

Zagadnienia dotyczące monitoringu wizyjnego w działalności Biura GIODO

Wprowadzenie

Korzystanie z systemów monitoringu rodzi coraz więcej pytań o prawny zakres ingerencji w prywatność osób fizycznych i o warunki, jakie systemy monitorujące powinny spełniać. Faktem jest, że różne podmioty stosują systemy monitoringu (wideonadzoru, monitoringu wizyjnego, czy audiowizualnego), a pozyskiwaniem tą drogą informacji zajmuje się coraz szerszy krąg podmiotów zarówno z sektora publicznego, jak i prywatnego. Skutkiem stosowania monitoringu może być utrwalanie wizerunku osób fizycznych, a następnie jego przechowywanie, opracowywanie i wykorzystywanie dla różnych celów. Tymczasem ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) nie reguluje w sposób szczególny tych kwestii. Niemniej zaznaczyć należy, że w polskim porządku prawnym istnieją przepisy branżowe, które zezwalają określonym podmiotom na stosowanie monitoringu, w tym na jednoczesne nagrywanie obrazu i dźwięku.

Biorąc pod uwagę fakt, że kwestie te są uregulowane jedynie w niektórych przepisach branżowych, oraz to, iż monitoring bywa coraz powszechniej wykorzystywany przez różne podmioty, w ocenie Generalnego Inspektora Ochrony Danych Osobowych (GIODO) kwestia ta wymaga pilnego uregulowania.

W tej sprawie 24 marca 2010 r. GIODO skierował do Ministra Spraw Wewnętrznych i Administracji wystąpienie dotyczące rozważenia możliwości zainicjowania prac legislacyjnych mających na celu unormowanie w przepisach rangi ustawowej ogólnych zasad dotyczących wideonadzoru. Ponadto 13 stycznia 2011 r., dr Wojciech Rafał Wiewiórowski w odpowiedzi na pismo prof. Ireny Lipowicz, Rzecznika Praw Obywatelskich podkreślił konieczność uregulowania kwestii dotyczących monitoringu (wideonadzoru) w odrębnym akcie prawnym, innym niż ustawa o ochronie danych osobowych, dzięki czemu możliwe byłoby m.in. zagwarantowanie odpowiedniego standardu ochrony informacji pozyskiwanych z wykorzystaniem monitoringu.

W opinii GIODO celowe byłoby, aby w osobnej ustawie określić m.in. ogólne zasady i warunki dopuszczalności stosowania monitoringu (wideonadzoru), wskazać podmioty/osoby, które mogłyby wykorzystywać systemy monitoringu czy wideonadzoru (tym bardziej takie, które służą do jednoczesnego monitoringu i nagrywania rozmów), określić cele, w jakich nadzór taki jest możliwy do zastosowania, a także okres przechowywania nagrań (w tym określenie, kiedy nagrania z wymienionych systemów mogą być utrwalane

i jak mogą być wykorzystywane, a kiedy wideonadzór ma się odbywać jedynie „na bieżąco”) i ich ewentualnego publikowania. Ponadto konieczne byłoby również unormowanie praw, jakie przysługują osobie, która może być objęta wideonadzorem.

Zaznaczył przy tym, że przy wprowadzaniu nowych regulacji należy zachować równowagę pomiędzy zagwarantowaniem praw jednostki a ogólnym interesem podmiotów, które stosować miałyby systemy monitoringu. Zgodnie bowiem z opinią (nr 4/2004) Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych, przy posługiwaniu się wideonadzorem respektować należy zasadę proporcjonalności, która to zasada dotyczy przede wszystkim wyboru odpowiedniej technologii, kryteriów wykorzystywania urządzeń w konkretnych sytuacjach oraz ustaleń dotyczących przetwarzania danych, odnoszących się także do zasad dostępu i okresu przechowywania. Zasada proporcjonalności oznacza także, że urządzenia służące do takiego nadzoru mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne czy ochrony, niewymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania.

Istotne znaczenie ma w tej materii – jak dalej traktuje ww. opinia – realizacja obowiązku informacyjnego wobec osób, których dane osobowe pozyskane zostały za pomocą wideonadzoru, zgodnie z wymogami art. 10 i 11 dyrektywy 95/46/WE. Wskazano przy tym, iż osoby te muszą mieć świadomość, że w miejscu, w którym się znajdują, prowadzone są czynności wideomonitoringu. Tablice informujące o zainstalowanym monitoringu powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Muszą także wskazywać cele działań nadzoru jak również administratora przetwarzania, natomiast wymiary tablic muszą być proporcjonalne do miejsca, gdzie są umieszczone.

Podmiotom stosującym monitoring w miejscach publicznych GODO przypomina zaś o konieczności przestrzegania obowiązujących obecnie przepisów prawa, które pozwalają na wyznaczenie pewnego obszaru działania, poza który nie należy wychodzić. Zgodnie bowiem z Konstytucją RP, ustawą o ochronie danych osobowych czy Kodeksem pracy, podmioty stosujące wideomonitoring powinny kierować się przede wszystkim tzw. zasadą adekwatności. Przewiduje ona, że pozyskiwać można jedynie te dane, które są niezbędne dla osiągnięcia wyznaczonego z góry, zgodnego z prawem celu.

Generalny Inspektor Ochrony Danych Osobowych podkreśla przy tym, że wszelkie działania ingerujące w prawo jednostki do jej prywatności powinny być dokonywane rozważnie i z poszanowaniem obowiązujących przepisów prawa.

Warto wskazać, że specjalne akty prawne regulujące ww. kwestie obowiązują już w niektórych państwach Unii Europejskiej, takich jak np. Szwecja, Niemcy czy Hiszpania. Dzięki nim łatwiej można uczynić zadość obowiązkom wynikającym z potrzeby ochrony danych osobowych i prawa do prywatności osób przebywających w miejscach znajdujących się pod nadzorem kamer.

W ocenie dra Wojciecha Rafała Wiewiórowskiego, omawiane kwestie nie są zupełnie oczywiste i nie zawsze są związane z kompetencjami Generalnego Inspektora Ochrony Danych Osobowych, bo nie zawsze monitoring wizyjny wiąże się z przetwarzaniem danych osobowych.

Jeżeli monitoring służy jedynie do podglądu danego miejsca, a nagranie nie jest zachowywane na twardym dysku komputera czy jakimkolwiek innym nośniku, to wówczas trudno mówić o przetwarzaniu danych osobowych. Z danymi osobowymi mamy natomiast do czynienia wówczas, gdy obraz z kamer zawiera wizerunki osób i jest utrwalony w systemie monitoringu na elektronicznym nośniku. W przypadku gdy taki zestaw danych zostanie skatalogowany poprzez przyporządkowanie indeksów do fragmentów nagrań zawierających wizerunki osób, wówczas należy uznać, że jest tworzony zbiór danych osobowych. Z danymi osobowymi mamy do czynienia także w sytuacji, kiedy system, który jest instalowany równolegle z monitoringiem, umożliwia powiązanie konkretnych nagrań z konkretną osobą.

Organy odpowiedzialne za gromadzenie i przechowywanie zapisów z kamer muszą stosować się wprost do przepisów ustawy o ochronie danych osobowych, co - biorąc pod uwagę specyfikę monitoringu wizyjnego – nie jest zadaniem łatwym. Nie zawsze wiadomo na przykład, jak zastosować przepisy dotyczące obowiązków administratora danych, wśród których wymienić można obowiązek informacyjny, jak również uprawnień osób, których dane dotyczą (choćby ich prawo do żądania uzupełnienia czy uaktualnienia danych).

Fakt, że zapisy z monitoringu miejskiego nie zawsze są związane z przetwarzaniem danych osobowych wcale nie zwalnia organów, które są w ich posiadaniu, z obowiązku zabezpieczania takich informacji przed dostępem osób nieuprawnionych. O ile takie nagranie zostałoby wykorzystane do innych celów (np. opublikowane w Internecie), wówczas podmiot danych może swoich praw dochodzić przed sądem.

Dlatego m.in. jednostkom samorządu terytorialnego, które zdecydowały się na udostępnienie obrazu z kamer monitoringu ulic w Internecie, GODO zaleca dużą ostrożność. Wskazuje, że instalowanie kamer, za pośrednictwem których dostępny jest widok jakiegoś miejsca, powinno odbywać się w taki sposób, aby zastosowana rozdzielczość uniemożliwiała rozpoznanie znajdujących się tam osób.

W dniu 24 sierpnia 2011 r. GIODO powtórnie wystąpił do Ministra Spraw Wewnętrznych i Administracji przekazując mu dokument „Wymagania w zakresie regulacji monitoringu” jako swój wkład do pracy nad przygotowaniem ustawy regulującej w sposób kompleksowy sprawę monitoringu w kontekście praw do ochrony wolności i prywatności.

I. Czynności kontrolne

W odniesieniu do **inspekcji** przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych na przestrzeni ostatnich dwóch lat (2010-2011) należy stwierdzić, że monitoring wizyjny nie stanowił przedmiotu odrębnych kontroli sektorowych. Wskazane zagadnienie było natomiast badane w toku kontroli, które obejmowały swoim zakresem sprawdzenie sposobów zabezpieczenia danych osobowych stosowanych przez administratorów danych osobowych oraz podmioty, którym powierzono przetwarzanie danych osobowych na zasadach określonych w art. 31 ustawy o ochronie danych osobowych. Wideomonitoring stanowi bowiem element systemu zabezpieczenia budynków i pomieszczeń (sale obsługi klienta, ciągi komunikacyjne, archiwa, serwerownie) oraz kontroli ruchu osobowego u wielu kontrolowanych administratorów danych, np. w bankach, towarzystwach ubezpieczeniowych, spółdzielniach mieszkaniowych, szkołach (różnego typu), placówkach medycznych, instytucjach publicznych (urzędach różnego szczebla).

Natomiast przetwarzanie danych osobowych pozyskanych z monitoringu wizyjnego należało do głównych zagadnień stanowiących przedmiot kontroli przeprowadzonych w hipermarketach, strażach gminnych, ośrodkach sportu i rekreacji, klubach sportowych oraz podmiocie (spółce kapitałowej) zarządzającym stadionem.

W toku wymienionych kontroli ustalono między innymi, że obraz rejestrowany przez kamery był zapisywany na nośnikach, np. kasetach VHS, płytach CD, twardych dyskach komputerów, serwerach lub jest dostępny wyłącznie w czasie rzeczywistym na ekranie urządzenia odtwarzającego. Zazwyczaj po upływie czasu określonego przez administratora danych zapisany obraz był kasowany – najczęściej poprzez nadpisanie kolejnego. W hipermarketach kopie obrazów były sporządzane w celu udostępnienia Policji w przypadku zaistnienia takich zdarzeń jak kradzież.

Na skutek czynności kontrolnych nie stwierdzono naruszenia prywatności oraz ochrony danych osobowych w związku z zastosowaniem wspomnianego wyżej sposobu zabezpieczenia. W szczególności nie napotkano na przypadki instalowania kamer przemysłowych w takich miejscach, jak toalety czy przebieralnie.

Poniżej przedstawione zostały przykłady kilku kontroli przeprowadzonych we wskazanych obszarach.

W wyniku kontroli przeprowadzonych w wybranych **strażach miejskich** (DIS-K-421/165/11, DIS-K-421/114/11 oraz DIS-K-421/115/11) ustalono, że w związku z wykonywaniem zadań określonych w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z 1997 r. Nr 123, poz. 779), stráže te stosują systemy monitoringu wizyjnego w celu obserwowania i rejestrowania obrazu zdarzeń w miejscach publicznych.

Przy użyciu systemów monitoringu wizyjnego stráže miejskie utrwalają m. in. następujące informacje: wizerunek osób, informacje o sposobie zachowania się osób oraz ich obecności w określonych miejscach, a także numery rejestracyjne pojazdów.

Straże dokonują identyfikacji osoby, której wizerunek został zarejestrowany przez system monitoringu wizyjnego wyłącznie w przypadku, gdy osoba ta naruszyła przepisy prawa.

Podkreślenia wymaga, iż zbieranie danych przy użyciu systemów monitoringu wizyjnego przez stráže miejskie odbywa się w celach związanych z ewentualną identyfikacją osób, których te dane dotyczą. Straże miejskie dysponując uprawnieniami wynikającymi z ustawy o strażach gminnych, w tym posiadając prawo dostępu do informacji zawartych w Centralnej Ewidencji Pojazdów i Kierowców, mają możliwość ustalenia tożsamości osób, których dane zostały zarejestrowane przez system monitoringu wizyjnego. Zatem informacje te należy uznać za dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych.

W toku kontroli ustalono, że dostęp do danych osobowych przetwarzanych przez stráže miejskie w systemach monitoringu wizyjnego był możliwy według kryterium miejsca zdarzenia (obraz z każdej z kamer monitoringu był zapisywany na odrębnej ścieżce - wyodrębnionym obszarze na dysku komputera) oraz chronologicznie według kryterium daty i czasu zdarzenia. W związku z powyższym, systemy monitoringu wizyjnego stráž miejskich zawierają zestawy danych osobowych dostępnych według określonych kryteriów i są zbiorami danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych.

Z punktu widzenia problematyki monitoringu wizyjnego na uwagę zasługują także kontrole przeprowadzone w 2011 r. w związku z organizowaniem **imprez masowych, w tym meczów piłki nożnej**.

Celem kontroli było ustalenie zgodności przetwarzania przez podmioty kontrolowane, danych osobowych z przepisami o ochronie danych osobowych, w szczególności sposób

realizacji obowiązku wyposażenia stadionów, na których odbywają się mecze piłki nożnej, w systemy elektroniczne służące m.in. do identyfikacji osób, sposób utrwalania przebiegu imprez masowych oraz sposób przetwarzania informacji dotyczących zakazu wstępu na imprezy masowe (tzw. zakazów stadionowych), zakazów klubowych oraz zakazów zagranicznych. Kontrole zostały podjęte z inicjatywy Generalnego Inspektora Ochrony Danych Osobowych na podstawie harmonogramu kontroli sektorowych na 2011 r.

Kontrole zostały przeprowadzone w 14 podmiotach, w tym w 4 ośrodkach sportu i rekreacji, w 9 klubach sportowych i w jednej spółce kapitałowej zarządzającej stadionem.

W toku przeprowadzonych kontroli ustalono, że stadiony, na których organizowane były mecze piłki nożnej, wyposażono w elektroniczne systemy kontroli wstępu, służące do identyfikacji osób, sprzedaży biletów, kontroli przebywania w miejscu i w czasie trwania meczu piłki nożnej, kontroli dostępu do określonych miejsc oraz weryfikacji informacji dotyczących osób objętych zakazem wstępu na imprezę masową (tzw. zakaz stadionowy), zakazem klubowym lub zakazem zagranicznym. Obowiązek wyposażenia stadionów w powyższe systemy wynika z art. 13 ust. 2 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 z późn. zm.) i ciąży na organizatorach imprez masowych - meczów piłki nożnej.

Zgodnie z art. 11 ust. 8 ustawy o bezpieczeństwie imprez masowych jej organizator utrwała, za pomocą urządzeń rejestrujących obraz i dźwięk, przebieg tej imprezy, a w szczególności zachowania osób.

Jak ustalono, kluby sportowe utrwały przebieg organizowanych przez siebie imprez masowych za pomocą systemów monitoringu, w które wyposażone były stadiony.

Nagrania z systemu monitoringu zawierały zestawy informacji dotyczących uczestników imprez masowych tworzące zbiory danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych. Dane te były przetwarzane wyłącznie w celu wskazanym w art. 11 ust. 9 ustawy o bezpieczeństwie imprez masowych, tj. wykorzystania zarejestrowanego obrazu i dźwięku w postępowaniu dowodowym w stosunku do osób zakłócających porządek.

W odniesieniu zaś do nagrań z monitoringu, na których utrwalony był zapis w postaci wizerunku i głosu, należało rozstrzygnąć, czy informacje te stanowią dane osobowe w rozumieniu art. 6 ustawy, a jeżeli tak, to czy tworzą one zbiór danych osobowych. Jak ustalono, system monitoringu umożliwia wykorzystanie nagrań z tego systemu do identyfikacji ww. uczestników, w szczególności poprzez wykorzystanie informacji, które zawiera system elektroniczny, o którym mowa w art. 13 ust. 2 ustawy o bezpieczeństwie

impres masowych, tj. poprzez powiązanie informacji z obu systemów. Dostęp do danych osobowych, które zawierają nagrania z systemów monitoringu, są dostępne według czasu oraz miejsca nagrania. W związku z tym uznano, iż nagrania z systemu monitoringu z przebiegu meczów piłki nożnej zawierają zestaw danych osobowych dostępnych według ww. kryteriów, a tym samym stanowią zbiór danych osobowych w rozumieniu art. 7 pkt 1 ustawy.

Oceniając wyniki kontroli przeprowadzonych w klubach sportowych stwierdzić należy, iż podmioty te w większości przypadków przetwarzały dane osobowe z naruszeniem przepisów o ochronie danych osobowych, aczkolwiek naruszenia te nie były bezpośrednio związane z monitoringiem wizyjnym.

II. Rejestracja zbiorów danych osobowych pochodzących z monitoringu wizyjnego

Administratorzy danych sporadycznie zgłaszają do rejestracji zbiory danych osobowych prowadzone w związku ze stosowaniem systemów monitoringu. Analiza rejestru zbiorów danych osobowych prowadzi do wniosku, iż dotychczas zostało zgłoszonych ok. 50 takich zbiorów.

Ze względu na parametry rejestru zbiorów danych osobowych nie jest możliwe podanie precyzyjnej informacji odnośnie liczby zgłoszonych do rejestracji zbiorów danych osobowych pochodzących z monitoringu. Wymagałoby to bowiem fizycznego przejrzenia ogromnej ilości zgłoszeń (na dzień 2 października 2012 r. do rejestru zostało wpisanych 118 647 zbiorów danych osobowych).

III. Pytania i skargi

W okresie od 2008 r. do września 2012 do Biura GIODO wpłynęło **80 pytań z prośbą o interpretację oraz 15 skarg dotyczących zagadnień związanych z monitoringiem.**

Wśród najczęściej zadawanych pytań były te dotyczące szeroko rozumianego monitoringu w miejscu pracy.

Pytano o kwestie związane dopuszczalnością wykorzystywania przez pracodawcę monitoringu wizyjnego do kontroli długości przerw i opuszczania przez pracownika miejsca pracy, obserwacja czynności wykonywanych podczas świadczenia pracy np. przez nauczyciela, lekarza, sprzedawcę, aptekarza, itd., instalacji w służbowych samochodach urządzeń GPS do kontroli tras i czasu pracy pojazdów wykorzystywanych przez pracowników

w czasie trwania delegacji (potrzeba taka wynikała z oceny pracodawcy co do bardzo niskiej wydajności pracy podczas delegacji w stosunku do nakładanych kosztów; urządzenie to miałoby monitorować i rejestrować trasę przejazdu, czas postoju i ewentualnie napełnianie zbiornika paliwem - czas, miejsce i ilość), a także dopuszczalność instalacji kamer wideo w punktach żywienia jak stołówki pracownicze, kuchnie, itp. Jedno z pytań dotyczyło podstaw prawnych monitoringu na korytarzach zakładu pracy w sytuacji, w której nikt nie pytał o zgodę ani nie informował o tym fakcie pracowników (DESiWM-083-17/08, DOLiS-035-39/09, DOLiS-035-1674/09, DOLiS-035-2411/09, DOLiS-035-458/10, DOLiS-035-1402/10, DOLiS-035-1633/10)

Podstawowym pytaniem, które najczęściej pojawiała się w kierowanych do GODO pismach, dotyczyło tego, czy informacje pochodzące z monitoringu w miejscu pracy są danymi osobowymi w rozumieniu ust. o ochronie danych osobowych. Pytano też, czy prawo zobowiązuje pracodawcę do poinformowania pracowników o zainstalowanym urządzeniu monitoringu w miejscu pracy oraz celu takiego działania, a jeśli tak, to czy przekazanie takiej informacji powinno mieć formę pisemną, a nawet – czy powinno się to odbywać podczas zawierania umowy o pracę, aby kandydat miał możliwość dokonania wyboru (DOLiS-035-39/09).

Na uwagę zasługuje pytanie zadane przez farmaceutkę zatrudnioną w aptece, w której zainstalowany był monitoring. Zwróciła się do GODO z pytaniem, czy ma ona prawo wglądu w nagranie, zwłaszcza w sytuacji, gdy przy realizacji recepty wyniknęło nieporozumienie z klientem, w skutek którego farmaceutka musiała z własnych pieniędzy pokryć stratę właściciela apteki. Jej pracodawca nie wyraził zgody na wgląd w nagrania celem ustalenia stanu faktycznego.

Do Generalnego Inspektora Ochrony Danych Osobowych trafiały też pytania o dopuszczalność instalowania modułu fonii do kamer monitoringu w miejscu pracy.

Na uwagę zasługuje pytanie skierowane od osoby fizycznej, jak z punktu widzenia ustawy o ochronie danych osobowych wygląda kwestia monitorowania pracownika/dydaktyka szkoły wyższej, podczas zajęć ze studentami. W analizowanym przypadku osoba monitorowana poinformowana została o tym fakcie wraz ze wskazaniem takiego działania celu (zapobieganie kradzieżom). Podgląd z kamer miał dyrektor, który obserwował i podsłuchiwał pracownika podczas prowadzenia zajęć.

W sprawach o takim charakterze GODO wskazywał, że pracodawca, przed zainstalowaniem kamer, powinien zastanowić się, czy nie istnieją inne, mniej ingerujące w prywatność pracownika środki umożliwiające osiągnięcie tego samego celu. W tym

kontekście warto też wskazać na Rekomendację Nr R(89)2 Komitetu Ministrów Rady Europy z 18 stycznia 1989 r. o ochronie danych osobowych wykorzystywanych dla potrzeb zatrudnienia nakazującą - poza poszanowaniem życia prywatnego i godności ludzkiej pracowników - informowanie ich lub konsultowanie się z nimi przed wprowadzeniem zautomatyzowanych systemów gromadzenia i wykorzystywania danych, ze szczególnym uwzględnieniem możliwości nawiązywania kontaktów towarzyskich i indywidualnych w miejscu pracy. Uregulowanie to jest istotne zwłaszcza dlatego, że polskie przepisy prawa pracy nie przewidują stosowania wideonadzoru w miejscu pracy.

Niemniej przyjąć można, że jeżeli monitoring jest prowadzony w miejscu pracy, to w ściśle określonych przypadkach takie działanie można uznać za uzasadnione interesem pracodawcy. Nie jest do tego wymagana zgoda pracownika, jednak co do zasady pracodawca powinien poinformować go wcześniej, że monitoring jest stosowany.

Jeśli jednak w wyniku zainstalowania monitoringu w miejscu pracy dochodzi do przetwarzania danych osobowych, to powinny być zachowane zasady ich ochrony, w szczególności prawo do kontroli procesu przetwarzania danych osobowych przez osobę, której dane dotyczą, tzn. prawo do wglądu do odpowiedniej części nagrania dotyczącego pracownika, zwłaszcza w sytuacji toczącego się wewnętrznego postępowania prowadzonego przez pracodawcę względem tego pracownika. Pracodawca - jako administrator danych osobowych - jest także zobowiązany do właściwego ich zabezpieczenia (DESiWM-083-17/08, DOLiS-035-39/09, DOLiS-035-1674/09, DOLiS-035-2411/09, DOLiS-035-458/10, DOLiS-035-1402/10, DOLiS-035-2174/10, DOLiS-035-2261/10, DOLiS-035-287/11, ZP-0601-100/11, DOLiS-035-39/09, DOLiS-035-411/12).

Monitoring w punktach usługowych (sklep, bank, urzędy skarbowe, urzędy miasta i gminy...)

- Pytanie dotyczyło podstaw prawnych stosowania monitoringu wizyjnego (niejednokrotnie łącznie z nagrywaniem głosu) w urzędach skarbowych, urzędach gmin, w pomieszczeniach wynajmowanych na potrzeby biurowe i w sklepach. Pytano także o kwestie związane z realizacją obowiązku informowania na drzwiach wejściowych o zainstalowaniu monitoringu w sklepie (DOLiS-035-1633/10, DOLiS-035-1633/10, DOLiS-035-218/11, DOLiS-035-2509/12, DOLiS-035-2933/10, DOLiS-035-113/11, DOLiS-035-1371/11, DOLiS-035-3671/11).

Spółdzielnie i wspólnoty mieszkaniowe

- W tym obszarze pytania dotyczyły legalności instalowania monitoringu wideo w pomieszczeniach należących do wspólnot mieszkaniowych lub spółdzielni mieszkaniowych, jak również zasad dostępu do zarejestrowanych materiałów. Ponadto, pytania dotyczyły legalności skierowania kamer na drzwi poszczególnych mieszkań, czy na same mieszkania (DOLiS-035-609/09, DOLiS-035-214/09, DOLiS-035-1563/09, DOLiS-035-1829/09, DOLiS-035-1487/10, DOLiS-035-1569/10, DOLiS-035-1999/10, DOLiS-035-2034/10, DOLiS-035-3134/10, DOLiS-035-2775/10, DOLiS-035-2873/10, DOLiS-035-380/11, DOLiS-035-2010/11, DOLiS-035-3445/11, DOLiS-035-3453/11, DOLiS-035-2271/12, DOLiS-035-133/12, DOLiS-035-1621/12).

Monitoring miejski/wiejski (ulice, parki skwery, place zabaw...)

Pytania dotyczyły legalności montażu monitoringu wizyjnego oraz udostępnienia uzyskanego obrazu z kamer w sieci Internet przez Urząd Gminy, jak również kwestii czy w ramach monitoringu miejskiego dochodzi do przetwarzania danych osobowych. Ponadto pytano o uprawnienia, jakimi powinien dysponować pracownik cywilny na stanowisku operatora Systemu Monitoringu Wizyjnego. Pojawiały się też pytania dotyczące skierowania kamer na prywatne posesje (DOLiS-035-889/09, DOLiS-035-1127/09, DOLiS-035-1319/09, DOLiS-035-1815/10, DOLiS-035-2882/10, DOLiS-035-190/11, DOLiS-035-2324/11, DOLiS-035-2528/11, DOLiS-035-1825/12).

Monitoring w środkach komunikacji

Pytanie od Miejskiego Przedsiębiorstwa Komunikacyjnego w kwestii możliwości udostępniania i przekazywania wizerunku pasażerów utrwalonego na monitoringu znajdującym się w autobusach komunikacji miejskiej ZTM (DOLiS-035-1945/09).

Monitoring w szatniach, przebieralniach, toaletach (sklepów, basenów...)

Zapytanie o podstawę prawną pozwalającą na instalację kamer połączonych z monitoringiem systemu ochrony w przebieralniach i szatniach basenu MOSIR. W sprawie tej GİODO podjął działania z urzędu (DOLiS-035-2461/09, DOLiS-035-1422/12).

Monitoring instalowany przez osoby prywatne

Pytanie dotyczące zgodności z prawem instalacji w ogródku przy bloku mieszkalnym przez jednego z mieszkańców kamery skierowanej na sąsiedni ogródek.

Pytanie od osoby fizycznej dotyczące podstaw prawnych zainstalowania na prywatnej posesji monitoringu wideo mającego na celu rejestrowanie działań jej sąsiada (DOLiS-035-793/10, DOLiS-035-2114/11).

Monitoring w pomieszczeniach Policji

Prośba Komendy Miejskiej Policji o wskazanie podstaw prawnych przetwarzania zbioru danych osobowych w postaci wizerunków osób zarejestrowanych za pomocą monitoringu wizyjnego zainstalowanego w Pomieszczeniu dla Osób Zatrzymanych (PDOZ) i Policyjnej Izbie Dziecka (DOLiS-035-1402/10).

W odniesieniu do **skarg** do dnia 19 września 2012 r. do Departamentu Orzecznictwa Legislacji i Skarg wpłynęło **16 skarg dotyczących monitoringu wizyjnego**. Wśród nich znalazło się sześć, w których nie prowadzono merytorycznego postępowania administracyjnego z powodu zaistnienia braków formalnych.

Zakres przedmiotowy rozpatrzonych skarg dotyczył kwestii: zastosowania przez pracodawcę monitoringu w miejscu pracy (DOLiS-035-1312/11, DOLiS-440-389/12), instalacji monitoringu miejskiego (DOLiS-440-93/10), udostępnienia TVP nagrania z kamery zamontowanej w samochodzie egzaminacyjnym zawierającym wizerunek skarżącego (DOLiS-440-169/10), niewypełnienia obowiązku informacyjnego wobec gości hotelowych w kwestii monitoringu zainstalowanym w obiekcie (DOLiS-440-694/10), instalacji przez osobę fizyczną monitoringu na wspólnej z innymi sąsiadami posesji (DOLiS-440-935/11), braku podstaw prawnych zainstalowania kamer w budynku oraz w windach przez wspólnotę mieszkaniową (DOLiS-440-960/11), odmowy udzielenia przez urząd miasta informacji dotyczącej zbioru danych osobowych w postaci zapisu obrazu i wizerunku skarżącego (DOLiS-440-448/12), zainstalowania kamer na podczerwień na działkach w rodzinnym ogrodzie działkowym przez jednego z działkowiczów (DOLiS-440-977/12) oraz instalacji kamery wideo przez osobę prywatną w miejscu zamieszkania (DOLiS-440-1074/12).