

Od:
Do: [petycje](#); [Stanowisko informacyjne CO KPRP](#); [sekretariat Biuro Dialogu i Korespondencji](#)
Temat: 57.4/2024 [PETYCJA]
Data: sroda, 17 stycznia 2024 07:32:23

dnia: 17-01-2024 roku

Wnoszaca:

Adres do korespondencji:

Adresat:

Sz. P. Prezydent Rzeczypospolitej Polskiej

PETYCJA

Na podstawie art. 2. ust. 2. pkt. 1), art. 2. ust. 3., art. 4. ust. 1., art. 4. ust. 5. – Ustawy z dnia 11 lipca 2014 roku o petycjach (t.j. Dz. U. 2018 poz. 870) przekladam petycje w interesie publicznym, droga mailowa w zakresie ponizej:

Temat petycji:

„Poprzez podjecie inicjatywy ustawodawczej w celu zmniejszenia inwigilacji, ingerencji w rejestrach panstwowych oraz zwiekszenia prywatnosci obywateli oraz adekwatnosci i minimalizacji przetwarzanych danych oraz zasady bycia zapomnianym w dokumentacji i Rejestrze Dowodów Osobistych”

Akt prawa w którym postulowana jest zmiana:

Ustawa z dnia 6 sierpnia 2010 roku o dowodach osobistych (tj. Dz. U. 2022 poz. 671);

Przedmiot petycji:

W ustawie z dnia 6 sierpnia 2010 roku o dowodach osobistych (tj. Dz. U. 2022 poz. 671) postuluje o:

- [POSTULAT 1] *Zmiane w art. 56. ust. 2. o brzmieniu: „Dane zgromadzone usuwa sie w niniejszym artykule ale takze po 5 latach od zgonu posiadacza dowodu osobistego oraz od wprowadzenia zmian.”*
- [POSTULAT 2] *Uchylenie art. 56. ust. 3.;*
- [POSTULAT 3] *Dodanie w art. 56. ust. 4. o brzmieniu: „ Osoba ma prawo do uzyskania informacji o udostepnionych dokumentach i informacji, nie pozniej niz w ciagu 30 dni po zakonczonym postepowaniu.”*
- [POSTULAT 4] *Dodanie art. 56c. o brzmieniu:*
„1. Sad wydaje postanowienie o udostepnieniu danych biorac pod uwage interes faktyczny, interes prawny wnoszacego.
2. Sad lub Urzad Ochrony Danych Osobowych lub Rzecznik Praw Obywatelskich lub Naczelna Izba Kontroli – dokonuje kontroli nad rzetelnoscia, celowoscia, gospodarnoscia, przydatnoscia, zasadnoscia udostepnienia i przetwarzania danych.
3. Organ dokonuje weryfikacji nad rzetelnoscia przetwarzanych danych nie rzadziej niz co 5 lat z urzedu ale takze na wniosek strony, prokuratora, sadu lub innych podmiotów ochrony danych osobowych i praw czlowieka”
- [POSTULAT 5] *Uchylenie art. 65. ust. 2. pkt. 1);*
- [POSTULAT 6] *Uchylenie art. 66.;*
- [POSTULAT 7] *Uchylenie art. 67.;*
- [POSTULAT 8] *Uchylenie art. 72.;*
- [POSTULAT 9] *Uchylenie art. 73.*

Uzasadniam nizej wymienionymi argumentami:

[UA] Celem i potrzeba zrealizowania postulatów jest:

- o zapobieganie nadmiernej udostępnianych danych poprzez weryfikację;
- o zapobieganie inwigilacji i ingerencji;
- o zapobieganie nieadekwatności przetwarzanych i udostępnianych danych i dokumentów;
- o zapobieganie przetwarzanych dokumentów nieważnych, unieważnionych, spersonalizowanych wadliwie ponieważ dana tożsamość nie istnieje. W przypadku wpisania numeru i serii dokumentu, który jest nieważny można przewidywać, że nie ma takiej osoby, dokument jest nieważny.

[UB] Stan faktyczny postulatów uzasadniam:

Obecnie bezterminowo przetwarza się dokumenty w Rejestrze Dowodów Osobistych mimo, że dokument unieważniony lub błędnie spersonalizowany nie zostanie już użyty z uwagi na odpowiedzialność karną, każdy po zmianie danych lub wydaniu nowego dokumentu, zobowiązany jest do aktualizacji danych w ośrodku życia codziennego.

[UC] Stan prawny:

- o Zgodnie z art. 51 Konstytucji, organy winny przetwarzać dane niezbędne w demokratycznym państwie prawnym w związku z powyższym przetwarzanie danych osób zmarłych nie zostanie wykorzystane przez organy do wykonywania niezbędnych zadań;
- o Zgodnie z zasadą przetwarzanych danych, art. 5. ust. 1. lit. c) RODO dane winny być „adekwatne, stosowne i nienadmierne do celów, jakimi są przetwarzane”
- o Zgodnie z zasadą przetwarzanych danych, art. 5. ust. 1. lit. d) RODO dane winny być „prawidłowe i w razie potrzeby **uaktualniane**; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe, w świetle celów ich przetwarzania, zostały **niezwłocznie usunięte** lub sprostowane”
- o Zgodnie z zasadą bycia zapomnianym zawartą w art. 17 RODO, każdy ma prawo do usunięcia danych osobowych, jeśli dane są niezbędne. Nie budzi wątpliwości, że dane osób zmarłych są zbędne, ponieważ przez Urząd nie zostaną wykorzystane do wykonywania zadań;
- o Zgodnie z Klauzulą RODO w dokumentacji dowodów osobistych i Rejestrze Dowodów Osobistych dane przetwarzane są w celu:

Pani / Pana dane będą przetwarzane w celu:

- wydania Pani/Panu dowodu osobistego.
- unieważnienia Pani/Pana dowodu osobistego z powodu:
- zgłoszenia utraty lub uszkodzenia dowodu,
- zmiany danych zawartych w dowodzie,
- upływu terminu ważności dowodu,
- utraty obywatelstwa polskiego lub zgonu.
- uzyskania przez Panią/Pana zaświadczenia o danych własnych zgromadzonych w Rejestrze Dowodów Osobistych

Źródło: <https://www.ujsoy.com.pl/jak-zalatwic-sprawe/ewidencja-ludnosci-i-dowodow-osobistych/klauzula-informacyjna-rod-1>

- w związku z powyższym przetwarzanie danych o dokumentach archiwalnych, historycznych, przeszłościowych po wydaniu nowego dokumentu lub w przypadku zgonu jest zbędne

- o Zgodnie z art. 1 – Ustawy z 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. 2020 poz. 164) danymi archiwalnymi o kategorii archiwalnej to materiały „Materiałami archiwalnymi” wchodzącymi do narodowego zasobu archiwalnego, zwanymi dalej „materiałami archiwalnymi”, są wszelkiego rodzaju akta i dokumenty, korespondencja, dokumentacja finansowa, techniczna i statystyczna, mapy i plany, fotografie, filmy i mikrofilmy, nagrania dźwiękowe i wideofonowe, dokumenty elektroniczne w rozumieniu przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848, 1590 i 2294) oraz inna dokumentacja, bez względu na sposób jej wytworzenia, mająca znaczenie jako źródło informacji o wartości historycznej o działalności Państwa Polskiego, jego poszczególnych organów i innych państwowych jednostek organizacyjnych oraz o jego stosunkach z innymi państwami, o rozwoju życia społecznego i gospodarczego, o działalności organizacji o charakterze politycznym, społecznym i gospodarczym, zawodowym i wyznaniowym, o organizacji i rozwoju nauki, kultury i sztuki, a także o działalności jednostek samorządu terytorialnego i innych samorządowych

jednostek organizacyjnych - powstała w przeszłości i powstająca współcześnie”.

- w związku z tym przetwarzanie bezterminowe (wieczyste) danych osób w Rejestrze Dowodów Osobistych jest zbędne.

o Zgodnie z art. 47 Konstytucji, każdy ma prawo do prywatności i ochrony życia rodzinnego. W związku z tym przetwarzanie i udostępnienie danych, zdarzeń z przebiegu życia, historia posiadanych danych i dokumentów obywateli i o obywatelach jest naruszeniem strefy prywatnej.

o Zgodnie z Wyrokiem Wojewódzkiego Sadu Administracyjnego w Warszawie z dnia 24 października 2011 roku o sygnaturze (II SA/Wa 625/11) w sprawie usuwania danych z KSIP mają zastosowanie przepisy ustawy o ochronie danych osobowych co oznacza, że usuwanie danych z innych systemów również mają zastosowanie ustawa o ochronie danych osobowych, Konstytucja, RODO, a nie ustawy szczególne lub poszczególne.

<https://www.infor.pl/prawo/nawosci-prawne/294364.Usuwanie-danych-osobowych-z-KSIP-w-opinii-sadu.html>

o Zgodnie z Wyrokiem Europejskiego Trybunału Sprawiedliwości z dnia 4 grudnia 2008 roku, Trybunał orzekł, że bezterminowe przechowywanie danych przez władze publiczne (...) jest niedopuszczalne w demokratycznym społeczeństwie i prowadzi do naruszenia art. 8 Europejskiej Konwencji Praw Człowieka stanowiącego o prawie do ochrony życia prywatnego.

<https://www.infor.pl/prawo/nawosci-prawne/294364.Usuwanie-danych-osobowych-z-KSIP-w-opinii-sadu.html>

o Zgodnie z RODO (dane nie mogą być przetwarzane, przechowywane) bezterminowo (wieczyste) mówi o tym między innymi motyw 39, art. 5 ust. 1 lit. e

Motyw (39): **Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne.** Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. **Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane.** Wymaga to w szczególności **zapewnienia ograniczenia okresu przechowywania danych do ściśle minimum.** Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. **Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe.** Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

Art. 5 ust. 1 lit. e „przechowywanie w formie umożliwiającej identyfikację osoby, której dane dotyczą, **przez okres nie dłuższy, niż jest to niezbędne** do celów, w których dane te są przetwarzane (...)”

Źródło: <https://poradnikprzedsiębiorcy.pl/-jak-dlugo-mozna-przechowywac-dane-osobowe>

o Zgodnie z hierarchią prawa wymieniona w art. 87 Konstytucji, Konstytucja jest ustawą zasadniczą, dlatego każdy ma prawo do prywatności i autonomii danych osobowych zawartych w artykule art. 47 i art. 51.

o Zgodnie z Opinią Rzecznika Generalnego w sprawie C 118/22 „Mozna się zastanawiać, czy art. 5 dyrektywy 2016/680 nie skrywa formy wewnętrznej sprzeczności logicznej. Zgodnie z tym przepisem bowiem mogą zatem istnieć dane osobowe przetwarzane przez organy ścigania, dla których nie byłoby właściwe ustalenie terminów usunięcia, ale w takiej sytuacji bezterminowego przechowywania danych **należy przewidzieć okresowy przegląd przez właściwe organy konieczności przechowywania tych danych oraz możliwość ich usunięcia, jeżeli przechowywanie nie jest już uzasadnione w świetle celu przetwarzania.** Można jednak zrozumieć i zaakceptować, że uzasadnionym celem jest zapewnienie środka zaradczego, aby zapobiec nadużyciom we wdrażaniu inwazyjnego mechanizmu.”

Źródło: <https://curia.europa.eu/juris/document/document.jsf?sessionId=DEC3D1757D86F30F7B24F85E4AF74FF9?text=&docid=274651&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=21748532>

o Zgodnie z zasadą pierwszeństwa prawa wspólnotowego „prawo unijne ma pierwszeństwo przed prawem krajowym państwa członkowskiego (włącznie z Konstytucją)” w związku z powyższym zasada minimalizacji danych i zasada bycia zapomnianym winna obowiązywać.

https://pl.m.wikipedia.org/wiki/Zasada_pierwszenstwa_prawa_wsp%C3%B3lnotowego

o Trybunał Sprawiedliwości UE w sprawach dotyczących funkcjonowania publicznych rejestrów w kontekście ochrony prawa do prywatności, podkreślał, że udostępnianie danych osobowych osobom trzecim stanowi ingerencję w prawa podstawowe ustanowione w art. 7 i 8 Karty Praw Podstawowych UE (KPP), niezależnie od tego, w jaki sposób te dane zostaną później wykorzystane.

<https://bip.brpo.gov.pl/pl/content/rpo-ms-dostep-dane-osobowe-rejestry-publiczne-odpowiedz>

o RPO zwraca uwagę na wyrok TSUE z 22 listopada 2022 r. w połączonych sprawach C-37/20 i C-601/20, dotyczący rejestru beneficjentów rzeczywistych. Trybunał podkreślił w nim, że udostępnienie każdej osobie dostępu do danych zawartych w powszechnym rejestrze stanowi nieproporcjonalną ingerencję w prawo do prywatności i ochrony danych osobowych

<https://bip.brpo.gov.pl/pl/content/rpo-ms-dostep-dane-osobowe-rejestry-publiczne-odpowiedz>

o Trybunał Sprawiedliwości UE orzekł w ubiegłym tygodniu, że informacje dotyczące operacji przeglądania danych osobowych danej osoby, dotyczące dat i celów tych operacji, stanowią informacje, które osoba ta ma prawo uzyskać od administratora

Czytaj więcej na Prawo.pl:

<https://www.prawo.pl/prawo/kazdy-ma-prawo-wiedziec-kiedy-i-jak-jego-dane-osobowe-byly.521912.html>

Wyrok Trybunału Sprawiedliwości UE z dnia 22 czerwca w sprawie C 579/21

o Odpis zupełny stanowi zaświadczenie o dokonaniu zmian, jest wydawany każdorazowo po dokonanej zmianie w celu aktualizacji danych i wymiany dokumentów. W przypadku wydania nowego dokumentu tożsamości (poprzednie dane i wzmianki dodatkowe) informujące o zmianie są nieprzydatne, nie są już potrzebne ponieważ są krótkim nośnikiem informacji praktycznej.

Mówi o tym między innymi: art. 35 ustęp 8, art. 37 ustęp 8, art. 39a ust. 2, art. 41 ust. 2, art. 42, art. 43, art. 67 ustęp 6 i 7, art. 73 ustęp 2 i 3, art. 95 ustęp 4 i 7, art. 110 ustęp 2, art. 127a ustęp 2.

o Zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 3 listopada 2022 roku w sprawie trybu i terminów przekazywania danych pomiędzy rejestrem PESEL, a rejestrami centralnymi; zmiany w rejestrze są przekazywane do innych rejestrów centralnych **w związku z tym przetwarzanie nieokreślone czasowo jest zbędne.**

o Zgodnie z art. 3, z art. 79 o dowodach osobistych ale także zgodnie z art. 65 kodeksu wykroczeń (dokument tożsamości jest dokumentem potwierdzającym tożsamość) w związku z tym należy posługiwać się aktualnymi dokumentami, aktualnymi danymi w celu potwierdzenia tożsamości ale także podczas legitymowania z chwilą odebrania nowego dokumentu, **w związku z tym przetwarzanie poprzednich danych jest zbędne.**

o Zgodnie z wyrokiem Trybunału w sprawie C-140/20 winna być kontrola sądu. „58. Z tego właśnie względu Trybunał stwierdził, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 karty nie stoi na przeszkodzie przepisom ustawodawczym umożliwiającym, w celu ochrony bezpieczeństwa narodowego, posłużenie się skierowanym do dostawców usług łączności elektronicznej nakazem uogólnionego i nieodróżnionego 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 może **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 (wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 168).”

o Zgodnie z wyrokiem Trybunału w sprawie C-140/20 winna być kontrola sądu. „106. **W celu zapewnienia w praktyce pełnej zgodności z tymi warunkami ważne jest, aby dostęp właściwych organów krajowych 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 przestępstwom, ich wykrywanie lub ściganie karne [wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 51 i przytoczone tam orzecznictwo].”

o Zgodnie z wyrokiem Trybunału w sprawie C-140/20 dane winny być udostępnione zgodnie z zasadą proporcjonalności „59. Jeśli chodzi o cel polegający na zapobieganiu przestępstwom, ich dochodzeniu, wykrywaniu i ściganiu, **Trybunał zauważył, że zgodnie z zasadą proporcjonalności jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniom dla bezpieczeństwa publicznego**

moga uzasadniac powazne ingerencje w prawa podstawowe ustanowione w art. 7 i 8 karty, takie jak te, które sa zwiazane z zatrzymywaniem danych o ruchu i danych o lokalizacji. A zatem jedynie takie ingerencje we wspomniane prawa podstawowe, które nie maja powaznego charakteru, moga byc uzasadnione celem polegajacym na zapobieganiu przestepstwom w ogólnosci, ich dochodzeniu, wykrywaniu i sciganiu (wyrok z dnia 6 pazdziernika 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, pkt 140 i przytoczone tam orzecznictwo).”

o Zgodnie z wyrokiem Trybunalu Konstytucyjnego w sprawie K 23/11 z dnia 30 lipca 2014 roku (strona 54) mozna wyczytac „1.10. Umozliwienie sluzbom policyjnym i ochrony panstwa pozyskiwania wiedzy o tresci, czasie i formach komunikowania sie jednostek, a takze monitorowania ich aktywnosci zyciowej w inny sposob, nieuchronnie popada w kolizje z prawem do ochrony prywatnosci, ochrona tajemnicy komunikowania sie, autonomia informacyjna, a w niektórych wypadkach (podsluchu lub monitoringu zainstalowanego w mieszkaniu) z nienaruszalnoscia mieszkania. **Co wiecej, samo istnienie przepisow uprawniajacych organy wladzy wykonawczej do takiego rodzaju czynnosci winno byc postrzegane jako ingerencja w konstytucyjnie chroniony status czlowieka i obywatela, którego źródłem jest przyrodzona i niezbywalna godnosc. Prawna dopuszczalnosc pozyskiwania informacji o jednostkach, niekiedy o sferach istotnych z punktu widzenia ich uczestnictwa w zyciu publicznym, negatywnie wpływa na korzystanie przez nie z konstytucyjnych wolnosci i praw. Niezaleznie od konkretnych, niekiedy zróżnicowanych form wkroczenia w sfera zycia prywatnego, sama nawet swiadomosc znajdowania sie pod ciaglym nadzorem wladz publicznych moze zniechecac jednostki do swobodnego korzystania z zagwarantowanych im konstytucyjnych wolnosci i praw. Moze to rodzić obawy, ze organy wladzy publicznej beda w nieuprawniony sposob gromadzic i wykorzystywac informacje o osobach.** Obawy te sa wyjątkowo silne w polskim spoleczenstwie, które przez dziesieciolecie reżimu komunistycznego bylo inwigilowane przez tajne sluzby bezpieczenstwa, najczesciej niesluzace dobrze rozumianym interesom własnego panstwa i jego wspólobywateli. **Z punktu widzenia konstytucyjnych gwarancji prawa do ochrony prywatnosci, a takze ochrony tajemnicy komunikowania sie, zdaniem Trybunalu, ingerencja wladzy publicznej w te sfere jest nie tylko pozyskanie przez wladze publiczne danych o jednostce po raz pierwszy. Ochrona prawa do prywatnosci i tajemnicy komunikowania sie rozciaga sie bowiem na cały proces pozyskiwania, gromadzenia, przechowywania oraz przetwarzania (w tym analizowania i porównywania) informacji o jednostkach.** Dlatego tez jako odrebne przejawy ingerencji w konstytucyjnie chroniony status jednostki –wymagajace kazdorazowo odrebnej legitymizacji konstytucyjnej – nalezaloby traktowac pozyskiwanie informacji m.in. o tresci komunikatów przekazywanych za pomoca sieci teleinformatycznych w toku kontroli operacyjnej, nalozenie na dostawców uslug telekomunikacyjnych obowiazku zatrzymywania danych o ruchu i lokalizacji, dostep do tych danych, ich nastepcza weryfikacje czy przekazanie innym organom (por. wyrok Federalnego Sadu Konstytucyjnego Niemiec z 2 marca 2010 r., sygn. 1 BvR 256/08, pkt 190).”

„1.13. Trybunal zwraca uwage na jeszcze jedna kwestie, majaca istotne znaczenie w dobie globalizacji i miedzynarodowej przestepczosci. **Organ wladzy publicznej zobowiazane sa do ochrony prywatnosci własnych obywateli również przed zagrozeniami plynacymi spoza samego panstwa. Obowiazek panstwa rozciaga sie w konsekwencji na zapewnienie ochrony prywatnosci przed monitorowaniem rozmaitych sfer aktywnosci**

zyciowej obywateli, w tym wiadomosci przesyłanych za pomoca sieci telekomunikacyjnych przez podmioty zagraniczne, a zwłaszcza panstwa obce. **Naruszenie prawa do ochrony prywatnosci zagwarantowanego w art. 47 Konstytucji moze bowiem nastapic nie tylko przez bezposrednie dzialanie polskich organów panstwa, pozyskujacych informacje o jednostkach w sposob niejawný. Nastapi to również w sytuacji braku**

dostatecznej ochrony obywateli przez panstwo przed ingerencja w te wolnosc, spowodowana dzialaniami innych podmiotów.

Trybunal Konstytucyjny podkreśla, ze ingerencja wladzy publicznej w prywatnosc czy autonomie informacyjna jednostek jest dopuszczalna wylacznie na zasadach okreslonych w Konstytucji, co w pelni dotyczy podejmowania zobowiazan miedzynarodowych przez wladze Rzeczypospolitej Polskiej”

W stronie 57 wyroku mozna wyczytac „Przepis art. 8 ust. 1 Konwencji **dotyczy szeroko rozumianego prawa do poszanowania prywatnej sfery zycia czlowieka, stanowiac tym samym najbardziej ogólna afirmacje autonomii jednostki w zakresie kształtowania wszelkich aspektów jej zycia oraz własnej osobowosci.** Istota tego prawa jest zapewnienie kazdej jednostce sfery prywatnosci (autonomii) chronionej przed ingerencja zewnetrzna, pochodzaca zarówno od panstwa, jak i podmiotów prywatnych (zob. np. L. Garlicki, uwaga 21 do art. 8, [w:] Konwencja o Ochronie Praw Czlowieka i Podstawowych Wolnosci. Tom I. Komentarz do artykulów 1- 18, red. L. Garlicki, P. Hofmanski, A. Wróbel, Warszawa 2010, s. 491).”

o Zgodnie z wyrokiem Trybunału Europejskiego w sprawie C-293/12 i C-594/12 można przeczytać:

33. Przy ustalaniu tego, czy mamy do czynienia z ingerencją w podstawowe prawo do poszanowania życia prywatnego, nie ma znaczenia, czy informacje związane z życiem prywatnym mają charakter wrażliwy, ani też to, czy też ze względu na te ingerencje zainteresowane osoby doświadczyły ewentualnych niedogodności (zob. podobnie wyrok Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 75).

34. Wynika stąd, że nałożony w art. 3 i 6 dyrektywy 2006/24 na dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności obowiązek zatrzymywania przez określony czas związanych z życiem prywatnym danej osoby i jej komunikacja danych takich jak te określone w art. 5 tej dyrektywy stanowi samoistną ingerencję w prawa zagwarantowane w art. 7 karty.

35. Za dodatkową ingerencję w to prawo podstawowe należy też uznać możliwość uzyskania dostępu do tych danych przez właściwe organy krajowe (zob., w odniesieniu do art. 8 EKPC, wyroki ETPC: z dnia 26 marca 1987 r. w sprawie Leander przeciwko Szwecji, seria A, nr 116, § 48; w sprawie Rotaru przeciwko Rumunii [GC], skarga nr 28341/95, § 46, ETPC 2000-V; a także w sprawie Weber i Saravia przeciwko Niemcom (déc.), skarga nr 54934/00, § 79, ETPC 2006-XI). W konsekwencji art. 4 i 8 dyrektywy 2006/24 określające zasady dostępu do danych przez właściwe organy krajowe również stanowią ingerencję w prawa zagwarantowane w art. 7 karty.

o Zgodnie z opinią Rzecznika Generalnego w sprawie C-817/19 przed Trybunałem Europejskim, można przeczytać „70. Trybunał orzekł już, że przepisy nakazujące lub dopuszczające przekazanie podmiotowi trzeciemu, takiemu jak organ publiczny, danych osobowych osób fizycznych należy, w braku zgody tych osób fizycznych i niezależnie od późniejszego wykorzystania tych danych, uznać za ingerencję w ich życie prywatne, a zatem za ograniczenie prawa podstawowego zagwarantowanego w art. 7 karty, bez uszczerbku dla możliwości ich ewentualnego uzasadnienia(52). Jest tak nawet w braku okoliczności pozwalających na zakwalifikowanie takiej ingerencji jako „poważnej”, i nie ma znaczenia, czy informacje związane z życiem prywatnym osób, których dotyczy, mają charakter wrażliwy czy nie lub czy zainteresowane osoby poniosły jakiegokolwiek negatywne konsekwencje z powodu tej ingerencji(53). Dostęp organów władzy publicznej do takich informacji stanowi również ingerencję w prawo podstawowe do ochrony danych osobowych zagwarantowane w art. 8 karty, ponieważ stanowi przetwarzanie danych osobowych(54). Podobnie, samoistna ingerencja w prawa zagwarantowane w art. 7 i 8 karty jest zatrzymywanie przez określony czas danych związanych z życiem prywatnym danej osoby(55).”

o Zgodnie m.in. z art. 13 prawa prasowego, policja korzysta z tego artykułu w celu ustalenia tożsamości osób podejrzanych, podejrzanych o nieustalonej tożsamości pod postacią wizerunku, w związku z tym Policja nie korzysta z zdjęć w Rejestrze Dowodów Osobistych w celu ustalenia tożsamości zwłok, poszukiwanych.

[UD] Obecny i proponowany stan prawny w celu podjęcia inicjatywy ustawodawczej przez organ w art. 118 Konstytucji:

o W obecnym stanie prawnym przetwarza się dane bezterminowo, wiecześnie w Rejestrze Dowodów Osobistych moja propozycja to wprowadzenie okresu czasowego przetwarzanych danych w rejestrach państwowych.

o W związku z powyższym, że sprawa dotyczy danych osobowych nad niniejszą ustawą jest ustawa o ochronie danych osobowych oraz RODO w szczególności zasada bycia zapomnianym oraz przepisy Konstytucji.

[UE] Przewidywana ocena skutków społecznych, gospodarczych, finansowych i prawnych w celu podjęcia inicjatywy ustawodawczej przez organ w art. 118 Konstytucji:

- o Zwiększenie prywatności obywateli;
- o Usprawnienie działanie systemów państwowych celem zapobiegania zawieszenia się i podazy na ataki;
- o Zwiększenie pojemności dysków, pendrive w których przetwarzane są dane osobowe, bez potrzeby zakupu nowych nośników informacji;
- o Zmniejszenie kosztów utrzymania systemów rejestrów państwowych;
- o Większa kontrola nad udostępnionymi danymi i dokumentami;
- o Zapobieganie nieadekwatności udostępnianych danych poprzez uchylenie przepisów o udostępnienie danych: pełnych, ograniczonych, a podlegających tylko i wyłącznie weryfikacji w celu potwierdzenia tożsamości.

Proszę o odpowiedź tylko na adres skrzynki mailowej.

Nie wyrażam zgody na ujawnienie: imienia, nazwiska, adresu, e-maila, miejscowości sporządzenia.

Z poważaniem,