Zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru

Przyjęte 10 listopada 2020 r.

Spis treści

Europejska Rada Ochrony Danych (EROD)

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady 2016/679/UE z dnia 27 kwietnia 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 (zwanego dalej „RODO")[1],

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[2],

uwzględniając art.12 i 22 swojego regulaminu wewnętrznego,

uwzględniając dokument roboczy Grupy Roboczej Art. 29 w sprawie uzasadnienia ingerencji w podstawowe prawa do prywatności i ochrony danych poprzez środki nadzoru przy przekazywaniu danych osobowych (niezbędne gwarancje europejskie, zwane dalej „PGE"), WP237,

PRZYJĘŁA NASTĘPUJĄCE ZALECENIA

1. WPROWADZENIE

1. W następstwie wyroku w sprawie Schrems I organy ochrony danych UE, zgromadzone w Grupie Roboczej Art. 29, bazując na orzecznictwie, określiły niezbędne gwarancje europejskie, których należy przestrzegać, aby zagwarantować, że ograniczenia prawa do prywatności i ochrony danych osobowych przez środki nadzoru przy przekazywaniu danych osobowych, nie wykraczają poza to, co jest niezbędne i proporcjonalne w społeczeństwie demokratycznym.

2. EROD pragnie podkreślić, że niezbędne gwarancje europejskie oparte są na orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „TSUE") w odniesieniu do art. 7, 8, 47 i 52 Karty praw podstawowych UE (zwanej dalej „Kartą") oraz, w zależności od przypadku, w orzecznictwie Europejskiego Trybunału Praw Człowieka (zwanego dalej „ETPC") w odniesieniu do art. 8 europejskiej konwencji praw człowieka (zwanej dalej: „EKPC"), w którym poruszano kwestię nadzoru w państwach będących stronami EKPC[3].

[1] Niniejszy dokument nie odnosi się do przypadków przekazywania lub dalszego przekazywania, objętych zakresem dyrektywy (UE) 2016/680.

[2] Odniesienia do „państw członkowskich" w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".

[3] W niniejszych zaleceniach termin „prawa podstawowe" pochodzi z Karty praw podstawowych UE. Obejmuje on jednak również „prawa człowieka", zawarte w europejskiej konwencji praw człowieka.

3. Aktualizacja niniejszego dokumentu ma na celu dalszy rozwój niezbędnych gwarancji europejskich, które pierwotnie opracowano w odpowiedzi na wyrok w sprawie Schrems I[4], w celu uwzględnienia wyjaśnień TSUE (i ETPC) od czasu jego pierwszej publikacji, w szczególności w przełomowym wyroku w sprawie Schrems II[5].

4. W swoim wyroku w sprawie Schrems II TSUE stwierdził, że przeprowadzone w świetle art. 7, 8 i 47 Karty badanie decyzji Komisji 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym mającym siedzibę w państwach trzecich nie doprowadziło do żadnych ustaleń, które mogłyby mieć wpływ na ważność tej decyzji, jakkolwiek unieważniło decyzję w sprawie Tarczy Prywatności. TSUE uznał, że decyzja w sprawie Tarczy Prywatności jest niezgodna z art. 45 ust. 1 RODO w świetle z art. 7, 8 i 47 Karty. Wyrok może zatem posłużyć za przykład sytuacji, gdy środki nadzoru w państwie trzecim (w tym przypadku był to art. 702 FISA i rozporządzenie wykonawcze nr 12 333 w Stanach Zjednoczonych) nie są dostatecznie ograniczone, zaś osoby, których dane dotyczą, nie mają dostępu do skutecznych środków ochrony prawnej w celu wykonania praw, zgodnie z wymogami prawa UE, co uniemożliwia uznanie stopnia ochrony w państwie trzecim za „merytorycznie równoważny" temu gwarantowanemu w Unii Europejskiej w rozumieniu z art. 45 ust. 1 RODO.

5. Powody unieważnienia decyzji w sprawie Tarczy Prywatności znajdują również zastosowanie do innych narzędzi przekazywania[6]. Jakkolwiek Trybunał dokonał wykładni art. 46 ust. 1 RODO w kontekście ważności standardowych klauzul umownych, to taka wykładnia ma zastosowanie do wszelkich przypadków przekazywania do państw trzecich w oparciu o jakiekolwiek narzędzie, o którym mowa w art. 46 RODO.[7]

6. Ostatecznie to do TSUE należy ocena, czy ingerencja w prawo podstawowe może być uzasadniona. Jednak w przypadku braku takiego orzeczenia i przy zastosowaniu obowiązującego orzecznictwa organy ochrony danych są zobowiązane do oceny indywidualnych przypadków, albo z urzędu albo w następstwie skargi, oraz do skierowania sprawy do sądu krajowego, jeżeli podejrzewają one, że przekazanie nie jest zgodne z art. 45, w przypadku decyzji stwierdzającej odpowiedni stopień ochrony, albo do zawieszenia lub zakazania przekazania, jeżeli uznają, że nie można zastosować art. 46 RODO, a ochrona przekazywanych danych wymagana na mocy prawa UE nie może zostać zapewniona za pomocą innych środków.

7. Celem zaktualizowanych niezbędnych gwarancji europejskich jest zapewnienie elementów pozwalających na zbadanie, czy środki nadzoru umożliwiające organom publicznym w państwie trzecim, tj. agencjom odpowiedzialnym za bezpieczeństwo narodowe lub organom ścigania, dostęp do danych osobowych można uznać za uzasadnioną ingerencję, czy też nie.

[4] Wyrok TSUE z dnia 6 października 2015 r., Maximillian Schrems przeciwko Data Protection Commissioner, sprawa C-362/14, UE:C:2015:650 (zwana dalej: „Schrems I").

[5] Wyrok TSUE z dnia 16 lipca 2020 r., Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi, sprawa C-311/18, ECLI:UE:C:2020:559 (zwana dalej: „Schrems II").

[6] Zob. Schrems II, pkt 105.

[7] Zob. Schrems II, pkt 92.

8. Niezbędne gwarancje europejskie stanowią bowiem część oceny, którą należy przeprowadzić w celu ustalenia, czy państwo trzecie zapewnia stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE, ale same w sobie nie mają na celu określenia wszystkich elementów niezbędnych do uznania, że dane państwo trzecie zapewnia taki stopień ochrony zgodnie z art. 45 RODO. Nie wskazują one również wszystkich elementów, które mogą być konieczne do rozważenia przy ocenie, czy system prawny państwa trzeciego uniemożliwia podmiotowi przekazującemu i odbierającemu dane zapewnienie odpowiednich zabezpieczeń zgodnie z art. 46 RODO.

9. W związku z tym elementy przedstawione w niniejszym dokumencie powinny być postrzegane jako niezbędne gwarancje, jakie należy znaleźć w państwie trzecim w trakcie oceny ingerencji w prawa do prywatności i ochrony danych, związanej ze środkami nadzoru państwa trzeciego, a nie jako wykaz elementów wykazujących, że system prawny państwa trzeciego jako całość zapewnia zasadniczo równoważny poziom ochrony.

10. Artykuł 6 ust. 3 Traktatu o Unii Europejskiej stanowi, że prawa podstawowe zapisane w EKPC są ogólnymi zasadami prawa UE. Jednakże, jak przypomina TSUE w swoim orzecznictwie, to ostatnie nie stanowi, dopóki Unia Europejska nie przystąpi do niego, instrumentu prawnego, który został formalnie włączony do prawa UE.[8] Stopień ochrony praw podstawowych wymagany na mocy art. 46 ust. 1 RODO należy zatem określić na podstawie przepisów tego rozporządzenia w świetle praw podstawowych zapisanych w Karcie. Mając na uwadze powyższe, zgodnie z art. 52 ust. 3 Karty, prawa w niej zawarte, odpowiadające prawom zagwarantowanym przez EKPC, mają mieć takie samo znaczenie i taki sam zakres jak prawa określone w tej konwencji, w związku z czym, jak przypomniał TSUE, należy uwzględnić orzecznictwo ETPC dotyczące praw, które są również przewidziane w Karcie praw podstawowych Unii Europejskiej, jako minimalny próg ochrony w celu interpretacji odpowiednich praw w Karcie[9]. Jednakże zgodnie z ostatnim zdaniem art. 52 ust. 3 Karty „[n]iniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę".

11. W związku z tym istota niezbędnych gwarancji nadal będzie częściowo oparta na orzecznictwie ETPC, w zakresie, w jakim Karta zgodnie z wykładnią TSUE nie przewiduje wyższego stopnia ochrony, który nakazuje inne wymogi niż orzecznictwo ETPC.

12. Niniejszy dokument wyjaśnia kontekst i szczegóły czterech niezbędnych gwarancji europejskich.

2. INGERENCJE W PRAWA PODSTAWOWE

13. Podstawowe prawa do poszanowania życia prywatnego i rodzinnego, w tym komunikacji, oraz do ochrony danych osobowych są określone w art. 7 i 8 Karty i mają zastosowanie do wszystkich osób. Ponadto w art. 8 określono warunki zgodności z prawem przetwarzania danych osobowych oraz uznano prawo dostępu do danych i ich sprostowania, a także nałożono wymóg, aby przepisy te podlegały kontroli niezależnego organu.

[8] Zob. Schrems II, pkt 98.

[9] Zob. sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in. (zwane dalej La Quadrature du Net i in.), pkt 124.

14. „[O]peracja polegająca na przekazywaniu danych osobowych z państwa członkowskiego do państwa trzeciego stanowi jako taka przetwarzanie danych osobowych”[10]. W związku z tym art. 7 i art. 8 Karty mają zastosowanie do tej konkretnej operacji, a ochrona przez nie zapewniania obejmuje również przekazywane dane, dlatego też osobom, których dane osobowe są przekazywane do państwa trzeciego, należy zapewnić stopień ochrony zasadniczo odpowiadający stopniowi ochrony zapewnianemu w Unii Europejskiej.[11]

15. Zdaniem TSUE, gdy dochodzi do naruszenia podstawowego prawa do poszanowania życia prywatnego, zapisanego w art. 7 Karty, przez przetwarzanie danych osobowych osoby fizycznej naruszane jest również prawo do ochrony danych, ponieważ takie przetwarzanie wchodzi w zakres stosowania art. 8 Karty i w związku z tym musi koniecznie spełniać wymóg ochrony danych określony w tym artykule.[12]

16. Dlatego też, jeżeli chodzi o ewentualną ingerencję w prawa podstawowe wynikające z prawa UE, obowiązek nałożony na dostawców usług łączności elektronicznej (...) do zatrzymywania danych o ruchu w celu udostępnienia ich, w razie potrzeby, właściwym organom krajowym, budzi wątpliwości co do zgodności z art. 7 i 8 Karty[13.] To samo dotyczy innych rodzajów przetwarzania danych, takich jak przekazywanie danych osobom innym niż użytkownicy lub dostęp do tych danych w celu ich wykorzystania[14], co w związku z tym pociąga za sobą ingerencję w te prawa podstawowe. Ponadto zgodnie z utrwalonym orzecznictwem dostęp do danych przez organ publiczny stanowi dalszą ingerencję.[15]

17. W celu stwierdzenia ingerencji nie ma znaczenia, „czy informacje dotyczące życia prywatnego mają charakter wrażliwy i bez względu na to, czy z powodu tej ingerencji zainteresowane osoby doświadczyły ewentualnych niedogodności”[16]. Trybunał podkreślił również, że to, czy zatrzymane dane zostały następnie wykorzystane, jest bez znaczenia[17].

18. Niemniej jednak prawa ustanowione w art. 7, 8 i 11 Karty nie wydają się stanowić prerogatyw o charakterze absolutnym, lecz należy je rozważać z uwzględnieniem ich funkcji społecznej[18].

19. Karta zawiera test niezbędności (konieczności) i proporcjonalności w celu określenia ograniczeń praw, które chroni. Artykuł 52 ust. 1 Karty określa zakres możliwych ograniczeń w artykułach 7 i 8, stwierdzając, że „Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób”.

[10] TSUE, Schrems II, pkt 83.
[11] TSUE, Schrems II, pkt 96.
[12] TSUE, Schrems II, pkt 170-171.
[13] TSUE, sprawa C-623/17, Privacy International (zwana dalej: Privacy International), pkt 60.
[14] TSUE, Privacy International, pkt 61.
[15] ETPC, Leander, pkt 48; ETPC, Rotaru pkt 46; TSUE, Digital Rights Ireland, pkt 35.
[16] TSUE, Schrems II, pkt 171 wraz z przywołanym orzecznictwem.
[17] TSUE, Schrems II, pkt 171 wraz z przywołanym orzecznictwem.
[18] TSUE, Privacy International, pkt 63.

20. TSUE powtórzył, że uregulowanie UE, pociągające za sobą ingerencję w prawa podstawowe zagwarantowane przez art. 7 i 8 Karty, „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 tych danych przed ryzykiem nadużyć", zwłaszcza gdy dane osobowe są przetwarzane automatycznie oraz „kiedy występuje znaczne ryzyko nieuprawnionego dostępu do tych danych".[19]

21. Zdaniem TSUE ochrona prawa do prywatności wymaga, aby wyjątki od prawa do ochrony danych i ograniczenia tego prawa „musiały być stosowane w zakresie, w jakim jest to absolutnie niezbędne". Ponadto cel leżący w interesie ogólnym należy pogodzić z prawami podstawowymi, których dotyczy dany środek, „dokonując zbilansowanego wyważenia" między takim celem a rozpatrywanymi prawami.[20]

22. W związku z tym dostęp, zatrzymywanie i dalsze wykorzystywanie danych osobowych przez organy publiczne w ramach środków nadzoru nie może wykraczać poza to, co jest ściśle konieczne, oceniane w świetle Karty, w przeciwnym razie „nie może być uważane za uzasadnione w społeczeństwie demokratycznym".[21]

23. Cztery niezbędne gwarancje europejskie, opracowane w następnym rozdziale, mają na celu doprecyzowanie, w jaki sposób oceniać poziom ingerencji w podstawowe prawa do prywatności i ochrony danych w kontekście środków nadzoru stosowanych przez organy publiczne w państwie trzecim przy przekazywaniu danych osobowych oraz jakie wymogi prawne muszą w związku z tym mieć zastosowanie, aby ocenić, czy takie ingerencje byłyby dopuszczalne na mocy Karty.

3. NIEZBĘDNE GWARANCJE EUROPEJSKIE

24. Po przeprowadzeniu analizy orzecznictwa EROD uważa, że mające zastosowanie wymogi prawne w celu uzasadnienia ograniczeń praw do ochrony danych i prywatności uznanych w Karcie można podsumować w czterech niezbędnych gwarancjach europejskich:

A. przetwarzanie powinno być oparte na jasnych, precyzyjnych i dostępnych zasadach;
B. należy wykazać niezbędność i proporcjonalność w odniesieniu do uzasadnionych zamierzonych celów;
C. powinien istnieć mechanizm niezależnej kontroli;
D. skuteczne środki ochrony prawnej muszą być dostępne dla osób fizycznych

25. Gwarancje te opierają się na niezbędnych prawach do prywatności i ochrony danych osobowych, które mają zastosowanie do wszystkich osób, niezależnie od obywatelstwa.

[19] TSUE, Privacy International, pkt 68 wraz z przywołanym orzecznictwem.
[20] TSUE, Privacy International, pkt 68 wraz z przywołanym orzecznictwem.
[21] TSUE, Privacy International, pkt 81.

Gwarancja A - Przetwarzanie powinno opierać się na jasnych, precyzyjnych i dostępnych zasadach

26. Zgodnie z art. 8 ust. 2 Karty dane osobowe powinny być między innymi przetwarzane „w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą”,[22] jak przypomniał TSUE w orzeczeniu w sprawie Schrems II. Ponadto, zgodnie z art. 52 ust. 1 Karty, wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą w UE być przewidziane ustawą. W związku z tym uzasadniona ingerencja musi być zgodna z prawem.

27. Ta podstawa prawna powinna określać jasne i precyzyjne zasady regulujące zakres i stosowanie danego środka oraz nakładające minimalne zabezpieczenia[23]. Ponadto Trybunał przypomniał, że „to uregulowanie musi być prawnie wiążące w prawie krajowym”[24]. W tym względzie TSUE wyjaśnił, że ocena mającego zastosowanie prawa państwa trzeciego powinna koncentrować się na tym, czy osoby fizyczne mogą się na nie powoływać i polegać na nim przed sądem[25]. Trybunał stwierdza zatem, że prawa przyznane osobom, których dane dotyczą, powinny być egzekwowalne przed sądami; jeżeli osobom fizycznym nie zapewnia się praw egzekwowalnych wobec organów publicznych, przyznanego poziomu ochrony nie można uznać za merytorycznie równoważnego temu gwarantowanemu w Karcie, wbrew wymogom ustanowionym w art. 45 ust. 2 lit. a) RODO.[26]

28. Ponadto Trybunał podkreślił, że prawo właściwe musi wskazywać, w jakich okolicznościach i w jakich warunkach można przyjąć środek przewidujący przetwarzanie takich danych[27] (zob. poniżej w sekcji „Gwarancja B” związek między tymi wymogami a zasadami niezbędności i proporcjonalności).

29. TSUE wskazał również, że „wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, że podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa”.[28]

30. Ponadto Europejski Trybunał Praw Człowieka „nie uważa, że nie ma żadnych podstaw do stosowania różnych zasad obejmujących z jednej strony dostępność i przejrzystość przepisów regulujących przechwytywanie konkretnej komunikacji konkretnych osób a z drugiej strony, bardziej ogólne programy inwigilacji”[29]. ETPC wyjaśnił również, że podstawa prawna powinna obejmować co najmniej definicję kategorii osób, które mogą podlegać inwigilacji, ograniczenie czasu trwania środka, procedurę, której należy przestrzegać przy badaniu, wykorzystywaniu i przechowywaniu uzyskanych danych, a także środki ostrożności, jakie należy podjąć przy przekazywaniu danych innym stronom.[30]

---

[22] Zob. Schrems II, pkt 173.

[23] Zob. Schrems II, pkt 175 i 180 oraz opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., pkt 139 wraz z przywołanym orzecznictwem.

[24] Zob. Privacy International, pkt 68 – powinno być również jasne, że we francuskiej wersji wyroku Trybunał posługuje się terminem „réglementation”, które jest szersze niż tylko akty Parlamentu.

[25] Zob. Schrems II, pkt 181; gdzie TSUE odwołuje się do prezydenckiej dyrektywy politycznej nr 28.

[26] Zob. Schrems II, pkt 181.

[27] Zob. Privacy International, pkt 68 w odniesieniu do prawa państw członkowskich.

[28] Zob. Schrems II, pkt 175 wraz z przywołanym orzecznictwem oraz Privacy International, pkt 65.

[29] ETPC, Liberty, pkt 63.

[30] ETPC, Weber i Saravia, pkt 95.

31. Ingerencja musi być również przewidywalna w odniesieniu do jej skutków dla jednostki, aby zapewnić jej odpowiednią i skuteczną ochronę przed arbitralnymi ingerencjami i ryzykiem nadużyć. W związku z tym przetwarzanie danych musi opierać się na precyzyjnej, jasnej, ale również dostępnej (tzn. publicznej) podstawie prawnej[31]. ETPC, odnosząc się do tej kwestii, przypomniał w sprawie Zakharov, że „wzmianka o «przewidywalności» w kontekście przechwytywania komunikatów nie może być taka sama jak w wielu innych dziedzinach". Stwierdził, że w kontekście tajnych środków nadzoru, takich jak przechwytywanie komunikatów, „przewidywalność nie może oznaczać, że dana osoba powinna być w stanie przewidzieć, kiedy organy prawdopodobnie przechwycą jej komunikaty, tak aby mogła odpowiednio dostosować swoje zachowanie". Biorąc jednak pod uwagę, że w tego rodzaju sytuacjach ryzyko arbitralności jest oczywiste „niezbędne jest posiadanie jasnych, szczegółowych zasad przechwytywania rozmów telefonicznych, zwłaszcza że dostępna technologia jest coraz bardziej wyrafinowana. Prawo krajowe musi być wystarczająco jasne, aby dać obywatelom odpowiednią wskazówkę co do okoliczności i warunków, na jakich władze publiczne są uprawnione do stosowania takich środków".[32]

Gwarancja B - Należy wykazać konieczność i proporcjonalność w odniesieniu do zgodnych z prawem zamierzonych celów

32. Zgodnie z pierwszym zdaniem art. 52 ust. 1 Karty wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą szanować istotę tych praw i wolności. Zgodnie z drugim zdaniem art. 52 ust. 1 Karty, w zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób[33].

33. Jeśli chodzi o **zasadę proporcjonalności**, Trybunał orzekł, w odniesieniu do przepisów państw członkowskich, że kwestię, czy ograniczenie prawa do prywatności i ochrony danych może być uzasadnione, należy oceniać z jednej strony badając **wagę ingerencji** spowodowanej takim ograniczeniem[34] oraz z drugiej sprawdzając, czy **znaczenie celu interesu publicznym,** do którego zmierza to ograniczenie, jest proporcjonalne do wagi ingerencji[35].

34. W sprawie La Quadrature du net i in. można zauważyć, że TSUE orzekł w odniesieniu do prawa państwa członkowskiego, a nie prawa państwa trzeciego, że cel polegający na ochronie bezpieczeństwa narodowego może, ze względu na jego znaczenie, uzasadniać środki pociągające za sobą poważniejsze ingerencje w prawa podstawowe niż te, które mogłyby być uzasadnione innymi celami, takimi jak zwalczanie przestępczości. Trybunał uznał jednak, że tak jest, o ile istnieją wystarczająco solidne podstawy do uznania, że dane państwo stoi w obliczu poważnego zagrożenia dla bezpieczeństwa

[31] ETPC, Malone, pkt 65 i 66.

[32] ETPC, Zakharov, pkt 229.

[33] Schrems II, pkt 174.

[34] W tym kontekście Trybunał uznał np., że „ingerencja wynikająca z gromadzenia w czasie rzeczywistym danych umożliwiających lokalizację urządzeń końcowych wydaje się szczególnie poważna, ponieważ dane te zapewniają właściwym organom krajowym środki umożliwiające dokładne i trwałe śledzenie ruchu użytkowników telefonów komórkowych (...)". (La Quadrature du Net i in., pkt 187 wraz z przywołanym orzecznictwem).

[35] La Quadrature du Net i in., pkt 131.

narodowego, które zostało wykazane jako rzeczywiste i aktualne lub możliwe do przewidzenia oraz z zastrzeżeniem spełnienia innych wymogów określonych w art. 52 ust. 1 Karty.[36]

35. W tym względzie zgodnie z utrwalonym orzecznictwem Trybunału odstępstwa od ochrony danych osobowych i jej ograniczenia powinny być stosowane jedynie w zakresie, w jakim jest to bezwzględnie konieczne[37]. W celu spełnienia tego wymogu, oprócz ustanowienia jasnych i precyzyjnych zasad dotyczących zakresu i stosowania danego środka, omawiane przepisy muszą ustanawiać minimalne gwarancje, tak aby osoby, których dane zostały przekazane, dysponowały wystarczającymi gwarancjami skutecznej ochrony ich danych osobowych przed ryzykiem nadużyć. „Powinno ono w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne. Konieczność zaopatrzenia w takie gwarancje jest istotna jeszcze bardziej wówczas, gdy dane osobowe są przetwarzane w sposób zautomatyzowany”.[38]

36. W sprawie Schrems II TSUE podkreślił, że ustawodawstwo państwa trzeciego, które nie wskazuje żadnych ograniczeń przyznanych mu uprawnień do wdrażania programów nadzoru do celów wywiadu zagranicznego, nie może zapewnić stopnia ochrony merytorycznie równoważnego temu gwarantowanemu przez Kartę. Zgodnie z orzecznictwem podstawa prawna umożliwiająca ingerencję w prawa podstawowe musi bowiem, w celu spełnienia wymogów zasady proporcjonalności, sama określać zakres wykonywania danego prawa.[39]

37. Odnosząc się do **zasady niezbędności**, TSUE wyjaśnił, że uregulowanie „umożliwiające generalnie przechowywanie wszelkich danych osobowych wszystkich osób fizycznych, których dane zostały przekazane z Unii Europejskiej (...) bez jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu i bez przewidzenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu władz publicznych do danych oraz na ich późniejsze wykorzystanie do określonych celów, ściśle ograniczonych, które mogą uzasadnić ingerencję, jaką stanowi zarówno dostęp, jak i wykorzystanie tych danych” nie jest zgodne z tą zasadą.[40] W szczególności należy uznać, że przepisy

[36] Pkt 136 i 137. Zob. również sprawę Privacy International, w której Trybunał uznał, że takie zagrożenia można odróżnić ze względu na swój charakter i szczególną wagę od ogólnego ryzyka wystąpienia napięć lub zakłóceń, nawet poważnych, mających wpływ na bezpieczeństwo publiczne. Pkt 75. Na przykład w wyroku La Quadrature du Net i in. Trybunał zauważył, że zautomatyzowana analiza danych o ruchu i lokalizacji obejmująca w sposób ogólny i niezróżnicowany dane osób korzystających z systemów łączności elektronicznej stanowi szczególnie poważną ingerencję, a zatem środek taki może spełniać wymóg proporcjonalności jedynie w sytuacjach, w których dane państwo członkowskie stoi w obliczu poważnego zagrożenia dla bezpieczeństwa narodowego, które zostało wykazane jako rzeczywiste i aktualne lub przewidywalne, oraz, oprócz innych warunków, pod warunkiem że okres zatrzymywania danych jest ograniczony do tego, co jest ściśle konieczne.

[37] Schrems II, pkt 176 wraz z przywołanym orzecznictwem.

[38] Schrems II, pkt 175.

[39] Schrems II, pkt 180.

[40] Schrems I, pkt 93 wraz z przywołanym orzecznictwem. Zob. jednak tym razem w odniesieniu do prawa państwa członkowskiego, a nie prawa państwa trzeciego, Privacy International, pkt 71, w tym cytowane orzecznictwo. W niniejszej sprawie Trybunał stwierdził, że przepisy państwa członkowskiego, które nakładają na dostawców usług łączności elektronicznej obowiązek ujawniania danych o ruchu i danych o lokalizacji agencjom bezpieczeństwa i wywiadu w drodze ogólnego i niezróżnicowanego przekazywania danych, wykraczają poza granice tego, co jest absolutnie niezbędne i nie można ich uznać za uzasadnione w społeczeństwie demokratycznym, zgodnie z wymogami dyrektywy o prywatności i łączności elektronicznej, czytanej w świetle Karty (ust. 81).

umożliwiające organom władzy publicznej ogólny dostęp do treści łączności elektronicznej naruszają istotę prawa podstawowego do poszanowania życia prywatnego, zagwarantowanego w art. 7 Karty.[41]

38. Tym razem jednak przy ocenie prawa państwa członkowskiego, a nie prawa państwa trzeciego, TSUE orzekł w sprawie La Quadrature du Net i in., że „ustawodawstwo nakładające obowiązek zatrzymywania danych osobowych musi zawsze spełniać obiektywne kryteria, które określają związek między zatrzymanymi danymi a zamierzonym celem”[42]. W tym samym kontekście w sprawie Privacy International Trybunał orzekł również, że prawodawca „musi opierać się na obiektywnych kryteriach w celu określenia okoliczności i warunków, na jakich właściwe organy krajowe mają uzyskać dostęp do przedmiotowych danych”.[43]

Gwarancja C - Mechanizm niezależnego nadzoru

39. EROD przypomina, że ingerencja ma miejsce w momencie gromadzenia danych, ale również w momencie uzyskania dostępu do danych przez organ publiczny w celu ich dalszego przetwarzania. ETPC wielokrotnie stwierdzał, że wszelka ingerencja w prawo do prywatności i ochrony danych powinna podlegać skutecznemu, niezależnemu i bezstronnemu systemowi nadzoru, który musi być zapewniony przez sędziego lub inny niezależny organ[44] (np. organ administracyjny lub parlamentarny). Niezależny nadzór nad wdrażaniem środków nadzoru został również uwzględniony przez TSUE w wyroku w sprawie Schrems II.[45]

40. ETPC uściśla, że chociaż uprzednie (sądowe) zezwolenie na stosowanie środków nadzoru jest ważnym zabezpieczeniem przed arbitralnością, należy również wziąć pod uwagę rzeczywiste funkcjonowanie systemu przechwytywania, w tym mechanizmy kontroli i równowagi w zakresie wykonywania władzy, oraz istnienie lub brak faktycznego nadużycia[46]. W sprawie Schrems II TSUE uwzględnił również zakres funkcji nadzorczej mechanizmu nadzoru, który nie obejmował indywidualnych środków nadzoru.[47]

---

[41] Schrems I, pkt 94.

[42] La Quadrature du Net i in., pkt 133. W tym kontekście Trybunał potwierdził, że dyrektywa o prywatności i łączności elektronicznej, czytana w świetle Karty, sprzeciwia się środkom ustawodawczym przewidującym, jako środek zapobiegawczy, ogólne i masowe zatrzymywanie danych o ruchu i danych dotyczących lokalizacji. Trybunał orzekł natomiast, że w sytuacjach poważnego zagrożenia dla bezpieczeństwa narodowego, które zostało wykazane jako rzeczywiste i aktualne lub możliwe do przewidzenia, prawodawca może zezwolić, w celu zapewnienia bezpieczeństwa narodowego, na zastosowanie instrukcji zobowiązującej dostawców usług łączności elektronicznej do przechowywania, w sposób ogólny i niedyskryminujący, danych o ruchu i lokalizacji. Środek taki musi jednak spełniać szczególne warunki. W szczególności nakaz może być wydany jedynie na czas ograniczony do tego, co jest ściśle niezbędne, który może zostać przedłużony w przypadku utrzymywania się tego zagrożenia (pkt 168).

[43] Privacy International, pkt 78 wraz z przywołanym orzecznictwem W sprawie Privacy International, w odniesieniu do dostępu organu do danych osobowych przekazanych na mocy prawa państwa członkowskiego, Trybunał orzekł, że „ogólny dostęp do wszystkich zatrzymanych danych, niezależnie od jakiegokolwiek związku, nawet pośredniego, z realizowanym celem nie może być uważany za ograniczony do tego, co absolutnie niezbędne” (pkt 77 -78).

[44] ETPC, Klass, pkt 17 i 51.

[45] Schrems II, pkt 179 i 183

[46] ETPC, Big Brother Watch w postępowaniu apelacyjnym, pkt 319-320.

[47] Schrems II, pkt 179.

41. W odniesieniu do prawa państw członkowskich TSUE zidentyfikował szereg środków, które są zgodne z prawem UE tylko wtedy, gdy podlegają skutecznej kontroli przeprowadzanej przez sąd lub niezależny organ administracyjny, którego decyzja jest wiążąca. Celem tej kontroli jest sprawdzenie, czy istnieje sytuacja uzasadniająca dany środek oraz czy przestrzegane są warunki i gwarancje, które należy ustanowić[48]. W przypadku gromadzenia danych o ruchu i lokalizacji w czasie rzeczywistym przegląd powinien umożliwić sprawdzenie *ex ante*, między innymi, czy jest to dozwolone wyłącznie w granicach tego, co jest absolutnie niezbędne. W przypadku należycie uzasadnionej pilnej potrzeby środki mogą być zastosowane bez takiej uprzedniej kontroli; Trybunał nadal jednak wymaga, aby kolejna kontrola została przeprowadzona w krótkim czasie.[49]

42. Jeżeli chodzi o niezależność mechanizmów kontroli w odniesieniu do środków nadzoru, można by uwzględnić ustalenia TSUE dotyczące niezależności organu w kontekście środków ochrony prawnej (zob. poniżej w ramach gwarancji D). Dodatkowe elementy znaleźć można w orzecznictwie ETPC. Trybunał ten opowiedział się za tym, aby to sędzia był odpowiedzialny za prowadzenie nadzoru. Nie jest jednak wykluczone, że inny organ może być odpowiedzialny „o ile jest wystarczająco niezależny od władzy wykonawczej”[50] oraz „władz prowadzących nadzór, a także posiada wystarczające uprawnienia i kompetencje do sprawowania skutecznej i ciągłej kontroli”.[51] ETPC dodał, że w ocenie niezależności należy wziąć pod uwagę „sposób powoływania i status prawny członków organu sprawującego nadzór”.[52] Obejmuje to „osoby uprawnione do sprawowania urzędu sądowego, mianowane przez parlament lub przez premiera. Natomiast minister spraw wewnętrznych, który nie tylko jest osobą z nominacji politycznej, ale i członkiem władzy wykonawczej, bezpośrednio zaangażowanym we wdrażanie szczególnych środków nadzoru, został uznany za niewystarczająco niezależnego”[53]. ETPC „zauważa również, że istotne jest, aby organ nadzorczy miał dostęp do wszystkich istotnych dokumentów, w tym do materiałów niejawnych”[54]. Ponadto ETPC bierze pod uwagę, „czy działalność organu nadzorczego jest otwarta na publiczną kontrolę”.[55]

Gwarancja D - Skuteczne środki ochrony prawnej muszą być dostępne dla osób fizycznych

43. Ostatnia niezbędna gwarancja europejska związana jest z prawami osób fizycznych do dochodzenia roszczeń. Osoba musi dysponować skutecznym środkiem prawnym w celu wyegzekwowania swoich praw, jeżeli uzna, że nie są one przestrzegane lub nie były przestrzegane. TSUE wyjaśnił w wyroku w Schrems I, że „uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 Karty. Artykuł 47 akapit pierwszy Karty stanowi bowiem, że każdy, kogo prawa i

[48] TSUE, La Quadrature du Net i in., pkt 168 i 189.

[49] TSUE, La Quadrature du Net i in., pkt 189.

[50] ETPC, Zakharov, pkt 258, Iordachi i in. przeciwko Mołdawii, pkt 40 i 51, a także Dumitru Popescu przeciwko Rumunii, pkt70-73.

[51] ETPC, Klass, pkt 56 i Big Brother Watch w postępowaniu apelacyjnym, pkt 318.

[52] ETPC, Zakharov, pkt 278.

[53] ETPC, Zakharov, pkt 278.

[54] ETPC, Zakharov, pkt 281.

[55] ETPC, Zakharov, pkt 283.

wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w tym artykule".[56]

44. Oceniając uregulowanie państwa członkowskiego, zezwalające na gromadzenie w czasie rzeczywistym danych o ruchu i danych o lokalizacji, Trybunał uznał, że powiadomienie jest konieczne, „aby umożliwić osobom, których dotyczy dany środek, skorzystanie z praw przysługujących im na mocy art. 7 i 8 Karty, tj. zażądanie dostępu do ich danych osobowych, które były przedmiotem tych środków, a także w stosownych przypadkach ich sprostowania lub usunięcia, oraz prawa do skutecznego środka prawnego przed sądem, zgodnie z art. 47 akapit pierwszy Karty".[57] Trybunał uznał jednak również, że powiadomienie osób, których dane zostały zebrane lub poddane analizie, musi nastąpić tylko w takim zakresie i w takim czasie, w jakim powiadomienie nie zagraża już zadaniom, za które organy te są odpowiedzialne[58].

45. Również dla ETPC kwestia skutecznego środka ochrony prawnej jest nierozłącznie związana z powiadomieniem danej osoby o środku nadzoru po tym, jak nadzór został zakończony. W szczególności Trybunał stwierdził, że „osoba zainteresowana ma co do zasady niewielkie możliwości odwołania się do sądu, chyba że osoba ta zostanie powiadomiona o środkach podjętych bez jej wiedzy i tym samym może zakwestionować ich zgodność z prawem wstecznie lub ewentualnie, osoba, która podejrzewa, że jej komunikaty są lub zostały przechwycone, może zwrócić się do sądów, tak że jurysdykcja sądów nie zależy od powiadomienia osoby podlegającej przechwytywaniu o przechwyceniu jej wiadomości"[59]. ETPC uznał zatem, że w niektórych przypadkach powiadomienie może nie mieć miejsca, należy jednak zapewnić skuteczny środek ochrony prawnej. W niniejszej sprawie Trybunał wyjaśnił, na przykład w sprawie Kennedy, że sąd oferuje wystarczające możliwości dochodzenia roszczeń, jeżeli spełnia szereg kryteriów, tj. niezależny i bezstronny organ, który przyjął własny regulamin postępowania, składający się z członków, którzy muszą sprawować lub sprawowali wysokie stanowiska sądowe lub być doświadczonymi prawnikami, oraz że nie ma żadnych obciążeń dowodowych, które można by pokonać, aby złożyć do niego wniosek[60]. Rozpatrując skargi osób fizycznych, sąd powinien mieć dostęp do wszystkich istotnych informacji,[61] w tym materiałów niejawnych. Ponadto powinien on mieć uprawnienia do usunięcia niezgodności.[62]

46. Artykuł 47 Karty odwołuje się do trybunału, nawet jeśli w wersjach językowych innych niż angielska preferowane jest słowo „sąd",[63] natomiast EKPC nakłada na państwa członkowskie jedynie obowiązek zapewnienia, że „każdy, kogo prawa i wolności zostały naruszone, ma prawo do skutecznego środka

[56] TSUE, Schrems I, pkt 95.
[57] Zob. La Quadrature du Net i in., pkt 190 oraz opinia TSUE 1/15, pkt 220.
[58] Zob. La Quadrature du Net i in., pkt 191.
[59] ETPC, Zakharov, pkt 234.
[60] ETPC, Kennedy, pkt 190.
[61] EROD dostrzega, że zdaniem Komisarza Praw Człowieka Rady Europy tzw. zasada „stron trzecich" (zgodnie z którą agencje wywiadowcze jednego kraju, dostarczające dane agencjom wywiadowczym innego, mogą nakładać na agencje otrzymujące obowiązek nieujawniania przekazanych danych żadnej stronie trzeciej) nie powinna mieć zastosowania do organów nadzorujących, aby nie podważać możliwości skutecznego środka ochrony prawnej (dokument tematyczny w sprawie demokratycznej i skutecznej kontroli nad krajowymi służbami bezpieczeństwa).
[62] ETPC, Kennedy, pkt 167.
[63] Słowo „trybunał" tłumaczone jest na przykład jako „Gericht" w języku niemieckim i „gerecht" w języku holenderskim.

odwoławczego do właściwego organu państwowego”,[64] który niekoniecznie musi być organem sądowym.[65]

47. W kontekście wyroku w sprawie Schrems II TSUE, oceniając adekwatność stopnia ochrony państwa trzeciego, powtórzył, że „jednostkom powinna przysługiwać możliwość skorzystania przed niezawisłym i bezstronnym sądem ze środków prawnych w celu uzyskania dostępu do dotyczących ich danych osobowych lub spowodowania korekty lub usunięcia takich danych”.[66] W tym samym kontekście TSUE uważa, że skuteczna ochrona sądowa przed takimi ingerencjami może być zapewniona nie tylko przez sąd, ale również przez organ,[67] który zapewnia gwarancje merytorycznie równoważne tym wymaganym na mocy art. 47 Karty. W orzeczeniu w sprawie Schrems II TSUE podkreślił, że należy zapewnić niezależność sądu lub organu, zwłaszcza władzy wykonawczej, ze wszystkimi niezbędnymi gwarancjami, w tym w odniesieniu do warunków odwołania[68] oraz że uprawnienia, które powinny zostać przyznane sądowi, muszą być zgodne z wymogami art. 47 Karty. W tym względzie organowi[69] przyznaje się uprawnienia do przyjmowania decyzji wiążących służby wywiadowcze, zgodnie z gwarancjami prawnymi, na których mogłyby się opierać osoby, których dane dotyczą[70].

4. UWAGI KOŃCOWE

48. Cztery niezbędne gwarancje europejskie należy postrzegać jako podstawowe elementy oceny poziomu ingerencji w podstawowe prawa do prywatności i ochrony danych. Nie powinny one być oceniane niezależnie, ponieważ są ściśle ze sobą powiązane, lecz w ujęciu ogólnym, dokonując przeglądu odpowiednich przepisów w odniesieniu do środków nadzoru, minimalnego poziomu gwarancji ochrony praw osób, których dane dotyczą, oraz środków ochrony prawnej przewidzianych w prawie krajowym państwa trzeciego.

49. Gwarancje te wymagają pewnego stopnia interpretacji, zwłaszcza że przepisy państw trzecich nie muszą być identyczne z ramami prawnymi UE.

50. Jak stwierdził ETPC w sprawie Kennedy, „ocena zależy od wszystkich okoliczności sprawy, takich jak charakter, zakres i czas trwania ewentualnych środków, podstawy wymagane do wydania nakazu, organy właściwe do ich zatwierdzenia, wdrożenia i kontroli oraz rodzaj środka ochrony prawnej przewidzianego w prawie krajowym”.[71]

51. W związku z tym ocena środków nadzoru w państwach trzecich w stosunku do niezbędnych gwarancji europejskich (NGE) może prowadzić do dwóch wniosków:

[64] Artykuł 13 EKPC.
[65] ETPC, Klass, pkt 67.
[66] Zob. Schrems II, pkt 194.
[67] Zob. Schrems II, pkt 197, w którym Trybunał wyraźnie używa tego słowa.
[68] Zob. Schrems II, pkt 195.
[69] Zob. Schrems II, pkt 197, w którym Trybunał wyraźnie używa tego słowa.
[70] Zob. Schrems II, pkt 196.
[71] ETPC, Kennedy, pkt 153.

- Przedmiotowe uregulowania w państwach trzecich nie są zgodne z NGE: w takim przypadku ustawodawstwo państwa trzeciego nie zapewniałoby poziomu ochrony zasadniczo równoważnego z poziomem gwarantowanym w UE.

- Przedmiotowe uregulowania w państwach trzecich spełniają wymogi NGE.

52. Oceniając, czy stopień ochrony jest odpowiedni, zgodnie z art. 45 RODO Komisja będzie musiała ocenić, czy NGE są spełnione w ramach elementów, które należy uznać za gwarantujące, że prawodawstwo państwa trzeciego jako całość zapewnia stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE.

53. Jeżeli podmioty przekazujące dane wraz z podmiotami odbierającymi dane opierają się na odpowiednich zabezpieczeniach na mocy art. 46 RODO, biorąc pod uwagę wymogi ustawodawstwa państwa trzeciego, mające szczególne zastosowanie do przekazywanych danych, musiałyby one zapewnić skuteczne osiągnięcie merytorycznie równoważnego stopnia ochrony. W szczególności, w przypadku gdy prawo państwa trzeciego nie spełnia wymogów NGE, oznaczałoby to zapewnienie, aby przedmiotowe prawo nie naruszało gwarancji i zabezpieczeń towarzyszących przekazaniu, tak aby stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE był nadal zapewniany.

54. EROD wydała dalsze wytyczne i zalecenia, które należy uwzględnić przy przeprowadzaniu oceny, w zależności od narzędzia przekazywania danych, które należy zastosować, oraz od konieczności zapewnienia odpowiednich zabezpieczeń, w tym, w stosownych przypadkach, środków uzupełniających.[72]

55. Ponadto należy zauważyć, że niezbędne gwarancje europejskie opierają się na wymogach prawa. EROD podkreśla, że niezbędne gwarancje europejskie opierają się na prawach podstawowych, które mają zastosowanie do wszystkich osób, niezależnie od ich obywatelstwa.

56. EROD powtarza, że niezbędne gwarancje europejskie są standardem odniesienia przy ocenie ingerencji związanej ze środkami nadzoru państw trzecich w kontekście międzynarodowego przekazywania danych. Standardy te wynikają z prawa UE oraz z orzecznictwa TSUE i ETPC, które są wiążące dla państw członkowskich.

[72] Dokument „Odpowiedni stopień ochrony przekazywanych danych osobowych”, WP 254 rev.01, Ostatnio zmieniony i przyjęty dnia 6 lutego 2018 r.; Zalecenia EROD nr 1/2020 w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, 10 listopada 2020 r.