



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*dr Wojciech R. Wiewiórowski*

**DOLiS – 033 – 523/13**

Warszawa, dnia 13 sierpnia 2014 r.

**Pan  
Grzegorz Karpiński  
Podsekretarz Stanu w  
Ministerstwie Spraw Wewnętrznych  
ul. Stefana Batorego 5  
02-591 Warszawa**

w odpowiedzi na pismo z dnia 9 lipca 2014 r. o sygnaturze: DP-I-0231-156/2013/MM dotyczące **Projektu założeń do projektu ustawy o monitoringu wizyjnym**, w jego wersji z dnia 7 lipca 2014 r., zwanego dalej „projektem założeń”, Generalny Inspektor Ochrony Danych Osobowych dziękuje za wzięcie po uwagę części sugestii GIODO przedstawionych jako komentarz do projektu założeń w wersji z dnia 18 grudnia 2013 r., zgłoszone pismem z dnia 22 stycznia 2014 r. o sygn. DOLiS-033-523/13. Mimo iż niniejsze pismo zawiera bardzo szeroką listę uwag i propozycji zmian, proszę potraktować je nie jako negację świetnej pracy wykonanej przez Ministerstwo, lecz jako wkład w dyskusję, która zdaniem GIODO powinna dążyć do jak najszybszego zakończenia prac nad projektem założeń.

**I. Uwagi ogólne.**

W szczególności, na słowa uznania zasługuje uwzględnienie wskazówek Generalnego Inspektora i widoczną zmianę paradygmatu przyświecającego wprowadzeniu regulacji monitoringu wizyjnego do polskiego porządku prawnego. Zmiana ta jest widoczna w samej systematyce projektu założeń, gdzie po określeniu zakresu przedmiotowego i podmiotowego projektu założeń (3.1.1), wskazano przede wszystkim zasady prowadzenia monitoringu wizyjnego (3.1.2),

zaprezentowano zagadnienia dotyczące prawa do informacji o objęciu monitoringiem i obowiązek informacyjny (3.1.3) oraz określono przedmiot ochrony – a mianowicie ochronę wizerunku lub charakterystycznych cech zarejestrowanego obiektu. By lepiej oddać cel projektowanej regulacji, jakim jest, zgodnie z pkt 1.1 „zapewnienie gwarancji przestrzegania praw i wolności konstytucyjnych poprzez unormowanie zasad prowadzenia monitoringu wizyjnego oraz określenie praw osób, których wizerunki są obserwowane”, być może należałoby zmienić kolejność proponowanych punktów i wcześniej, jeśli nie na pierwszym po celu miejscu, umieścić przedmiot ochrony projektu założeń. Dopiero po nim można by określić zarówno zakres przedmiotowy oraz podmiotowy projektu założeń – dane osobowe przetwarzane w ramach systemu wideo-monitoringu, oraz administratorów danych, jak również krąg podmiotów uprawnionych do dostępu do tychże danych.

Zastanawiające jest pominięcie w pkt 1 projektu założeń („Cel i istota projektowanej regulacji”) odniesienia do prawa do ochrony informacji dotyczących osoby (art. 51 Konstytucji, Dz. U. z 1997 r. Nr 78, poz. 483 z późn. zm.) oraz wśród aktów wyliczonych w pkt. 2 projektu założeń („Obowiązujący Stan Prawny”) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), zwanej dalej **ustawą o ochronie danych osobowych** oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024). W istocie, w obecnym stanie prawnym, to ta ustawa stanowi podstawę przetwarzania danych osobowych w systemach monitoringu wizyjnego. Należy podkreślić, że intencją ustawodawcy było objęcie polskich obywateli wyższym standardem ochrony niż ten przewidziany przepisami Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. L 281/31 z 23.11.1995 r.) (wyłączenie przetwarzania danych dźwiękowych i obrazowych ujęte w pkt 16 preambuły). Polska ustawa o ochronie danych osobowych nie ma takiego wyłączenia i obejmuje również kwestie związane z przetwarzaniem danych dźwiękowych i obrazowych dokonywanych dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub w trakcie działań organów państwowych w dziedzinie prawa karnego lub innych działań niewchodzących w zakres prawa Unii Europejskiej. Stąd zasadnym wydaje się uwzględnienie ustawy o ochronie danych osobowych jako jednego z najważniejszych aktów prawnych spośród obowiązujących w momencie opracowania założeń do projektu ustawy. Pominięcie kwestii

wzajemnego stosunku tych dwóch aktów prawnych może prowadzić do stworzenia systemu ochrony równoległego do systemu ochrony danych osobowych. Może to doprowadzić do dublowania obowiązków administratorów systemów monitoringu.

Nie może spotkać się z aprobatą Generalnego Inspektora postulowana możliwość dopuszczenia wprowadzania monitoringu wizyjnego w zakładach pracy i innych, wskazanych w umowach, miejscach, **w celu optymalizacji lub weryfikacji sposobów wykonywana powierzonych obowiązków** wynikających ze stosunku pracy lub umów cywilnoprawnych. Jest to wyraźne odejście od celów określonych w poprzednim projekcie założeń (z 18 grudnia 2013 r.). Należy zwrócić uwagę, że takie rozwiązanie przeczy zasadom wynikającym z prawa pracy. O ile monitoring wizyjny wykorzystywany do celów ochrony mienia i osób nie wzbudzał nigdy zastrzeżeń GIODO o ile był odpowiednio uzasadniony, o tyle *"optymalizacja lub weryfikacja sposobów wykonywana powierzonych obowiązków "* jest sformułowaniem zdecydowanie zbyt szerokim.

Wątpliwość rodzi także szeroki zakres i pewne niedookreślenie wszelkich celów, dla których może być stosowany monitoring wizyjny. W tekście projektu obok w/w celu oraz zapewnienia bezpieczeństwa i porządku publicznego lub ochrony osób i mienia, pojawiają się także ogólnikowe określenia, takie jak „zarządzanie kryzysowe” (punkt 3.1.1. oraz 3.2.1.) czy „monitoring wizyjny prowadzony na cele publiczne” (definicja proporcjonalności w punkcie 3.1.2.). Należy także zwrócić uwagę, że monitoring może być prowadzony, gdy jest to konieczne i niemożliwym jest zapewnienie realizacji w/w dookreślonych celów innymi sposobami, które nie ingerują w sposób tak znaczący, jak stała obserwacja, w prawa jednostki. Należy w tym miejscu zasugerować wskazanie w sposób możliwie wyczerpujący celów, dla których może być prowadzony monitoring i ujęcie ich w części projektowanej regulacji dotyczącej zasad ogólnych (patrz punkt 3.1.2.).

Generalny Inspektor zwraca uwagę, iż przepisy ustawy mogą mieć wpływ na znaczącą liczbę aktów prawnych i konieczność ich zmiany w zakresie kompetencji organów regulowanych postanowieniami tych aktów.

W odniesieniu do poszczególnych zapisów projektu założeń następujące zagadnienia, w opinii Generalnego Inspektora Ochrony Danych Osobowych, wymagają doprecyzowania. Dla

przejrzystości odniesień będą one formułowane w kolejności przedstawienia zagadnień w projekcie założeń.

## II. Uwagi szczegółowe.

Zakres przedmiotowy regulacji ujęty w **punkcie 3.1.1.** obejmuje m.in. osoby prywatne oraz jednostki organizacyjne niebędące osobami prawnymi oraz osoby fizyczne. Wydaje się, iż doszło do oczywistej omyłki pisarskiej i projektodawca w trzecim punkcie wyliczenia ma na myśli osoby prawne.

Generalny Inspektor zwraca uwagę na konieczność przyszłego dostosowania obecnie obowiązujących przepisów szczególnych wymienianych przez projektodawcę (dotyczących uprawnień służb i metod prowadzenia monitoringu w sytuacjach specyficznych) do zasad ustalonych w toku obecnie prowadzonych prac.

W zakresie wyłączenia spod przepisów projektowanej ustawy systemów monitoringu wizyjnego, które nie umożliwiają identyfikacji osób, Generalny Inspektor uważa, iż takie przypadki powinny być uregulowane przepisami projektowanej ustawy. Postanowienia te powinny być rozwinięte przez projektodawcę. Mogłyby one wskazywać na obowiązek informowania osób obserwowanych, do jakiego celu takie systemy są wykorzystywane i że w toku ich działania nie dochodzi do przetwarzania obrazów umożliwiających identyfikację, a jedynie do określania liczby osób przebywających na danym obszarze itp. Funkcjonowanie takich systemów monitoringu bez udzielenia informacji o celu i metodzie działania może w świadomości osoby obserwowanej oznaczać formę nadzoru, która narusza jej prawa konstytucyjne, mimo iż możliwości tych systemów nie mają pozwalać na identyfikację osób obserwowanych. Może też dochodzić do wrażenia, iż administrator takiego systemu nie dopełnia obowiązku informacyjnego, o którym mowa w projekcie założeń. Aby uniknąć takich błędów, konieczne wydaje się informowanie osób nt. rzeczywistych celów obecności tego typu kamer i systemu monitoringu.

W tym miejscu należy ponownie zwrócić uwagę projektodawcy na możliwość korelacji pomiędzy przepisami przyszłej ustawy regulującej kwestię monitoringu, jako formy przetwarzania danych osobowych podlegającej także przepisom ustawy o ochronie danych osobowych.

Jak wskazano we wstępie pisma, Generalny Inspektor popiera wprowadzenie katalogu ogólnych zasad, którym ma podlegać monitoring, a o których mowa w **punkcie 3.1.2.** Jako że mają one mieć zastosowanie do wszystkich systemów monitoringu, koniecznym jest, aby miały one precyzyjny i ograniczający charakter. **Dlatego też sugeruje się określenie możliwych celów,**

którym ma służyć monitoring wizyjny przy okazji definiowania zasady celowości. Przewidywane przez projektodawcę dwa główne cele (bezpieczeństwo publiczne, ochrona osób i mienia) nie muszą obejmować wszystkich sytuacji, dla których będzie możliwe wykorzystywanie monitoringu. Szeroki zakres aktywności ludzkiej może oznaczać stosowanie różnych form monitoringu dla innych celów. Także one mogłyby być objęte regulacją. Dodatkowo należy zweryfikować, czy możliwa będzie zmiana celu przez administratora. W przypadku dopuszczenia takiej możliwości, konieczne byłoby ustalenie zasad takiego wykorzystania monitoringu w nowym celu. Przykładowo, regulacja taka została przewidziana w art. 26 ust. 2 ustawy o ochronie danych osobowych.

W odniesieniu do zasady proporcjonalności Generalny Inspektor zwraca uwagę na dwa aspekty. Nie jest zrozumiałym, dlaczego zasada ta miałaby mieć zastosowanie wyłącznie w przypadku monitoringu prowadzonego na cele publiczne. Zasada ta powinna obejmować formy monitoringu stosowane także w celach prywatnych z uwagi na fakt, iż może on obejmować także fragmenty przestrzeni publicznej.

Ocena, czy monitoring wizyjny może być stosowany, jak słusznie stwierdził projektodawca, powinna opierać się na ocenie efektywności alternatywnych, możliwych do zastosowania środków mających na celu realizowanie zadań w zakresie bezpieczeństwa i porządku publicznego lub ochrony osób i mienia. Wątpliwość natomiast budzi obecna formuła przeprowadzenia takiej oceny. Podmiot wprowadzający monitoring powinien mieć pewność, iż monitoring będzie miał pozytywny wpływ na podniesienie poziomu bezpieczeństwa. Nie będzie to jednakże możliwe przy obecnie proponowanym brzmieniu, w którym użyto słów „inne środki **wydają się** być mniej efektywne”. Może to spowodować dowolność w ocenie innych środków mających zapewnić bezpieczeństwo społeczeństwu, co nie jest dopuszczalne w przypadku tego niezwykle ważnego zagadnienia. Należy tutaj przypomnieć także stanowisko Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwanej dalej Grupą roboczą art. 29. Szerokie rozprzestrzenienie monitoringu w przestrzeni publicznej i prywatnej nie powinno w sposób nieuzasadniony ograniczać praw i wolności jednostki.<sup>1</sup>

Generalny Inspektor zwraca uwagę, iż wśród zasad określonych przez projektodawcę **brak jest zasady ograniczenia czasowego przetwarzania danych** uzyskanych w toku pracy systemów monitoringu. Ma ona bezpośredni związek z okresem retencji danych, o którym mowa w punkcie 3.1.7. Szczegółowe uwagi na ten temat zostaną poczynione w dalszej części pisma.

---

<sup>1</sup> Opinia Grupy Roboczej art. 29 nr 4/2004 o przetwarzaniu danych osobowych przy pomocy wideomonitoringu z dnia 11 lutego 2004 r., 11750/02/EN WP89, s. 4.

Na zakończenie należy zwrócić uwagę, iż katalog zasad mających regulować monitoring wizyjny powinien mieć zastosowanie do wszystkich rodzajów przestrzeni, które podlegają uregulowaniu przepisami projektowanej ustawy. Nie wydaje się właściwym różnicowanie dopuszczalności stosowania monitoringu w zależności od celów, jakim ma służyć. Jest to w szczególności widoczne w przypadku zasady proporcjonalności, gdzie wskazano, iż zastosowanie monitoringu prowadzonego na cele publiczne ma być możliwe, jeżeli inne środki wydają się być mniej efektywne. Obecna forma zapisu sugeruje, że ocena taka nie będzie konieczna w przypadku tworzenia systemów w innych celach.

W odniesieniu do proponowanego w **punkcie 3.1.3.** wyłączenia praw kontrolnych wynikających z art. 32 i 33 ustawy o ochronie danych osobowych Generalny Inspektor Ochrony Danych Osobowych wyraża swój zdecydowany sprzeciw. **Takie całkowite ograniczenie uprawnień jednostki należy uznać za nieproporcjonalne naruszenie konstytucyjnych zasad wyrażonych w art. 51 ust. 3 oraz ust. 4 Konstytucji RP.** Przedstawione przez projektodawcę przyczyny takiego stanu rzeczy są nieprzekonujące i niewystarczające w świetle obowiązujących przepisów prawa oraz nie przechodzą testu proporcjonalności rozwiązań prawnych. Niczym niepoparta obawa przed nadmiernym, wielokrotnym korzystaniem z tych uprawnień, która miałaby destabilizować funkcjonowanie systemów, nie może oznaczać wyeliminowania praw kontrolnych osoby obserwowanej. To m.in. te prawa mają umożliwić właściwe i sprawne wykorzystywanie systemów monitoringu wizyjnego dla celów określonych w projekcie. Zewnętrzna kontrola wykonywana przez osoby uprawnione jest jednym z elementów szeroko pojętych mechanizmów weryfikujących prawidłowość funkcjonowania systemów, w których może dochodzić do przetwarzania danych osobowych, wizerunków osób fizycznych oraz innych dóbr ludzkich chronionych prawem. Koniecznym jest przerehabilitowanie tego fragmentu w taki sposób, aby zapewnić poszanowanie praw jednostki przy jednoczesnym umożliwieniu administratorom systemów monitoringu ich sprawnego funkcjonowania. Ustawodawca przewidział taką możliwość chociażby w art. 23 ustawy o udostępnianiu informacji gospodarczej i wymianie danych gospodarczych (Dz. U. z 2010 r. nr 81 poz. 530, z późn. zm.). Zaś uprawnienie w zakresie dostępu do wizerunku zostało potwierdzone w wyroku Trybunału Konstytucyjnego z dnia 12 marca 2014 r. (sygn. akt P 27/13), który dotyczył wymagania od właściciela podania danych osoby prowadzącej pojazd, którym dokonano wykroczenia drogowego bez możliwości sprawdzenia zdjęcia z fotoradaru, które taki czyn dokumentuje. Należy także nadmienić, iż projektowane rozporządzenie

o ochronie danych osobowych<sup>2</sup>, którym zostanie wprowadzona jednolita, unijna regulacja będzie wzmacniać prawa kontrolne jednostki. Wszystkie akty prawne dotyczące choćby w najmniejszym stopniu przetwarzania danych osobowych będą musiały być z tymi zasadami komplementarne. Obecne doświadczenia z prawami kontrolnymi jednostek wskazują, że uprawnienia te nie są przez większość podmiotów danych nadużywane.

Przyznanie prawa dostępu do nagrań osobie obserwowanej powinno być także możliwe z innych uzasadnionych przyczyn. Może to mieć miejsce chociażby w sytuacji dochodzenia odszkodowań w postępowaniu cywilnym od sprawców szkód na własności, takich jak wypadki komunikacyjne czy przypadki dewastacji mienia. Z drugiej strony umożliwienie dostępu jedynie pewnym służbom państwowym (o czym mowa w szczególności w uwagach do punktu 3.7.) może powodować nierównowagę pozycji stron w ewentualnych postępowaniach.

W opinii Grupy Roboczej art. 29 postuluje się nawet na potrzebę **przygotowania przez administratora polityki prywatności**, w której rozwinięte i uszczegółowione byłyby m.in. informacje o administratorze danych, celach prowadzenia monitoringu, jego formach i zasięgu (techniczne możliwości systemu, w tym automatyczna identyfikacja), znanych lub przewidywanych kategoriach odbiorców danych, okresach retencji czy procedurze dostępu do nagrań. Byłby to dokument informacyjny dostępny w przystępnej formie dla osoby obserwowanej w siedzibie administratora lub na jego stronie internetowej. W tym zakresie projektodawca przewidział jedynie zróżnicowany obowiązek informowania o zasięgu działania systemu w punktach 3.2.5., 3.3.2. i 3.4. Zakres informacji udzielanych osobom obserwowanym powinien być oczywiście uzależniony od stopnia ingerencji w prawa jednostki.

W związku z omówionymi wyżej prawami kontrolnymi jednostki sugeruje się zbadanie relacji między projektowaną regulacją a przepisami art. 24 i 25 ustawy o ochronie danych osobowych dotyczącymi obowiązku informacyjnego. Z uwagi na specyfikę prowadzenia monitoringu wizyjnego, pełna realizacja tych norm przez administratora systemu może być znacząco utrudniona.

Generalny Inspektor zwraca uwagę na ocenę projektodawcy wyrażoną w **punkcie 3.1.4.** w zakresie, czy „obraz z monitoringu przedstawiający osobę, lecz będący jedynie podglądem danego miejsca w przestrzeni publicznej, nie stanowi danych osobowych, a danymi osobowymi jest dopiero obraz utrwalony na nośnikach danych.” Uprzejmie przypominam, że obraz przetwarzany przez elementy systemu monitoringu będzie stanowił dane osobowe w każdej sytuacji, gdy będzie

---

<sup>2</sup> Wniosek dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, COM(2012) 11, Dz. Urz. C 102 z dnia 5 kwietnia 2012 r., s. 24.

on dotyczył zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zgodnie z postanowieniem art. 6 ust. 2 ustawy o ochronie danych osobowych, osobą możliwą do zidentyfikowania jest m.in. osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. **Tak więc podgląd danego miejsca za pośrednictwem monitoringu może stanowić o przetwarzaniu danych osobowych.** Należy nadmienić, że ciągły rozwój technologii audiowizualnych pozwala coraz precyzyjniej obserwować i utrwalać czynniki, o których mowa w art. 6 ustawy o ochronie danych osobowych, zawierającym definicję pojęcia danych osobowych. Powołanie się w projekcie założeń na obraz utrwalony na nośnikach danych odpowiada raczej definicji zbioru danych, która została określona w art. 7 pkt 1 ustawy o ochronie danych osobowych, niż definicji danych osobowych. Zgodnie z tym przepisem zbiorem danych jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. **Nie jest więc koniecznym utrwalenie obrazu na nośniku, aby mógł on być uznany za dane osobowe.**

Projektodawca słusznie wskazuje na konieczność zapewnienia ochrony całości oglądanego lub nagrywanego obrazu, gdyż może on zawierać dane osobowe. Z uwagi na to konieczne jest także wskazanie przepisów ustawy o ochronie danych osobowych, w szczególności dotyczących praw kontrolnych jednostki, jako mających zastosowanie do regulowanej materii. Zgodnie z przedstawioną powyżej definicją danych osobowych, Generalny Inspektor zwraca uwagę, iż także inne obiekty poza wskazanymi obrazami pojazdu o cechach pozwalających na identyfikację osoby fizycznej będącej właścicielem lub użytkownikiem pojazdu, będą podlegały takiej ochronie.

Generalny Inspektor prosi o wyjaśnienie i rozwinięcie przez projektodawcę niejasnej koncepcji, zgodnie z którą ochrony wizerunku nie będą naruszać zanonimizowane nagrania, które będą mogły być upowszechniane. Obecnie obserwowane są przypadki nieprawidłowej anonimizacji, które wskazują na potrzebę przeprowadzania każdorazowo oceny skutków upowszechniania takich nagrań.

W zakresie słownika ustawowego (**punkt 3.1.5.**), który ma zawierać zbiór definicji, Generalny Inspektor sugeruje dodanie oraz uzupełnienie pewnych pojęć.

Pominięcie definicji osoby obserwowanej w słowniku należy uznać za konsekwencję całkowitego pomijania uprawnień jednostki wynikających z Konstytucji oraz ustaw i nie znajduje zrozumienia organu ochrony danych osobowych.

Projektodawca z drugiej strony bardzo szeroko określa zakres podmiotów uprawnionych do korzystania z systemów monitoringu wizyjnego. Powinno zostać wyraźnie wskazane, czy zakres



tych podmiotów będzie enumeratywny. Jest to istotne z uwagi na konieczność tworzenia spójnego prawa, w którym podmioty uprawnione na podstawie przepisów regulujących ich działalność nie będą miały ograniczonego dostępu do danych na podstawie przepisów szczególnych (vide art. 50 ust 3. ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, Dz. U. 2013 poz. 1442 z późn. zm.). Wyliczenie podmiotów uprawnionych powinno się opierać na dokładnym określeniu, po przeprowadzeniu dogłębnych analiz, które z nich powinny uzyskać uprawnienia do dostępu do systemów monitoringu utrzymywanych przez inne podmioty. Nadanie nowych uprawnień powinno być dokonane poprzez zmianę odpowiednich ustaw pragmatycznych.

W swoich uwagach do projektu założeń z 18 grudnia 2013 r. Generalny Inspektor zgłosił, i nadal podtrzymuje, propozycję wprowadzenia definicji przetwarzania obrazu, który dotyczyłby możliwości monitorowania osób obserwowanych, obiektów umożliwiających identyfikację, czy służących do realizacji innych celów, przykładowo do określania liczby osób przebywających na danym terenie.

Definicja systemu monitoringu wizyjnego wydaje się być fragmentaryczna i powinna obejmować obok wskazanych elementów także procedury przetwarzania informacji, w tym ich udostępniania, zabezpieczania i wykonywania innych operacji oraz polityki prywatności dostępne dla osób obserwowanych.

Projektodawca powinien rozważyć możliwość wprowadzenia do słownika ustawowego definicji administratora bezpieczeństwa systemu monitoringu wizyjnego w celu uniknięcia możliwości pomylenia tego podmiotu z administratorem systemu. Szerszy komentarz na temat administratora bezpieczeństwa poczyniono w uwagach do punktu 3.1.6.

W związku z objęciem przepisami projektu przestrzeni prywatnej koniecznym wydaje się zdefiniowanie, kiedy przestrzeń prywatna ma charakter otwarty. Posłuży to uzyskaniu jasności i pewności na temat zakresu uregulowania przepisami przyszłej ustawy. W tym celu można wykorzystać wyjaśnienia przedstawione przez projektodawcę w punkcie 3.1.1.

Z uwagi na szeroki zakres definicji automatycznej identyfikacji osoby należy rozważyć, w celu uzyskania precyzji, możliwość przeniesienia części definicji dotyczącej określenia cech lub właściwości obiektu do odrębnego hasła – automatycznej identyfikacji obiektów. Dodatkowo należy wyjaśnić czy możliwość analizowania określonych zdarzeń (jak stany emocjonalne czy kierunek poruszania się osoby – punkt 3.5.) łączy się jedynie z pojęciem automatycznej identyfikacji osób czy także dotyczyć obiektów.

Definicja zanonimizowanych nagrań, jako możliwego efektu przetwarzania obrazu, powinna dotyczyć także możliwości następcej deidentyfikacji tożsamości obserwowanej osoby. Ma to szczególne znaczenie w przypadku ewentualnego upublicznienia nagrań oraz dostępu osób

obserwowanych do nagrań, na których zostały one zarejestrowane, w celu realizacji ich praw kontrolnych.

W odniesieniu do **punktu 3.1.6.** Generalny Inspektor przypomina jedynie, że zapewnienie bezpieczeństwa funkcjonowania systemu powinno obejmować także wprowadzenie i stosowanie odpowiednich procedur przetwarzania obrazów. W zakres szeroko rozumianego zjawiska zabezpieczenia obrazu powinna wchodzić także konieczność zapobiegania negatywnym działaniom wobec urządzeń przesyłających i rejestrujących obrazy (nośniki), a nie tylko skierowanym przeciw samym nagraniom.

Podobnie jak w przypadku zabezpieczenia systemu przez jego administratora, także podmiot, któremu powierzono realizację zadań związanych z administrowaniem systemem na podstawie umowy, powinien wprowadzić odpowiednie środki zabezpieczenia. W zakres ten wchodzi także procedury dotyczące m.in. metod zabezpieczenia oraz informowania administratora i ewentualnie osób obserwowanych o przypadkach zaistnienia niepożądanego dostępu do systemu. Umowa pomiędzy tymi podmiotami powinna zawierać wszystkie istotne postanowienia, w taki sposób, aby zabezpieczyć interesy jej stron oraz osób obserwowanych.

Koniecznym wydaje się też doprecyzowanie, czy administrator będzie wystawiał upoważnienie dostępowe także pracownikom podmiotu, który wykonuje operacje w systemie na jego zlecenie i innym osobom, które mają uzyskiwać dostęp do systemu. Projektowane przepisy powinny przewidywać możliwość uregulowania tej kwestii w umowie i wymieniać zagadnienia, które mają być jej przedmiotem.

W obliczu postępującego rozwoju nowoczesnych technologii podmioty, którym powierzono systemy często korzystają z usług innych podmiotów. Generalny Inspektor zwraca uwagę, iż uregulowanie tych kwestii także powinno mieć miejsce w dodatkowych przepisach stwarzających gwarancje ochrony informacji objętych monitoringiem. Niezbędnym wydaje się wyposażenie administratora w narzędzia umożliwiające mu zachowanie kontroli i uniemożliwienie wyłączania odpowiedzialności poszczególnych podmiotów.

Z podanych względów i coraz częstszego stosowania **przetwarzania danych w tzw. chmurze** (cloud computing) konieczne jest rozstrzygnięcie, czy taki model biznesowy powinien być dopuszczony dla przechowywania lub innych form przetwarzania materiału pochodzącego z monitoringu wizyjnego. Jeśli odpowiedź byłaby twierdząca, niezbędnym będzie ustalenie odpowiednich wymogów zabezpieczenia danych monitoringu. Jest to związane z faktem, iż wiele systemów chmurowych wykorzystuje zasoby na całym świecie, które mogą należeć do wielu podmiotów. Dane są często migrowane do krajów, które nie zapewniają odpowiedniego poziomu ochrony, o czym mowa poniżej.

Generalny Inspektor podnosi także potrzebę doprecyzowania postanowień dotyczących **administratora bezpieczeństwa systemu monitoringu**. Nie jest jasnym, czy powołanie takiej osoby będzie obowiązkowe, czy będzie stanowiło uprawnienie administratora systemu? Koniecznym jest określenie, jakie podmioty będą mogły pełnić tę funkcję. Czy będą to jedynie osoby fizyczne zatrudnione przez administratora, czy także profesjonalści świadczący takie usługi? Podmioty te powinny być przygotowane merytorycznie do pełnienia tej niezwykle odpowiedzialnej funkcji. Doświadczenia z obecnie występującymi problemami z obsadzaniem tej funkcji oraz wypełnianiem obowiązków na podstawie przepisów ustawy o ochronie danych osobowych doprowadziły do potrzeby jej nowelizacji i uszczegółowienia funkcji administratora bezpieczeństwa informacji. Regulacja ta jest aktualnie procedowana (rządowy projekt ustawy o ułatwieniu wykonywania działalności gospodarczej – druk sejmowy nr 2606). W dokumencie tym przesądzono, iż funkcję administratora bezpieczeństwa powinna pełnić jedynie osoba fizyczna. Jest to rozwiązanie tożsame z tym ujętym w tzw. Dyrektywie o ochronie danych osobowych<sup>3</sup> oraz projekcie rozporządzenia o ochronie danych osobowych, o którym mowa w uwagach do punktu 3.1.3. powyżej.

W projekcie brak jest wzmianki na temat możliwości przesyłania obrazów i ich nagrań do państw trzecich. Należy wyraźnie określić, czy takie działanie ma być dopuszczalne. Jeżeli tak, koniecznym wydaje się wprowadzenie zasad przekazywania danych do państw trzecich i przyjęcia definicji państwa trzeciego w słowniku ustawowym, o którym mowa w punkcie 3.1.5. projektu założeń. Może się to okazać niezbędne w związku z obostrzeniami, jakie ustawa o ochronie danych osobowych nakłada na przekazywanie danych osobowych do państw niezapewniających odpowiedniego poziomu ochrony w rozumieniu art. 47 i kolejnych przepisów ustawy. Aktualność zachowują uwagi o chmurze obliczeniowej poczynione powyżej w uwagach do punktu 3.1.6.

Projektodawca powinien też zapewnić skuteczność realizacji wprowadzanych dla administratorów systemów obowiązków. Nieprzewidzenie skutecznych sankcji powoduje, że rozwiązania proponowane w ustawie stają się blankietowymi. Możliwym i czasem obserwowanym zdarzeniem jest przykładowo niepowoływanie przez administratora z państwa trzeciego swojego przedstawiciela na terytorium RP. W obecnym stanie prawnym nie wiąże się to z żadnymi konsekwencjami. Przypadki takie mogą też mieć miejsce w związku z funkcjonowaniem systemów, które mają służyć monitorowaniu przestrzeni. Należy im aktywnie przeciwdziałać poprzez wprowadzenie już od początku funkcjonowania regulacji odpowiednich mechanizmów dotyczących m.in. zakresu obowiązków i odpowiedzialności przedstawicieli oraz określenia pozycji podmiotów z państw trzecich związanych z funkcjonującymi na terenie RP systemów monitoringu.

---

<sup>3</sup> Dyrektywa 95/46 WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. L 281/31 z 23 listopada 1995 r.)

Generalny Inspektor zwraca uwagę na **punkt 3.1.7.**, w którym określono maksymalny termin przechowywania nagrań na 90 dni. **Jest to termin o 60 dni dłuższy niż zaproponowany w projekcie założeń z grudnia 2013 r. maksymalny okres.** Mimo pozostawienia administratorom swobody w zdefiniowaniu okresu retencji z perspektywy funkcjonowania poszczególnych systemów, wprowadzenie tak długiego okresu maksymalnego może spowodować, iż część z nich będzie go stosować automatycznie. Celem, który przyświeca projektodawcy ma być, zgodnie z treścią dokumentu, ochrona porządku publicznego oraz osób i mienia, a nie dostarczenie dowodów organom ścigania. Argumenty projektodawcy dotyczące okresu prowadzenia śledztw są chybione, gdyż jak wskazano, możliwym będzie zabezpieczenie zarejestrowanego obrazu jako dowodu. Mimo określenia krótkiego okresu retencji dla własnych celów, administrator systemu mógłby zabezpieczyć przed usunięciem (zgodnie z przyjętą przez niego procedurą) i przechowywać dłużej nagrania, które będą stanowiły zapis zdarzeń mających znaczenie dla organów ścigania, osób poszkodowanych i innych mających uzasadniony interes. 3-miesięczny okres trwania śledztwa nie powinien być uzasadnieniem dla dopuszczania tak długiego okresu retencji. Ewentualne nagranie, które mogą być istotne z punktu widzenia śledztwa, mogą być zabezpieczane w okresie krótszym, gdyż sprawdzenie funkcjonujących w okolicy ewentualnego zdarzenia systemów monitoringu będzie wykonywane w pierwszej kolejności. W takiej sytuacji będą one podlegały przepisom o retencji, które powinny regulować działanie prokuratury czy innych szeroko pojętych organów ścigania.

W styczniu 2014 r. Generalny Inspektor sygnalizował, iż proponowany 30-dniowy okres retencji może być nadmiernym. W tym miejscu należy powtórzyć przedstawioną wówczas argumentację. W niektórych państwach maksymalny okres przechowywania wynosi 72 godziny. W zakresie tym celowe wydaje się zróżnicowanie tego okresu w zależności od potrzeb. Należy zauważyć, że zbyt długi okres przechowywania naraża w większym stopniu obserwowane osoby na monitorowanie ich zachowań. Dotyczy to przypadków, gdy na skutek braku bieżącego nadzoru w celu wyszukania zdarzenia, które zaszło w bliżej nieznanym czasie, przeszukać trzeba będzie wiele dni nagrań. Można przypuszczać, że zaproponowany bardzo długi czas przechowywania nagrań spowoduje brak bieżącego nadzoru wielu miejsc, co z kolei może wpłynąć bardziej negatywnie niż pozytywnie na bezpieczeństwo miejsc, a także na zwiększenie skali obserwowania.

Niezrozumienie budzi także możliwość nakazania przez organ uprawniony odzyskania nagrań, które zostały skasowane bądź nadpisane w normalnym toku czynności, zgodnie z procedurami przyjętymi przez administratora systemu. Sugeruje to, iż celem podmiotów uprawnionych będzie zbieranie informacji w sposób masowy i nieograniczony, których analiza

może doprowadzić do poznania przyzwyczaję i sposobu codziennego funkcjonowania osób obserwowanych.

Podsumowując, możliwość przechowywania nagrań w systemie przez okres do 90 dni i ich odzyskiwania na polecenie uprawnionego organu wydaje się być niezgodne z zasadą celowości prowadzenia monitoringu. Ma on wszakże być stosowany w celu szybkiego wykrywania i dokumentowania niezgodnych z prawem zachowań, które mogą zagrażać bezpieczeństwu i porządkowi publicznemu lub ochronie osób i mienia. Konieczne jest przedstawienie dalszych wyjaśnień przez projektodawcę w tym zakresie, aby uniknąć nieporozumień na temat rzeczywistych kierunków regulacji tego powszechnie już stosowanego rozwiązania technicznego.

Odpowiedzialność za zabezpieczanie, przechowywanie i usuwanie nagrań ma leżeć po stronie administratora, który ma wyznaczyć do wykonywania tych zadań operatorów systemu. Konieczne jest doprecyzowanie, czy wyznaczenie stanowi obowiązek czy uprawnienie administratora systemu? Projektodawca powinien także doprecyzować, czy oznacza to wyłączenie możliwości przeniesienia tych funkcji na podmiot, który w imieniu administratora i na jego rzecz odpowiada za funkcjonowanie systemu, czy też rozwiązanie takie ma być do tych podmiotów i ich pracowników stosowane odpowiednio? Czy kwestia ta ma być uregulowana w umowach wiążących administratora i podmiot, któremu system powierzono?

Generalny Inspektor co do zasady popiera wymóg interoperacyjności urządzeń stosowanych do przechowywania nagrań. Możliwym rozwiązaniem wydaje się określenie specyfikacji dopuszczalnych formatów zapisu na wzór formatów danych określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

W **punkcie 3.1.8.** wskazano w sposób bardzo lakoniczny, iż uprawnienia kontrolne w zakresie zgodności prowadzenia monitoringu wizyjnego będą przysługiwać Generalnemu Inspektorowi Ochrony Danych Osobowych. Jest to rozwiązanie nowe i niekonsultowane dotychczas z organem ochrony danych osobowych. W chwili obecnej Generalny Inspektor dysponuje uprawnieniami w zakresie kontroli przetwarzania danych osobowych przez podmioty funkcjonujące na terenie Polski. **Ewentualne rozszerzenie kompetencji na regulowany szczegółowo, nowy i znaczący obszar, jakim jest monitoring wizyjny, wymagałoby wprowadzenia istotnych zmian do ustawy o ochronie danych osobowych oraz znaczącego wzmocnienia finansowego i organizacyjnego Biura GODO w wieloletniej perspektywie.**

Postulowany rejestr systemów monitoringu wizyjnego oraz wydawanie pozwoleń na prowadzenie pewnych rodzajów monitoringu należy ponownie rozważyć, mając na uwadze

podejmowane dążenia liberalizujące obowiązek rejestracji zbiorów danych osobowych. Są one widoczne zarówno w pracach nad rozporządzeniem unijnym o ochronie danych osobowych oraz w procedowanym przez Parlament projekcie ustawy o ułatwieniu wykonywania działalności gospodarczej, o którym mowa powyżej (patrz uwagi do punktu 3.1.6). Obecnie prowadzony ogólnokrajowy, jawny rejestr zbiorów danych osobowych ma na celu umożliwienie podmiotom danych uzyskania informacji o istniejących zbiorach, ich administratorach oraz m.in. celach ich utrzymywania (zgodnie z art. 40-42 ustawy o ochronie danych osobowych). W wyżej wspomnianym projekcie ustawy przewiduje się wzmocnienie uprawnień kontrolnych administratorów bezpieczeństwa informacji (odpowiedników administratorów bezpieczeństwa systemu monitoringu w obecnym projekcie) także w zakresie zbiorów z danymi zwykłymi. A zbiory danych rejestrowane w Biurze Generalnego Inspektora dotyczyć będą jedynie danych wrażliwych w rozumieniu art. 27 ustawy o ochronie danych osobowych.

Ewentualne wprowadzenie obowiązku rejestracji i uzyskiwania zgody Generalnego Inspektora na prowadzenie systemu z możliwością automatycznej identyfikacji, o której mowa w uwagach do punktu 3.5., może prowadzić do dublowania procedur. Projektowane założenia nie odnoszą się do tego, jak miałyby wyglądać procedura rejestracji systemów ani procedura związana z wyrażaniem zgody przez Generalnego Inspektora na prowadzenie takiej formy monitoringu. Powinny one być ujęte w dokumencie rangi ustawowej, jeżeli ustawodawca uzna potrzebę wprowadzenia takich kompetencji dla organu kontroli, którym niekoniecznie musi być organ ds. ochrony danych osobowych. **Należy odesłać w tym miejscu także do uwag do punktu 3.2.3. na temat zakresu kompetencji organu kontroli.**

Tworzenie nowych kompetencji rad jednostek samorządu terytorialnego, o której mowa w **punkcie 3.2.2.** powinno być uregulowane w ustawach dotyczących tych podmiotów, aby zachować zgodność z zasadami techniki prawodawczej. O ile możliwym wydaje się upoważnienie organów stanowiących gmin do podejmowania decyzji o wprowadzeniu albo rozbudowie systemów monitoringu oraz uchwalania przez gminy programów zapobiegania przestępczości oraz ochrony bezpieczeństwa obywateli i porządku publicznego, zdaniem Generalnego Inspektora będzie to oznaczać konieczność rozszerzenia katalogu przepisów wymagających nowelizacji, o którym mowa w punkcie 5 projektu założeń.

Także w tym punkcie w 3-cim akapicie zapisano, że organ podejmujący decyzję o budowie lub rozbudowie systemu monitoringu zobowiązany będzie do uzyskania **analizy potrzeb i celowości budowy systemu**, zawierającej prognozę skuteczności funkcjonowania systemu, analizę rozwiązań alternatywnych, opinię właściwej miejscowo jednostki Policji, oraz w miarę możliwości

straży gminnej (miejskiej), co do specyfiki zagrożeń w danym rejonie oraz optymalnego rozmieszczenia kamer. W zapisie powyższym wątpliwość budzi użycie zwrotu „uzyskania analizy” a nie „przeprowadzenia analizy” w kontekście jasnego wskazania, kto analizę taką powinien wykonać lub zlecić jej wykonanie. Ponadto celowym wydaje się, aby przeprowadzana analiza zawierała ocenę wpływu projektowanego systemu na prywatność (tzw. *Privacy Impact Assessment*). Bez tej ostatniej brak będzie danych do zastosowania zasady proporcjonalności, o której mowa w danym akapicie.

Właściwym działaniem wydaje się także wyjaśnienie pojęcia wskaźników służących określeniu skuteczności systemów monitoringu wizyjnego z perspektywy wdrażania ww. programów. Mogłoby to przyjąć formę rozporządzenia wykonawczego, jeżeli mechanizm miałaby cechować posunięta szczegółowość.

Zdaniem Generalnego Inspektora ocena funkcjonalności systemów monitoringu, o której mowa w **punkcie 3.2.3.** także powinna zawierać ocenę wpływu na prywatność osób obserwowanych, tak by możliwym była weryfikacja efektów realizacji programów zapobiegania przestępczości w szerszej perspektywie ochrony praw jednostki. W projekcie założeń nie wskazano, co wydaje się oczywistym, iż celem przeprowadzania oceny funkcjonalności będzie także wprowadzanie ewentualnych zmian w zasięgu i metodach funkcjonowania systemu monitoringu. Pozwoliłoby to zachować równowagę pomiędzy potrzebą zapewniania porządku a ochroną praw jednostki.

Generalny Inspektor sugeruje także rozważenie możliwości objęcia wymogiem dokonywania okresowej oceny systemów funkcjonujących w zamkniętej przestrzeni publicznej. Nie musiałaby ona oczywiście przybierać takiej samej formy, jak w przypadku monitoringu otwartej przestrzeni publicznej. Jednakże powinna ona być dostępna m.in. dla osób obserwowanych, które z tej przestrzeni korzystają. Z uwagi na jej publiczny charakter nie wydaje się celowym całkowicie odmienne traktowanie tego rodzaju przestrzeni.

W związku z obowiązkiem rejestracji systemów monitoringu w otwartej przestrzeni (**punkt 3.2.4.**) należy odesłać do uwag poczynionych powyżej w punkcie 3.1.8. **O ile powinny istnieć uprawnienia i organ do kontroli systemów monitoringu, to nie jest pewnym, czy Generalny Inspektor Ochrony Danych Osobowych jest właściwym podmiotem z uwagi na szeroki zakres obecnie realizowanych już zadań i obecne możliwości organizacyjne. Warto rozważyć, biorąc pod uwagę znaczenie takiego systemu ewidencyjnego dla Policji, czy to właśnie Komendant Główny Policji nie powinien być organem powołanym do prowadzenia takiego systemu ewidencyjnego. Z pewnością wpłynęłoby to pozytywnie na interoperacyjność tej ewidencji z systemami teleinformatycznymi Policji.**

Koniecznym jest też zwrócenie uwagi projektodawcy, iż wojewodowie sprawują nadzór jedynie nad ewidencją wyposażenia straży gminnych (zgodnie z art. 9 ust. 2. pkt 3 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych, Dz. U. 2013 r. poz. 1383, z późn. zm.). W tym zakresie oczywiście mieszczą się środki techniczne służące do obserwowania i rejestrowania obrazu zdarzeń w miejscach publicznych. Jednakże nie obejmuje to sposobów obserwowania i rejestrowania obrazu, co będzie istotą funkcjonowania systemu monitoringu w rozumieniu projektu założeń.

Ze względu na użyty przez projektodawcę w drugim akapicie spójnik „natomiast” wyjaśnienia wymaga zakres ewentualnych uprawnień kontrolnych Generalnego Inspektora. Powstaje pytanie, czy w stosunku do prowadzących monitoring straży gminnych, innych jednostek gminy albo podmiotów zewnętrznych monitorujących na podstawie umowy kontrole Generalnego Inspektora będą wyłączone, a sprawowany będzie jedynie nadzór przez wymienione organy gminy, czy też zarówno kontrola, jak i nadzór będą mogły być prowadzone niezależnie.

Pewność i jasność obowiązywania norm prawnych wymaga w omawianym przypadku dokładnego określenia obszaru objętego monitoringiem w otwartej przestrzeni publicznej i podawanie tej wiadomości do publicznej wiadomości (**punkt 3.2.5.**) w sposób zaproponowany przez projektodawcę. Nie jest to zadanie trudne przy obecnym stanie technik audiowizualnych stosowanych do monitorowania. Ustalenie całkowitego zasięgu monitoringu i poinformowanie osób obserwowanych pozwoli lepiej oceniać jego wpływ na poprawę bezpieczeństwa.

Wymogi stawiane przed operatorami systemów (**punkt 3.2.6.**) należy uznać za właściwe. Jednakże konieczne wydaje się zdefiniowanie przez projektodawcę katalogu przestępstw, które będą uniemożliwiały zatrudnienie osób skazanych. W obecnym stanie jest to zapis wysoce nieprecyzyjny. Powinni oni być szkoleni także w zakresie ochrony praw osób obserwowanych przed bezpodstawnym i nieuzasadnionym obserwowaniem ich poczyną.

Formuła szczegółowego określenia katalogu wymagań wobec operatorów systemu powinna być także zastosowana w przypadku określania wymagań stawianych przed administratorami bezpieczeństwa systemu monitoringu, o których mowa w punkcie 3.1.6. Koniecznym wydaje się także określenie wzajemnych relacji (zakresu zadań, podległości, odpowiedzialności) pomiędzy podmiotami wykonującymi funkcje w ramach systemu (operatorzy, administrator bezpieczeństwa) oraz administratorem systemu.

Generalny Inspektor nie widzi podstaw do całkowicie odmiennego traktowania monitoringu w pasie ruchu drogowego (**punkt 3.2.7.**). W projektowanym obecnie Zintegrowanym Systemie Poboru Opłat oraz testowanym systemie odcinkowego pomiaru prędkości będzie dochodzić do przetwarzania danych pojazdów, których użytkownicy powinni uiścić opłaty za przejazd albo naruszających ograniczenia prędkości. O ile obecnie faktycznie nie jest możliwa identyfikacja osób



podróżujących pojazdami, nie oznacza to, że nie będzie dochodzić do identyfikacji obiektu w rozumieniu projektu założeń. Może to mieć wpływ na prawa jednostki. Także przygotowywana koncepcja Krajowego Systemu Zarządzania Ruchem, nad którą prace rozpoczyna Ministerstwo Infrastruktury i Rozwoju powinna być dostosowana do zasad przyszłej ustawy o monitoringu wizyjnym w zakresie, w jakim będą wykorzystywane mechanizmy obserwacji wizyjnej.

Generalny Inspektor zgadza się z projektodawcą w kwestii ograniczenia obowiązków administratorów systemów (**punkt 3.3.1.**) monitorujących zamknięte przestrzenie publiczne, w sytuacji gdy mają one na celu ochronę osób i mienia. Ograniczenie to nie powinno jednakże dotyczyć zakresu stosowanych zabezpieczeń, które powinny być odpowiednie do charakteru przetwarzanych obrazów i danych osobowych oraz możliwości drastycznego ograniczenia praw kontrolnych osób obserwowanych.

Jak wskazano w uwagach wstępnych, prowadzenie monitoringu w celu **optymalizacji lub weryfikacji sposobów wykonywania powierzonych obowiązków wynikających ze stosunku pracy lub umów cywilnoprawnych** budzi wątpliwości z punktu widzenia testu legalności i adekwatności. Jako rozwiązanie nieproporcjonalne może on być zastąpiony przez inne metody, jak chociażby nadzór wykonywany przez przełożonych, czy badanie efektywności na podstawie obiektywnych kryteriów wydajności dostosowanych do rodzaju wykonywanej pracy. Należy przypomnieć, iż Generalny Inspektor wielokrotnie zwracał uwagę na przepisy Kodeksu pracy (Dz. U. z 1998 r. Nr 21 poz. 94, z późn. zm.) ustalające zakres danych, które mogą być przez pracodawcę przetwarzane. W art. 22<sup>1</sup> określono zasadniczy katalog danych osobowych pracownika, które mogą być przetwarzane przez pracodawcę. Nie ma wśród nich danych pozyskiwanych za pomocą systemu monitoringu wizyjnego. Także sądy krajowe wypowiadały się na ten temat wielokrotnie. Utrwalone orzecznictwo Naczelnego Sądu Administracyjnego (sygn. I OSK 249/09 oraz I OSK 2436/12) mówi o potrzebie poszanowania przez pracodawcę prywatności pracownika, a jej ewentualne ograniczenie nie może naruszać praw i swobód jednostki.

Dodatkowo należy zwrócić uwagę, iż w zakresie przetwarzania danych osobowych w związku z zatrudnieniem prowadzone są obecnie prace nad Projektem Rekomendacji w sprawie ochrony danych osobowych wykorzystywanych dla celów zatrudnienia z dnia 15 kwietnia 2014 r., prowadzonych przez Komitet konsultacyjny ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS Nm 108). Powołany projekt szczegółowo określa warunki dopuszczające stosowanie monitoringu wizyjnego w zakładach pracy i takie uszczegółowienie wydaje się niezbędne również w przyszłym projekcie ustawy.

Generalny Inspektor widzi potrzebę ponownego zweryfikowania, czy wszystkie obszary mające podlegać odpowiedniemu stosowaniu przepisów o zamkniętej przestrzeni publicznej (**punkt 3.3.3.**) zostały właściwie opisane. Obecnie prowadzony monitoring w środkach transportu jest także kierowany na otwartą przestrzeń publiczną (kamery na przedzie pojazdu oraz obserwujące z zewnątrz wejścia do pojazdu). To samo może dotyczyć kamer w urządzeniach bankomatowych zlokalizowanych w otwartej przestrzeni publicznej.

Weryfikacji powinna także podlegać potrzeba prowadzenia stałego monitoringu w lasach stanowiących własność Skarbu Państwa i parkach narodowych. Przede wszystkim są to tereny powszechnie dostępne. Wszakże odpowiednie służby mogą prowadzić dochodzenia, które odbywają się na podstawie wyraźnych przepisów określających kompetencje do obserwowania, w odpowiedzi na zdarzające się przypadki naruszenia prawa. Rozumiejąc potrzebę realizacji zadań odpowiednich służb i przeciwdziałania przestępstwom przeciw środowisku i przeciwdziałanie szkodnictwu leśnemu lub łowieckiemu, należy zachować szczególną ostrożność. Swobodne stosowanie monitoringu wizyjnego może powodować poczucie stałej obserwacji i nadzoru oraz, w sytuacjach szczególnych, naruszać godność osób obserwowanych. Jak wskazano powyżej może to mieć wpływ na swobodę poruszania się jednostek i inne prawa konstytucyjne chronione. Nie można zapominać, iż duża część użytkowników terenów leśnych korzysta z nich w sposób zgodny z prawem w celu szeroko pojętej rekreacji.

Projektodawca słusznie wyłącza w **punkcie 3.4.** spod proponowanych przepisów monitoring funkcjonujący wyłącznie w przestrzeni prywatnej, która nie jest dostępna dla osób postronnych. Obowiązek oznaczania przestrzeni monitorowanej, jeżeli obejmuje ona wycinek otwartej przestrzeni publicznej, jest zgodny z metodami informowania o monitoringu postulowanymi dla innych rodzajów przestrzeni. Jednakże nie można się zgodzić z wyłączeniem obowiązku informacyjnego względem osób obserwowanych. W celu zapewnienia im prawa dostępu możliwym jest ograniczenie zakresu informacji podawanych przez administratora. Przykładowo nie musiałby on podawać swojego imienia i nazwiska, a jedynie określać adres kontaktowy. Należy przy okazji zwrócić uwagę, iż administratorzy monitoringu prywatnego już obecnie stosują oznaczenia na swoich posesjach informujące o obserwowaniu przestrzeni i że jest to teren prywatny. Przy określaniu piktogramu informującego o działaniu systemu monitoringu obejmującego wycinek przestrzeni publicznej powinno się wziąć ten fakt pod uwagę w celu uniknięcia pomyłek.

Automatyczna identyfikacja (**punkt 3.5.**) będzie wymagała dostępu do danych identyfikacyjnych osób obserwowanych. Oznacza to konieczność ich pozyskiwania i przechowywania w sposób zapewniający ich bezpieczeństwo. Także możliwość określania

kierunku poruszania się osób obserwowanych, czy ich stanu emocjonalnego, będą wchodziły w zakres danych osobowych tych osób, które będzie trzeba chronić.

Wydaje się zasadnym, aby projektodawca wyjaśnił, czy systemu automatycznej identyfikacji będą także obejmowały obiekty, takie jak samochody, które mogą być identyfikowane poprzez dostęp do odpowiednich rejestrów publicznych. Mają tutaj zastosowanie zwłaszcza uwagi poczynione do punktu 3.2.7. powyżej.

Próby odróżnienia pojęcia przetwarzania obrazu od pojęcia przetwarzania danych w rozumieniu ustawy o ochronie danych osobowych podejmowane przez projektodawcę są niezrozumiałe i nieskuteczne. Za każdym razem, gdy dochodzi do przetwarzania informacji o osobie możliwej do zidentyfikowania, mamy do czynienia z przetwarzaniem jej danych osobowych. Uprawnienia Generalnego Inspektora wynikające z ustawy o ochronie danych osobowych w tym zakresie nie będą stosowane odpowiednio, ale wprost, gdyż dotyczą kontroli przetwarzania danych osobowych.

Umieszczenie postanowień o automatycznej identyfikacji osób sugeruje, iż możliwym będzie stosowanie takiej formy obserwacji we wszystkich przestrzeniach, w których dopuszczone będzie stosowanie monitoringu. Koniecznym jest podkreślenie, iż ta forma obserwacji jest wysoce inwazyjna w stosunku do praw jednostki, w szczególności prawa do prywatności i prawa do ochrony danych osobowych. Projektodawca nie wskazał niestety szczegółowych warunków dopuszczalności takiego przetwarzania obrazu, jego ograniczeń oraz katalogu podmiotów, który będzie mógł stosować to rozwiązanie.

Ograniczenia w zakresie możliwości prowadzenia monitoringu wizyjnego (**punkt 3.6.**) wskazane przez projektodawcę mają charakter wrywkowy i nie określają wszystkich problemów, które mogą wiązać się z obserwowaniem osób. Stosowanie monitoringu przestrzeni publicznej jest uznawane za naruszenie swobody poruszania się, która jest zagwarantowana w przepisach krajowych i unijnych. Jednostka ma uzasadnione oczekiwanie respektowania jej prawa do prywatności także w przestrzeni publicznej, gdzie może być ono jedynie częściowo ograniczone. Ograniczenia te muszą być niezbędne i proporcjonalne do osiągnięcia konkretnych i istotnych z punktu widzenia społeczeństwa demokratycznego celów. Po raz kolejny należy podkreślić, że nie może to oznaczać całkowitego wyłączenia praw kontrolnych jednostki, która jest jednocześnie podmiotem danych osobowych. Prawo do swobodnego przemieszczania się nie może być ograniczone przez świadomość ciągłego pozostawania w obszarze monitorowanym.<sup>4</sup>

---

<sup>4</sup> Opinia Grupy Roboczej art. 29 nr 4/2004, s. 6.

Dopuszczenie w systemach monitoringu funkcjonalności aktywowanych wskutek wystąpienia zdarzenia dźwiękowego (**punkt 3.6.1.**) sugeruje, wbrew zapewnieniom projektodawcy, że systemy monitoringu mogą być wyposażone w urządzenia do odbioru dźwięku z obserwowanego obszaru. Z ostrożności warto zauważyć, że mogą one mieć wystarczające możliwości techniczne, aby służyć do bieżącego przekazywania lub rejestracji dźwięków. W skrajnych przypadkach może to posłużyć do monitorowania rozmów prowadzonych przez osoby obserwowane. Należy podjąć wszelkie starania w celu uniemożliwienia takiego wykorzystywania systemów monitoringu od momentu ich projektowania i ulepszania tych już istniejących. Powinno to mieć miejsce zarówno na poziomie technicznym (kamery pozbawione możliwości nagrywania dźwięku), jak i organizacyjnym (stosowanie oprogramowania uniemożliwiającego korzystanie z takich właściwości zainstalowanego już sprzętu itp.).

Do funkcjonalności systemu aktywowanych wystąpieniem określonych zdarzeń mogą znaleźć zastosowanie przepisy ustawy o ochronie danych osobowych zabraniające rozstrzygania indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym (art. 26a ustawy). Automatyczne klasyfikowanie określonych (np. zdefiniowanych jako podejrzanego) zachowań osób obserwowanych nie może w sposób ostateczny wpływać na ich traktowanie (możliwość zatrzymania, śledzenia itp.). W takich sytuacjach zawsze konieczna jest kontrola dokonywana przez operatora systemu, który podejmuje decyzje na temat wykorzystania zasobów systemu monitoringu. Stanowisko takie reprezentuje obok Generalnego Inspektora także Grupa Robocza art. 29.

Zakaz prowadzenia monitoringu naruszającego godność człowieka (**punkt 3.6.2.**) powinien być rozszerzony na miejsca i sytuacje, w których może dojść do naruszenia tajemnicy jednostki. Mowa tutaj o ograniczeniu lub całkowitym wyłączeniu możliwości obserwowania osób w chwili, gdy wprowadzają one kod PIN w toku realizacji transakcji finansowych (bankomaty, terminale płatności itp.) czy korzystają z zabezpieczeń swoich urządzeń elektronicznych (kody dostępowe każdej postaci do telefonów komórkowych, smartphone'ów, tabletów, komputerów osobistych itp.). Można to osiągnąć w dwojaki sposób. Miejsca takie mogą być wyłączone spod bezpośredniego monitoringu (np. nieinstalowanie kamer w pobliżu bankomatów, terminali płatniczych itp.) albo poprzez takie zaprogramowanie urządzeń monitorujących, które będzie uniemożliwiało obserwację operatorom (np. poprzez rozmazywanie obrazu) czy też szkolenie operatorów, którzy nie powinni w taki sposób wykorzystywać powierzonych im urządzeń.

Powstaje także pytanie, czy wyliczenie przedstawione przez projektodawcę w zakresie gabinetów lekarskich dotyczy także obiektów ochrony zdrowia oraz czy nie powinno dotyczyć placówek oświatowych i wychowawczych.

Niezrozumienie Generalnego Inspektora budzi ograniczenie zakazu stosowania atrap kamer jedynie do otwartej przestrzeni publicznej (**punkt 3.6.3.**). Powinien on obejmować także obszary zamkniętej przestrzeni publicznej i przestrzeni prywatnej objęte monitoringiem. Niezależnie od celu prowadzenia obserwacji, jednostka ma prawo do informacji, kiedy rzeczywiście jest objęta monitoringiem. Celowe wprowadzenie osoby obserwowanej w błąd, co do objęcia pewnej przestrzeni nadzorem, narusza jej prawo do prywatności i może wpływać na zmianę jej zachowań, tym samym naruszając wolność człowieka określoną w art. 31 Konstytucji RP. Ochrona osób i mienia w takim przypadku może być osiągnięta przez zastosowanie innych środków, co byłoby zgodne z jedną z głównych zasad mających wg projektodawcy zastosowanie w tej regulacji, to jest z zasadą proporcjonalności.

Uprawnienia służb porządkowych do korzystania z systemów monitoringu wizyjnego (**punkty 3.7. – 3.10**) powinny w każdym przypadku wynikać z przepisów dotyczących ich działalności. Na obecnym etapie brak jest szczegółów procedury uzyskiwania dostępu do monitoringu wizyjnego. Prawa administratorów do odmowy udostępnienia systemów zostały jedynie wzmiankowo opisane. Jest to niedopuszczalne z uwagi na odpowiedzialność administratora za udostępnienie systemu osobom niepowołanym i wiążącymi się z tym karami. Dlatego też Generalny Inspektor będzie poświęcał szczególną uwagę przygotowywanym i rozwiniętym przez projektodawcę propozycjom.

Rejestr udostępnień jak i dokumentacja funkcjonariuszy/żołnierzy realizujących uprawnienia (dalej zwani funkcjonariuszami) (**punkt 3.7.**) powinna zawierać wszystkie próby uzyskania dostępu, także te, w których administrator z uzasadnionych przyczyn odmówił dostępu. Będzie to miało pozytywny wpływ na transparentność działań funkcjonariuszy. Dostęp uprawnionych podmiotów powinien być realizowany przez administratorów bez zbędnej zwłoki po dokonaniu oceny zasadności. Oznacza to także, iż nie może on negatywnie wpływać na podstawowe cele monitoringu realizowane przez administratora.

Ustne żądanie funkcjonariusza (**punkt 3.8.**) nie powinno być podstawą uzyskania dostępu do obrazu. Jako że jest to niesformalizowana metoda, może w pewnych sytuacjach prowadzić do nieprawidłowości. Nie daje także materialnych dowodów administratorowi monitoringu na przedmiotowe uzyskanie dostępu, czy przekazanie nagrań, o którym mowa poniżej. Można sobie oczywiście wyobrazić przypadki, gdy jest to konieczne z uwagi na potrzebę natychmiastowej ochrony istotnej wartości (np. życie czy zdrowie ludzkie), gdy nie będzie możliwe zachowanie wymogów sformalizowanej procedury, a dostęp umożliwi skuteczniejszą ochronę takiej istotnej wartości.

Także sporządzanie kopii nagrań (**punkt 3.9.**) nie powinno odbywać się na podstawie ustnego żądania funkcjonariusza, nawet upoważnionego przez swojego przełożonego albo dowódcę służby z przyczyn wskazanych powyżej. Sporządzenie kopii na podstawie pisemnego wniosku powinno odpowiadać uprawnieniom właściwych służb wynikającym z regulujących ich działalność aktów prawnych rangi ustawowej. W żadnym wypadku projektowana regulacja nie powinna rozszerzać kompetencji służb *en masse*.

Projektodawca pominął w tym punkcie kwestię ewentualnej odpłatności za sporządzanie kopii przez administratora systemu. Należy założyć, iż częste wnioski uprawnionych podmiotów mogą w sposób znaczący podnieść koszty funkcjonowania systemu monitoringu, co może pośrednio negatywnie wpływać na jego skuteczność powodowaną koniecznością przenoszenia środków finansowych na te zadania. Angażowanie operatorów systemu do sporządzenia kopii nagrań nie powinno negatywnie wpływać na realizację ich obowiązków związanych z bieżącą obsługą systemu. Należy także rozważyć, czy wszyscy operatorzy systemu powinny być uprawnieni albo upoważnieni przez administratora do sporządzania kopii nagrań.

Jedynie na marginesie należy stwierdzić, iż uprawnienia i zasady dostępu do oraz postępowania z uzyskanymi nagraniami przez uprawnione według projektu podmioty powinny być w każdym przypadku ujęte w przepisach ustaw regulujących ich działalność. Powoływanie się na przepisy ustawy o Policji nie powinno oznaczać możliwości nadania analogicznych, szerokich uprawnień innym służbom aktem prawnym, który ma regulować zasady prowadzenia monitoringu.

Upoważnienie do korzystania z systemów monitoringu należących do innych administratorów (**punkt 3.10.**) nie jest obecnie uregulowane w ustawach pragmatycznych. Przyjęcie takiej regulacji oznaczałoby tworzenie nowych uprawnień dla służb *en masse* i obowiązków po stronie administratorów. Możliwość taka powinna być wykorzystywana wyłącznie w toku prowadzonych przez odpowiednie służby postępowań. Projektodawca słusznie zauważa, że nie powinno to utrudniać realizacji celu funkcjonowania danego systemu. Sugeruje to, iż możliwym jest odmowa udzielenia dostępu przez administratora. Kwestia ta powinna zostać rozwinięta przez projektodawcę w celu zapewnienia jasności co do uprawnień administratora.

Fakt skorzystania z systemu powinien być udokumentowany także w zakresie podstawy prawnej takiego dostępu (np. sygnatury postępowania, w związku z którym prowadzono czynności) oraz zasięgu monitorowanej przestrzeni, który był obserwowany przez funkcjonariuszy. Także w tym przypadku administrator powinien odnotować próby uzyskania dostępu, na które nie wyraził zgody. Dostęp do systemu powinien odbywać się wyłącznie poprzez stanowiska operatorów systemu, bez możliwości uzyskiwania zdalnego dostępu, jak ma to miejsce w przypadku

udostępniania Policji danych telekomunikacyjnych. Konieczne jest precyzyjne określenie tej kwestii.

Sancjonowanie nieprzestrzegania przepisów (**punkt 3.11.**) ma się odbywać na gruncie przepisów prawno-administracyjnych. Jednocześnie projektodawca nie określił podmiotów, które miałyby takie sankcje nakładać. Generalny Inspektor zwraca uwagę, że na gruncie ustawy o ochronie danych osobowych obok sankcji administracyjnych funkcjonuje także reżim przepisów karnych mający zastosowanie do niezgodnego z prawem obchodzenia się ze zbiorami danych oraz danymi osobowymi. Należy nadmienić, że mogą one mieć zastosowanie do systemów monitoringu, w których będzie miało miejsce przetwarzanie danych osobowych.

Uwagę zwraca także możliwość karania za bezprawne dopuszczenie się technicznego odzyskania zarejestrowanego obrazu z monitoringu wizyjnego po upływie maksymalnego czasu jego przechowywania. Niezależnie od istnienia takiej technicznej możliwości, Generalny Inspektor prosi o odpowiedź na pytanie, czy możliwym będzie odzyskanie zarejestrowanego obrazu zgodnie z prawem? Ewentualne dopuszczenie takiego stanu byłoby w sprzeczności z postulowaną przez Inspektora zasadą celowości i ograniczenia czasowego przetwarzania obrazu, związanych z nimi danych osobowych oraz okresami retencji, które niniejszy projekt ma także ustalić.

Widoczna jest jednocześnie potrzeba rozwinięcia i wyjaśnienia kwestii odpowiedzialności porządkowej lub dyscyplinarnej administratora albo osób pracujących na jego rzecz za uniemożliwienie podmiotom uprawnionym bezzwłocznego wglądu do systemu albo sporządzenia kopii nagrań z systemu. Czy projektowana regulacja ma tworzyć nowy rodzaj odpowiedzialności, poza tym znanym z ustawy Kodeks pracy? Jeżeli tak, to na jakich zasadach?

Generalny Inspektor zwraca uwagę, iż jego sugestia sformułowana w piśmie z 22 stycznia br. w sprawie możliwości karania za prowadzenie monitoringu wizyjnego, w miejscu, które może skutkować naruszeniem godności osoby obserwowanej nie została przez projektodawcę przyjęta. Pozostawienie jedynie możliwości ścigania na wniosek pokrzywdzonego przestępstwa określonego w art. 266 § 1 Kodeksu karnego wydaje się być niewystarczającym w obliczu możliwego braku świadomości osoby pokrzywdzonej, iż wobec niej był prowadzony nielegalny monitoring. W tym także miejscu należy ponownie podkreślić konieczność zagwarantowania praw kontrolnych osoby obserwowanej.

Odnosnie proponowanego jednorocznego okresu *vacatio legis* (**punkt 3.12.**) Generalny Inspektor poddaje w wątpliwość możliwość dostosowania się do projektowanych przepisów wszystkich podmiotów, które mogą zostać objęte przyszłą regulacją. Jest to w szczególności

zasadne w obliczu znaczącej liczby funkcjonujących już obecnie systemów monitoringu, które musiałyby zostać w tak szybkim czasie dostosowane do nowych i często dalekosiężnych wymogów.

Odnosnie zgodności projektu z prawem UE (**punkt 4**) Generalny Inspektor poddaje w wątpliwość, czy projektowana regulacja jest zgodna z postanowieniami Dyrektywy 95/46/WE. Projekt, poprzez całkowite pominięcie prawa osoby obserwowanej m.in. do dostępu do danych jej dotyczących, może naruszać w szczególności prawa ujęte w art. 12 i kolejnych w/w dyrektywy.

Na zakończenie należy zauważyć, iż choć projekt uwzględnia procedury oceny zasadności wprowadzana monitoringu (ocena wpływu monitoringu wizyjnego i przeprowadzanie konsultacji), niektóre rozwiązania powinny ulec sprawdzeniu pod względem jak najszerzej ochrony prywatności od momentu tworzenia systemów monitoringu wizyjnego (tzw. *Privacy by Design*) oraz zastosowania na szerszą skalę ocen wpływu na prywatność osób obserwowanych (*Privacy Impact Assessment*).

Generalny Inspektor Ochrony Danych Osobowych jednocześnie deklaruje dalszą gotowość do udziału w pracach legislacyjnych nad projektem i udzielenia wszelkiej pomocy i wyjaśnień projektodawcy w zakresie przedstawionych do projektu założeń sugestii. Jednocześnie, zważywszy obszerność zagadnień ujętych w projekcie, Generalny Inspektor zastrzega sobie możliwość składania dalszych uwag.