EU:C:2024:371.

uprawniony do odmowy udzielenia wspomnianego dostępu, jeżeli jest on wnioskowany w ramach dochodzenia dotyczącego przestępstwa, które w sposób oczywisty jest przestępstwem mniejszej wagi w świetle warunków społecznych panujących w danym państwie.

2. Standard międzynarodowy

W przywołanym wcześniej stanowisku Rzecznika Praw Obywatelskich szeroko omawiany był także standard międzynarodowy związany z możliwością zatrzymywania danych telekomunikacyjnych, dopuszczalnej ingerencji w prawo do prywatności, a także naruszania tajemnicy korespondencji[19]. Niezależnie jednak od wcześniejszych orzeczeń Europejskiego Trybunału Praw Człowieka (ETPC), na szczególną uwagę zasługuje ostatnie rozstrzygnięcie w sprawach połączonych Pietrzak p. Polsce oraz Bychawska-Siniarska i in. p. Polsce[20].

Rozstrzygnięcie ETPC obejmowało skargi łącznie pięciu obywateli polskich na polskie ustawodawstwo zezwalające na system tajnej inwigilacji obejmujący zarówno kontrolę operacyjną, jak też zatrzymywanie telekomunikacyjnych, pocztowych i cyfrowych danych. ETPC w wyroku orzekł jednogłośnie, że doszło do trzech naruszeń art. 8 Konwencji (prawa do poszanowania życia prywatnego, prawa do poszanowania życia rodzinnego, a także prawa do poszanowania korespondencji). ETPC stwierdził, że ustawodawstwo krajowe w przedmiotowej sprawie nie zapewniło wystarczających zabezpieczeń przed nadmierną ingerencją w życie prywatne jednostek, a brak tych

[19] Wyroki ETPC: 1) z 02.08.1984 r. w sprawie Malone przeciwko Zjednoczonemu Królestwu, skarga nr 8691/79; 2) z 24.04.1990 r. w sprawie Kruslin przeciwko Francji, skarga nr 11801/85 oraz w sprawie Huvig przeciwko Francji, skarga nr 11105/84; 3) z 29.06.2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; 4) z 10.02.2009 r. w sprawie Iordachi i inni przeciwko Mołdawii, skarga nr 25198/02; 5) z 02.09.2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05; 6) z 04.12.2015 r. w sprawie Zakharov przeciwko Rosji, skarga nr 47413/06; 7) z 12.01.2016 r. w sprawie Szabó i Vissy przeciwko Węgrom, skarga nr 37138/14.

[20] Wyrok ETPC z 28.05.2024 r. w sprawach połączonych: Pietrzak przeciwko Polsce, skarga nr 72038/17 oraz w sprawie Bychawska-Siniarska i in. przeciwko Polsce, skarga nr 25237/18.

gwarancji nie został także odpowiednio zrównoważony przez mechanizm kontroli sądowej.

W szczególności, mając na uwadze zakres uchwalonej ustawy – Prawo komunikacji elektronicznej, ETPC uznał, że przepisy krajowe, na podstawie których dostawcy usług i technologii informacyjno-komunikacyjnych (ang. *information and communication technologies*, ICT) zobowiązani byli do zatrzymywania danych komunikacyjnych w sposób ogólny do ewentualnego wykorzystania w przyszłości przez odpowiednie organy krajowe, są niewystarczające do tego, by móc stwierdzić, że ingerencja w prawo skarżących do poszanowania ich życia prywatnego była ograniczona do tego, co konieczne w demokratycznym społeczeństwie.

Należy także podkreślić, iż w tej sprawie ETPC uznał za właściwe zbadanie polskiego ustawodawstwa. Uznał bowiem, że skarżący mogli twierdzić, iż są ofiarami naruszenia Konwencji, chociaż nie mogli argumentować na poparcie swoich wniosków, że zostali poddani konkretnemu środkowi inwigilacji. Z tych samych także powodów ETPC uznał, że samo istnienie zaskarżonych przepisów, w tym w szczególności przepisów dotyczących zatrzymywania danych telekomunikacyjny w sposób ogólny, nieukierunkowany, przez okres 12 miesięcy, stanowiło ingerencję w prawa skarżących na mocy art. 8 Konwencji.

W ocenie Rzecznika Praw Obywatelskich powyższe rozstrzygnięcie ETPC ma fundamentalne znaczenie dla dalszych prac nad ustawą PKE i nie może zostać przez ustawodawcę zlekceważone.

III. Uwagi szczegółowe

1. Ogólne i nieukierunkowane zatrzymywanie danych telekomunikacyjnych - zbyt szeroki zakres zbierania danych

Mając na uwadze przedstawione powyżej argumenty wynikające z obowiązującego standardu międzynarodowego, Rzecznik Praw Obywatelskich

krytycznie odnosi się do faktu, że w rządowym projekcie ustawy PKE (druk nr 423), a także w uchwalonej przez Sejm w dniu 12 lipca 2024 r. ustawie, **przepis dotyczący retencji danych telekomunikacyjnych (art. 47) powiela dotychczasowe rozwiązania tak szeroko komentowane i krytykowane jako niespełniające standardów konstytucyjnych, międzynarodowych i europejskich**. Przedsiębiorcy telekomunikacyjni zostaną bowiem zobowiązani – w myśl przywołanego powyżej przepisu – do zbierania danych, o których mowa w art. 49 ustawy, a mianowicie danych dotyczących publicznie dostępnych usług telekomunikacyjnych niezbędnych do:

1) jednoznacznego zidentyfikowania zakończenia sieci, telekomunikacyjnego 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

- przy czym szczegółowy katalog tych danych ma zostać określony w akcie wykonawczym do uchwalonej ustawy (por. kolejny punkt niniejszej opinii).

Jak wynika z materiału informacyjnego załączonego przez Radę Ministrów do projektu ustawy[21], danymi niezbędnymi do ustalenia w stacjonarnej publicznej sieci telekomunikacyjnej:

1) zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, są:
   a) numer zakończenia stacjonarnej publicznej sieci telekomunikacyjnej, z

[21] https://legislacja.rcl.gov.pl/projekt/12382350/katalog/13040650#13040650 (dostęp 15.07.2024).

którego inicjowane jest połączenie,

b) imię i nazwisko albo nazwa oraz adres abonenta, któremu przydzielono numer określony w lit. a;

2) zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie, są:

a) numer zakończenia publicznej sieci telekomunikacyjnej użytkownika końcowego, do którego jest kierowane połączenie,

b) imię i nazwisko albo nazwa oraz adres użytkownika końcowego, do którego jest kierowane połączenie;

c) daty i godziny połączenia oraz czasu jego trwania są:

d) data i godzina nieudanej próby połączenia lub zestawienia i zakończenia połączenia, zgodnie z czasem lokalnym,

e) czas trwania połączenia z dokładnością do 1 sekundy;

f) rodzaju połączenia jest określenie wykorzystanej usługi;

3) lokalizacji telekomunikacyjnego urządzenia końcowego są:

a) adres lokalizacji telekomunikacyjnego urządzenia końcowego, z którego inicjowano połączenie,

b) adres lokalizacji telekomunikacyjnego urządzenia końcowego, do którego jest kierowane połączenie.

Ponadto danymi niezbędnymi do ustalenia w ruchomej publicznej sieci telekomunikacyjnej:

1) zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, są:

a) numer MSISDN użytkownika końcowego, inicjującego połączenie,

b) imię i nazwisko albo nazwa oraz adres użytkownika końcowego, inicjującego połączenie, jeżeli udostępnił te dane,

c) numer IMSI użytkownika końcowego, inicjującego połączenie,

d) pierwsze 14 cyfr numeru IMEI albo numer ESN telekomunikacyjnego

urządzenia końcowego, inicjującego połączenie,

e) data i godzina pierwszego zalogowania telekomunikacyjnego urządzenia końcowego do ruchomej publicznej sieci telekomunikacyjnej, zgodnie z czasem lokalnym, oraz współrzędne geograficzne lokalizacji stacji BTS, poprzez którą dokonano tego zalogowania

- w przypadku użytkownika usługi przedpłaconej;

2) zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie, są:

a) numer MSISDN użytkownika końcowego, do którego kierowane jest połączenie,

b) imię i nazwisko albo nazwa oraz adres użytkownika końcowego, do którego jest kierowane połączenie, jeżeli udostępnił te dane,

c) numer IMSI użytkownika końcowego, do którego jest kierowane połączenie,

d) pierwsze 14 cyfr numeru IMEI albo numer ESN telekomunikacyjnego urządzenia końcowego, do którego kierowane jest połączenie,

e) data i godzina pierwszego zalogowania telekomunikacyjnego urządzenia końcowego do ruchomej publicznej sieci telekomunikacyjnej, zgodnie z czasem lokalnym, oraz współrzędne geograficzne lokalizacji stacji BTS, poprzez którą dokonano tego zalogowania

- w przypadku użytkownika usługi przedpłaconej;

3) daty i godziny połączenia oraz czasu jego trwania są:

a) data i godzina nieudanej próby połączenia lub zestawienia i zakończenia połączenia zgodnie z czasem lokalnym,

b) czas trwania połączenia z dokładnością do 1 sekundy;

4) rodzaju połączenia jest określenie wykorzystanej usługi;

5) lokalizacji telekomunikacyjnego urządzenia końcowego, z którego inicjowano połączenie, są:

a) w przypadku telekomunikacyjnego urządzenia końcowego znajdującego się na terytorium Rzeczpospolitej Polskiej:

aa) w czasie inicjowania połączenia identyfikator anteny stacji BTS,

ab) w czasie, przez który zatrzymywane są dane odnośnie połączenia:

- współrzędne geograficzne stacji BTS, w obszarze której znajdowało się telekomunikacyjne urządzenie końcowe,
- azymut, wiązkę i zasięg roboczy anteny stacji BTS,

b) w przypadku telekomunikacyjnego urządzenia końcowego, znajdującego się poza granicami Rzeczypospolitej Polskiej - identyfikator MCC i identyfikator sieci MNC, w której zainicjowano połączenie;

6) lokalizacji telekomunikacyjnego urządzenia końcowego, do którego było kierowane połączenie, są:

a) w przypadku telekomunikacyjnego urządzenia końcowego znajdującego się na terytorium Rzeczypospolitej Polskiej:

aa) w czasie rozpoczęcia odbioru połączenia identyfikator anteny stacji BTS,

ab) w czasie, przez który zatrzymywane są dane odnośnie połączenia:

- współrzędne geograficzne stacji BTS, w obszarze której znajdowało się telekomunikacyjne urządzenie końcowe,
- azymut, wiązkę i zasięg roboczy anteny stacji BTS,

b) w przypadku telekomunikacyjnego urządzenia końcowego znajdującego się poza granicami kraju - identyfikator MCC i identyfikator sieci MNC, do której zostało skierowane połączenie.

Danymi zaś niezbędnymi w przypadku usługi dostępu do Internetu, usługi poczty elektronicznej i usługi telefonii internetowej:

1) do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, są:

a) identyfikator użytkownika,

b) numer przydzielony użytkownikowi końcowemu, korzystającemu z dostępu dial-up,

c) identyfikator użytkownika i numer przydzielony użytkownikowi końcowemu inicjującemu połączenie kierowane do publicznej sieci telekomunikacyjnej,

d) adres IP,

e) imię i nazwisko albo nazwa oraz adres użytkownika końcowego, któremu w czasie połączenia przypisano adres IP, a także identyfikator użytkownika lub przydzielony mu numer w telefonii internetowej,

f) identyfikator zakończenia sieci, w którym użytkownik końcowy uzyskał dostęp do Internetu, w szczególności identyfikator cyfrowej linii abonenckiej DSL (Digital Subscriber Line), numer wykorzystywanego portu sieciowego lub adres MAC urządzenia końcowego inicjującego połączenie;

2) do ustalenia daty i godziny połączenia oraz czasu jego trwania są:

a) data i godzina każdorazowego połączenia i rozłączenia z Internetem, zgodnie z czasem lokalnym, wraz z przydzielonymi dynamicznie lub statycznie adresami IP wykorzystywanymi w czasie trwania połączenia oraz identyfikatorem użytkownika,

b) data i godzina zalogowania i wylogowania z usługi poczty elektronicznej i telefonii internetowej, zgodnie z czasem lokalnym.

Danymi niezbędnymi w przypadku usługi poczty elektronicznej i usługi telefonii internetowej do ustalenia:

1) zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie, są:

a) numer przydzielony użytkownikowi końcowemu, do którego jest kierowane połączenie w telefonii internetowej,

b) imię i nazwisko albo nazwa oraz adres zarejestrowanego użytkownika końcowego usługi poczty elektronicznej lub usługi telefonii internetowej, do którego jest kierowane połączenie, oraz identyfikator tego użytkownika;

2) rodzaju połączenia jest określenie wykorzystanej usługi, w tym numer wykorzystanego portu sieciowego.

W świetle powyższego nie ma wątpliwości, że katalog danych zbieranych o użytkownikach jest niezwykle szeroki, co budzi uzasadnione wątpliwości Rzecznika Praw Obywatelskich w zakresie konieczności ich zbierania tych danych w demokratycznym państwie prawa, a także ich adekwatności do wyznaczonego celu. Brak zasadności dla szczegółowego określenia wskazanych powyżej danych w akcie wykonawczym zostanie omówiony w dalszej części niniejszej opinii.

Analizując brzmienie art. 47 PKE należy zaznaczyć, że przeanalizowane orzecznictwo TSUE wskazuje na to, że **przepisy przewidujące prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, są sprzeczne z prawem unijnym.** W ścisłym poszanowaniu zasady proporcjonalności, w celu walki z poważną przestępczością, można przewidzieć uogólnione i niezróżnicowane zatrzymywanie adresów IP. Ustawodawca jednak winien w takiej sytuacji badać zarówno wagę ingerencji, którą jest ograniczenie praw i wolności, a także sprawdzać, czy znaczenie celu ogólnego, do którego zmierza to ograniczenie, pozostaje w relacji do tej wagi. **Przestępczości, nawet szczególnie poważnej, nie można natomiast utożsamiać z zagrożeniem bezpieczeństwa narodowego, gdyż takie podejście mogłoby wprowadzić kategorię pośrednią między bezpieczeństwem narodowym a bezpieczeństwem publicznym.**

Przepis przewidujący możliwość zbierania danych winien uwzględniać dorobek orzeczniczy TSUE. Rzecznik Praw Obywatelskich podziela w tym względzie stanowisko

Rzecznika Generalnego, który wielokrotnie w swoich opiniach poprzedzających wydanie wyroków retencyjnych podkreślał, że **stworzenie regulacji krajowych zgodnych z dyrektywą 2002/58/WE, a także uwzględniających tworzony na przestrzeni ponad dekady sposób jej interpretacji, wynikający z orzecznictwa TSUE, jest trudnym wyzwaniem dla krajowego ustawodawcy**. Konieczne jest bowiem uwzględnienie wszystkich możliwych wariantów wskazywanych dotychczas przez TSUE, a także okoliczności, w jakich dopuszczalne są określone ingerencje. Jednakże w każdym wypadku **pozostawienie wariantu, w którym powielone jest uogólnione i nieukierunkowane zatrzymywanie danych, jest sprzeczne z przywołanymi powyżej rozstrzygnięciami TSUE**. Ponadto, warto zaznaczyć, że także Komisja Wenecka w swojej opinii z 2016 r. zaleciła, by **pozyskiwanie najważniejszych danych telekomunikacyjnych i internetowych ograniczono do najgroźniejszych sytuacji, a także, aby skrócić czas przechowywania danych oraz zadbać o nienaruszanie tajemnicy adwokackiej**[22].

Ponadto z brzmienia uzasadnienia projektu ustawy wynika, że omawiane przepisy były projektowane – w szczególności w zakresie ustalenia jednolitych struktur udostępniania danych retencyjnych w celu znacznego przyśpieszenia czynności operacyjnych i procesowych – na podstawie dezyderatu nr 7 Komisji do spraw Służb Specjalnych nr KSS/VIII/Z-819/2018 z dnia 28 października 2018 r. dotyczącego ujednolicenia formatów danych telekomunikacyjnych i bankowych pozyskiwanych przez służby i organy ścigania. **W ocenie Rzecznika Praw Obywatelskich, wymagana jest zatem – zwłaszcza w kontekście późniejszych wypowiedzi TSUE – ponowna analiza mająca na celu wypracowanie standardów i przepisów uwzględniających jego późniejsze orzecznictwo.**

2. Upoważnienie do wydania aktów wykonawczych

[22] Poland - Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016), CDL-AD(2016)012-e (https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD%282016%29012-e, dostęp 07.07.2024).

Przepis art. 49 ust. 2 PKE zawiera upoważnienie do wydania aktu wykonawczego, w którym ma być określony szczegółowy zakres zatrzymywanych danych. W tym kontekście trzeba podkreślić, że w swoim orzecznictwie Trybunał Konstytucyjny konsekwentnie wskazywał na niezgodność takich delegacji z Konstytucją RP przez to, że naruszają wymaganie ustawowej formy dla ograniczeń prawa do prywatności i autonomii informacyjnej jednostki[23]. Zgodnie bowiem z art. 51 Konstytucji RP, każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Nikt jednocześnie nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

Prywatność człowieka stanowi wolność konstytucyjnie chronioną ze wszystkimi wynikającymi z tego konsekwencjami. **Przede wszystkim oznacza to swobodę działania jednostek w ramach wolności, tak długo, aż ustawa (oraz wykonujący ją akt rangi podustawowej), nie określi jej granic.** Ustawodawca wprowadzając ograniczenia konstytucyjnych wolności i praw, w tym przypadku prawa do prywatności i autonomii informacyjnej, musi spełniać przede wszystkim warunki wynikające z art. 31 ust. 3 Konstytucji. Jednym z nich jest ustawowa forma ograniczenia, czego uchwalona ustawa nie uwzględnia we wskazanym powyżej zakresie.

3. Uwagi zgłoszone przez Prezesa Urzędu Ochrony Danych Osobowych

Należy także wskazać, że uwagi zgłaszane przez Prezesa Urzędu Ochrony Danych Osobowych (UODO) na etapie rządowego procesu legislacyjnego nie zostały w całości uwzględnione. Prezes UODO podnosił kwestię uogólnionej retencji danych telekomunikacyjnych i zatrzymywania ich na okres 12 miesięcy przewidzianych w art. 47 projektu.

Rzecznik Praw Obywatelskich podziela także pogląd Prezesa UODO zaprezentowany w przekazywanych do projektu ustawy PKE uwagach, zgodnie z którym

[23] Wyrok TK z 18.12.2014 r., sygn. akt. K 33/13.

stosowany obecnie model bezwarunkowego gromadzenia danych o wszystkich użytkownikach nie zapewnia stosowania wynikających z przepisów rozporządzenia 2016/679 zasad dotyczących przetwarzania danych osobowych:

1) zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a),
2) zasady ograniczenia celu (art. 5 ust. 1 lit. b),
3) zasady minimalizacji danych (art. 5 ust. 1 lit. c),
4) zasady ograniczenia przechowywania (art. 5 ust. 1 lit. e)

- jak również wynikającej z art. 51 ust. 2 Konstytucji RP zasady ograniczenia gromadzenia informacji o obywatelach przez władze publiczne.

4. Konkluzje

W ocenie Rzecznika Praw Obywatelskich uchwalone przepisy ustawy PKE winny zostać zmienione we wskazanym zakresie, gdyż zaproponowany model bezwarunkowego gromadzenia danych o wszystkich użytkownikach usług telekomunikacyjnych budzi wątpliwości co do zgodności z Konstytucją RP, Europejską Konwencją Praw Człowieka oraz Kartą Praw Podstawowych Unii Europejskiej.