



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Mirosław Wróblewski

Warszawa, 23 września 2026 r.

DPNT.413.7.2026

**Pan Maciej Kierwiński
Minister Spraw Wewnętrznych
i Administracji**

Szanowny Panie Ministrze,

działając na podstawie art. 52 ust. 1 ustawy o ochronie danych osobowych¹ zwracam się do Pana Ministra z uprzejmą prośbą i wnioskiem o podjęcie pogłębionej analizy podstaw prawnych co do działań Policji, polegających na:

- 1) przetwarzaniu danych osobowych za pomocą pozyskiwania stałego dostępu, w trybie teletransmisji do monitoringu wizyjnego stosowanego przez jednostki samorządu terytorialnego, jak również
- 2) stosowania przez Policję oraz strażę gminne (miejskie) sprzętu monitorującego wyposażonego w technologię rozpoznawania twarzy lub analizy innych cech biometrycznych,

w celu zapewnienia skutecznego stosowania i zgodności z przepisami rozporządzenia 2016/679² oraz ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości³.

Niniejsze wystąpienie kieruję do Pana Ministra w reakcji na docierające do Prezesa Urzędu Ochrony Danych Osobowych sygnały od jednostek samorządu

¹ Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 r. poz. 1781 ze zm.).

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), dalej jako: rozporządzenie 2016/679.

³ Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125, z 2022 r. poz. 1700).

terytorialnego o występowaniu do nich przez organy Policji z wnioskami o zawarcie porozumień dotyczących korzystania z monitoringu gminnego (miejskiego), na mocy których Policja uzyskać ma stały i nieograniczony dostęp do systemu monitoringu wizyjnego w trybie teletransmisji wizji w czasie rzeczywistym. Wystąpienie kierowane jest również w odpowiedzi na pismo Sekretarza Stanu w MSWiA ze stycznia 2026 r. sygn. DPP-WNP.(...).2026, w którym wyrażone zostało stanowisko resortu w tym przedmiocie.

Pragnę jednocześnie poinformować, że do Prezesa UODO wpływa coraz więcej pytań, w tym od organów Policji, dotyczących legalności stosowania i możliwości korzystania z urządzeń monitoringu wizyjnego wyposażonych dodatkowo w technologię rozpoznawania twarzy.

Takie działanie Policji budzi poważne wątpliwości organu nadzorczego do spraw ochrony danych osobowych z punktu widzenia zgodności z obowiązującymi przepisami prawa, zarówno polskimi, jak i prawa UE.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych zachodzi potrzeba przeprowadzenia co najmniej pogłębionej analizy prawnej **legalności i proporcjonalności** pozyskiwania oraz wykorzystywania przez Policję danych osobowych, także szczególnych kategorii, w ramach monitoringu, celem zagwarantowania poszanowania konstytucyjnie chronionych praw i wolności podmiotów danych, w tym prawa do prywatności oraz prawa do autonomii informacyjnej jednostki.

I. Uwagi ogólne.

Prezes Urzędu Ochrony Danych Osobowych nie kwestionuje potrzeby zapewnienia bezpieczeństwa na terytorium RP, co należy do ustawowych zadań Policji, niemniej ich realizacja powinna odbywać się z uwzględnieniem ograniczeń wynikających z przepisów prawa, w tym z zakresu ochrony danych osobowych.

Zgodnie z **konstytucyjną zasadą legalizmu** organy władzy publicznej są uprawnione do działania jedynie na podstawie i w granicach prawa, a pozyskiwanie informacji o obywatelach przez władze publiczne oraz ograniczenia konstytucyjnych praw (w tym prawa do ochrony życia prywatnego) mogą być ustanowione tylko w ustawie i odbywać się jedynie w zakresie wyłącznie **niezbędnym**, zgodnie z zasadami **proporcjonalności, celowości** oraz **klauzulami limitacyjnymi** dla ingerencji w prawa i wolności jednostki, z poszanowaniem zasad demokratycznego państwa prawa⁴. Kompetencja do pozyskiwania informacji o obywatelu, poprzez określony zakres i środek przetwarzania, nie może być domniemywana i musi wynikać z konkretnie sformułowanego przepisu prawa. Obowiązuje ścisła, zawężająca wykładnia przepisów określających kompetencje organu państwa, które powinny być sformułowane w sposób konkretny i precyzyjny, wraz z określeniem co najmniej: celu przetwarzania, jego

⁴ Zob. art. 7, 31 ust. 3, 47, 51 ust. 1 i 2 Konstytucji RP, a także art. 8 w zw. z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej.

przedmiotowego i podmiotowego zakresu, oraz warunków niezbędności dla realizacji zadania publicznego⁵.

II. Stała teletransmisja obrazu z monitoringu miejskiego.

Na podstawie art. 20 ust. 1 i 1c ustawy o Policji⁶, formacja ta dysponuje uprawnieniem do przetwarzania informacji, w tym danych osobowych. Uprawnienie to podlega **ograniczeniu** jedynie do informacji i danych **niezbędnych** do realizacji zadań ustawowych i wykonywaniem uprawnień związanych m.in. z prowadzeniem postępowań lub czynności służbowych w tym zakresie. Przetwarzanie danych osobowych powinno zatem ograniczać się zasadniczo do katalogu określonego w art. 14 ww. ustawy, tj. do czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych, administracyjno-porządkowych, czy procesowych, prowadzonych w celu rozpoznawania, zapobiegania, wykrywania przestępstw, przestępstw skarbowych, wykroczeń, poszukiwania osób i innych określonych w przepisie⁷.

Posiadane przez Policję uprawnienie do „obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych” (art. 15 ust. 5a), dotyczy jedynie sytuacji, gdy funkcjonariusze Policji „**wykonują czynności**” w celu realizacji zadań określonych w art. 14 ustawy.

Kompetencji do stosowania środków technicznych rejestrowania przestrzeni publicznej w warunkach prowadzenia określonych, skonkretyzowanych czynności służbowych, nie należy zatem utożsamiać z kompetencją do prowadzenia stałego i pełnego wideonadzoru przestrzeni publicznej w celu zapewnienia na terenach budynków użyteczności publicznej, czy w obszarach przestrzeni publicznych ogólnie pojmowanego porządku publicznego. Uprawnienia Policji co do zasady dotyczą środków stosowania rejestracji obrazu w charakterze narzędzia przeciwdziałania wobec skonkretyzowanych i sprecyzowanych zagrożeń, w ramach skoordynowanych postępowań lub czynności wobec konkretnych czynów, zjawisk, zdarzeń lub osób – nie zaś jako środka stałego, systematycznego wideo-nadzoru szerokiego zakresu przestrzeni publicznej o charakterze ogólnoprewencyjnym, który prowadziłby do przetwarzania bardzo szerokiego zakresu danych osobowych obywateli, co do których w zdecydowanej większości nie istnieją żadne przesłanki wszczęcia postępowań karnych, wykroczeniowych, czy prowadzenia innego rodzaju czynności.

Cele monitoringu prowadzonego przez jednostki samorządu terytorialnego są inne. Ustawową podstawą do stosowania monitoringu gminnego (miejskiego) są art. 9a oraz art. 50 ust. 2 ustawy o samorządzie gminnym⁸ – gmina może stosować

⁵ Warunki te wynikają zarówno z ustawy zasadniczej, jak i dyspozycji art. 6 ust. 3 rozporządzenia 2016/679.

⁶ Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2021 r. poz. 1882 ze zm.).

⁷ Katalog rozszerzony także o kompetencje i czynności określone w odrębnych ustawach.

⁸ Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 1465)

monitoring wizyjny miejsc publicznych w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej oraz ochrony mienia komunalnego. **Cele i zakres przetwarzania zostały jasno i konkretnie określone w ustawie i nie mogą być w związku z tym rozszerzane**⁹, np. na cele realizowane przez Policję. Zawarcie porozumienia pomiędzy jednostką Policji, na podstawie której gmina miałaby przekazywać w sposób **stały**, w trybie teletransmisji na żywo sygnał wizji **ze wszystkich kamer**, jak również udzielić **pełnego** dostępu do infrastruktury technicznej systemu monitoringu oznacza *de facto*, że Policja dokonywałaby przetwarzania danych osobowych w bardzo szerokim zakresie, takim samym jak pierwotny administrator (gmina), a jednocześnie do celów istotnie odmiennych od tych, które wyznacza art. 9a ust. 1 ustawy o samorządzie gminnym. W praktyce prowadziłoby to do funkcjonującego jedynie na podstawie porozumienia stałego, bieżącego i długotrwałego współprowadzenia monitoringu wizyjnego w celu nadzoru określonej przestrzeni, równoległe do gminy, w tym samym zakresie – jednak w innych, niedookreślonych celach.

Przepisy prawa nie przewidują natomiast możliwości przekazania kompetencji do prowadzenia monitoringu przez organ gminy innemu organowi, w tym Policji. Jeżeli prawodawca przewidział wyłączną kompetencję do zapewnienia bezpieczeństwa organowi publicznemu, to kompetencja ta nie powinna być przez wykonawcę normy współdzielona czy przenoszona na jednostki organizacyjne Policji lub wykonywane przez podmiot, który nie jest adresatem takiej normy. Odrębność kompetencji samorządu i Policji w zakresie zapewnienia bezpieczeństwa została podkreślona przez ustawodawcę w art. 3 ustawy o Policji¹⁰.

Tak szeroka forma wideonadzoru wykracza poza zakres czynności, które można uznać za wykonywanie przez Policję ustawowych zadań. Dotyczyć będzie bowiem w znaczącej części osób, wobec których nie są prowadzone czynności procesowe, służbowe, czy zdarzeń związanych z rozpoznawaniem, wykrywaniem, czy zapobieganiem czynom zabronionym.

Za niewłaściwe należy uznać również powoływanie się w tym kontekście na normę określoną w **art. 20 ust. 1e ustawy o Policji**. Na podstawie art. 20 ust. 1-1d tej ustawy Policja jest bowiem uprawniona do pozyskiwania danych osobowych i informacji ze zbiorów prowadzonych przez organy władzy publicznej. Organy te z kolei zobowiązane są do nieodpłatnego udostępniania informacji i danych osobowych. Dane takie i informacje pozyskiwane są jednak na wniosek Policji. Art. 20 ust. 1e ustawy o Policji określa wyjątek od wnioskowego trybu pozyskiwania danych, dopuszczając, że dane zgromadzone w zbiorach danych mogą być udostępniane przez organ władzy publicznej w drodze teletransmisji (stałego dostępu), ale tylko w przypadku wyrażenia przez organ

⁹ Por. art. 9 ust. 3 ustawy o samorządzie gminnym.

¹⁰ Zob. wyrok Trybunału Konstytucyjnego z 22 marca 2007 r. sygn. akt U 1/07 – tezy 6-9.

udostępniający zgody i gdy spełnione zostały łącznie wszystkie określone w przepisie warunki¹¹.

Przed wszystkim, przepis ten odnosi się jedynie do udzielania stałego dostępu do „zbiorów danych” i jedynie w celu pobierania z nich poszczególnych informacji, niezbędnych dla realizacji zadań ustawowych. Wykładnia systemowa, celowościowa i funkcjonalna treści art. 20 ustawy o Policji przemawia za uznaniem, że pojęcie „zbiór danych” odnosi się w tym kontekście do usystematyzowanych rejestrów lub ewidencji¹², z których możliwe jest pobieranie **jednostkowych danych, których pozyskanie jest konieczne dla prowadzonego postępowania lub realizowanych czynności**. W ocenie organu nadzorczego, stosowanie rozszerzającej wykładni art. 20 ust. 1e ustawy o Policji, w taki sposób, aby stanowił on podstawę do udzielania stałego wglądu do monitoringu wizyjnego w czasie rzeczywistym – w sposób umożliwiających przeglądanie dowolnych danych, bez wskazania wyraźniej podstawy prawnej ich pozyskiwania oraz bez możliwości weryfikacji celowości wykorzystywania danych i środków kontroli – jest nieuzasadnione¹³. Taki dostęp prowadzić może bowiem do udostępniania danych w sposób (i w zakresie) z istoty swojej nadmiarowy.

Podstawy do przekazywania nagrań monitoringu wizyjnego w trybie stałej transmisji obrazu w czasie rzeczywistym nie może stanowić również art. 9 ust. 5 pkt 6 ustawy o strażach gminnych¹⁴ określający, że współpraca Policji i straży polega m.in. na „wymianie informacji w zakresie obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych”. Przepis ten należy interpretować w sposób ścisły, zgodnie z zasadą legalizmu, a więc jako dopuszczający wymianę informacji o stosowanych środkach monitoringu wizyjnego. Nie może on jednak stanowić podstawy do wymiany treści nagrań, w szczególności, gdy taka wymiana miałaby przyjmować formę stałego dostępu w czasie rzeczywistym.

Z punktu widzenia wykładni systemowej nie można pominąć również okoliczności, że ustawowe uprawnienie do **samodzielnego** stosowania środków rejestracji obrazu (określone w art. 15 ust. 5a ustawy o Policji), czy **ogólnie** sformułowana kompetencja do pozyskiwania danych osobowych ze zbiorów danych innych podmiotów publicznych (art. 20 ust. 1d i 1e ustawy o Policji) nie są równoznaczne z udzieleniem Policji uprawnienia do pozyskiwania obrazu z monitoringu wizyjnego prowadzonego przez inny podmiot w formie teletransmisji.

W opinii organu nadzorczego taka kompetencja powinna zostać sformułowana w sposób **konkretny** – powinna odnosić się w sposób kierunkowy do uprawnienia

¹¹ Zob. treść art. 20 ust. 1e pkt 1-3 ustawy o Policji.

¹² Zob. treść art. 20 ust. 1d pkt 1 ustawy o Policji.

¹³ Do pozyskiwania danych w trybie bezwnioskowym przez organy władzy publicznej krytycznie odniósł się również Naczelny Sąd Administracyjny w wyroku z dnia 3 grudnia 2021 r., sygn. III OSK 590/21 dotyczącym pozyskiwania danych z rejestru PESEL przez komorników sądowych.

¹⁴ Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. z 2021 r. poz. 1763).

pozwalającego na uzyskanie dostępu w czasie rzeczywistym do rejestrowanego przez inny podmiot obrazu – analogicznie jak ustawodawca czyni to w innych ustawach¹⁵.

Wyraźnie w tym miejscu podkreślić należy, że powyższe rozważania dotyczą sytuacji, w której teletransmisja wizji ma charakter systematyczny, długotrwały, polegający na pełnym współdzieleniu infrastruktury ze wszystkich urządzeń monitorujących. Odnosząc się do stanowiska zawartego we wspomnianym na wstępie piśmie Pana Ministra, **organ nadzorczy nie kwestionuje, że czasowy i ograniczony dostęp do infrastruktury monitoringu będzie w niektórych sytuacjach jak najbardziej zasadny**. Dostęp do monitoringu wizyjnego powinien mieć jednak co do zasady charakter możliwie ograniczony czasowo i miejscowo w zakresie niezbędnym do realizacji celów w związku z prowadzonymi czynnościami służbowymi, w takim zakresie, który jest podyktowany koniecznością wynikającą z okoliczności prowadzonej sprawy, konkretnego postępowania o czyn lub przeciwko osobie, czy z realizacją czynności mających zapewnić bezpieczeństwo przed skonkretyzowanym zagrożeniem, przy równoległym spełnieniu ustawowych wymogów procesowych i formalnych.

Tymczasem, w przedstawianych jednostkom samorządu terytorialnego porozumieniach przyjmowane są dalece ogólne i bardzo szerokie postanowienia, określające, że Policji przekazywane mają być zasadniczo wszystkie dane z systemu monitoringu wizyjnego w publicznych obszarach określonego miasta, wraz sygnałem podglądu w czasie rzeczywistym ze wszystkich kamer, w tym kamer specjalnych, umieszczonych na statkach latających, pojazdach, kamer mobilnych lub tymczasowych oraz pełnym dostępem infrastruktury brzegowej podsieci monitoringu, przy jednoczesnym braku ustanowienia ram czasowych udostępniania (porozumienia zawierane mają być na czas nieokreślony). Jednocześnie, cele pozyskiwania danych określone są w sposób wysoce ogólny, wręcz blankietowy, poprzez odwołanie jedynie do „wykonywania zadań lub czynności” określonych w art. 1 i 14 ustawy o Policji, które to przepisy zawierają niemal zupełny katalog wszystkich zadań i czynności realizowanych przez ww. formację. Powyższe budzi poważne wątpliwości pod względem spełnienia konstytucyjnych zasad proporcjonalności i demokratycznego państwa prawa, ale także dotyczących przetwarzania danych osobowych zasad: zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, a także co do realizacji obowiązków administratora i praw podmiotów danych określonych w rozdziale III rozporządzenia 2016/679, w tym obowiązków informacyjnych oraz rozliczalności.

Korzystanie z publicznej infrastruktury monitoringu wizyjnego w celach ogólnych, w tym prewencyjnych, przez organy ścigania może powodować poważne zagrożenia dla **konstytucyjnie chronionych praw i wolności jednostki**, w tym godności, wolności, równości, prawa do prywatności oraz autonomii informacyjnej. Może również wzbudzać wątpliwości co do potencjalnego wykorzystywania takich narzędzi, szczególnie dlatego, że pozyskiwanie danych przez Policję może przyjmować charakter niejawnny. Na tego

¹⁵ Por. art. 25 ust. 6d i 6g ustawy z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587).

rodzaju zagrożenia wskazał także Rzecznik Praw Obywatelskich, w wystąpieniu kierowanym do Szefa Agencji Bezpieczeństwa Wewnętrznego¹⁶.

III. Przetwarzanie danych biometrycznych w kontekście urządzeń monitorujących.

A. Otoczenie prawne, orzecznictwo i doktryna.

Korzystanie z technologii rozpoznawania twarzy jest nierozdzielnie związane z przetwarzaniem danych osobowych, w tym **szczególnych kategorii danych**. Wizerunek danej osoby i dane biometryczne¹⁷ są cechami biologicznymi tej osoby – opierają się na jej indywidualnych cechach i pozwalają na jej jednoznaczną identyfikację, zwłaszcza przy powiązaniu i porównaniu z innymi informacjami, w tym osobowymi lub też służyć mogą dla identyfikacji osób. Podkreślenia wymaga, że ogólne rozporządzenie o ochronie danych osobowych klasyfikuje wizerunki twarzy jako dane biometryczne wtedy, gdy podlega „specyficznemu przetwarzaniu technicznemu umożliwiającemu unikalną identyfikację lub uwierzytelnienie osoby fizycznej”¹⁸. Zwykle wiąże się to z wykorzystaniem danych z obrazu do utworzenia indywidualnego szablonu cyfrowego lub profilu, który z kolei jest wykorzystywany do automatycznego dopasowywania lub identyfikacji obrazów.

Rodzaj przetwarzania biometrycznego, zdefiniowany w opinii nr 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych przez Grupę Roboczą Art. 29¹⁹ został jako „automatyczne przetwarzanie obrazów cyfrowych, które zawierają twarze osób fizycznych w celu identyfikacji, uwierzytelniania/weryfikacji lub kategoryzacji tych osób”²⁰, niezależnie od tego, czy osoby fizyczne wyraziły zgodę lub posiadają wiedzę na temat jego wykorzystania. Korzystanie z rozpoznawania twarzy z użyciem technologii biometrycznej ma więc bezpośredni lub pośredni wpływ na szereg podstawowych praw i wolności zagwarantowanych w przepisach prawa: Karty praw podstawowych Unii Europejskiej²¹, Konstytucji RP oraz rozporządzenia 2016/679.

Przetwarzanie danych biometrycznych zostało uregulowane w art. 9 rozporządzenia 2016/679, a w przypadku organów ścigania – w art. 10 dyrektywy (UE)

¹⁶ Por. stanowisko wyrażone w wystąpieniu Rzecznika Praw Obywatelskich w sprawie udostępniania organom ścigania stałego dostępu do kamer monitoringu zainstalowanego w pojazdach komunikacji publicznej: <https://bip.brpo.gov.pl/pl/content/abw-kamery-tramwaje-warszawa-rpo>

¹⁷ Zgodnie z art. 3 pkt 13 dyrektywy 2016/680: „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, takie jak wizerunek twarzy lub dane daktyloskopijne

¹⁸ Motyw 51 rozporządzenia 2016/679.

¹⁹ Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE jako niezależny organ doradczy w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE. Z dniem 25 maja 2018 r. Grupę Roboczą Art. 29 zastąpiła EROD.

²⁰ Opinia Grupy Roboczej Art. 29 nr 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych, przyjęta w dniu 27 kwietnia 2012 r., 00720/12/PL WP193.

²¹ Dz.U.UE.C.2007.303.1 z dnia 2007.12.14., zob. Artykuł 8 ust. 1 Karty.

2016/680. **Przetwarzanie danych biometrycznych jest zgodne z prawem jedynie w szczególnych okolicznościach, określonych w art. 9 ust. 2 rozporządzenia 2016/679** (m.in. gdy osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie lub gdy jest to niezbędne ze względu na istotny interes publiczny). Jeżeli prawodawca czy wykonawca normy (administrator) powołuje się na niezbędność przetwarzania związaną z ważnym interesem publicznym na podstawie prawa Unii lub prawa państwa członkowskiego (art. 9 ust. 2 lit. g rozporządzenia 2016/679) przetwarzanie musi być proporcjonalne do zamierzonego celu i należy wprowadzić odpowiednie środki w celu ochrony praw podstawowych osoby, której dane dotyczą. Wszelkie działania podejmowane przez podmioty publiczne (w tym przez organy ścigania czy samorządu terytorialnego) powinny mieć oparcie w obowiązujących przepisach prawa regulujących ich działalność (art. 7, 31, 51 Konstytucji RP).

Zgodnie z zasadą legalności, rzetelności wyrażonymi w **art. 4 ust. 1 lit. a dyrektywy 2016/680** – dane osobowe mogą być przetwarzane wyłącznie wtedy, kiedy istnieje podstawa prawna ich przetwarzania. Podstawa prawna do przetwarzania (w tym pozyskiwania) danych osobowych powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami. Zgodnie art. 13 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W ww. ustawie uregulowane są w szczególności zasady przetwarzania danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej – dane szczególnych kategorii (zw. danymi wrażliwymi). Zgodnie z art. 14 ust. 1 ww. ustawy przetwarzanie wskazanych danych jest co do zasady zabronione, chyba że spełniony jest jeden z warunków wskazanych w ust. 2 tego artykułu, w tym w szczególności, gdy przepisy prawa zezwalają na ich przetwarzanie (pkt 1), by właściwy organ mógł legalnie przetwarzać dane biometryczne w celach, o których mowa w art. 1 pkt 1 ustawy z 14 grudnia 2018 r., takie uprawnienie musi wynikać wprost z przepisu prawa rangi ustawy. Zwolnienia z podstawowych praw i uzasadnionych interesów osoby fizycznej powinny być stosowane jako wyjątek, a nie jako reguła, a pominięcie informacji może być dozwolone w ramach postępowania przygotowawczego tylko tak długo, jak takie ograniczenie stanowi konieczny i proporcjonalny środek²².

Przetwarzanie danych biometrycznych jest dozwolone tylko wtedy, gdy jest to „ściśle niezbędne” do konkretnych celów zapobiegania przestępstwom, prowadzenia

²² Opinia Grupy Roboczej Art. 29 2017/258 w sprawie niektórych kluczowych kwestii związanych z dyrektywą w sprawie egzekwowania prawa (2016/680). Przyjęto 20.11.2017 r.

dochodzeń w ich sprawie, ich wykrywania lub ścigania lub wykonywania kar (art. 10 dyrektywy 2016/680). W motywie 33 zdanie 3 dyrektywy 2016/680 prawodawca wskazał, że: „Prawo państwa członkowskiego regulujące przetwarzanie danych osobowych w ramach zakresu zastosowania niniejszej dyrektywy powinno co najmniej określać cele ogólne, dane osobowe mające podlegać przetwarzaniu, cele przetwarzania oraz procedury pozwalające chronić integralność i poufność danych osobowych oraz procedury niszczenia tych danych, a tym samym powinno zapewniać dostateczną ochronę przed ryzykiem nadużyć i arbitralności”.

Ścisłe kryterium konieczności (niezbędności) wynika także z orzecznictwa TSUE²³.

Zwrócić uwagę należy na obawy dotyczące adekwatności stosowania inwazyjnego stosowania kamer, na które wskazał Wysoki Komisarz ONZ ds. Praw Człowieka w 2018 r.: „Tworzenie masowych baz danych biometrycznych budzi poważne obawy dotyczące praw człowieka. Takie dane są szczególnie wrażliwe, ponieważ z definicji są nierozdzielnie związane z konkretną osobą i jej życiem, a także mogą być poważnie nadużywane. Na przykład kradzież tożsamości na podstawie danych biometrycznych jest niezwykle trudna do zaradzenia i może poważnie wpłynąć na prawa jednostki. Ponadto dane biometryczne mogą być wykorzystywane do innych celów niż te, do których zostały zebrane, w tym do nielegalnego śledzenia i monitorowania osób fizycznych. Biorąc pod uwagę te zagrożenia, należy zwrócić szczególną uwagę na kwestie konieczności i proporcjonalności w gromadzeniu danych biometrycznych”. W związku z tym, że ich instalacja opiera się na szeroko opracowanych podstawach prawnych, systemy biometrycznego nadzoru wideo unikają konieczności wykazania konkretnego celu ich instalacji w poszczególnych miejscach, w których mają siedzibę.

EDRI (European Digital Rights) – największa europejska sieć ochrony praw i wolności w sferze cyfrowej – wskazała w swoich analizach, że każde wykorzystanie danych biometrycznych, które mogłoby prowadzić do masowej inwigilacji, jest z natury niepotrzebne i nieproporcjonalne w świetle europejskiego prawa dotyczącego praw człowieka, dodając, że praktyki masowej inwigilacji biometrycznej nadmiernie naruszają prywatność, ochronę danych oraz równość²⁴.

Grupa Robocza Art. 29 stwierdziła, że „ściska konieczność” wymaga dalszej wykładni, ponieważ orzecznictwo TSUE nie wyjaśniło jego znaczenia, oraz stwierdziła, że pojęcie to należy rozumieć jako „wezwanie do zwrócenia szczególnej uwagi na zasadę konieczności”²⁵. Zbieranie danych biometrycznych może odbywać się zgodnie z

²³ Zob. sprawy połączone C 293/12 i C 594/12 Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. i Kärntner Landesregierung i in., 2014 r., pkt 52 I nast.

²⁴ EDRI „The rise and rise of biometric mass surveillance in EU. A legal analysis of biometric mass surveillance practices in Germany, The Netherlands, and Poland.

²⁵ Opinia w sprawie niektórych kluczowych kwestii dyrektywy w sprawie egzekwowania prawa (UE 2016/680) dostępna na stronie <https://ec.europa.eu/newsroom/article29/item-detail>. CFM?item_id=610178, s. 7-8.

konstytucyjnym porządkiem prawnym tylko pod warunkiem wprowadzenia odpowiednich zabezpieczeń w celu ochrony podstawowych praw osób, których dane dotyczą.

Przetwarzanie danych biometrycznych dokonywane być powinno również z uwzględnieniem Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo przyjętych w dniu 29 stycznia 2020 r. przez Europejską Radę Ochrony Danych²⁶. EROD wskazała w nich, że wykorzystywanie danych biometrycznych, a zwłaszcza technologii rozpoznawania twarzy, wiąże się ze zwiększonymi ryzykami dla praw osób, których dane dotyczą. Kluczowe jest, by korzystanie z takich technologii odbywało się z należyтым uwzględnieniem zasad zgodności z prawem, konieczności, proporcjonalności i minimalizacji danych, jak określono w rozporządzeniu 2016/679. Podczas gdy używanie takich technologii może być postrzegane jako szczególnie skuteczne, prawodawcy powinni jednak najpierw ocenić ich wpływ na podstawowe prawa i wolności oraz rozważyć zastosowanie mniej inwazyjnych środków do osiągnięcia prawnie uzasadnionego celu przetwarzania. Ww. wytyczne są pomocne zarówno dla ustawodawcy, jak i dla wykonawców norm.

Co do wykorzystywania monitoringu wizyjnego w przestrzeni publicznej lub stosowanego w miejscach publicznie dostępnych, takich jak np. dworce kolejowe, stacje przesiadkowe metra, z których ludzie korzystają i nie mają innego wyboru, niezależnie od tego, czy sprzeciwiają się gromadzeniu swoich danych, czy nie, zwrócić uwagę należy na zgodę osoby, której dane dotyczą na wykorzystanie jej wizerunku w takich okolicznościach.

W wyroku Michael Schwarz przeciwko Stadt Bochum²⁷ Trybunał Sprawiedliwości Unii Europejskiej potwierdził, że zgoda osoby, której dane dotyczą, jest wątpliwa, jeżeli osoba nie ma rzeczywistego wyboru, by sprzeciwić się przetwarzaniu jej danych. Bez odpowiedniego pozyskania świadomej zgody osoby, których dane dotyczą, podmioty danych mogą nie mieć pojęcia, że ich dane osobowe są gromadzone, jakie dane osobowe obejmuje to gromadzenie, kto zbiera dane lub do jakich celów służy ich gromadzenie.

Z kolei w sprawie S i Marper przeciwko Zjednoczonemu Królestwu²⁸ (skarga nr 30562/04 i 30566/04), Europejski Trybunał Praw Człowieka orzekł, że powszechne i masowe przetwarzanie i zatrzymywanie danych biometrycznych stanowi nieproporcjonalną ingerencję w prawa zapisane w art. 8 ust. 1 Konwencji o ochronie praw człowieka²⁹: „ochrona danych osobowych ma fundamentalne znaczenie dla korzystania z prawa do poszanowania życia prywatnego i rodzinnego

²⁶ Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo dostępne są pod linkiem: <https://www.uodo.gov.pl/pl/414/1332>.

²⁷ C-291/12 Schwarz przeciwko Stadt Bochum (TSUE, 2013) 2 C.M.L.R. 5

²⁸ S i Marper przeciwko Zjednoczonemu Królestwu, Applications nos. 30562/04 i 30566/04 (ETPC, 4 grudnia 2008 r.).

²⁹ Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U.1993.61.284 z dnia 1993.07.1

zagwarantowanego w art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności. Prawo krajowe musi zapewnić odpowiednie zabezpieczenia przed użyciem danych osobowych niezgodnym z gwarancjami tego artykułu. Potrzeba zabezpieczeń jest jeszcze większa w przypadku ochrony danych osobowych poddawanych automatycznemu przetwarzaniu, w tym używanych dla celów policyjnych. Prawo krajowe musi w szczególności zapewnić, aby dane takie były: istotne ze względu na cel ich gromadzenia oraz zachowane w formie umożliwiającej identyfikację osoby, której dotyczą, nie dłużej niż przez okres wymagany ze względu na wymieniony cel. Prawo krajowe musi również zapewnić odpowiednie gwarancje skutecznej ochrony przechowywanych danych osobowych przed niewłaściwym użyciem lub nadużyciem. Jest to szczególnie ważne przy ochronie specjalnych kategorii danych bardziej wrażliwych”.

Konieczne jest również wzięcie pod uwagę wyroku Trybunału Sprawiedliwości Unii Europejskiej z 26 stycznia 2023 r. w sprawie C-205/21, w którym podkreślono, że przetwarzanie danych biometrycznych i genetycznych przez organy policji dla celów prowadzenia czynności dochodzenia, walki z przestępczością i utrzymania porządku publicznego jest dopuszczone prawem państwa członkowskiego, gdy prawo tego państwa członkowskiego zawiera wystarczająco jasną i precyzyjną podstawę prawną dla zezwolenia na wspomniane przetwarzanie. Ponadto wskazano, że przepisy krajowe przewidujące systematyczne zbieranie danych biometrycznych i genetycznych każdej osoby, której przedstawiono zarzuty popełnienia umyślnego przestępstwa ściganego z oskarżenia publicznego, jest co do zasady niezgodne z wymogiem wskazanym w art. 10 dyrektywy 2016/680, zgodnie z którym przetwarzanie szczególnych kategorii danych wskazanych w tym artykule powinno być dozwolone wyłącznie wtedy, jeżeli jest bezwzględnie niezbędne. Jednocześnie motyw 41 rozporządzenia 2016/679 i motyw 33 dyrektywy 2016/679 wskazują, że podstawa prawna lub akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających. Należy również wziąć pod uwagę wpływ na przestrzegających prawa obywateli korzystających ze swoich praw podstawowych, takich jak prawo do wolności wypowiedzi na mocy art. 10 Konwencji o ochronie praw człowieka oraz prawo do wolności zgromadzeń i zrzeszania się na mocy art. 11 tej konwencji. Podmioty/organy przetwarzające dane biometryczne przy zastosowaniu technologii rozpoznawania twarzy muszą przestrzegać wszystkich obowiązujących zasad i przepisów dotyczących ochrony danych oraz muszą być w stanie wykazać, że takie zastosowanie jest ściśle niezbędne i proporcjonalne w określonym kontekście ich stosowania oraz że nie narusza praw osób, których dane dotyczą³⁰. W Wytycznych Konwencji 108 dotyczących rozpoznawania twarzy wskazano,

³⁰ Wytyczne konwencji 108 „Wytyczne dotyczące rozpoznawania twarzy” z 8 stycznia 2021 r., T-PD(2020)03rev4. W ww. Wytycznych zostało wskazane, że cele egzekwowania prawa odpowiadają „celom policji” w Praktycznym przewodniku dotyczącym wykorzystywania danych osobowych w sektorze policji, zob. Komitet Konwencji 108, Praktyczny przewodnik dotyczący wykorzystywania danych osobowych w

że do celów identyfikacji należy przestrzegać ścisłej konieczności i proporcjonalności zarówno podczas tworzenia bazy danych, jak i wdrażania technologii rozpoznawania twarzy w niekontrolowanym środowisku. Przepisy powszechnie obowiązującego prawa powinny zatem określać jasne parametry i kryteria, których organy egzekwujące prawo powinny przestrzegać, dla tworzenia bazy danych do konkretnych, zgodnych z prawem i wyraźnych celów egzekwowania prawa (na przykład w przypadku podejrzenia poważnych przestępstw lub zagrożenia bezpieczeństwa publicznego).

Istotne jest, aby dokonać osobnej analizy pod względem uczynienia zadość przepisom Aktu w sprawie sztucznej inteligencji³¹, szczególnie pod względem zakazanych praktyk i systemów wysokiego ryzyka³². W tym kontekście zwrócić należy uwagę na kwestie związane z **profilowaniem**, którego definicja legalna została zawarta w art. 4 pkt 4 rozporządzenia 2016/679 i art. 3 pkt 4 dyrektywy 2016/680. Jest to zautomatyzowane przetwarzanie danych osobowych służące do oceny niektórych czynników osobowych osoby fizycznej (np. do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się). Motyw 38 ww. dyrektywy 2016/680 stanowi, że: „Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie stosowano względem niej decyzji analizującej jej cechy osobiste, opierającej się wyłącznie na przetwarzaniu automatycznym, która ma niekorzystne skutki prawne dla takiej osoby lub poważnie na nią wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, wraz z konkretną informacją dla osoby, której dane dotyczą, i prawem do uzyskania interwencji ludzkiej, a zwłaszcza prawem do wyrażenia własnego stanowiska, uzyskania wyjaśnienia decyzji wydanej wskutek takiej analizy lub zaskarżenia tej decyzji. Profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, powinno być zakazane na warunkach określonych w art. 21 i 52 Karty”. Zestawiając te definicje z definicją systemu sztucznej inteligencji nietrudno dojść do wniosku, że algorytmy sztucznej inteligencji analizujące dane osobowe mogą dokonywać profilowania. Ogólne rozporządzenie o ochronie danych

sektorze policji (T-PD(2018)01), dostępny na: <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>.

³¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).

³² Zob. wspólna opinia Europejskiej Rady Ochrony Danych i Europejskiego Inspektora Ochrony Danych (EIOD) dotycząca zakazu wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w przestrzeni publicznej oraz niektórych innych zastosowań sztucznej inteligencji, które mogą prowadzić do niesprawiedliwej dyskryminacji, a także opinia Europejskiej Rady Ochrony Danych 28/2024 z 17 grudnia 2024 r. w sprawie wykorzystywania danych osobowych do opracowywania i wdrażania modeli sztucznej inteligencji: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl

osobowych wymaga przekazania osobom, których dane dotyczą informacji o automatycznym podejmowaniu decyzji, w tym o profilowaniu, oraz informacji o zasadach ich podejmowania, jednocześnie zaznaczając o konsekwencjach tego przetwarzania dla osoby, której dane dotyczą, zgodnie z art. 13 lub 14, w zależności od kogo pochodzą dane osobowe. Prawa osób, których dane dotyczą, określone w dyrektywie 2016/680 są podobne do praw przewidzianych w rozporządzeniu 2016/679 i muszą być zagwarantowane przez prawodawcę. Jest tutaj dopuszczalna interwencja ludzka ze strony administratora, który ma prawo wyrażenia własnego stanowiska oraz zakwestionowania danej decyzji. Poza profilowaniem rozporządzenie 2016/679 stanowi w art. 22 ust. 1 o zautomatyzowanym podejmowaniu decyzji, a więc takim, w którym człowiek nie uczestniczy. Ogólne ramy systemu ochrony danych osobowych wskazują na względny zakaz zautomatyzowanego podejmowania decyzji. Wskazany przepis ma zastosowanie tylko do takich zautomatyzowanych decyzji, które wywołują wobec danej osoby skutki prawne lub w podobny sposób istotnie na nią wpływają. Co istotne, zgodnie z rozporządzeniem 2016/679, co do zasady podmioty danych mają prawo do tego, by nie podlegać zautomatyzowanym decyzjom. Powyższe nie ma zastosowania w przypadkach, gdy decyzja: jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub opiera się na wyraźnej zgodzie osoby, której dane dotyczą. W przypadku systemów sztucznej inteligencji wykorzystujących monitoring, w zdecydowanej większości przypadków będzie dochodziło do przetwarzania danych osobowych (np. profilowanie, automatyczne podejmowanie decyzji), co może prowadzić do naruszeń praw podstawowych.

B. Inicjatywa legislacyjna.

Odnosząc się do powyższych rozważań, w opinii Prezesa UODO brak jest w polskim systemie prawa przejrzystych i wyczerpujących przepisów prawa regulujących kwestie związane ze stosowaniem urządzeń monitoringu wizyjnego przez organy Policji oraz wykorzystywania danych biometrycznych.

W świetle ogólnych przepisów ustawy o Policji dotyczących przetwarzania danych osobowych, na podstawie art. 20 ust. 1-1d i 2b w zw. z art. 1 ust. 1 pkt 4 i art. 14 ust. 2 ustawy o Policji, Policja posiada uprawnienia do przetwarzania danych biometrycznych, w tym w postaci wizerunku (zdjęcia) w celu realizacji zadań ustawowych Policji w zakresie wykrywania i ścigania sprawców przestępstw. Nie istnieje natomiast **odpowiednia podstawa prawna do przetwarzania danych biometrycznych za pomocą monitoringu wizyjnego**. Taka podstawa prawna powinna w szczególności przewidywać gwarancje proporcjonalności i niezbędności dla poszanowania praw podmiotów danych przy przetwarzaniu danych szczególnych kategorii, jakimi są dane

biometryczne, oraz dla przetwarzania danych w sposób zautomatyzowany, czy dla profilowania. W celu realizacji zadań ustawowych Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, z zachowaniem ograniczeń wynikających z art. 19 (art. 20 ust. 1 ustawy o Policji). Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może dotyczyć danych osobowych, o których mowa w art. 14 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, tj. m.in. danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej.

Z ww. przepisów wynika, że dotąd ustalone przez ustawodawcę unormowania **są niewystarczające, bowiem nie spełniają wymagań dla norm mogących stanowić podstawę prawną do stosowania technologii biometrycznych**, w tym rozpoznawania twarzy, w szczególności nie zawierają konkretnej normy odnoszącej się wprost do stosowania takich technik, uwzględniającej wymogi konieczności i proporcjonalności oraz jasno wskazującej warunki i okoliczności, w których organy ścigania są uprawnione do ich wykorzystywania. Zauważyć należy, że używanie technologii w postępowaniu prowadzonym przez organy ścigania ma wpływ na postępowanie karne i przetwarzanie tych informacji nie tylko przez Policję, ale i przez organy wymiaru sprawiedliwości.

Podstawy prawnej legalizującej stosowanie monitoringu, który w sposób stały przetwarzałby dane biometryczne nie może stanowić także oczekujący na wejście w życie art. 20 ust. 1aa ustawy o Policji³³. Przepis ten zezwala Policji na przetwarzanie danych biometrycznych w postaci wizerunków twarzy, ale **wyłącznie w zakresie identyfikacji lub weryfikacji tożsamości osoby, której dotyczą wykonywane zadania lub czynności wykrywcze czy dowodowe**. Przetwarzanie danych biometrycznych może zatem dotyczyć jedynie osoby sprawcy, osoby poszukiwanej, czy z innego powodu typowanej w toku prowadzonych czynności. Przepis ten nie może jednak stanowić podstawy prawnej do przetwarzania w sposób stały, systematycznych danych biometrycznych wszystkich osób postronnych objętych monitoringiem, czy do badań przesiewowych/eliminacyjnych³⁴.

W ocenie organu nadzorczego, wymagane jest podjęcie prac legislacyjnych, mających na celu **ustawowe uregulowanie** w sposób kompleksowy kwestii związanych ze stosowaniem różnego rodzaju form monitoringu przez Policję, w tym także monitoringu wykorzystującego biometryczne rozpoznawanie tożsamości, poprzez wprowadzenie:

- 1) konkretnej podstawy prawnej,
- 2) właściwe określenie warunków przetwarzania,

³³ Wprowadzony ustawą z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu (Dz. U. z 2024 r. poz. 1688), art. 19 pkt 1.

³⁴ Por. wyroki TSUE z dnia 19 marca 2026 r. w sprawie o sygn. C-371/24, z 30 stycznia 2024 r. w sprawie o sygn. C- 118/22 oraz z dnia 26 stycznia 2023 r. C-205/21.

- 3) metod, środków technicznych, zakresu oraz form przetwarzania,
- 4) sposobów postępowania z danymi sensytywnymi,
- 5) **środków ochrony praw osób**, których dane dotyczą, a nade wszystko
- 6) **przejrzyste określenie celów do jakich monitoring biometryczny może być stosowany, a w jakim zakresie jego stosowanie jest niedozwolone.**

Aby organy ścigania mogły przetwarzać dane biometryczne w związku z wykonywaniem ich ustawowych zadań, powinny dysponować przepisami, które ogólnie określają klauzule zapewniające, że techniki rozpoznawania biometrycznego są stosowane tylko **w realnie wymaganym i niezbędnym, adekwatnym zakresie** – tak aby służył on wyłącznie zapewnieniu bezpieczeństwa (a nie innym, ubocznym, niepożądanym celom), w sposób proporcjonalny dla praw osób, których dane dotyczą, uwzględniając jednocześnie gwarancje wynikające z przepisów o ochronie danych osobowych.

Jeżeli tego rodzaju monitoring miałby dotyczyć szerszego kręgu osób, przepisy powinny określać wymóg pozyskiwania danych w zakresie proporcjonalnym do celów przetwarzania. Przede wszystkim określać wyczerpująco i przejrzyście:

- 1) **rodzaje przestępstw, zjawisk kryminogennych lub działań prewencyjnych** w stosunku do których techniki biometrycznej identyfikacji mogłyby być używane – **ograniczając się do najpoważniejszych czynów zabronionych czy zagrożeń;**
- 2) **reguły dostępu i wykorzystywania zebranych danych,**
- 3) sposoby i zakres **udostępniania** danych, w szczególności w stosunku do innych służb państwa,
- 4) czas, po jakim te dane osobowe, które nie stały się dowodem w danej sprawie, zostaną usunięte.

Zmiany w prawie wprowadziłyby jednolite kryteria oraz standardy bezpieczeństwa i poufności danych, a także procedury zapobiegające ryzykom wykorzystywania nagrań w celach niezgodnych z *ratio legis*, takim jak niedozwolone profilowanie, śledzenie, czy inwigilacja. Regulacja ustawowa jest kluczowa dla ustalenia jednolitego standardu przetwarzania danych osobowych wprowadzając przejrzyste i rzetelne reguły postępowania, z korzyścią nie tylko dla osób, których dane dotyczą, ale również dla wykonawców norm (administratorów, podmiotów przetwarzających).

Osobnej analizie należy podjąć się w stosunku do przepisów **ustawy o strażach gminnych**, biorąc pod uwagę wagę i specyfikę zadań wykonywanych przez te formacje oraz zakres współpracy z jednostkami organizacyjnymi gminy, rozstrzygając czy w ogóle – a jeżeli tak, to w jakim zakresie i w jakich celach – funkcjonariusze straży mogą wykorzystywać technologie biometrycznego przetwarzania danych pozyskiwanych z rejestracji obrazu.

IV. Podsumowanie.

W związku z przedstawionymi powyżej okolicznościami, **zwracam się z uprzejmą prośbą o podjęcie przez Pana Ministra analizy** pod względem zasadności i podstaw prawnych zawierania przez jednostki Policji porozumień z organami samorządów terytorialnych dotyczących przekazywania pełnego, stałego i długotrwałego obrazu wizji z monitoringu – w dotychczasowo stosowanej formie.

Jednocześnie, liczę również na rozważenie przez Pana Ministra kwestii związanych z wykorzystywaniem technik biometrycznych w urządzeniach służących do rejestrowania obrazu zdarzeń w miejscach publicznych przez funkcjonariuszy Policji wykonujących czynności służbowe, pod względem ich legalności, a także możliwych i oczekiwanych zmian legislacyjnych regulujących tę materię.

Wyrażam nadzieję, że w drodze stosownej i przemyślanej regulacji ustawowej możliwe jest wprowadzenie stabilnych rozwiązań prawnych, które z jednej strony zapewniałyby Policji skuteczne środki zapewniania bezpieczeństwa obywateli, z drugiej zaś stosowne środki gwarancyjne, dając rękojmię respektowania – kluczowych w demokratycznym państwie prawa – praw do prywatności, do autonomii informacyjnej obywateli, do możliwości swobodnego funkcjonowania w przestrzeni publicznej, poprzez stosowanie technologii rejestracji obrazu w zakresie realnie niezbędnym i adekwatnym, w sposób przejrzysty i zapewniający środki kontroli procesów przetwarzania.

W przypadku podjęcia prac legislacyjnych w związku z przedstawionymi powyżej zagadnieniami Prezes Urzędu Ochrony Danych Osobowych deklaruje gotowość do eksperckiego wsparcia przy wypracowywaniu konkretnych przepisów, także w drodze spotkań służbowych, mających na celu szersze omówienie przedmiotowej materii.

W świetle przedstawionej powyżej argumentacji uprzejmie proszę o odniesienie się do tego wystąpienia na **piśmie w ustawowym terminie 30 dni** od daty jego otrzymania.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

Do wiadomości:

Pani Sylwia Gregorczyk-Abram
Rzecznik Praw Obywatelskich