



Warszawa, 19-01-2026 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

II.519.916.2025.DC

Pan Marcin Kierwiński

**Minister Spraw Wewnętrznych i
Administracji**

/ePUAP/

Szanowny Panie Ministrze,

problematyka policyjnych rejestrów danych – zbiorów big data¹ - jest zagadnieniem nabierającym znaczenia i aktualności. Obecnie bowiem, Policja i inne służby mogą gromadzić znaczną liczbę danych osobowych², w tym także danych wrażliwych – danych genetycznych, biometrycznych, dotyczących pochodzenia rasowego lub etnicznego, a następnie przetwarzać te dane bez wiedzy jednostki. Celem przetwarzania danych osobowych jest „zapobieganie i zwalczanie przestępczości”. Dodatkowo, w ramach mechanizmów współpracy UE przewidziano obowiązki zapewnienia wymiany/dostępu do baz danych obejmujących dane genetyczne, daktyloskopijne, wizerunek, a także związane z umożliwieniem zautomatyzowanego

¹ Zob. definicję big data na stronie:

<https://www.europarl.europa.eu/topics/pl/article/20210211STO97614/big-data-definicja-korzysci-wyzwania-infografika>.

² Zgodnie z art. 3 pkt 1 dyrektywy 2016/680 „dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

przetwarzania i przeszukiwania danych³. Z perspektywy praw i wolności jednostki, zarówno zautomatyzowane przetwarzanie (przeszukiwanie danych osobowych) bez jej wiedzy, jak i przechowywanie tych danych w różnych rejestrach danych przez trudny do oszacowania czas, stwarza realne zagrożenie nieproporcjonalnej i nadmiernej ingerencji w prawo do prywatności⁴. Obecnie w Polsce, dane o osobach w jakiegokolwiek roli zaangażowanych w postępowanie karne, postępowanie w sprawach o wykroczenia, czy w działania Policji o charakterze administracyjno-porządkowym mogą być przetwarzane m.in. w Krajowym Rejestrze Karnym⁵, Krajowym Centrum Informacji Kryminalnych⁶, Rejestrze Sprawców Przestępstw na Tle Seksualnym⁷,

³ Zob. art. 32 rozporządzenia 2024/982.

⁴ Zob. wyrok ETPC z 13.02.2020 r. w sprawie Gaughran p. Zjednoczonemu Królestwu; skarga nr 45245/15.

⁵ Rejestr prowadzony na podstawie ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (t.j. Dz. U. z 2024 r. poz. 276), w którym gromadzone są dane m.in. o wyrokach skazujących, warunkowo umarzających postępowanie, osobach tymczasowo aresztowanych oraz informacje o nieletnich wobec których orzeczono środki wychowawcze, poprawcze, lecznicze lub umieszczono w schronisku dla nieletnich (art. 1 ustawy o KRK). Przepisy ustawy regulują zasady dostępu do danych, precyzując krąg podmiotów mogących uzyskać informacje o jednostce, zasady przetwarzania danych oraz wprowadzają terminy ich usunięcia (art. 14 ustawy o KRK).

⁶ Rejestr prowadzony na podstawie ustawy o przetwarzaniu informacji kryminalnych (ustawa z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych (t.j. Dz. U. z 2024 r. poz. 376 z późn. zm.). Zgodnie z art. 13 tej ustawy, zakres przetwarzanych informacji obejmuje m.in. czas i miejsce popełnionego przestępstwa, sygnaturę akt, informacje o osobie, przeciwko której prowadzono postępowanie karne lub karne skarbowe albo prowadzono czynności operacyjne, dane o rachunkach bankowych itp. Przepisy regulują także czas przechowywania danych (art. 14 ustawy o KCIK), który wynosi 15 lat.

⁷ Rejestr prowadzony na podstawie ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich; Dz. U. z 2024 r. poz. 1802 z późn. zm.; (art. 4 i nast. ww. ustawy); zbiór ten dzieli się na trzy podzbiory (bazy: Rejestr z dostępem ograniczonym; Rejestr publiczny; Rejestr osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, wydała postanowienie o wpisie w Rejestrze) , a ustawa reguluje procedurę wpisu do rejestru, organy uprawnione do dokonania wpisu, przesłanki jego dokonania. Z uwagi na charakter wpisu w rejestrze (przede wszystkim charakter prewencyjny, który ma zapobiegać zagrożeniom przestępstwami przeciwko wolności seksualnej i obyczajności), co do zasady wpisu w Rejestrze się nie usuwa (art. 8 ustawy);

Systemie Wspomagania Dowodzenia Policji⁸, zbiorze danych DNA⁹, zbiorze danych daktyloskopijnych, tj. Centralnej Registraturze Daktyloskopijnej oraz zbiorze automatycznie przetwarzającym dane daktyloskopijne¹⁰, a także w Krajowym Systemie Informacyjnym Policji.

Krajowy System Informacyjny Policji jest prowadzony na podstawie art. 21nb ustawy Policji, a w istocie na podstawie zarządzenia nr 70 Komendanta Głównego Policji z

⁸ Rejestr prowadzony na podstawie art. 20e – 20g ustawy o Policji (t.j. Dz. U. z 2025 r. poz. 636); przetwarza się tam dane o przestępstwach i wykroczeniach (zob. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 października 2019 r. w sprawie prowadzenia rejestru wykroczeń, przetwarzania w nim informacji oraz sposobów i trybu udzielania informacji o osobach z tego rejestru (t.j. Dz. U. z 2023 r. poz. 715) oraz o sprawcach tych czynów zabronionych. Zakres przetwarzanych danych jest szeroki, obejmuje bowiem dane dotyczące osoby (m.in. imię, nazwisko, imiona i nazwiska rodowe rodziców, datę urodzenia, PESEL, dokument tożsamości, obywatelstwo i płeć, źródła utrzymania - art. 20f ust. 2 ustawy o Policji), a także informacje o czynie zabronionym oraz o rozstrzygnięciach sądu. Ustawa o Policji reguluje także zasady przetwarzania danych, precyzuje krąg podmiotów mających dostęp do zbioru danych oraz określa ramy czasowe przetwarzania ww. danych wprowadzając terminy ich usunięcia z rejestru (art. 20f ust. 15 ustawy o Policji).

⁹ Rejestr prowadzony na podstawie art. 21a ustawy o Policji, w których przetwarzane są dane genetyczne m.in. osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2022 r. poz. 1689); osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (przepis ten uprawnia funkcjonariuszy ABW, Policji i Straży Granicznej do pobrania linii papilarnych, utrwalana wizerunku twarzy lub nieinwazyjnego pobierania materiału biologicznego w przypadku gdy: 1) istnieje wątpliwość co do tożsamości osoby lub; 2) istnieje podejrzenie nielegalnego przekroczenia granicy Rzeczypospolitej Polskiej albo wątpliwość co do deklarowanego celu pobytu na terytorium Rzeczypospolitej Polskiej, lub 3) istnieje podejrzenie co do zamiaru nielegalnego przebywania na terytorium Rzeczypospolitej Polskiej, lub 4) istnieje podejrzenie związku osoby ze zdarzeniem o charakterze terrorystycznym, lub 5) osoba mogła uczestniczyć w szkoleniu terrorystycznym), oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego, osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość, zwłok ludzkich o nieustalonej tożsamości, śladów nieznanymi sprawców przestępstw itd. Ustawa precyzuje także cel przetwarzania danych osobowych (art. 21d ustawy o Policji), procedury weryfikacji oraz wprowadza maksymalne terminy przechowywania danych (art. 21e ust. 2 ustawy o Policji).

¹⁰ Zbiory prowadzone na podstawie art. 21h ustawy o Policji. Przetwarzane są w nich dane m.in. osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób, osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego, osób poszukiwanych (art. 21h ust. 2 ustawy o Policji). Przepis art. 21k ustawy o Policji precyzuje cel przechowywania i przetwarzania danych daktyloskopijnych, art. 21l ustawy o Policji wskazuje, kiedy dane zostaną usunięte.

dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji. Krajowy System Informacyjny Policji jest scentralizowanym zbiorem danych osobowych nie tylko osób podejrzanych, podejrzanych i oskarżonych, ale także pokrzywdzonych i innych osób w jakikolwiek sposób zaangażowanych w postępowanie karne lub postępowanie w sprawach o wykroczenia. System ten jest w zasadzie nadzbiorem danych policyjnych – zbiorem big data – przetwarzającym w sposób zautomatyzowany i niezautomatyzowany szeroki zakres danych o jednostkach. System działa niezależnie od innych systemów policyjnych, tj. usunięcie danych z określonego zbioru (np. KRK czy systemu danych daktyloskopijnych) nie oznacza, że zostaną one automatycznie usunięte z KSIP.

W rejestrach ustawodawca określa podstawę, cel, zasady udostępniania oraz (często) mechanizmy retencji i usuwania danych. Na tym tle KSIP pozostaje rozwiązaniem nietypowym: o bardzo szerokiej funkcjonalności, przy relatywnie szczątkowej regulacji ustawowej i przeniesieniu kluczowych reguł (zakres, retencja, usuwanie) do zarządzenia Komendanta Głównego Policji. W przypadku KSIP jedyną ustawową podstawą jest art. 21nb ustawy o Policji. Przepis art. 21nb ust. 1 ustawy o Policji stanowi, że „Komendant Główny Policji prowadzi Krajowy System Informacyjny Policji, zwany dalej "KSIP", będący zestawem zbiorów danych, w którym przetwarza się informacje, w tym dane osobowe, w związku z realizacją zadań ustawowych”, czyli m. in. zapobieganiu i zwalczaniu przestępczości, prowadzeniu działań operacyjnych, czy poszukiwaniu osób zaginionych i identyfikacji osób. Podstawą funkcjonowania KSIP jest zarządzenie nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji. Zgodnie z § 3 zarządzenia, KSIP jest scentralizowanym zestawem zbiorów danych obejmującym zakresem działania terytorium całego kraju oraz złożony ze zbiorów danych:

- 1) zbioru Osoba,
- 2) zbioru Fakt, w tym wykazu informacji tworzących Biuletyn KSIP,
- 3) zbioru Rzecz,
- 4) zbioru Podmiot,
- 5) zbioru Pokrzywdzeni,
- 6) rejestru wykroczeń, obejmującego swoim zakresem informacje, w tym dane osobowe, o osobach i wykroczeniach, o których mowa w art. 20f ust. 1-3 ustawy o Policji,

przetwarzane w zbiorze Osoba, Fakt, Rzecz i Pokrzywdzony w formie rejestracji, o których mowa w § 16 ust. 1 pkt 11, § 32, § 35 ust. 1 pkt 6 oraz § 39 ust. 2”.

KSIP jest w zasadzie „superzbiorem” łączącym w jedno bazy danych funkcjonujące w Policji i mającym dostęp (funkcjonalność) w zakresie pozyskiwania informacji z innych zbiorów danych¹¹. Systemy KSIP umożliwiają również zautomatyzowane lub częściowo zautomatyzowane przekazywanie informacji pomiędzy innymi systemami, a także przekazywanie danych do innych państw korzystających z Systemu Informacji Schengen (SIS), oraz innych systemów przewidzianych w prawie UE lub umowach międzynarodowych (w określonych przypadkach i trybach)¹². W rejestrze przetwarzane są dane osobowe¹³, w tym także dane daktyloskopijne, wizerunek, dane genetyczne, inne dane wrażliwe (np. pochodzenie rasowe lub etniczne)¹⁴.

Administratorem zbiorów danych jest Komendant Główny Policji, ale jego obowiązki w zakresie danych osobowych, co do zasady wykonują odpowiedni Dyrektorzy Komendy Głównej Policji¹⁵. Nadzór nad jakością i aktualnością informacji przetwarzanych przez KSIP jest zdecentralizowany – sprawują go kierownicy komórek organizacyjnych komend wojewódzkich Policji¹⁶. Zarządzenie określa także zasady nadawania, zmiany

¹¹ Zob. § 4, a zwłaszcza § 4 ust. 2 Zarządzenia o KSIP.

¹² Por. § 5 Zarządzenia o KSIP.

¹³ § 3 ust. 2 Zarządzenia o KSIP określa zakres przetwarzanych danych osobowych. Są to dane pozyskane m.in. na podstawie: art. 20 ust. 1-1d i 2ad-2ba ustawy o Policji, a także art. 20f ust. 1-3 ustawy o Policji w rejestrze wykroczeń, art. 20f ust. 13 ustawy o Policji, art. 16, art. 18f w zw. z art. 16 oraz art. 20 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2018 r. poz. 484 oraz z 2019 r. poz. 125), które zostały uzyskane przez Policję w związku z wymianą informacji, o której mowa w art. 20 ust. 2aa ustawy o Policji oraz pobrane i przekazane Komendantowi Głównemu Policji przez Policję, Agencję Bezpieczeństwa Wewnętrznego oraz Straż Graniczną na podstawie oraz na zasadach, w sposób i w trybie określonym w przepisach art. 10 ustawy o działaniach antyterrorystycznych oraz przepisach rozporządzenia PRM w sprawie pobierania danych osób niebędących obywatelami RP obejmujące: 1) wizerunek twarzy osób, o których mowa w art. 10 ust. 1 ustawy o działaniach antyterrorystycznych wraz z danymi osobowymi tych osób i informacją o podstawie prawnej utrwalenia oraz pobrania danych osobowych, 2) informacje o fakcie pobrania odcisków linii papilarnych lub materiału biologicznego od osób, o których mowa w art. 10 ust. 1 ustawy o działaniach antyterrorystycznych, informacje o oznaczeniu profilu DNA tych osób i jego zarejestrowaniu w zbiorze danych DNA, o którym mowa w art. 21a ust. 1 ustawy o Policji, a także informacje dotyczące zarejestrowania odcisków linii papilarnych tych osób w zbiorach danych daktyloskopijnych, o których mowa w art. 21h ust. 1 ustawy o Policji wraz z ich danymi osobowymi oraz informacją o podstawie prawnej pobrania.

¹⁴ Zob. § 17 ust. 2 pkt 6 Zarządzenia o KSIP.

¹⁵ § 5 Zarządzenia o KSIP.

¹⁶ Por. § 8, 8a Zarządzenia o KSIP.

oraz cofania uprawnień do przetwarzania danych osobowych w KSIP¹⁷, a także procedurę informowania o naruszeniu zasad przetwarzania danych osobowych¹⁸. Mimo, że KSIP – jak to zostało wcześniej wskazane – jest swego rodzaju „superzbiorem”, łączącym dane pochodzące z innych baz danych, to funkcjonuje częściowo niezależnie od nich. W konsekwencji, usunięcie danych z jednego zbioru nie oznacza automatycznego usunięcia danych z KSIP. Przepis § 109 ust. 2 zarządzenia o KSIP pozwala na dalsze przetwarzanie tych danych, mimo ich usunięcia z innych policyjnych rejestrów. W przypadku rejestru wykroczeń (§ 107 Zarządzenia KGP o KSIP) oraz innych rejestrów, wprost wskazano, że usunięcia dokonuje się „po weryfikacji”. W praktyce mechanika usuwania w KSIP może powodować, że dane (w szczególności identyfikatory i powiązania dotyczące AFIS/DNA) pozostają w KSIP, mimo usunięcia z właściwych baz źródłowych – zwłaszcza, gdy są przetwarzane równolegle na innej podstawie prawnej. To wymaga doprecyzowania ustawowego i jednoznacznych reguł retencji. Zarządzenie KGP o KSIP nie reguluje terminów przechowywania danych, a zastosowanie znajdują ogólne regulacje wynikające z ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości.

Chociaż w KSIP przetwarzane są różne rodzaje danych, różnych podmiotów w związku z realizowaniem przez Policję zadań ustawowych¹⁹, to poniższe uwagi będą odnosiły się tylko do przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości. Ograniczenie zakresu rozważań wiąże się z koniecznością zbadania zgodności przetwarzania danych osobowych w KSIP z prawem unijnym i Konstytucją. Niezgodność ta była już także sygnalizowana w piśmie Prezesa UODO z 17 maja 2024 r.²⁰ w związku z wydaniem przez TSUE wyroku w sprawie C-118/22²¹. Prezes UODO zwracał uwagę na czas przechowywania i przetwarzania danych osobowych osób podejrzanych i skazanych za przestępstwa, bez uwzględnienia charakteru popełnionego przez nich czynu zabronionego, a także na brak efektywnej kontroli sądowej nad zbiorem danych KSIP oraz braku ustawowej

¹⁷ Zob. rozdział 4 Zarządzenia o KSIP.

¹⁸ Zob. rozdział 4a Zarządzenia o KSIP.

¹⁹ Np. w związku ze statystką, czy informacje dotyczące osób, które usiłowały popełnić samobójstwo albo je popełniły.

²⁰ Pismo do Ministra ds. Europejskich można znaleźć na stronie: <https://uodo.gov.pl/pl/138/3117>.

²¹ Wyrok TSUE z 30 stycznia 2024 r., C-118/22, NG przeciwko Direktor na Glavna direktsia „Natsionalna politisia” pri Ministerstvo na vatreshnite raboti – Sofia; <https://curia.europa.eu/juris/document/document.jsf?jsessionid=9BE4DF7465B92C0A5916916778898F3C?text=&docid=282264&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=4848677>.

podstawy do przetwarzania danych osobowych. Mimo inicjatywy Prezesa UODO, przepisy nie zostały zmienione ani nie zostały podjęte żadne działania w celu wyeliminowania niezgodności prawa krajowego z przepisami unijnymi²².

I. Zasady przetwarzania danych osobowych, w tym danych genetycznych i biometrycznych w związku ze zwalczaniem i zapobieganiem przestępczości w prawie unijnym

Zasady gromadzenia, przetwarzania i przechowywania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości wynikają w pierwszej kolejności z art. 4 ust. 1 dyrektywy 2016/680. Obowiązkiem państw członkowskich UE jest zapewnienie, by dane osobowe były:

- a) przetwarzane zgodnie z prawem i rzetelnie;
- b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami;
- c) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;
- d) 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;
- e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;
- f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych²³.

W motywach do dyrektywy 2016/680 wyjaśniono, że zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych wymaga przetwarzania danych osobowych w szerszym kontekście.

Oznacza to, że **dane osobowe zebrane w związku z konkretnym czynem (postępowaniem karnym) mogą być przetwarzane także w innych sprawach,**

²² Z odpowiedzi Ministerstwa Spraw Wewnętrznych i Administracji skierowanej do Prezesa UODO wynika, że zdaniem Ministerstwa przepisy nie budzą wątpliwości odnośnie do zgodności z Konstytucją. Zob. odpowiedź o sygn. DPP-WNP.0164.2.2025.JK.

²³ Zob. motyw nr 28 i nast. do dyrektywy 2016/680.

jeśli celem jest zapobieganie i zwalczanie przestępczości oraz ustalenie powiązań pomiędzy różnymi, wykrytymi czynami zabronionymi²⁴. Konieczne jest jednak zagwarantowanie adekwatności przetwarzania danych osobowych oraz zbierania ich we właściwym zakresie w kontekście celów, jakie mają być realizowane. **„Należy w szczególności zapewnić, by zebrane dane osobowe nie były nadmierne i by okres ich przechowywania był nie dłuższy, niż jest to niezbędne do osiągnięcia celu ich przetwarzania”**. Przetwarzanie danych osobowych powinno odbywać się zgodnie z zasadą subsydiarności, tj. dopiero wtedy, gdy cel przetwarzania danych osobowych nie może zostać rozsądnie osiągnięty innymi sposobami. Konieczne jest także wdrożenie odpowiednich zabezpieczeń, by dane osobowe nie były przechowywane przez czas dłuższy, niż jest to niezbędne. Przepisy krajowe powinny zatem wprowadzać terminy usuwania danych lub ich okresowego przeglądu²⁵. W odniesieniu do danych wrażliwych – danych genetycznych, biometrycznych, dotyczących pochodzenia rasowego lub etnicznego, itp., przepisy prawa unijnego zwiększają rygoryzm przetwarzania danych osobowych. Zgodnie z art. 10 dyrektywy 2016/680 przetwarzanie takich danych jest dozwolone wyłącznie wtedy, jeśli jest to bezwzględnie niezbędne, podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, oraz:

- a) jest dopuszczone prawem Unii lub prawem państwa członkowskiego;
- b) jest niezbędne dla ochrony żywotnych interesów osoby fizycznej, której dane dotyczą, lub innej osoby; lub
- c) takie przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

W orzecznictwie TSUE wskazuje się, że art. 10 dyrektywy 2016/680 „służy zapewnieniu wzmocnionej ochrony osoby, której dane dotyczą, ponieważ ze względu na ich szczególną wrażliwość i kontekst, w jakim są one przetwarzane, rozpatrywane dane mogą powodować (...) poważne ryzyko naruszenia podstawowych praw i wolności, takich jak prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych, zagwarantowane w art. 7 i 8 Karty”²⁶. W konsekwencji przetwarzanie takich danych wymaga, poza ogólną podstawą prawną, spełnienia surowszych

²⁴ Zob. motyw nr 27 do dyrektywy 2016/680.

²⁵ Zob. motyw nr 26 do dyrektywy 2016/680.

²⁶ Wyrok TS z 28.11.2024 r., C-80/23, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3783743; pkt 53.

warunków: musi być dopuszczane prawem oraz podlegać odpowiednim zabezpieczeniom dla praw i wolności osób, których dane dotyczą, a ingerencja powinna spełniać rygorystycznie oceniany wymóg bezwzględnej niezbędności.

Zasady gromadzenia i przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości są stopniowo precyzowane w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej. Z perspektywy analizowanego zagadnienia istotne znaczenie ma pięć orzeczeń²⁷:

- wyrok TSUE z dnia 26 stycznia 2023 r., C-205/21²⁸;
- wyrok TSUE z dnia 16 listopada 2023 r., C-333/22²⁹;
- wyrok TSUE z dnia 30 stycznia 2024 r., C-118/22³⁰;
- wyrok TSUE z dnia 28 listopada 2024 r., C-80/23³¹;
- wyrok TSUE z dnia 20 listopada 2025 r., C-57/23³².

W wyroku w sprawie C-205/21 TSUE analizował, co oznacza wymóg dopuszczalności przetwarzania danych wrażliwych – danych genetycznych – zgodnie z prawem UE lub prawem państwa członkowskiego (art. 10 lit. a dyrektywy 2016/680). Trybunał uznał,

²⁷ Warto także obserwować orzecznictwo TSUE dotyczące ochrony danych osobowych i ich przetwarzania w związku z zapobieganiem i zwalczaniem przestępczości w odniesieniu do gromadzenia danych oraz ich przechowywania. Obecnie w Trybunale czekają na rozpoznanie pytania prejudycjalne dotyczące: 1. efektywności kontroli sądowej weryfikacji uprawnień administratora danych osobowych (sprawa C-333/22); 2. stopnia rozróżniania danych osobowych określonych kategorii podmiotów, a także zgodności ogólnego celu „zapobiegania i zwalczania przestępczości” jako podstawy przechowywania danych genetycznych na podstawie wewnętrznych regulacji policji (sprawa C-57/23); 3. dopuszczalności systematycznego zbierania danych identyfikacyjnych (odcisków palców i wizerunku) osób, co do których istnieje co najmniej jeden powód, by podejrzewać, że popełniły one przestępstwo, a także kwestii dopuszczalności odrębnego ścigania i skazania osoby, która odmówiła poddania się zebraniu danych identyfikacyjnych, nawet jeśli osoba ta nie była ścigana ani skazana za przestępstwo, które stanowiło podstawę zastosowania tego środka (sprawa C-371/24); 4. dopuszczalności przetwarzania danych osobowych (zebranych, zarejestrowanych i przechowywanych) oskarżonego, dotyczących miejsca urodzenia, narodowości, obywatelstwa, miejsca zamieszkania, wykształcenia, sytuacji rodzinnej i uprzedniej karalności, w sytuacji gdy zebrane w ten sposób dane osobowe w żaden sposób nie są niezbędne dla celów postępowania karnego (sprawa C-5/25).

²⁸ Wyrok TS z 26.01.2023 r., C-205/21, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3477462.

²⁹ Wyrok TS z 16.11.2023 r., C-333/22, LIGUE DES DROITS HUMAINS ASBL I BA PRZECIWKO ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE, LEX nr 3625790.

³⁰ Wyrok TS z 30.01.2024 r., C-118/22, NG PRZECIWKO DIREKTOR NA GLAVNA DIREKTSIA „NATSIONALNA POLITSIA “PRI MVR - SOFIA, LEX nr 3659240.

³¹ Wyrok TS z 28.11.2024 r., C-80/23, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3783743.

³² Wyrok TS z 20.11.2025 r., C-57/23, JH PRZECIWKO POLICEJNÍ PREZIDIUM, LEX nr 3943394.

że przepis ten należy interpretować zgodnie z art. 52 ust. 1 Karty Praw Podstawowych UE, a zatem wszelkie ograniczenia w korzystaniu z praw podstawowych muszą być „przewidziane ustawą”. **Wymóg ten zakłada istnienie jasnej i precyzyjnej**

podstawy prawnej zezwalającej na ograniczenie prawa do prywatności jednostki

³³. Przymusowe pobranie próbek do badań genetycznych i biometrycznych jest dopuszczalne, ale pod warunkiem istnienia skutecznej sądowej kontroli nad taką decyzją. Ponadto, muszą istnieć wystarczające dowody na to, że określona osoba popełniła przestępstwo umyślne ścigane z oskarżenia publicznego i odmawia dobrowolnego poddania się badaniom³⁴. Przepisy prawa krajowego powinny także dokonywać wyraźnego rozróżnienia pomiędzy gromadzeniem i przechowywaniem danych osobowych osób podejrzewanych o popełnienie przestępstwa, a danymi osób pokrzywdzonych, świadków oraz osób powiązanych ze świadkami lub pokrzywdzonymi³⁵.

Dopuszczając możliwość przymusowego pobierania danych genetycznych i biometrycznych, TSUE zastrzegł jednak, że przepisy prawa unijnego sprzeciwiają się rozwiązaniom krajowym, które pozwalają na systematyczne i uogólnione gromadzenie danych każdej osoby, której przedstawiono zarzuty. Gromadzenie i przechowywanie tego rodzaju danych wymaga szczególnego respektowania zasady minimalizacji danych i proporcjonalności. W przypadku danych genetycznych i biometrycznych (oraz innych danych wrażliwych z art. 10 dyrektywy 2016/680) należy wykazać ściśle określony cel pozyskania i przechowywania danych, ograniczyć go do niezbędnego zakresu (być może wystarczające jest pobranie danych biometrycznych, nie ma zatem konieczności pozyskiwania danych genetycznych), a także należy respektować zasadę proporcjonalności (dane powinny być gromadzone i przechowywane tylko w takim zakresie, w jakim jest to konieczne dla realizacji celów w postaci zapobiegania i zwalczania przestępczości). Rozwinięciem wyroku w sprawie C-205/21 jest orzeczenie TSUE z dnia 28 listopada 2024 r., w którym Trybunał wskazał, że sytuacja, w której to

³³ Por. wyrok TS z 26.01.2023 r., C-205/21, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3477462; pkt 64 i 65.

³⁴ Por. wyrok TS z 26.01.2023 r., C-205/21, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3477462; pkt 85 i 86.

³⁵ Por. wyrok TS z 26.01.2023 r., C-205/21, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3477462; pkt 83 i 84.

dopiero sąd ocenia spełnienie warunku „bezwzględnej niezbędności”³⁶, np. badając zasadność przechowywania danych albo dopuszczalność ich zgromadzenia, nie jest w stanie zapewnić odpowiedniej ochrony prawnej osobom, których pobranie danych dotyczyło³⁷. To organ, który dokonuje pobrania danych – organ postępowania przygotowawczego – jest w pierwszej kolejności zobowiązany do analizy konieczności i przydatności pozyskania danych wrażliwych, a w związku z tym – do stosowania w praktyce zasady proporcjonalności i minimalizacji danych osobowych.

Kolejnym istotnym orzeczeniem jest wyrok TSUE w sprawie C-333/22, dotyczący kwestii **istnienia „skutecznego środka prawnego” przeciwko decyzjom organów policyjnych dotyczących przetwarzania danych osobowych**³⁸. Zgodnie bowiem z art. 17 ust. 1 dyrektywy 2016/680 „w odniesieniu do przypadków, o których mowa w art. 13 ust. 3, art. 15 ust. 3 i art. 16 ust. 4 tej dyrektywy, państwa członkowskie mają obowiązek przyjęcia środków przewidujących, że „osoba, której dane dotyczą, może wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego”. Cel przetwarzania danych osobowych na podstawie dyrektywy 2016/680 wymaga umożliwienia organom państwowym – powołanym do zapobiegania i zwalczania przestępczości efektywnego działania. W związku z tym przepisy unijne pozwalają na ograniczenie bezpośrednio wykonywania prawa do informacji o przetwarzaniu danych osobowych, a także prawa dostępu „w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należyтым uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej”, aby „uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub

³⁶ W pkt 58 wyroku w sprawie C-80/23 TSUE wskazał, że „Należy zatem stwierdzić, że wykładnia prawa krajowego, w ramach której sąd odsyłający zamierza sam ocenić, czy zbieranie danych biometrycznych i genetycznych osoby, której dane dotyczą, jest 'bezwzględnie niezbędne', nie może zagwarantować zgodności z prawem Unii ustawodawstwa krajowego takiego jak to, o którym mowa w pkt 57 niniejszego wyroku, jako że nie pozwala ona w każdym razie zaradzić brakowi ciężącego na właściwych organach na mocy tego ustawodawstwa obowiązku weryfikacji i wykazania 'bezwzględnej niezbędności' takiego zbierania danych”³⁶. Zob.: wyrok TS z 28.11.2024 r., C-80/23, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3783743, pkt 58. Zob. także pkt 56 i 57 wskazanego orzeczenia.

³⁷ Zob.: wyrok TS z 28.11.2024 r., C-80/23, MINISTERSTVO NA VATRESHNITE RABOTI, GLAVNA DIREKTSIA ZA BORBA S ORGANIZIRANATA PRESTAPNOST PRZECIWKO V.S., LEX nr 3783743, pkt 59-61.

³⁸ Stan faktyczny, jaki zainicjował pytanie prejudycjalne był następujący. Skarżąca zwróciła się do belgijskiego organu ochrony danych o wykonanie jej prawa do informacji na temat przetwarzania jej danych osobowych przez policję. Organ ten przeprowadził weryfikację, ale poinformował ją wyłącznie o „zakończeniu sprawdzenia” – bez żadnych dalszych szczegółów.

procedur”, „uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar”, „chronić bezpieczeństwo publiczne”, „chronić bezpieczeństwo narodowe” lub „chronić prawa i wolności innych osób”. Ponadto art. 15 ust. 3 tej dyrektywy przewiduje, że administrator może nie informować osoby, której dane dotyczą, o każdej odmowie lub o każdym ograniczeniu dostępu i o przyczynach tej odmowy lub tego ograniczenia, jeżeli udzielenie tych informacji godziłoby w którykolwiek z wyżej wymienionych celów uzasadnionych interesem publicznym³⁹. **W takiej sytuacji, prawa osoby, której dane osobowe się przetwarza, wykonywane są za pośrednictwem organu nadzorczego, niezależnego od administratora danych osobowych.** TSUE wskazał ponadto, że art. 46 ust. 1 lit. g) dyrektywy 2016/680 wymaga, aby „każdemu właściwemu organowi krajowemu powierzono zadanie sprawdzenia zgodności przetwarzania z prawem na podstawie art. 17 tej dyrektywy, czyli wskutek wniosku opierającego się na tym ostatnim przepisie”. Osoba, której dane osobowe są przetwarzane, powinna mieć jednak możliwość zainicjowania sądowej kontroli zasadności, prawidłowości, a także weryfikacji sposobu, w jaki organ nadzorczy wywiązał się ze spoczywającego na nim obowiązku „przeprowadzenia wszelkich niezbędnych weryfikacji”⁴⁰. Należy zatem przekazać jej taki zakres informacji, który pozwoli realnie skorzystać z drogi sądowej. Chociaż ograniczenia w zakresie informowania o przetwarzaniu danych osobowych są dopuszczalne, m.in. z uwagi na bezpieczeństwo narodowe, to nie mogą one naruszać istoty prawa do

³⁹ Por.: wyrok TS z 16.11.2023 r., C-333/22, LIGUE DES DROITS HUMAINS ASBL I BA PRZECIWKO ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE, LEX nr 3625790, pkt 42.

⁴⁰ Por. wyrok TS z 16.11.2023 r., C-333/22, LIGUE DES DROITS HUMAINS ASBL I BA PRZECIWKO ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE, LEX nr 3625790, pkt 52. Chodzi o możliwość zainicjowania sądowej kontroli, wtedy, kiedy osoba otrzymała jedynie informację, że weryfikacja prawidłowości przetwarzania danych osobowych została zakończona.

informacji i prawa dostępu do danych osobowych, a nadto – muszą być proporcjonalne i uzasadnione⁴¹.

W sprawie C-118/22 spornym zagadnieniem była dopuszczalność przechowywania danych osobowych, w tym danych biometrycznych i genetycznych, osób skazanych za przestępstwa przez nieograniczony czas, mimo zatarcia skazania. Trybunał uznał, że państwa powinny wprowadzić odpowiednie⁴² terminy usuwania danych osobowych lub okresowego przeglądu konieczności przechowywania danych, a także zagwarantować środki proceduralne służące zapewnieniu przestrzegania tych terminów⁴³. Przepisy dyrektywy 2016/680⁴⁴ nie przewidują jednak wprowadzenia bezwzględnych ograniczeń czasowych przechowywania danych osobowych, po upływie których powinny one zostać usunięte⁴⁵. Niekiedy bowiem dalsze przechowywanie i przetwarzanie danych osobowych osób skazanych (w tym także w sytuacji, kiedy skazanie zostało już zatarte) może przyczynić się do realizacji celu ogólnego dyrektywy 2016/680. Nie można wykluczyć, że osoby takie mogą brać udział w popełnianiu przestępstw innych niż te, za które zostały skazane⁴⁶. TSUE zwrócił jednak uwagę na kwestię poszanowania zasady proporcjonalności oraz wagi przestępstwa (społeczną szkodliwość). **„Nie jest tak, że w stosunku to wszystkich osób prawomocnie skazanych za przestępstwo objęte tym pojęciem istnieje taki sam stopień ryzyka udziału w popełnieniu innych przestępstw, co uzasadniałoby jednolity okres przechowywania dotyczących ich**

⁴¹ Zob. pkt 67 wyroku TSUE, gdzie Trybunał wskazał, że do państw członkowskich należy jednak w ramach ich autonomii proceduralnej wdrożenie środków niezbędnych do zagwarantowania, zgodnie z art. 53 ust. 1 tej dyrektywy, **skutecznej kontroli sądowej zarówno istnienia i zasadności powodów uzasadniających ograniczenie przekazywania informacji**, jak i prawidłowego wykonania przez organ nadzorczy jego zadania polegającego na weryfikacji zgodności przetwarzania z prawem. „W tym względzie ujęte w tym ostatnim przepisie pojęcie „skutecznego środka prawnego przed sądem” należy interpretować w świetle motywu 86 wspomnianej dyrektywy, zgodnie z którym **sądy, przed którymi wszczęto postępowania przeciwko organowi nadzorczemu, „powinny wykonywać pełną jurysdykcję w sprawie, w tym w zakresie ustalenia okoliczności faktycznych i prawnych istotnych dla rozstrzygnięcia sprawy”**.

⁴² Por. art. 5 dyrektywy 2016/680.

⁴³ Por. wyrok TS z 30.01.2024 r., C-118/22, NG PRZECIWKO DIREKTOR NA GLAVNA DIREKTSIA „NATSIONALNA POLITSIA” PRI MVR - SOFIA, LEX nr 3659240, pkt 43 i 44.

⁴⁴ Por. art. 16 dyrektywy 2016/680.

⁴⁵ Por. wyrok TS z 30.01.2024 r., C-118/22, NG PRZECIWKO DIREKTOR NA GLAVNA DIREKTSIA „NATSIONALNA POLITSIA” PRI MVR - SOFIA, LEX nr 3659240, pkt 52.

⁴⁶ Samo bowiem zatarcie skazania nie czyni zbędnym przechowywanie danych. Por. pkt 70 i nast. opinii Rzecznika Generalnego Piritia Pikamae z dnia 15 czerwca 2023 r.; <https://curia.europa.eu/juris/document/document.jsf?text=&docid=274651&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=7225299>.

danych. I tak, w niektórych przypadkach, biorąc pod uwagę czynniki takie jak charakter i waga popełnionego przestępstwa lub brak powrotu do przestępstwa, ryzyko, jakie stanowi osoba skazana, niekoniecznie będzie uzasadniać utrzymanie do chwili jej śmierci dotyczących jej danych w przewidzianym w tym celu krajowym rejestrze policyjnym. W takich przypadkach nie będzie już niezbędnego związku między przechowywanymi danymi a zamierzonym celem. Ich przechowywanie nie będzie zatem zgodne z zasadą minimalizacji danych ustanowioną w art. 4 ust. 1 lit. c) dyrektywy 2016/680 i będzie wykraczać poza okres niezbędny do celów, dla których są one przetwarzane, wbrew art. 4 ust. 1 lit. e) tej dyrektywy”.

Systemowe, długotrwałe przechowywanie danych biometrycznych i genetycznych (oraz innych danych osobowych) osób podejrzewanych i skazanych za przestępstwa stwarza wysokie ryzyko niezgodności z art. 10 dyrektywy 2016/680, zwłaszcza gdy ma charakter masowy, niezróżnicowany i oparty na automatyzmie, bez realnych, egzekwowalnych mechanizmów przeglądu i usuwania. Niezróżnicowane (co do rodzaju przestępstwa i potencjalnego ponownego wejścia w konflikt z prawem) i masowe przetwarzanie danych narusza zasadę proporcjonalności⁴⁷. Przechowywanie danych biometrycznych i genetycznych osób prawomocnie skazanych – nawet dożywotnio – może być uzasadnione, np. w celu umożliwienia ścigania innych przestępstw, także po dłuższym czasie od ich popełnienia. Warunkiem jest jednak spełnienie przesłanki bezwzględnej konieczności z art. 10 dyrektywy 2016/680.

Oznacza to, że praktyka taka musi uwzględniać indywidualne okoliczności – takie jak charakter i waga popełnionego przestępstwa, jego kontekst, związek z innymi sprawami karnymi czy uprzednią karalność danej osoby. Państwa członkowskie UE są zobowiązane – na podstawie art. 5 dyrektywy 2016/680 – do określenia odpowiednich terminów przechowywania danych osobowych. TSUE podkreśla, że termin taki może być uznany za odpowiedni wyłącznie wtedy, gdy **uwzględnia konkretne, istotne okoliczności uzasadniające przechowywanie danych. Samo odniesienie do śmierci osoby, której dane dotyczą, nie może być domyślnie uznane za proporcjonalny i uzasadniony okres przechowywania, zwłaszcza jeśli stosuje się je automatycznie wobec wszystkich skazanych.**

Na uwagę zasługuje także najnowszy wyrok TSUE z dnia 20 listopada 2025 r. w sprawie C-57/23, który m.in. analizował kwestię podstawy prawnej przetwarzania danych

⁴⁷ Decyzja ETPC z 16.01.2007 r., 30562/04, S. I MARPER v. WIELKA BRYTANIA, LEX nr 245147.

osobowych w związku z zapobieganiem i zwalczaniem przestępczości. W tym orzeczeniu TSUE, odwołując się do orzecznictwa ETPC wskazał, że „każdy akt stanowiący podstawę prawną przetwarzania danych osobowych powinien posiadać określone cechy, a mianowicie zasadniczo powinien on być przede wszystkim zgodny z normami wyższego rzędu, następnie – dostępny, i wreszcie – **wystarczająco przewidywalny, to znaczy w rozsądnym stopniu w okolicznościach danej sprawy, by umożliwić zainteresowanym jednostkom odpowiednie dostosowanie ich zachowania, co oznacza, że akt ten wystarczająco wyraźnie określa zakres i warunki wykonywania uprawnień przyznanych właściwym organom**”⁴⁸. W prawie unijnym, a zwłaszcza w kontekście art. 8 i 10 dyrektywy 2016/680, pojęcie „prawo państwa członkowskiego” należy rozumieć jako przepisy o charakterze generalnym ustanawiające minimalne warunki zbierania, przechowywania i usuwania takich danych. TSUE zaakceptował, że w pewnych konfiguracjach normatywnych doprecyzowanie „minimalnych warunków” zbierania, przechowywania i usuwania danych może następować również poprzez linię orzecniczą sądów krajowych, ale tylko przy spełnieniu wymogu dostępności i przewidywalności tej wykładni oraz przy zachowaniu standardu jasnych, kontrolowalnych granic uznania organu. Na tym tle rozwiązanie, w którym kluczowe elementy przetwarzania, usuwania i kryteriów dalszego przechowywania danych są kształtowane w aktach wewnętrznych lub „regułach” niewyrażonych w przepisie generalnym, a skierowanych do „wewnątrz” organów policyjnych, nie spełnia standardu „quality of law” (dostępność, jasność, przewidywalność) wymaganego dla ingerencji w prawa z art. 7 i 8 Karty.

Podsumowując wymagania, jakie wynikają z prawa unijnego względem ustawodawcy krajowego w odniesieniu do gromadzenia, przechowywania i przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości:

1. **Musi istnieć podstawa prawna w przepisach powszechnie obowiązującego prawa pozwalająca na gromadzenie, przetwarzanie i przechowywanie danych osobowych.** Na gruncie standardu unijnego kluczowa jest jakość podstawy prawnej (quality of law), natomiast w porządku krajowym – ze względu na art. 51 Konstytucji – zasady i tryb gromadzenia oraz udostępniania danych powinny wynikać z ustawy, a w odniesieniu do danych z art. 10 dyrektywy 2016/680 wymóg ten jest

⁴⁸ Por. Pkt 57 i cytowane tam orzecznictwo wyroku TS z 20.11.2025 r., C-57/23, JH PRZECIWKO POLICEJNÍ PREZIDIUM, LEX nr 3943394.

szczególnie rygorystyczny. W tych sytuacjach, standard legislacyjny (miejsca aktu prawnego w hierarchii źródeł prawa) jest wyższy i co do zasady wszelkie operacje na danych wrażliwych powinny mieć podstawę ustawową;

2. **Zakres gromadzenia danych osobowych osób podejrzewanych o popełnienie przestępstwa musi być zróżnicowany w odniesieniu m.in. do wagi przestępstwa.** Niedopuszczalne jest gromadzenie danych biometrycznych i genetycznych w każdej sprawie karnej (w każdej sprawie o przestępstwo). Dane te powinny być gromadzone tylko wtedy, gdy jest to bezwzględnie konieczne (art. 10 dyrektywy 2016/680). Oceny zasadności i „bezwzględnej konieczności” muszą dokonywać organy policyjne decydujące o potrzebie pobrania danych biometrycznych i genetycznych, ponieważ następca kontrola sądowa nie gwarantuje odpowiedniego zabezpieczenia praw osoby podejrzanej;
3. **Odmienne zasady w odniesieniu do zakresu i sposobu gromadzenia danych osobowych powinny istnieć w odniesieniu do osób podejrzewanych o popełnienie przestępstwa oraz do osób pokrzywdzonych, świadków i innych.** W przypadku osób podejrzewanych o popełnienie przestępstwa, możliwość przymusowego pobrania danych genetycznych i biometrycznych (oraz innych danych wrażliwych) nie jest wykluczona, bowiem służby państwowe powinny mieć możliwość skutecznego realizowania swoich funkcji;
4. **Przepisy krajowe powinny umożliwiać sądową kontrolę (weryfikację) przetwarzania danych osobowych.** W związku ze specyfiką przetwarzania danych osobowych dla realizacji celów z dyrektywy 2016/680, niekiedy jest konieczne ograniczenie bezpośredniego wykonywania praw osoby, której dane osobowe są przetwarzane, i zagwarantowanie, by były wykonywane one pośrednio – przez niezależny organ nadzorczy, odrębny od administratora danych osobowych. Od decyzji niezależnego organu nadzorczego powinno przysługiwać prawo do zainicjowania sądowej kontroli – weryfikacji – prawidłowości przetwarzania danych osobowych. Sądowa kontrola powinna być efektywna, co oznacza, że uzasadnienie decyzji organu nadzorczego musi być odpowiednio precyzyjne, by stwarzać szansę polemizowania z argumentacją, jaka leżała u podstawy rozstrzygnięcia. Kontrola ta nie może być ograniczona do zagadnień technicznych (formalnych), ale powinna odnosić się także do kwestii merytorycznych;

5. **Przechowywanie danych osobowych, a zwłaszcza czas ich przechowywania powinien uwzględniać zasadę minimalizacji danych osobowych i być ograniczony do tego, co jest konieczne.** Przy ocenie przydatności dalszego przechowywania danych osobowych należy brać pod uwagę przede wszystkim wagę przestępstwa oraz realność ponownego wejścia w konflikt z prawem. Niedopuszczalne jest bezterminowe przechowywanie danych genetycznych i biometrycznych w każdej sprawie.

II. Ocena zgodności krajowych rozwiązań z prawem unijnym

Oceniając zgodność rozwiązań krajowych z wymogami, jakie płyną z prawa unijnego – art. 4 dyrektywy 2016/680 oraz orzecznictwa TSUE – wątpliwości pojawiają się przede wszystkim w kontekście zasad gromadzenia, przechowywania i przetwarzania danych biometrycznych, genetycznych i innych danych wrażliwych z art. 10 dyrektywy 2016/680, a także dotyczą one sposobu funkcjonowania KSIP.

II.1. Podstawa prawna funkcjonowania KSIP

W przypadku KSIP **pierwsza wątpliwość odnosi się do podstawy prawnej funkcjonowania tego zbioru danych.** Jediną ustawową podstawą funkcjonowania KSIP jako odrębnego systemu jest art. 21nb ustawy o Policji. Pozostałe przepisy ustawy o Policji (np. dotyczące rejestru wykroczeń, czy SWD) regulują podstawy pobierania i pozyskiwania określonych kategorii danych. Sam KSIP działa przede wszystkim na podstawie zarządzenia Komendanta Głównego Policji. Zarządzenia są aktami wewnętrznymi – skierowanymi do „wewnątrz” jednostek organizacyjnych. Zarządzenie Komendanta Głównego Policji obowiązuje jednostki organizacyjne podległe Komendantowi oraz funkcjonariuszy Policji. Nie może ono stanowić podstawy decyzji wobec ogółu obywateli, czy innych podmiotów. Nie kreuje zatem uprawnień dla ogółu obywateli ani nie może nakładać na nich żadnych obowiązków. Nie może także stanowić podstawy ograniczenia praw i wolności obywatelskich⁴⁹.

⁴⁹ Por. art. 31 ust. 3 Konstytucji, tj. przepis, który reguluje podstawy i granice dopuszczalnego limitowania praw i wolności jednostki. Katalog źródeł prawa wynika z art. 87 Konstytucji. Ma charakter zamknięty. Akty prawa wewnętrznego – prawa wewnętrznie obowiązującego – unormowano w art. 93 Konstytucji. Zob. szerzej: P. Radzewicz [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz, wyd. II*, red. P. Tuleja, Warszawa 2023, art. 87.

Chociaż prawo unijne nie wymaga każdorazowego uregulowania kwestii przetwarzania danych osobowych w akcie prawnym o randze ustawy⁵⁰, to zasady przetwarzania (oraz inne działania wykonywane na danych osobowych) powinny mieć podstawę w przepisach powszechnie obowiązującego prawa. Z perspektywy prawa UE kluczowe jest, aby zasadnicze reguły przetwarzania wynikały z takiego aktu – niezależnie od jego formy w krajowej hierarchii źródeł prawa. Warto jednak zauważyć, że polska Konstytucja wprowadza wyższy standard ochrony danych osobowych niż wynika to z prawa unijnego. Zgodnie z art. 51 ust. 1 ustawy zasadniczej, jednostka może być zobowiązana wyłącznie na podstawie ustawy do ujawnienia danych niej dotyczących. Także tylko ustawa może ograniczać prawo dostępu do urzędowych dokumentów i zbiorów danych (art. 51 ust. 3 Konstytucji). Ponadto zasady i tryb gromadzenia oraz udostępniania danych osobowych muszą zostać określone w ustawie (art. 51 ust. 5 Konstytucji). Z perspektywy prawa Unii (w szczególności art. 8 i 10 dyrektywy 2016/680) minimalnym wymogiem jest, aby kluczowe reguły przetwarzania danych wynikały z aktu powszechnie obowiązującego, dostępnego i przewidywalnego dla jednostki. Na gruncie art. 51 Konstytucji zasady i tryb gromadzenia oraz udostępniania danych muszą wynikać z ustawy, a w odniesieniu do danych wrażliwych wymóg ten powinien być traktowany szczególnie rygorystycznie. Oznacza to, że zasadnicze elementy KSIP (zakres danych, cele, retencja, usuwanie, kontrola) powinny być uregulowane ustawowo, a ewentualne akty wykonawcze mogą co najwyżej doprecyzowywać kwestie techniczne w granicach delegacji ustawowej do wydania rozporządzenia.

W przypadku KSIP podstawa do gromadzenia danych znajduje się w ustawie (ustawach), ale z przepisów ustawowych nie wynika, że dane osoby, która miała kontakt z Policją⁵¹, zostaną wprowadzone do systemu informacyjnego Policji, a następnie będą przechowywane i przetwarzane. Całość funkcjonowania KSIP została określona w zarządzeniu, czyli akcie prawnym o charakterze wewnętrznym. Dostęp do zbiorów KSIP jest ograniczony – w pierwszej kolejności z uwagi na brak informacji o tym systemie, przekazywanej osobie, która ma kontakt z funkcjonariuszem Policji.

⁵⁰ P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II*, Warszawa 2022, art. 6.

⁵¹ Np. była legitymowana. Zob. § 43 ust. 1 pkt 8 Zarządzenia KGP o KSIP. Dane są wprowadzane także wtedy, gdy osoba jest poddawana kontroli osobistej.

Wykonywanie uprawnień w związku z np. naruszeniem bezpieczeństwa danych osobowych nie jest bezpośrednie. Administrator danych nie ma obowiązku informowania osoby, której dane osobowe pobrano, o naruszeniach albo zagrożeniu dla bezpieczeństwa danych. Informacje takie są przekazywane Prezesowi Urzędu Danych Osobowych⁵². Pośrednie wykonywanie uprawnień nie jest samo w sobie wykluczone na gruncie prawa unijnego. W modelu przyjętym dla KSIP budzi jednak poważne wątpliwości konstytucyjne co do standardu z art. 51 (zwłaszcza w zakresie ustawowej podstawy i granic ograniczenia prawa dostępu do zbiorów oraz realnej kontroli sądowej). Ponadto, osoba, której dane osobowe są przetwarzane, powinna mieć możliwość zainicjowania sądowej kontroli zasadności, prawidłowości, a także weryfikacji sposobu, w jaki organ nadzorczy wywiązał się ze spoczywającego na nim obowiązku „przeprowadzenia wszelkich niezbędnych weryfikacji”. Tymczasem, także w tym zakresie prawo do informacji oraz prawo dostępu do informacji został ograniczony aktem prawnym niebędącym źródłem powszechnie obowiązującego prawa i niebędącym ustawą.

Warto podkreślić, że ustawodawca zdaje się dostrzegać problematyczny charakter podstaw prawnych funkcjonowania KSIP – przynajmniej w odniesieniu do danych biometrycznych i genetycznych. W ustawie z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu⁵³ zmieniany jest art. 21nb ustawy o Policji, dodając przepisy szczególne odnoszące się do przetwarzania wizerunku oraz danych daktyloskopijnych⁵⁴. **Poza zakresem proponowanych zmian pozostają jednak dane genetyczne. Dodatkowo, należy zwrócić uwagę na czas, kiedy ustawa z 18 października 2024 r. wejdzie w życie.** Dokładny dzień wejścia w życie tych przepisów jest powiązany z uruchomieniem systemu EES (start operacyjny: 12 października 2025 r., wdrożenie etapowe; pełna operacyjność: 10 kwietnia 2026

⁵² Por. § 6 zarządzenia KGP o KSIP.

⁵³ Ustawa z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu (Dz. U. poz. 1688).

⁵⁴ Zob. art. 19 pkt 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu

r.)⁵⁵ i przyjęciem przez Komisję Europejską stosownych regulacji⁵⁶. Stopniowe wdrażanie tego systemu rozpoczęło się 12 października 2025 r.⁵⁷ i będzie kontynuowane przez kolejne 6 miesięcy. Niemniej wydaje się, że konieczne jest odrębne i kompleksowe uregulowanie kwestii przetwarzania danych osobowych przez Policję w KSIP w innej ustawie.

II.2. Zakres gromadzenia i przetwarzania danych osobowych osób podejrzewanych o popełnienie przestępstwa

Druga wątpliwość, jaka wiąże się z funkcjonowaniem KSIP, to **zakres gromadzenia i przetwarzania danych osobowych osób podejrzewanych o popełnienie przestępstwa**. W zbiorze „Osoba” gromadzi się i przetwarza się szeroki zestaw informacji o osobach, które podejrzewa się o popełnienie przestępstwa albo czynu karalnego (w przypadku nieletnich)⁵⁸. Rejestrowani są nie tylko podejrzani o popełnienie przestępstwa w znaczeniu procesowym⁵⁹, ale także m.in. osoby, które podejrzewa się o popełnienie wykroczenia, osoby naruszające przepisy ruchu drogowego⁶⁰, czy osoby, które zostały wylegitymowane⁶¹. Zgodnie z art. 51 ust. 2 Konstytucji, władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych

⁵⁵ Entry-Exit System. Unijny system wjazdu i wyjazdu. Zob.: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz. U. UE. L. z 2017 r. Nr 327, str. 20 z późn. zm.).

⁵⁶ Por. 26 ustawy z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu. O wejściu w życie systemu EES decyduje Komisja Europejska po tym, jak spełnione zostaną następujące warunki: a) przyjęto środki, o których mowa w art. 36 i w art. 50 ust. 4 i 5 rozporządzenia 2017/2226; b) eu-LISA oświadczyła, że z pozytywnym wynikiem zakończono wszechstronny test EES, który eu-LISA przeprowadza we współpracy z państwami członkowskimi; c) państwa członkowskie zatwierdziły uzgodnienia techniczne i prawne dotyczące zbierania i przekazywania danych, o których mowa w art. 16-20, do EES i powiadomiły o nich Komisję; d) państwa członkowskie przekazały Komisji powiadomienia, o których mowa w art. 65 ust. 1, 2 i 3.

⁵⁷ Zob. komunikat na stronie: <https://www.gov.pl/web/katar/nowy-system-wjazdu-wyjazdu--wdrozenie-od-12-pazdziernika-2025-r> oraz <https://travel-europe.europa.eu/pl/ees>.

⁵⁸ Por. § 16 Zarządzenia KGP o KSIP.

⁵⁹ Por. § 17 Zarządzenia KGP o KSIP.

⁶⁰ § 16 ust. 1 pkt 16 Zarządzenia KGP o KSIP.

⁶¹ Zob. art. 15 ust. 1 ustawy o Policji. Warto przypomnieć wcześniejsze wystąpienie RPO w kwestii legitymowania i istnienia uzasadnionego powodu do legitymowania: <https://bip.brpo.gov.pl/pl/content/rpo-policja-obywatel-legitymowanie-uniemozliwianie-czynnosci-kgp-odpowiedz>. Pojawia się pytanie, czy każda osoba, która została wylegitymowana, znajduje się rejestrze KSIP, a jeśli tak – to jaki jest zakres przetwarzania danych osobowych.

informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. W zarządzeniu KGP o KSIP zakres gromadzonych danych o jednostce jest uporządkowany od tzw. rejestracji procesowej (najszerzy zakres)⁶² w przypadku popełnienia przestępstwa ściganego z oskarżenia publicznego lub przestępstwa skarbowego⁶³ do rejestracji osób, które zostały legitymowane⁶⁴. Rejestracja osoby legitymowanej zawiera:

- „1) nazwę jednostki lub komórki organizacyjnej Policji dokonującej rejestracji;
- 2) identyfikator kadrowy odpowiednio osoby dokonującej rejestracji oraz zlecającej rejestrację, jeżeli rejestracji dokonano na zlecenie;
- 3) numer PESEL, jeżeli jest znany;
- 4) powód (przyczynę) legitymowania;
- 5) identyfikator kadrowy policjanta dokonującego legitymowania;
- 6) datę, godzinę i miejsce legitymowania;
- 7) określenie rodzaju i numeru dokumentu tożsamości, którym osoba legitymowana się posługuje lub dokumentu, na podstawie którego ustalono tożsamość tej osoby;
- 8) określenie rodzaju, marki, typu lub numeru rzeczy posiadanych przez osobę legitymowaną;
- 9) określenie związku legitymowania z imprezą masową (identyfikator imprezy masowej RIM);

⁶² Zakres gromadzonych danych obejmuje – w przypadku rejestracji procesowej – także dane wrażliwe: ujawniające pochodzenie rasowe lub etniczne; ujawniające poglądy polityczne, przekonania religijne, światopoglądowe lub przynależność do związków zawodowych; stanowiące dane genetyczne w rozumieniu art. 4 pkt 4 ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w zakresie danych dotyczących wyników analizy kwasu deoksyrybonukleinowego (DNA) wyłącznie o niekodującej części DNA, o których mowa w pkt 3; stanowiące dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej w rozumieniu art. 4 pkt 2 ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w tym w zakresie wizerunku twarzy utrwalonego w postaci zdjęć sygnalitycznych lub danych daktyloskopijnych, o których mowa w pkt 1 i 2; dotyczące zdrowia w rozumieniu art. 4 pkt 3 ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości; dotyczące seksualności i orientacji seksualnej (§ 17 ust. 3 pkt 13 Zarządzenia KGP o KSIP).

⁶³ § 17 Zarządzenia KGP o KSIP.

⁶⁴ § 23 Zarządzenia KGP o KSIP.

10) określenie rodzaju i wyniku czynności służbowych podjętych wskutek legitymowania”⁶⁵. Dodatkowo, rejestracja osoby legitymowanej może zawierać informacje, takie jak w przypadku rejestracji procesowej z § 17 ust. 2 pkt 1-10⁶⁶.

Z uwagi na powszechność legitymowania⁶⁷, wydaje się, że Policja mogła zgromadzić obszerny zbiór (big data) danych o jednostkach, obejmujący osoby podejrzewane o poważne przestępstwa jak i drobne wykroczenia, a także – zachowania niestanowiące żadnego czynu zabronionego, które jednak skutkowały podjęciem działań przez Policję. Sama potencjalna przydatność informacji i możliwość wykorzystania ich w celu zapobiegania i zwalczania przestępczości nie jest wystarczająca dla ingerencji w prawo do prywatności, **zwłaszcza w sytuacji, gdy dane znajdujące się w zbiorze KSIP będą przetwarzane, mogą zostać powiązane z informacjami, które znajdują się w innych rejestrach, nie tylko policyjnych, do których KSIP może mieć dostęp.**

Wątpliwości – poza rejestracją procesową, w związku z przedstawieniem zarzutu popełnienia przestępstwa – budzą także podstawy prawne do podawania tak szczegółowych informacji o osobie, która nie jest w żadnym aspekcie zaangażowana w postępowanie karne.

W przypadku rejestracji procesowej⁶⁸ w zakresie danych obejmujących dane genetyczne i biometryczne, problematyczna jest podstawa prawna pozwalająca

⁶⁵ § 23 ust. 3 Zarządzenia KGP o KSIP.

⁶⁶ 1) nazwiska (aktualne oraz poprzednio używane);

2) imiona (aktualne oraz poprzednio używane);

3) imiona rodziców i nazwisko rodowe matki;

4) datę i miejsce urodzenia;

5) posiadane obywatelstwo lub obywatelstwa;

6) narodowość;

7) płeć;

8) numer PESEL, jeżeli osoba rejestrowana go posiada;

8a) numer narodowy stanowiący numer identyfikujący osobę w państwie innym niż Rzeczypospolita Polska (odpowiednik numeru PESEL) oraz państwo (kraj), w którym osoba posiada ten numer, w przypadku, gdy osoba ta nie posiada numeru PESEL;

9) miejsca zameldowania i pobytu (miejsca zamieszkania), w tym adres lub adresy;

10) rodzaj i numer dokumentu tożsamości, którym osoba się posługuje lub dokumentu, na podstawie którego ustalono tożsamość osoby;

⁶⁷ RPO informował o praktyce, kiedy funkcjonariusz Policji miał obowiązek wylegitymować 3 osoby dziennie. Brak jest publicznie dostępnych danych dotyczących liczby legitymowań w skali roku.

⁶⁸ Na marginesie warto zauważyć, że rejestracja procesowa do 2019 r. była dokonywana na podstawie przepisów ustawy o Policji – art. 20 ust. 2a. Przepis art. 20 ust. 2a uchylony przez art. 58 pkt 6 lit. c ustawy z dnia 14 grudnia 2018 r. (Dz.U.2019.125) zmieniającej nin. ustawę z dniem 6 lutego 2019 r.

na ich zebranie. Wydaje się, że jedyną podstawą jest art. 74 § 2 k.p.k.⁶⁹, który umożliwia pobranie m.in. odcisków palców czy próbek do badań porównawczych w każdej sprawie o przestępstwo lub przestępstwo skarbowe. Możliwe jest także zastosowanie środków przymusu bezpośredniego wobec oskarżonego lub osoby podejrzanej, jeśli nie chce ona dobrowolnie poddać się tym czynnościom (art. 74 § 3a k.p.k.). Przepisy wprost nie odnoszą się do możliwości pobrania danych biometrycznych i genetycznych od pokrzywdzonego oraz świadka, w tym zastosowania wobec tego uczestnika postępowania środków przymusu bezpośredniego. Jedynie art. 192 § 1 k.p.k. stanowi, że „jeżeli karalność czynu zależy od stanu zdrowia pokrzywdzonego, nie może on sprzeciwić się oględzinom i badaniom niepołączonym z zabiegiem chirurgicznym lub obserwacją w zakładzie leczniczym”. Prawo do odmowy poddania się badaniom przysługuje jedynie osobom, które mogą odmówić składania zeznań (art. 182 k.p.k.) albo zostały zwolnione z zeznawania (art. 185 k.p.k.). W ramach badań i oględzin dopuszczalne jest pobranie próbek do badań genetycznych i biometrycznych.

Brak jest jednak różnicowania dopuszczalności gromadzenia danych biometrycznych lub genetycznych⁷⁰. Z danych dostępnych publicznie, wydaje się, że dane genetyczne i biometryczne są gromadzone zgodnie z zasadą proporcjonalności. W 2024 r.⁷¹ w bazie AFIS przybyło 160.845 nowych wpisów, a w bazie danych genetycznych - 45 625⁷². Jednocześnie, w 2024 r. zakończono postępowania karne wobec 377.398 osób⁷³. Tzn. nie jest tak, że przedstawienie zarzutów automatycznie oznacza, że od podejrzanego pobiera się

⁶⁹ Chociaż przepisy ustawy o Policji, tj. art. 20 ust. 1k, pozwalają na pobranie tych danych, ale wydaje się, że nie w celu rejestracji procesowej.

⁷⁰ Nie w każdym przypadku popełnienia poważnego przestępstwa jest konieczne pozyskanie danych biometrycznych czy genetycznych. W przypadku np. tzw. zbrodni fakturowych, co do zasady, pozyskanie tego rodzaju danych wrażliwych jest zbędne dla

⁷¹ Brak jest publicznie dostępnych, aktualnych danych, które by podawały, ile jest wpisów w bazie AFIS i CODIS. Z danych na rok 2018 wynika, że baza AFIS obejmowała niecałe 4 miliony wpisów (<https://bibliotekanauki.pl/articles/2067392.pdf>). Z doniesień medialnych wynika, że baza profili DNA nie była rozwijana przez kilka lat (<https://tvn24.pl/polska/policyjna-baza-dna-w-centralnym-laboratorium-kryminalistycznym-wreszcie-ruszyła-z-miejsca-st8503966>).

⁷² Dane dostępne na stronie: <https://clkp.policja.pl/clk/aktualnosci/255044,Kolejny-pracowity-rok-za-nami.html>.

⁷³ Dane dostępne na stronie Prokuratury Krajowej: <https://www.gov.pl/web/prokuratura-krajowa/sprawozdania-statystyczne-za-2024-rok>. W bazie AFIS rejestruje się dane nie tylko osób podejrzewanych i oskarżonych. Nie można zatem przyjąć, że 42,6% podejrzewanych jest rejestrowanych w bazie. Niemniej, gdyby istotnie prawie połowa osób, którym przedstawiono zarzuty albo „typowano” na podejrzanego została „wpisana” do bazy danych daktyloskopijnych, to taki wynik byłby niepokojący z perspektywy zasady proporcjonalności.

odciski palców i rejestruje w bazie AFIS czy danych genetycznych. Wydaje się zatem, że organy procesowe, co do zasady, dokonują oceny „bezwzględnej konieczności” z art. 10 dyrektywy 2016/680 w przypadku pobrania danych biometrycznych i genetycznych. Problematiczna jest natomiast kwestia gwarancji proceduralnych dla osoby, której dane biometryczne lub genetyczne pobrano. Co do zasady, jedyną możliwością zaskarżenia czynności pobrania tych danych, jest złożenie zażalenia w trybie art. 302 k.p.k., w ramach tzw. horyzontalnej kontroli postępowania przygotowawczego. Dostępne mechanizmy kontroli sądowej mają charakter ograniczony i nie zapewniają pełnej, efektywnej weryfikacji przesłanki „bezwzględnej niezbędności” oraz proporcjonalności pobrania i dalszego przechowywania danych (w tym realnej kontroli czasu retencji i usuwania). Analizując krajowe rozwiązania w perspektywie wymagań, jakie wynikają z orzecznictwa TSUE, sytuacja, w której to organ procesowy pozyskujący dane biometryczne i genetyczne dokonuje oceny konieczności pobrania tych danych, jest sytuacją optymalną. Jednak konieczne jest wprowadzenie – w jakiejś formie – sądowej kontroli (albo kontroli organu sądowego) nad prawidłowością pobrania/pozyskania danych, uwzględniając czas przechowywania danych oraz możliwość ich usunięcia⁷⁴.

W kontekście pobierania danych biometrycznych i genetycznych wątpliwości budzi jednak treść art. 20 ust. 1k ustawy o Policji⁷⁵, który stanowi, że „w przypadku podejrzanych Policja pobiera wyciski ze śluzówki policzków oraz dane osobowe, o których mowa w art. 21a ust. 2 pkt 2 lit. b-h i art. 21h ust. 2 pkt 2 i 3, w celach, o których mowa w art. 15 ust. 1 pkt 3a lit. d”. Wydaje się, że przepisy ustawy o Policji są częściowo konkurencyjne względem art. 74 § 2 k.p.k. i zastępują mechanizm oceny bezwzględnej konieczności pobrania danych biometrycznych i genetycznych, obligatoryjnym pobraniem tych danych w każdej sytuacji, kiedy określonej osobie zostały przedstawione zarzuty.

II.3. Czas przechowywania danych w KSIP

Zarządzenie KGP o KSIP nie precyzuje, jaki jest czas przechowywania danych osobowych. Przepis § 104 zarządzenia wprowadza obowiązek weryfikacji przydatności informacji. Komórki organizacyjne Policji, które zarejestrowały dane osobowe, a także dyrektor KGP mają obowiązek raz w roku zbadać, czy istnieją informacje, których

⁷⁴ Zob. uwagi niżej dotyczące czasu przechowywania danych.

⁷⁵ Art. 20 ust. 1k dodany przez art. 58 pkt 6 lit. b ustawy z dnia 14 grudnia 2018 r. (Dz.U.2019.125) zmieniającej nin. ustawę z dniem 6 lutego 2019 r.

dalsze przechowywanie jest zbędne oraz w zakresie legalności, prawidłowości i aktualności przetwarzanych informacji. Zarządzenie KGP o KSIP w § 105 precyzuje, jakie czynniki powinny zostać uwzględnione. Są to m.in. rodzaj i charakter czynu wyczerpującego znamiona przestępstwa, rodzaj i charakter dobra chronionego naruszonego popełnionym przestępstwem, formy sprawstwa i umyślności, zagrożenie sankcją karną, liczba popełnionych przestępstw, czas, który upłynął od momentu wprowadzenia informacji, w tym danych osobowych, do zbiorów danych KSIP do momentu dokonywania oceny, a także powzięcie przez Policję wiarygodnej informacji m.in. o uniewinnieniu danej osoby prawomocnym wyrokiem sądu, ewentualnie, że czyn nie zawierał znamion czynu zabronionego albo brak jest dostatecznie uzasadnionych przesłanek podejrzenia jego popełnienia. Każda z tych okoliczności jest jedynie okolicznością, która może – ale nie musi – prowadzić do usunięcia danych z rejestru KSIP. Oprócz corocznej weryfikacji, „przegląd” danych osobowych, jakie są gromadzone w KSIP, jest dokonywany na podstawie art. 16 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości. Administrator danych dokonuje weryfikacji nie rzadziej niż co 10 lat od zebrania, uzyskania, pobrania lub aktualizacji danych, zaś celem jest ustalenie, czy istnieją dane, których dalsze przechowywanie jest zbędne.

Jednocześnie, przepisy zarządzenia KGP o KSIP nie wprowadzają maksymalnych terminów przechowywania danych osobowych i obligatoryjnego ich usunięcia z rejestrów⁷⁶. Nawet jeśli dane np. osoby legitymowanej zostaną usunięte z systemu SWD po upływie 5 lat⁷⁷, to dane mogą pozostać w KSIP, jeśli dane osoby legitymowanej znajdują się też w zbiorze np. notowania kryminalnego albo jeśli została zarejestrowana „przy okazji” innej rejestracji osób w ramach „rejestracji procesowej”⁷⁸. Podobnie w przypadku usuwania danych z systemów przechowywania danych genetycznych i biometrycznych. Przepis § 109 ust. 1 zarządzenia KGP o KSIP co do zasady nakazuje usunięcie danych z KSIP, jeśli zostały one uprzednio usunięte z baz

⁷⁶ W ustawie z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu wprowadza się obowiązek przeglądu danych co 10 lat, co i tak ma miejsce obecnie ze względu na obowiązujące regulacje ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości. Nowelizacja nie odnosi się jednak do maksymalnego okresu przechowywania danych osobowych. Zob. art. 19 pkt 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu.

⁷⁷ Zob. art. 20g ust. 4 ustawy o Policji

⁷⁸ Zob. § 108 ust. 3a Zarządzenia KGP o KSIP.

danych AFIS⁷⁹ i zbioru danych DNA⁸⁰. Istnieje jednak możliwość dalszego przechowywania i przetwarzania danych wrażliwych (art. 10 dyrektywy 2016/680), „gdy te same dane osobowe w zbiorach danych KSIP są przetwarzane również na innej podstawie prawnej, aniżeli podstawa prawna do przetwarzania danych daktyloskopijnych lub informacji o wynikach analizy kwasu deoksyrybonukleinowego (DNA)”⁸¹. Przykładowo zatem, jeśli dane osobowe oskarżonego były przetwarzane równolegle – w dwóch sprawach – w jednej z tych spraw pobrano materiał genetyczny, a następnie w tej sprawie zapadł wyrok uniewinniający, to usunięcie danych z bazy danych DNA nie oznacza usunięcia ich z bazy KSIP, jeśli w równolegle prowadzonym postępowaniu, zapadło inne orzeczenie niż uniewinnienie albo prawomocne umorzenie z uwagi na brak danych dostatecznie uzasadniających podejrzenie popełnienia przestępstwa lub brak znamion czynu zabronionego. W efekcie usunięcie danych z AFIS/ bazy DNA nie musi automatycznie przekładać się na usunięcie powiązanych wpisów w KSIP.

Z perspektywy czasu przechowywania danych osobowych w KSIP w najtrudniejszej sytuacji znajdują się:

- osoby, które zostały skazane za średnie i drobne przestępstwa (zarówno te, które zostały skazane na karę pozbawienia wolności, jaki i te, względem których odstąpiono od wymierzenia kary), i których skazanie się zatarło;
- osoby, których postępowanie zostało warunkowo umorzone;

⁷⁹ Zgodnie z art. 21l ust. 2 ustawy o Policji, dane osobowe ze zbioru danych daktyloskopijnych usuwa się w przypadku gdy: 1) zostało umorzone postępowanie z uwagi na to, że: a) czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia, b) zdarzenie lub okoliczność, w związku z którymi wprowadzono dane osobowe do zbioru danych, nie ma znamion czynu zabronionego; 2) osoba, której dane dotyczą: a) została uniewinniona prawomocnym wyrokiem sądu, b) ukończyła 100. rok życia, c) zmarła; 3) utracą swoją przydatność eliminacyjną, jednakże nie dłużej niż po upływie 5 lat od dnia ustania stosunku służbowego lub pracy - w przypadku osób, o których mowa w art. 20 ust. 1l.

⁸⁰ Tożsame przesłanki oraz terminy usunięcia danych genetycznych wprowadza art. 21e ust. 2 ustawy o Policji, dodając jedną dodatkową podstawę w postaci ustalenia tożsamości zwłok ludzkich.

⁸¹ Zob. § 109 ust. 2 ustawy o Policji.

- osoby, których postępowanie zostało umorzone z powodów innych niż brak danych dostatecznie uzasadniających popełnienie przestępstwa albo brak znamion czynu zabronionego (art. 17 § 1 pkt 2 *in fine* – 11 k.p.k.)⁸².

W tych bowiem trzech przypadkach, funkcjonowanie rejestru KSIP oraz dokonana rejestracja procesowa, są w pełni niezależne od KRK czy KCIK. Usunięcie danych z KRK, czy KCIK nie sprawia, że usunięty zostaje wpis w KSIP. **Żadne przepisy ustaw nie wprowadzają maksymalnego terminu przechowywania danych osobowych. Przepisy zarządzenia KGP o KSIP także nie precyzują granic temporalnych przetwarzania i przechowywania danych osobowych. W praktyce usunięcie wpisu w KSIP jest możliwe po stwierdzeniu „braku przydatności”.**

Prowadzi to do sytuacji, kiedy dane osobowe sprawców średnich i drobnych przestępstw mogą być przetwarzane i przechowywane w zakresie szerszym niż jest to konieczne w społeczeństwie demokratycznym, tj. nie w celu zapobiegania i zwalczania przestępczości, ale z uwagi na „potencjalną przydatność” ocenianą z perspektywy organów ścigania. Jest to realne zagrożenie, bowiem weryfikacja „przydatności” przetwarzania danych osobowych jest dokonywana wewnątrz organów policyjnych – tj. została powierzona organom wskazanym w § 104 zarządzenia KGP o KSIP. Analizując praktykę funkcjonowania KSIP można wskazać na sytuacje, kiedy KGP odmawiała usunięcia wpisu z KSIP w sytuacji, gdy osoba została skazana za drobne przestępstwo kilkanaście lat wcześniej, co było jednorazową sytuacją, zaś po usunięciu wpisu z KRK nie może skutecznie domagać się usunięcia wpisu w rejestrze KSIP. Wnioskowanie o usunięcie danych z KSIP do Komendanta Głównego Policji spotyka się z decyzją odmowną. Komendant Główny Policji wskazuje m.in., że KSIP „jest rejestrem generującym (służącym do zbierania i przetwarzania) informacje o osobach w związku z wszczętymi i prowadzonymi przez Policję postępowaniami (głównie karnymi) bez

⁸² Wątpliwości może budzić sytuacja, kiedy czyn został popełniony w warunkach kontratypu, a umorzenie postępowania nastąpiło na podstawie art. 17 § 1 pkt 2 *in fine* k.p.k., tj., kiedy ustawa stanowi, że sprawca nie popełnia przestępstwa. Jeśli ta okoliczność zostałaby ustalona na rozprawie – zapadłby wyrok uniewinniający. Jednocześnie, w przypadku przesłanek z art. 17 § 1 pkt 1 i 2 k.p.k., przepisy Zarządzenia KGP o KSIP rozróżniają okoliczności skutkujące usunięciem wpisu, w zależności od tego, czy zapadł wyrok uniewinniający, czy umorzono postępowanie. Jeśli zapadł wyrok uniewinniający – obejmuje on zakresem w całości przesłanki z art. 17 § 1 pkt 1 i 2 k.p.k. i wpis powinien zostać usunięty z rejestru. Jeśli zapadła decyzja o umorzeniu postępowania na podstawie art. 17 § 1 pkt 1 lub 2 *in principio* – także. Jednocześnie, jeśli podjęto decyzję o umorzeniu postępowania z uwagi na kontratyp (art. 17 § 1 pkt 2 *in fine*) albo z innych powodów z art. 17 § 1 pkt 3 – 11 k.p.k. to przepisy nie wprowadzają żadnych zasad szczególnych dotyczących usunięcia wpisu z rejestru. Taki wpis, osoby, która została zarejestrowana procesowo, może zostać usunięty na zasadach takich jak stosuje się np. do osób skazanych.

względu na sposób ich zakończenia, więc jako taki nie może stanowić podstawy do wnioskowania o sposobie zakończenia tych postępowań, a tym bardziej nie przesądza o statusie osoby jako karanej lub niekaranej”, a także, że „rejestracja w KSIP ma charakter pomocniczy dla oceny kryminologicznej danej osoby, dokonywanej przez Policję” i w żaden sposób nie stygmatyzuje osoby, która – mimo zatarcia skazania – widnieje w rejestrze⁸³.

Kryteria oceny przydatności dalszego przechowywania danych osobowych, jakie wprowadza § 105 zarządzenia KGP o KSIP są poprawne i implementują wymagania, jakie wynikają z przepisów prawa unijnego. Służą bowiem wdrożeniu zasady minimalizacji danych osobowych i ograniczaniu ich przetwarzania „dla wygody” organów ścigania, czy zapobieganiu stworzeniu wielkiego zbioru danych o jednostkach – nadmiernego z perspektywy funkcjonowania państwa prawa. Mają one jednak charakter wewnętrzny i pozostawiają szeroki margines uznania. **Sytuacja, w której organ ma kontrolować samego siebie, z ograniczonymi kompetencjami nadzorczymi niezależnych organów stwarza ryzyko nadużyć.** Można to dostrzec analizując orzecznictwo sądów administracyjnych. Oceniając zasadność dalszego przechowywania danych osobowych, Komendant Główny Policji zwykle powołuje się na przesłankę przydatności danych albo zbędności danych dla realizacji zadań Policji. Wojewódzki Sąd Administracyjny w Warszawie zwrócił uwagę, że ocena przesłanki „zbędności danych” – gdy jest dokonywana wyłącznie z punktu widzenia realizacji przez Policję jej ustawowych zadań – jest na tyle ogólna, że „biorąc tylko je pod uwagę, możliwe byłoby zakwalifikowanie wszystkich zebranych przez Policję danych osobowych jako niezbędnych dla realizacji jej zadań, co umożliwiłoby bezterminowe przechowywanie danych pomimo osiągnięcia celu, w którym zostały zebrane”⁸⁴. Tymczasem, jak wskazuje się w orzecznictwie, kluczowym wyznacznikiem dla oceny dopuszczalności przetwarzania danych osobowych w KSIP jest cel gromadzenia określonych informacji. Determinuje to konieczność dokonywania każdorazowej, zindywidualizowanej oceny wniosków o usunięcie danych z tego zbioru, **Ustalenie celu, w jakim dane są przetwarzane, kształtuje okres, przez jaki dane mogą być**

⁸³ Nie jest też tak, że obywatele nie odczuwają negatywnych konsekwencji dalszego – po zatarciu skazania – wpisu w KSIP. W jednej ze spraw prowadzonych w Biurze Rzecznika Praw Obywatelskich wyciąg o ukaraniach za wykroczenia od 2002 r. został dołączony do wniosku o ukaranie (sprawa prowadzona w BRPO pod sygnaturą: II.519.267.2021). Nie jest zatem tak, że wpis w KSIP ma skutek jedynie „wewnętrzny”, tj. wykorzystywany dla celów pracy Policji, ale może wpływać na sytuację jednostek „na zewnątrz”.

⁸⁴ Wyrok WSA w Warszawie z 4.12.2024 r., II SA/Wa 675/24, LEX nr 3846565; wyrok WSA w Warszawie z 28.04.2022 r., II SA/Wa 3288/21, LEX nr 3414146.

przetwarzane. Przy czym cel musi zostać określony konkretnie i musi być zasadny w świetle realizacji ustawowych zadań Policji, a nie określony w sposób ogólnikowy. Natomiast w przypadku ustania celu, dla którego dane są przetwarzane, niezbędne jest ich usunięcie⁸⁵.

II.4. Efektywność zewnętrznego nadzoru nad KSIP – nadzór Prezesa Urzędu Ochrony Danych Osobowych oraz sądów administracyjnych

Zewnętrzny nadzór nad działaniem KSIP oraz zewnętrzna ocena celowości dalszego przechowywania i przetwarzania danych osobowych są ograniczone.

Co do zasady bowiem, nadzór sprawuje Komendant Główny Policji – albo inne osoby upoważnione – będący administratorem danych osobowych.

Prezes Urzędu Danych Osobowych ma uprawnienia nadzorcze wynikające z art. 5 ust. 1 ustawy o ochronie danych osobowych. Może rozpatrywać skargi osób, których dane osobowe są przetwarzane niezgodnie z prawem i prowadzić postępowania w tym zakresie. W ramach postępowania prowadzonego w UODO może stwierdzić niezgodność z prawem przetwarzania danych osobowych, tj. przykładowo, że dalsze przetwarzanie danych osobowych nie służy realizacji celów związanych z zapobieganiem i zwalczaniem przestępczości. W jednym z orzeczeń Wojewódzki Sąd Administracyjny w Warszawie⁸⁶ stwierdził, że Prezes UODO może dokonywać „własnej, autonomicznej oceny czy przetwarzanie danych osobowych strony postępowania następuje zgodnie z prawem, a w szczególności zgodnie z art. 13 ust. 1 ustawy z dnia 14 grudnia 2018 r., który stanowi, że właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Ocena legalności przetwarzania danych musi również uwzględniać, że w myśl art. 31 ust. 1 pkt 5 tej ustawy, administrator zapewnia, aby dane osobowe były przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania. (...) Skoro jednak ustawodawca przyznał Prezesowi Urzędu Ochrony Danych Osobowych uprawnienia nadzorcze zmierzające do oceny czy przetwarzanie danych osobowych ma miejsce w zgodzie z przepisami, to nie sposób uznać, jak czyni to Komendant Główny Policji, że organ był związany ustaleniami Policji

⁸⁵ Wyrok WSA w Warszawie z 23.01.2025 r., II SA/Wa 571/24, LEX nr 3887162.

⁸⁶ Wyrok WSA w Warszawie z 4.12.2024 r., II SA/Wa 675/24, LEX nr 3846565.

w zakresie niezbędności przetwarzanych danych. Przyjęcie takiego stanowiska czyniłoby bowiem dokonywaną przez Prezesa UODO kontrolę całkowicie iluzoryczną”.

Warto zwrócić uwagę, że Komendant Główny Policji, w postępowaniach sądowo-administracyjnych, kwestionuje uprawnienie Prezesa UODO do żądania usunięcia wpisu w rejestrze KSIP, podnosząc, że żaden przepis ustawy o ochronie danych osobowych takiego uprawnienia wprost nie przyznaje. Taka wykładnia przepisów ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości oraz przepisów kompetencyjnych Prezesa UODO została zakwestionowana w wyroku Naczelnego Sądu Administracyjnego z dnia 17 października 2025 r., III OSK 2223/22⁸⁷. NSA stwierdził tam, że wbrew odmiennemu zapatrywaniu Komendanta Głównego Policji do kompetencji Prezesa UODO należy ocena prawidłowości dalszego przetwarzania danych osobowych przez ich administratora, tj. Komendanta Głównego Policji. Zgodnie bowiem z art. 5 ust. 1 pkt 1 i 6 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości „do zadań Prezesa Urzędu Ochrony Danych Osobowych, należy monitorowanie i egzekwowanie stosowania przepisów ww. ustawy oraz wydanych na jej podstawie aktów wykonawczych oraz rozpatrywanie skarg osób, których dane osobowe są przetwarzane niezgodnie z prawem, i prowadzenie postępowań w tym zakresie. (...) **Prezes UODO jest w powyższym zakresie organem kontrolnym (art. 6 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości) wyposażonym w kompetencje o charakterze nadzorczym w stosunku do administratora danych osobowych (art. 8 ust. 1-3 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości). Kompetencji nadzorczych Prezesa UODO wobec administratora danych osobowych nie wyklucza obowiązek realizacji zadań Policji przez Komendanta Głównego Policji”.** Stanowisko NSA wprost potwierdzające uprawnienie Prezesa UODO do nakazania usunięcia danych z KSIP jest słuszne. W praktyce warto jednak doprecyzować w ustawie o Policji relację między obowiązkami w zakresie prowadzenia KSIP a wykonywaniem środków naprawczych organu nadzorczego (Prezesa UODO), aby ograniczyć spory kompetencyjne i przyspieszyć wykonywanie decyzji.

⁸⁷ Wyrok NSA z 17.10.2025 r., III OSK 2223/22, LEX nr 3932512.

Także kontrola sprawowana przez sądy administracyjne ma ograniczony zakres. Jak wskazał Prezes UODO w piśmie z dnia 17 maja 2024 r., przepisy ustawy o ochronie danych osobowych „wymagają jedynie od administratora zgodności działania z przepisami regulującymi wykonywanie ustawowych zadań Policji i to do administratora należy ostateczna ocena potrzeby dalszego przetwarzania danych w KSIP”⁸⁸. Kontrola sądowa ma w zasadzie charakter formalny – dotyczy kompetencji do wydania określonej decyzji, jakości sporządzonego uzasadnienia – a nie merytoryczny, tj. oceny zasadności dalszego przetwarzania danych osobowych.

III. Wnioski

Po pierwsze, **konieczne jest uregulowanie funkcjonowania KSIP w zakresie praw i obowiązków obywateli w akcie o randze ustawy, a nie w zarządzeniu KGP**. Chodzi nie tylko o zapewnienie dostępności aktów prawnych – ustawy i rozporządzenia są publikowane w Dzienniku Ustaw, każdy może się z nimi zapoznać, a odszukanie w Internecie zarządzeń Komendanta Głównego Policji może być utrudnione (a nie każdy ma dostęp do systemów takich jak LEX czy Legalis). Przede wszystkim chodzi o unormowanie zasad zbioru danych osobowych w sposób zgodny ze standardami wynikającymi z art. 51 Konstytucji. Nie jest wystarczające odesłanie ustawowe z art. 21nb ustawy o Policji. W szczególności uwagę powyższą należy odnieść do kwestii przetwarzania i przechowywania danych biometrycznych i genetycznych. Zmiany, jakie wprowadzone zostały ustawą o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu pomijają bowiem kwestię przetwarzania danych genetycznych, a ponadto – jej stosowanie jest powiązane z uruchomieniem systemu EES (start operacyjny: 12 października 2025 r.; pełna operacyjność: 10 kwietnia 2026 r.).

Po drugie, **celowe jest wprowadzenie zróżnicowanych zasad gromadzenia, przetwarzania i przechowywania danych osobowych w zależności od wagi przestępstwa**. Decyzja o usunięciu tych danych nie może być w pełni uznaniowa, skoncentrowana na przesłance „przydatności danych”. Być może celowe byłoby doprecyzowanie tej przesłanki, by ograniczyć zakres uznania administracyjnego, a także wprowadzić możliwość zautomatyzowanego usuwania danych osobowych, tj. wprowadzić reguły retencji i usuwania oparte na ustawowych kryteriach (waga czynu, wynik postępowania, upływ czasu, brak recydywy), z możliwością ich technicznej automatyzacji przy zachowaniu kontroli tej decyzji przez odpowiedni organ.

⁸⁸ Pismo do Ministra ds. Europejskich można znaleźć na stronie: <https://uodo.gov.pl/pl/138/3117>, s. 7.

Po trzecie, **konieczne jest wprowadzenie maksymalnych terminów przechowywania danych w KSIP, zwłaszcza w tych sytuacjach, gdy dane osobowe zostały usunięte z innych rejestrów – KCIK, SWD, rejestru wykroczeń itp.**

Powyższe odnosi się przede wszystkim do rejestracji procesowej, rejestracji osób zatrzymanych i legitymowanych. Obecnie dane w KSIP mogą być przechowywane mimo usunięcia ich z innych rejestrów, a przesłanką jest ocena przydatności.

Konieczność sporządzenia kryminologicznej oceny danej osoby, zwłaszcza jeśli popełniła ona czyn zabroniony kilkanaście, kilkadziesiąt lat temu, nie uzasadnia utrzymywania sytuacji, gdy informacje o osobie – w tym dane wrażliwe – mogą być w łatwy sposób pozyskane przez funkcjonariuszy Policji (a niekiedy mogą wpływać na sposób traktowania jednostki w praktyce czynności policyjnych).

Po czwarte, **niezbędne jest wzmocnienie kontroli zewnętrznej nad KSIP – w szczególności UODO i sądów administracyjnych.** Ocena sądów administracyjnych koncentrująca się na formalnych aspektach rozpoznawanej sprawy jest nieefektywna z perspektywy ochrony praw jednostek przed nieuprawnioną ingerencją w sferę życia prywatnego. Możliwe jest np. doprecyzowanie ustawowych przesłanek retencji, przesłanek usuwania danych, by możliwa była sądowa ocena merytoryczna np. decyzji KGP o odmowie usunięcia danych zarejestrowanych w KSIP. Dodatkowo, wprost wskazanie kompetencji Prezesa UODO do usuwania danych zarejestrowanych w KSIP przecięłoby spory i istotnie ograniczyłoby pole do kwestionowania przez KGP tego uprawnienia Prezesa UODO i odmawiania wykonania decyzji o usunięciu danych. Rozważenia warte jest także rozszerzenie uprawnienia sądów karnych do oceny zasadności pobrania danych biometrycznych i genetycznych na podstawie art. 74 § 2 k.p.k. i ewentualne umożliwienie sądowi karnemu nakazania usunięcia tych danych.

Po piąte, **wskazane wydaje się wzmocnienie uprawnień informacyjnych jednostki, przez np. poinformowanie jej o wpisaniu danych do KSIP i konsekwencjach tego wpisu, a także – po upływie jakiego terminu może ona domagać się usunięcia danych.**

Mając na uwadze przedłożone racje, stosownie do art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich⁸⁹, zwracam się do Pana Ministra z uprzejmą prośbą o dokonanie analizy wskazanych w niniejszym stanowisku problemów i rozważenie zainicjowania zmian legislacyjnych we wskazanych zakresach.

⁸⁹ Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r., poz. 1264).

Będę wdzięczny za poinformowanie mnie o stanowisku zajęтым w przedstawionej materii.

Z wyrazami szacunku

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

Do wiadomości:

- Pan Mirosław Wróblewski Prezes Urzędu Ochrony Danych Osobowych (ePUAP).