Wymagania w zakresie regulacji monitoringu

Wstęp

Technologie rejestracji obrazu znajdują coraz szersze zastosowanie – w wielu miejscach – począwszy od kabin dźwigów osobowych, wnętrza środków komunikacji, domków jednorodzinnych, a skończywszy na monitorowaniu hal produkcyjnych, obiektów sportowych, a nawet całych miast. Podstawowym składnikiem tej technologii jest kamera, która sprowadza obraz najbliższego otoczenia do postaci sygnałów elektrycznych analogowych lub cyfrowych. Tak przekształcony obraz może być przekazywany na duże odległości – do centrum obserwacyjnego, gdzie odtwarzany jest na monitorach i/lub zapisywany na elektronicznych nośnikach danych. Czynności związane ze stosowaniem kamer do rejestracji, przesyłania, zapamiętywania i obróbki obrazu ogólnie nazywane są wideofilmowaniem. W szczególnych przypadkach, gdy celem wideofilmowania jest między innymi zapewnienie kontroli nad obserwowanym obiektem, w tym nadzoru nad zachodzącymi tam zdarzeniami, czynności takie nazywamy wideonadzorem lub monitoringiem, bądź audio-wideomonitoringiem, jeśli rejestrowany jest nie tylko obraz otoczenia, ale i dźwięki. W niniejszym opracowaniu stosowanie technologii wideofilmowania we wszystkich wyżej wymienionych znaczeniach nazywane będzie ogólnie monitoringiem. W zależności od celu i okoliczności wideofilmowania obraz rejestrowany przez kamery może być przekazywany do centrum obserwacyjnego, gdzie jest:

– tylko oglądany,

– oglądany i zapisywany na elektronicznych nośnikach informacji lub

– tylko zapisywany.

W pierwszym przypadku stosowanie kamer ma na celu np. poszerzenie pola widzenia osoby sprawującej nadzór nad powierzonym terenem. Zebranie w jednym pomieszczeniu obrazu z kilku kamer pozwala wówczas jednej osobie na obserwację terenu z wielu różnych miejsc, co nie byłoby możliwe w warunkach tradycyjnych, tj. bez zastosowania kamer. Kamery do bieżącej obserwacji stosuje się również w celach promocji miejsc turystycznych, takich jak plaże, stoki narciarskie, czy też zjawisk przyrodniczych lub naukowych, np. do podglądu bocianiego gniazda. Drugi przypadek, tj. obserwację i zapis obrazu na elektronicznych nośnikach informacji, stosuje się wtedy, gdy oprócz doraźnego celu, jakim jest obserwacja terenu, istnieją też inne, np. zapamiętanie obrazu dla celów dowodowych lub zapewnienie możliwości ponownej obserwacji obrazu w celu przyjrzenia się jego szczegółom. Ostatni przypadek, tj. tylko zapisywanie obrazu – w celu zapewnienia możliwości jego

odtworzenia w przyszłości – stosuje się wtedy, gdy rejestracja obrazu ma służyć głównie celom dowodowym i prewencyjnym, tj. zniechęcającym do popełnienia zabronionych czynów na skutek łatwych możliwości ich wykrycia, a równoległa obserwacja i zapamiętywanie wiązałoby się z niewspółmiernie wielkimi kosztami. Ten ostatni przypadek stosowany jest np. w środkach komunikacji miejskiej, w pomieszczeniach, gdzie znajdują się bankomaty, salach kasowych, kasynach itp. Sam zapis obrazu stosowany jest również wtedy, gdy chodzi głównie o wykorzystanie go w celach informacyjnych, jak to ma miejsce w przypadku Google Street View czy systemu Zumi.

W większości przypadków wideofilmowania chodzi jednak o sprawowanie kontroli nad określonym obszarem w celu zwiększenia szeroko rozumianego bezpieczeństwa. Cel ten jest osiągany głównie poprzez działanie czynnika odstraszającego od popełnienia określonych czynów zabronionych, typu rozbój, kradzież, czy też innych niedozwolonych zachowań, jak również poprzez działania zapobiegawcze, takie jak szybka interwencja ograniczająca lub całkowicie eliminująca wystąpienie niepożądanych zdarzeń. Osiągnięcie wymienionych celów zależy jednak nie od faktu samego stosowania wideonadzoru, ale przede wszystkim od skuteczności jego wykorzystywania w określonym celu. Z danych London Evening Standard z września 2007 r. wynika np., że w miejscach o dużej koncentracji kamer nie odnotowano większej wykrywalności przestępstw niż w miejscach, gdzie ich nie było w ogóle. Podobnie jeśli chodzi o liczbę przestępstw – obecność kamer nie wpłynęła na zmniejszenie ich liczby[1].

W większości zastosowań technologii wideofilmowania, zwłaszcza w tych gdzie celem jest zwiększenie bezpieczeństwa czy też dyscypliny i wydajności pracy, jednym z głównych obiektów wideofilmowania jest człowiek i jego działanie. Zastosowania te określane są często pojęciem wideonadzoru. W systemach tego typu wg opinii[2] Grupy roboczej ds. ochrony danych osobowych, ustanowionej na mocy art. 29 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 (zwanej dalej Grupą roboczą art. 29), w większości przypadków mamy do czynienia z przetwarzaniem danych osobowych. Zgodnie z reprezentowanym tam poglądem pojęcie danych osobowych obejmuje informacje dostępne w jakiejkolwiek formie, na przykład alfabetycznej, liczbowej,

[1] Justin Davenport, *London Evening Standard, Tens of thousands of CCTV cameras, yet 80% of crime unsolved,* dostępne na: http://www.thisislondon.co.uk/news/article-23412867-details/Tens+of+thousands+of+CCTV+cameras%2C+yet+80%25+of+crime+unsolved/article.do; zob. też Paweł Wittich, *niewielki Brat,* Akademia Monitoringu Wizyjnego, Newsletter nr 3, maj-czerwiec 2009, dostępne na: http://www.specialisedprojects.com.pl/aktualnosci.php?czytaj=70n.

[2] Opinia 4/2007 w sprawie pojęcia danych osobowych, przyjęta w dniu 20 czerwca przez Grupę roboczą art. 29; dokument dostępny na: http://ec.europa.eu/justice_home/fsj/privacy/docs/ wpdocs/2007/wp136_pl.pdf

graficznej, fotograficznej czy akustycznej. Danymi osobowymi są zatem także wizerunki osób fizycznych, jak i profile otaczających je przedmiotów, ułatwiających często identyfikację osób. Jest to zgodne z intencją zawartą w motywach 14 i 15 preambuły do dyrektywy 95/46/WE. W motywie 14 mówi się: „Jeżeli w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, niniejsza dyrektywa powinna mieć zastosowanie do przetwarzania takich danych". W motywie 15 doprecyzowuje się, że przetwarzanie takich danych jest objęte dyrektywą 95/46/WE, ale tylko wtedy, gdy „jest ono zautomatyzowane lub jeśli dane zawarte są lub przeznaczone do umieszczenia w zamkniętym układzie zbiorów, zorganizowanym według określonych kryteriów dotyczących osób fizycznych w celu zapewnienia łatwego dostępu" do nich. Należy jednak zauważyć, że wymienione kryterium, dotyczące automatyzacji przetwarzania, w przypadku wideofilmowania jest na ogół spełnione. Wideonadzór, w części dotyczącej rejestracji obrazu lub dźwięku, jest z zasady procesem automatycznym. Czynnikiem zaś, który nie jest zautomatyzowany w całym procesie wideonadzoru, bardzo często jest bieżąca analiza rejestrowanego obrazu lub analiza obrazu zarejestrowanego, którą wykonuje człowiek. Chociaż i na tym odcinku coraz częściej stosowane są rozwiązania zautomatyzowane[3], takie jak automatyczna detekcja ruchu, czy też analiza inteligentna –ukierunkowana na rozpoznanie człowieka. Niezależnie jednak od zastosowanej metody analizy rejestrowanych obrazów – każdy przypadek, gdzie obraz rejestrowany jest automatycznie, należy uznać za czynność zautomatyzowaną, a więc czynność objętą dyrektywą 95/46/WE. Podkreślenia wymaga, że w świetle art. 3 ust 2 dyrektywy 95/46/WE jej zakres przedmiotowy nie obejmuje operacji przetwarzania danych w zakresie współpracy policyjnej i sądowej w sprawach karnych oraz „przetwarzania związanego z bezpieczeństwem publicznym, obronnością, bezpieczeństwem państwa (łącznie ze stanem gospodarki państwa, kiedy przetwarzanie danych dotyczy bezpieczeństwa państwa) oraz z działalnością państwa w dziedzinach prawa karnego". Ograniczenie to znajduje również odzwierciedlenie w motywie 16 preambuły do dyrektywy, który stanowi, że „przetwarzanie danych dźwiękowych i obrazowych, np. w przypadku nadzoru kamer wideo, nie wchodzi w zakres stosowania niniejszej dyrektywy, jeśli dokonywane jest dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub też w trakcie

[3] John Honovich, *Security Manager's Guide to Video Surveillance*, dostępne na: http://ipvideomarket.info/book/Security _Manager_Guide_Video_Surveillance_v3_0.pdf.

działań państwowych w dziedzinie prawa karnego lub innych działań niewchodzących w zakres prawa wspólnotowego".

Wykluczenie powyższe nie obejmuje jednak przypadku stosowania nadzoru kamer wideo w supermarketach, muzeach, restauracjach, kawiarniach i w wielu innych sytuacjach, gdzie celem jest przeciwdziałanie kradzieżom i oszustwom, a nie zapewnienie bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego, czy też rejestracja działań organów państwowych w dziedzinie prawa karnego lub innych działań niewchodzących wówczas w zakres prawa wspólnotowego.

Warto jednak zaznaczyć, że Traktat z Lizbony zniósł uprzednią strukturę filarową prawa UE oraz wprowadził nową, wszechstronną podstawę prawną dla ochrony danych osobowych we wszystkich politykach UE, w tym w dawnym III filarze UE. W chwili obecnej ograniczenie wynikające z motywu 16 preambuły oraz art. 3 ust. 2 tiret pierwsze dyrektywy 95/46/WE traci na znaczeniu ze względu na treść art. 16 Traktatu o funkcjonowaniu Unii Europejskiej. W konsekwencji tych zmian oraz w związku z szybkim rozwojem nowych technologii obecnie w Komisji Europejskiej trwają prace nad zmianą dyrektywy 95/46/WE, które mają wyjść naprzeciw wyzwaniom, jakie niesie ze sobą rozwój nowych technologii i postęp cywilizacyjny[4]. Pierwszym wynikiem tych prac, które zapoczątkowane zostały w maju 2009 r. na konferencji zorganizowanej przez Komisję Europejską pt. „Personal data – more use, more protection?", jest komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów zatytułowany „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej"[5]. W komunikacie tym wyraźnie podkreśla się potrzebę zachowania wysokiego poziomu ochrony danych osobowych we wszystkich obszarach działania Unii oraz potrzebę kompleksowych regulacji w tym zakresie.

Nadmienić również należy, że dyrektywa 95/46/WE nie jest jedynym aktem prawnym dotyczącym ochrony danych osobowych, który ma zastosowanie do przetwarzania danych osobowych w związku ze stosowaniem systemów wideonadzoru.

W szczególności należy zwrócić uwagę na Konwencję nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzoną w Strasburgu dnia 28 stycznia 1981 r., której zakres zastosowania nie ma takich ograniczeń jak

[4] Zob. http://ec.europa.eu/justice/policies/privacy/review/index_en.htm.

[5] Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów zatytułowany „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", Bruksela dnia 4.11.2010 r., dokument KOM(2010) 609 wersja ostateczna.

w dyrektywie 95/46/WE. W konwencji tej dane dotyczące osoby – w formie nagrania wideo jej wizerunku czy też głosu – nie są traktowane w jakiś szczególny sposób. To że ochrona danych przedstawiających wizerunek osoby, a szczególnie nagranie obrazu i/lub dźwięku przedstawiające osobę w określonych działaniach jest przedmiotem konwencji, wynika z jej art. 1, który stanowi, że: konwencja ma na celu „zapewnienie każdej osobie fizycznej, bez względu na narodowość lub miejsce zamieszkania, poszanowanie jej praw i podstawowych wolności, a w szczególności jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych (ochrona danych)". Prywatność z kolei to termin, który – w najszerszym znaczeniu – określa możliwość jednostki lub grupy osób do utrzymania posiadanej wiedzy, informacji, zachowań i działań odnoszących się do danej grupy lub swojej osoby tylko dla siebie. Niewątpliwie wszelkie nagrania obrazu i/lub dźwięku przedstawiające wizerunek/wypowiedź osoby fizycznej są danymi ujawniającymi jej zachowania. O znaczeniu, jakie ma monitoring dla ochrony prywatności osoby fizycznej w świetle ochrony prywatności, o której mowa w Konwencji nr 108, świadczy raport dotyczący zasad, jakie w celu ochrony prywatności powinny być stosowane przy pozyskiwaniu i przetwarzaniu danych za pomocą środków monitoringu wizyjnego, opracowany przez Grupę projektową w zakresie Ochrony Danych Osobowych (CJ-PD), przyjęty przez Europejski Komitet ds. Współpracy Prawnej (CDCJ) na 78. spotkaniu w dniach 20–23 maja 2003 r., czy też raport tzw. Komisji Weneckiej przy Radzie Europy pt. „Wideonadzór Miejsc Publicznych przez Władzę oraz Ochrona Praw Człowieka" z marca 2007 r.

W wielu przypadkach głównym obiektem wideofilmowania nie jest osoba czy grupa osób, lecz określone miejsce – w celu wczesnego wykrycia niepożądanych zdarzeń i możliwości podjęcia odpowiednich działań prewencyjnych lub interwencyjnych. Wideofilmu ze wskazanego przedziału czasu (odcinka nagrania) nie można w związku z tym przypisać do określonej osoby, lecz do określonego miejsca i czasu. Jeśli w miejscu tym sfilmowana zostanie osoba, to tylko dlatego, że się tam ona znalazła, a nie dlatego, że to właśnie ona miała zostać sfilmowana. Identyfikacja sfilmowanej osoby staje się wówczas celem wtórnym – i to tylko wtedy, gdy jest to niezbędne do podjęcia określonych działań dochodzeniowo-śledczych. Zapis takiego obrazu nie jest zazwyczaj wyposażony w mechanizmy mogące indeksować utworzony zbiór obrazów wg osób, które zostały w ten sposób zarejestrowane.

Przeciwieństwem takiej sytuacji będzie monitoring konkretnej osoby, czy też osób – w miejscu pracy, szkole, samochodzie (np. w czasie zdawania egzaminu na prawo jazdy),

kabinie, przymierzalni w sklepie, czy też w miejscach prywatnych zajmowanych przez ich właścicieli i/lub lokatorów.

W obu sytuacjach przetwarzane dane, niezależnie od tego czy jest to tylko obraz, czy też obraz i dźwięk, w sposób istotny różnią się od danych osobowych o charakterze tekstowym, gdzie można wskazać zakres przetwarzanych danych, dokonywać na nich operacji typu wyszukania danych wg imienia i nazwiska, wyszukiwania osób z określonego przedziału wiekowego, wg miejsca zatrudnienia, wykształcenia itp. Ponadto w jednej sytuacji przetwarzaniu poddawane są dane, które w sposób selektywny są zbierane i wstępnie przetworzone przez człowieka, w drugiej natomiast – przetwarzanie danych na etapie ich pozyskiwania realizowane jest głównie w sposób automatyczny. Udział człowieka w systemach monitoringu ogranicza się najczęściej do obserwacji obrazów rejestrowanej przestrzeni w celu reakcji na niepożądane zdarzenia lub przeglądania obrazów już zarejestrowanych.

Odmienność ta sprawia, że nie jest możliwe stosowanie takich samych zasad do przetwarzania danych tekstowych i do przetwarzania danych obrazowych zawartych w systemach monitoringu wizyjnego czy audiowizualnego. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwana dalej w skrócie u.o.d.o. reguluje w sposób ogólny głównie przetwarzanie danych osobowych o charakterze tekstowym. Wiele zawartych w niej reguł nie da się wprost zastosować do danych osobowych o charakterze obrazowym, które przetwarzane są w systemach monitoringu.

Stąd też istnieje dość pilna potrzeba odrębnej ustawowej regulacji stosowania wideonadzoru, albowiem w wielu sytuacjach dochodzi tam do przetwarzania danych osobowych i następuje ingerencja w prywatność osoby, która chroniona jest mocą przepisów ustawy z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz. U. z 1997 r., Nr 78 poz. 483 z późn. zm.) oraz w prawie międzynarodowym i UE. Także, biorąc pod uwagę regulacje u.o.d.o, w praktyce problemem może być m. in. wykonywanie przez administratora wielu obowiązków wynikających z przepisów o ochronie danych osobowych, np. obowiązku informacyjnego, o którym mowa w art. 24 u.o.d.o, czy też zapewnienie realizacji uprawnień kontrolnych osobie, której dane dotyczą (art. 32 i art. 33 u.o.d.o).

Wskazać warto na opinię nr 4/2004 Grupy roboczej artykułu 29 – europejskiego niezależnego organu ds. ochrony danych osobowych i prywatności – gdzie zwrócono uwagę m.in. na konieczność respektowania zasady proporcjonalności (dane muszą być adekwatne i

istotne dla celów przetwarzania) przy posługiwaniu się monitoringiem, co oznacza przede wszystkim, że urządzenia służące do takiego monitoringu mogą być stosowane wyłącznie jako środki pomocnicze, jeśli istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, niewymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania dla realizacji powyższych prawnie uzasadnionych celów Ta sama zasada dotyczy również wyboru odpowiedniej technologii, kryteriów wykorzystywania urządzeń w konkretnych sytuacjach oraz ustaleń dotyczących przetwarzania danych, odnoszących się także do zasad dostępu i okresu przechowywania. Ponadto w opinii tej wskazano, iż osoby, których dane dotyczą, powinny być świadome faktu prowadzenia tego rodzaju monitoringu, a w szczególności posiadać szczegółowe informacje na temat miejsc objętych takim systemem.

Nie ulega przy tym wątpliwości, iż wszelkie działania ingerujące w prawo do prywatności w życiu osobistym powinny być prowadzone z poszanowaniem obowiązujących przepisów prawa. Zgodnie z art. 31 ust. 3 Konstytucji RP ograniczenia w korzystaniu z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. W przypadku zaś gdy celem przetwarzania jest zapewnienie innych, również konstytucyjnych praw, np. wskazanego w art. 54 ust. 1 Konstytucji RP prawa do wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji, to ich realizacja musi być w równowadze z prawem do wolności i prywatności.

Ponadto, zgodnie z art. 47 Konstytucji RP, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W art. 233 ust. 1 Konstytucji RP podkreśla się przy tym, że prawo to nie może podlegać ograniczeniom także w stanach nadzwyczajnych. Skoro zatem przepisy Konstytucji RP chronią przedmiotowe prawo w sytuacji zagrożenia, to tym bardziej nie mogą wprowadzać w tym zakresie ograniczeń wówczas, kiedy płynące z powyższego „korzyści" nie są wystarczające dla uznania zasadności ingerencji o takim charakterze. W wyroku z dnia 20 marca 2006 r. o sygn. akt K 17/05 Trybunał Konstytucyjny podkreślił: „(...) Nie można (...) tracić z pola widzenia faktu, że prawo do prywatności ma charakter szczególny w systemie praw i wolności konstytucyjnych (...)". Obowiązek poszanowania prawa do prywatności wynika również z faktu, iż Rzeczpospolita Polska, jako państwo członkowskie

Unii Europejskiej, jest stroną europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, sporządzonej w Rzymie w dniu 4 listopada 1950 r., która w art. 8 ustanawia prawo do „poszanowania życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji". Podkreślić należy, że coraz częściej informacje dotyczące wizerunku osób, informacje o obecności w określonych miejscach, o sposobie zachowania, jak również treść wypowiedzi itp., są utrwalane i mogą być wykorzystywane w różnych celach.

W niektórych przypadkach konieczność stosowania systemów monitoringu wynika z obowiązujących przepisów (np. w kasynach, na stadionach w czasie imprez masowych). W innych sytuacjach monitoring może być stosowany z uwagi na szczególnie ważny, usprawiedliwiony cel określonych podmiotów, zarówno publicznych, jak i prywatnych. Systemy te stosowane są nie tylko w celach zapewnienia bezpieczeństwa, lecz także szeroko rozumianego „nadzoru". Obszar takich zastosowań nie posiada odpowiednich regulacji, a obejmuje np. monitorowanie miejsc pracy w celu nadzoru pracowników, monitoring w środkach komunikacji miejskiej celem sprawdzenia natężenia ruchu, czy też monitoring we wspólnotach mieszkaniowych lub spółdzielniach w celu ochrony mienia.

1. Cel i zakres pożądanych regulacji

Regulacje dotyczące monitoringu powinny w szczególności określić miejsca i okoliczności, w jakich stosowanie monitoringu jest dopuszczalne, prawa i obowiązki podmiotu prowadzącego monitoring, prawa osób objętych monitoringiem, jak również zasady dotyczące wykorzystywania danych zebranych w procesie monitoringu. Określone w tych regulacjach warunki prawne stosowania monitoringu powinny zapewnić równowagę między uzasadnionymi potrzebami podmiotów stosujących monitoring i prawem do prywatności osób, które zostały objęte monitoringiem.

1.1. Zakres przedmiotowy regulacji

Zakres przedmiotowy regulacji – biorąc pod uwagę wytyczne dokumentu „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", tj. powołanego na s. 6 (przypis 5) komunikatu Komisji Europejskiej – powinien obejmować zarówno warunki stosowania monitoringu w celu poprawy bezpieczeństwa, jak również warunki stosowania monitoringu dla innych celów, także w celu usprawnienia procesów zarządzania, np. poprzez ich optymalizację i/lub automatyzację (jak monitoring pracowników w miejscu pracy, monitoring ruchu drogowego dla celów synchronizacji świateł na skrzyżowaniu w zależności od natężenie ruchu pieszych i pojazdów, monitoring parkingów w celach automatyzacji

rozliczeń za korzystanie z miejsca i informowania o wolnych lub zajętych miejscach itp.), jeżeli w obrębie monitorowanego obszaru pojawiają się lub mogą się pojawić osoby fizyczne.

W pierwszym przypadku chodzi o monitoring wizyjny, który jest stosowany w celu wspomagania kontroli dostępu i zapewnienia bezpieczeństwa siedzib i mienia oraz znajdujących się w nich ludzi i informacji. Jako główny cel takiego monitoringu wymienia się zwykle poprawę bezpieczeństwa poprzez zapobieganie wszelkiego rodzaju incydentom. W praktyce tego typu monitoring często nie tylko zapobiega incydentom (powstrzymuje potencjalnych sprawców), ale również pozwala zabezpieczyć dowody, jeśli incydenty wystąpią. W takich zastosowaniach ważnym parametrem technicznym systemu jest rozdzielczość i jakość pozyskanych danych. Albowiem gdy zebrany materiał ma stanowić dowód w sprawie, dowód ten jest tym lepszy, im obraz jest bardziej ostry i im większe są proporcje obiektu będącego punktem zainteresowania na tle całego obrazu monitorowanej przestrzeni.

W drugim przypadku chodzi o system monitoringu, który może pełnić funkcję czynnika automatyzującego określone procesy, jak np. udostępnianie miejsc parkingowych i rozliczanie opłat parkingowych, pobieranie opłat za korzystanie z autostrad, tuneli czy promów. System ten może również służyć do zbierania informacji w celu optymalizacji np. sygnalizacji świetlnej na drogach w zależności od natężenia ruchu, do sterowanie procesami technologicznymi itp. Zastosowanie monitoringu powinno tu podlegać regulacjom związanym z ochroną danych osobowych tylko wtedy, gdy w zakresie przetwarzanych danych znajdują się lub mogą się znaleźć dane osobowe, np. wizerunki osób, numery rejestracyjne samochodów, numery kart kredytowych lub inne elementy identyfikujące lub mogące doprowadzić do identyfikacji osób, których one dotyczą.

W zakres przedmiotowy regulacji dotyczącej stosowania monitoringu powinny wchodzić również zastosowania monitoringu w innych celach niż wymienione wyżej, np. monitoring na potrzeby reklamy miejsc turystycznych, promocji określonych imprez oraz inne nieuregulowane w ramach odrębnych przepisów szczególnych jego zastosowania [6].

[6] Proponowana regulacja nie ingeruje w przepisy odrębne dotyczące stosowania monitoringu określonych miejsc i zdarzeń, jak np. monitoring w kasynach czy monitoring imprez masowych, które zostały określone odpowiednio w przepisach rozporządzenia Ministra Finansów z dnia 3 czerwca 2003 r. w sprawie warunków urządzania gier i zakładów wzajemnych (Dz. U. z 2003 r. Nr 102, poz. 946) oraz ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. z 2009 r. Nr 62, poz. 504) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10 stycznia 2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej (Dz. U. z 2011 r. Nr 16, poz. 73).

Przedmiotowa regulacja powinna dotyczyć wszelkich form monitoringu, niezależnie od stosowanej technologii (analogowej, cyfrowej), niezależnie od tego czy obraz jest tylko przekazywany do centrum obserwacyjnego, czy przekazywany i rejestrowany oraz niezależnie od stopnia zaawansowania narzędzi używanych do automatycznego przetwarzania rejestrowanych obrazów. Regulacja ta powinna jednocześnie uwzględniać specyficzne dla poszczególnych technologii cechy, parametry i funkcjonalności. Powinna ona obejmować stosowanie monitoringu stacjonarnego, tzn. wykonywanego przy użyciu kamer zainstalowanych na stałe, jak i monitoringu doraźnego – wykonywanego przy użyciu kamer przenośnych, w tym kamer, którymi bezpośrednio operuje człowiek, ukierunkowując je na określone miejsca.

W ramach warunków stosowania monitoringu przedmiotem regulacji powinno być:

1) Określenie zasad, warunków i okoliczności, w jakich monitoring może być stosowany, w tym wskazanie organu lub organów odpowiedzialnych za kontrolę legalności monitoringu oraz wydawanie zgód i zezwoleń na jego zastosowanie[7].

2) Wskazanie przestrzeni i sposobu jej oznaczenia, w odniesieniu do której monitoring może być stosowany, oraz przestrzeni lub jej fragmentów, wobec których monitoringu nie należy stosować.

3) Wskazanie technicznych i organizacyjnych warunków, jakie musi spełniać podmiot przed wprowadzeniem monitoringu, w czasie stosowania monitoringu oraz podczas jego usuwania.

4) Określenie praw i obowiązków podmiotu stosującego monitoring.

5) Określenie praw osób, których wizerunki zostały zarejestrowane w systemie monitoringu.

6) Określenie odpowiedzialności karnej wobec podmiotów naruszających zasady i warunki stosowania monitoringu.

1.2. Zachowanie zgodności z innymi regulacjami, w tym regulacjami dotyczącymi ochrony danych osobowych. Rejestracja systemów monitoringu

W regulacji dotyczącej stosowania monitoringu należy podjąć decyzję co do sposobu realizacji dla systemów monitoringu kontroli wstępnej, o której mowa w art. 20 dyrektywy

[7] W niniejszym dokumencie nie rozstrzyga się, czy zastosowanie monitoringu w Polsce powinno być regulowane w formie wydawania zgód, zgłaszania do wskazanego urzędu, czy bez tych obowiązków – pod warunkiem spełnienia określonych wymagań.

95/46/WE. Zadanie to w odniesieniu do zbiorów danych osobowych realizowane jest w ustawie o ochronie danych osobowych poprzez wprowadzenie obowiązku rejestracji zbiorów danych osobowych. Specyfika systemów monitoringu, w tym charakter i struktura zbiorów danych stanowiących nagrania z monitoringu powodują, że nie można w tym zakresie przenieść rozwiązań wprowadzonych w ustawie o ochronie danych osobowych. W toku ustanawiania szczegółowych regulacji w tym zakresie sugeruje się rozważenie następujących propozycji:

1) Wprowadzenia obowiązku zgłaszania projektów systemu monitoringu do akceptacji przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) lub inny urząd, w przypadku gdy w systemie stosowane są elementy automatycznego przetwarzania obrazu mające na celu rozpoznanie osób, identyfikację określonego typu ich zachowań, określenie intencji ich postępowania lub inne mechanizmy wprowadzające indeksację zarejestrowanych obrazów z danymi osobowymi. Celem takiego zgłoszenia byłaby weryfikacja przez GIODO zastosowanych przez administratora środków ochrony danych osobowych na podstawie przekazanego projektu systemu i przewidzianych w nim środków ochrony danych. Wypełnienie obowiązku zgłoszenia systemu monitoringu do GIODO zwalniałoby administratora od obowiązku zgłaszania zbioru danych osobowych, jeśli taki powstawałby w wyniku wdrożenia do stosowania takiego systemu.
2) Wprowadzenia obowiązku zgłaszania zbiorów danych osobowych tworzonych w wyniku stosowania monitoringu. Przy takim rozwiązaniu należałoby dokładnie określić warunki zaklasyfikowania powstałego w wyniku monitoringu nagrania do danych osobowych. W szczególności należałoby wskazać, że za zbiór danych osobowych uważa się wyłącznie nagrania, w których występuje relacja pomiędzy elementami nagrania (obrazem) i danymi identyfikującymi osoby. W przeciwnym bowiem razie, zgodnie z definicją zbioru zawartą w art. 7 pkt 1 u.o.d.o., nagrania, w którym występują wizerunki osób fizycznych, nie można uznać za zbiór danych osobowych – z uwagi na brak w strukturze takiego zestawu danych informacji o charakterze osobowym, które dostępne byłyby według określonych kryteriów. Alternatywnym rozwiązaniem mogłoby być również rozwiązanie polegające na zmianie definicji zbioru danych osobowych zawartego w u.o.d.o. w taki sposób, że pojęcie to obejmowałoby również zbiory danych powstałe w wyniku nagrań

obrazów zarejestrowanych w systemach monitoringu wizyjnego i audiowizualnego.

3) Połączenie obydwu rozwiązań, tj. wprowadzenia obowiązku zgłoszenia, o którym mowa w punkcie 1, oraz zgłoszenia zbioru, o którym mowa w punkcie 2.

4) Wprowadzenie obowiązku rejestracji lub notyfikacji systemów monitoringu, w których są lub mogą być przetwarzane dane osobowe, niezależnie od stopnia ich technologicznego zaawansowania i automatycznie wykonywanych czynności przetwarzania danych.

W przypadku podejmowania decyzji o wprowadzeniu do przedmiotowej regulacji instytucji kontroli wstępnej – rozważenia wymagają zasady jej przeprowadzania oraz wskazanie organów upoważnionych i zobowiązanych do przeprowadzania związanych z tym czynności. Czy będzie to organ centralny, czy podmioty o strukturze terytorialnej? Czy kontrola wstępna będzie dotyczyła jedynie systemów monitoringu rejestrowanych przez np. GIODO? Czy do GIODO mają być zgłaszane wszystkie systemy monitoringu, czy tylko te o szczególnych możliwościach w zakresie przetwarzania danych osobowych? Jeśli tak, to co z pozostałymi systemami monitoringu i ewentualnie kto będzie sprawował nadzór nad legalnością ich funkcjonowania? W przypadku wprowadzenia obowiązku przeprowadzania kontroli wstępnej dla wszystkich systemów, w zależności od przyjętego rozwiązania (organ centralny czy inne organy o strukturze terytorialnej) konieczne będzie uregulowanie sposobu ewidencjonowania rozstrzygnięć kontroli wstępnej i przekazywania informacji między podmiotami dokonującymi rejestracji w zakresie ustaleń stwierdzonych w czasie kontroli wstępnej.

W powyższym zakresie w różnych krajach europejskich przyjęto różne rozwiązania. Warto jednak zwrócić uwagę, że w krajach, gdzie zagadnienie monitoringu zostało uregulowane – czy to w ustawach obejmujących przetwarzanie danych osobowych, czy w specjalnych ustawach poświęconych monitoringowi – zawsze przewidziano albo instytucję wydawania zezwoleń, albo instytucję rejestracji lub notyfikacji systemów monitoringu. W większości krajów instytucją wydawania zezwoleń lub notyfikacji objęto wszystkie rodzaje systemów monitoringu, w których rejestrowane są obrazy z możliwością ich późniejszego odtworzenia. Jedynie w niektórych krajach obowiązek rejestracji i wydawania zezwoleń ograniczony został do systemów charakteryzujących się szczególnymi możliwościami przetwarzania rejestrowanych obrazów.

W Hiszpanii np. – zgodnie z ustawą strukturalną nr 4/1997 z 4 sierpnia 1997 r., dotyczącą korzystania z kamer wideo przez służby zajmujące się bezpieczeństwem w miejscach publicznych – przewidziano, że zainstalowanie kamer wideo lub jakiegokolwiek innego urządzenia technicznego służącego do wykonywania nagrań wymaga uzyskania zezwolenia specjalnej komisji, której będzie przewodniczył sędzia i w której składzie członkowie organu administracyjnego wydającego zezwolenie nie będą stanowili większości. Podobne przepisy odnoszą się w Hiszpanii również do sektora prywatnego.

W Belgii z kolei – zgodnie z ustawą z dnia 21 marca 2007 r., regulującą instalowanie i użytkowanie kamer monitorujących – przyjęto zasady wymagające od podmiotu, który zamierza wprowadzić monitoring, uzyskania pozytywnej opinii rady gminy, w której znajduje się monitorowane miejsce i notyfikacji tego systemu do Komisji Ochrony Życia Prywatnego. W związku z powyższym podmiot, który ma zamiar wprowadzić stosowanie monitoringu, zobowiązany jest przedstawić odpowiednio przygotowany projekt takiego monitoringu do zaopiniowania radzie gminy, w której znajduje się monitorowane miejsce. Rada gminy wydaje opinię o zasadności stosowania monitoringu po konsultacjach z szefem strefy policyjnej, w której znajduje się dane miejsce. Dopiero po uzyskaniu pozytywnej opinii rady gminy podmiot może podjąć decyzję o wprowadzeniu monitoringu. Decyzja ta musi być przekazana, najpóźniej w przeddzień uruchomienia systemu monitoringu, do Komisji Ochrony Życia Prywatnego i do szefa strefy policyjnej, w której znajduje się dane miejsce.

We Włoszech, gdzie zasady stosowania monitoringu uregulowane zostały w ustawie dotyczącej przetwarzania danych osobowych, przewidziano, że zgłoszenie systemów monitoringu do Urzędu Rzecznika Ochrony Danych Osobowych jest obligatoryjne tylko w sytuacji kiedy z uwagi na zastosowane technologie mogą zaistnieć szczególne zagrożenia dla ochrony danych osobowych. Zgłoszenie jest jednak bezwzględnie wymagane, jeśli system nadzoru wizyjnego występuje w połączeniu z zastosowaniem biometrii lub w połączeniu z systemem rozpoznawania twarzy – w celu np. identyfikacji osób lub ich intencji czy nastroju.

1.3. Wyłączenia, które nie wchodzą w zakres przedmiotowej regulacji

Proponuje się, aby regulacje zawarte w niniejszym dokumencie – z uwagi na specyfikę niektórych okoliczności, w których dochodzi do rejestracji obrazu – nie dotyczyły:

1) wideorozmów i wideokonferencji;

2) prostych zestawów wideofonowych bez możliwości nagrywania, instalowanych np. przy bramach wjazdowych na posesję, wejściach do budynku, lokali itp.;
3) zastosowania kamery do celów artystycznych lub dziennikarskich (takich jak tworzenie filmów bądź nagrywanie lub emisja wiadomości);
4) nagrywania bądź emisji materiałów z konferencji, seminariów, spotkań czy szkoleń; materiałów do celów dokumentalnych, szkoleniowych, edukacyjnych;
5) nagrań lub zdjęć wykonywanych do osobistego użytku;
6) zastosowań monitoringu satelitarnego przez wojsko lub inne służby specjalne.

1.4. Proponowany zakres podmiotowy regulacji

Proponuje się, aby warunki i zasady stosowania oraz wykorzystywania monitoringu będące przedmiotem projektowanych regulacji miały zastosowanie do:

1) organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych;
2) podmiotów niepublicznych realizujących zadania publiczne;
3) osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi;
4) osób fizycznych, jeżeli monitoring obejmuje otwartą lub zamkniętą przestrzeń przeznaczoną do użytku publicznego.

1.5. Wyłączenia podmiotów, których niniejsze regulacje nie obejmują

Proponuje się, aby z uwagi na specyfikę podmiotów i przysługujące im prawo do wolności i swobody wyrażania swoich opinii przedmiotowe regulacje nie dotyczyły:

1) osób fizycznych, jeżeli obszar objęty monitoringiem nie wykracza poza teren lub obiekty stanowiące ich własność i przeznaczone do wyłącznego użytku tych osób;
2) działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

2. Proponowane definicje

1) Monitoring (wideonadzór) – zdalny odbiór obrazu lub obrazu i dźwięku z przestrzeni znajdującej się w polu widzenia kamer zainstalowanych w określonych punktach w pobliżu monitorowanego obszaru.

2) System monitoringu – zespół kamer, urządzeń przesyłowych, elektronicznych nośników danych, urządzeń rejestracji danych, urządzeń odtwarzających zarejestrowane dane oraz oprogramowania wykorzystywanego w celu osiągnięcia określonej funkcjonalności w zakresie monitoringu.

3) Kamera – urządzenie służące do konwersji optycznego obrazu otoczenia znajdującego się w polu widzenia tego urządzenia na postać sygnału analogowego lub cyfrowego zapisywalnego na elektronicznych nośnikach informacji.

4) Kamera przenośna, przenośny system monitoringu – kamera/system monitoringu stosowane doraźnie w określonym miejscu, na czas w którym odbywa się określone zdarzenie.

5) Kamera stacjonarna, stacjonarny system monitoringu – kamera/system monitoringu, w którym kamera/kamery umieszczone są na stałe w określonych miejscach w pobliżu monitorowanej przestrzeni. Stacjonarną kamerą bądź stacjonarnym systemem są również kamera/system, w których operator zdalnie może zmieniać ustawienie kamery, zmieniając w ten sposób obszar w polu widzenia kamery lub jej ustawienia, np. poprzez zawężenie lub poszerzenie pola widzenia kamery.

6) Rejestracja obrazu – proces zapisu na określonego typu nośniku danych sygnałów elektromagnetycznych lub informacji cyfrowej powstałych w wyniku przekształcenia obrazu znajdującego się w polu widzenia kamery do postaci sygnałów elektromagnetycznych lub cyfrowych.

7) Otwarta przestrzeń publiczna – miejsca dostępne publicznie, takie jak ulica, parkingi, place targowe, place przeznaczone na imprezy masowe, stadiony, parki przeznaczone do użytku publicznego i inne obszary o podobnym przeznaczeniu.

8) Zamknięta przestrzeń publiczna – obiekty ogrodzone, sale i inne pomieszczenia, takie jak np. muzea, hale sportowe, supermarkety, sklepy, biura obsługi klienta

różnych instytucji, do których wstęp nie jest ograniczony posiadaniem określonych uprawnień.

9) System rozpoznawania/analizy obrazu – oprogramowanie lub urządzenie umożliwiające w czasie rzeczywistym identyfikację obiektów, które znalazły się w polu widzenia kamery, a także ocenę ich zachowań lub intencji.

3. Obowiązki informacyjne, jakie powinny wykonać podmioty stosujące monitoring, oraz sposób ich wykonania

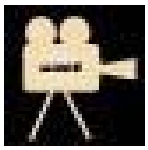
Podmiot stosujący monitoring powinien poinformować osoby, które potencjalnie mogą znaleźć się w obszarze objętym monitoringiem, że monitoring jest stosowany, jaki jest jego cel, jaki obejmuje teren oraz kto nim zarządza.

Podmiot ten powinien przekazać informacje o swojej nazwie i o adresie swojej siedziby, obszarze stosowania oraz celu i ewentualnie podstawie prawnej monitorowania, jeśli taki obowiązek na nim spoczywa, stosownie do obowiązujących przepisów prawa. Sposób wypełnienia tego obowiązku powinien być dostosowany do okoliczności i miejsca, którego dotyczy. Powinien uwzględniać między innymi kategorie osób, które mogę przebywać w monitorowanych obszarach, w tym znajomość języków, i w związku z tym w miejscach gdzie występuje koncentracja osób nieznających języka polskiego – informować w języku angielskim lub za pomocą powszechnie przyjętych znaków graficznych. W odniesieniu do treści przekazywanych informacji tekstowych sugeruje się, aby brzmienie standardowej klauzuli informującej o stosowaniu monitoringu było następujące:

Monitoring prowadzony jest przez … /tu nazwa podmiotu/, z siedzibą w … /tu adres siedziby podmiotu/, w celu … /tu wskazanie celu/ i obejmuje … /tu wskazanie obszaru, jaki objęty jest monitoringiem/, stosownie do przepisów ustawy … /tu powołanie stosownego aktu prawa o randze co najmniej ustawy/ Więcej informacji uzyskać można telefonicznie /tu numer telefonu podmiotu/, drogą elektroniczną /tu adres poczty elektronicznej, wskazanie stosownej strony internetowej podmiotu/.

Informacje tego typu powinny być umieszczane – odpowiednio – w obszarze, obiekcie czy innym miejscu objętym monitoringiem. Tak by były łatwo dostrzeżone, bez potrzeby szczegółowych oględzin otoczenia. Oznacza to, że za nieprawidłowe należy uznać rozwiązanie polegające na umieszczeniu informacji o monitoringu np. w miejscu zasłoniętym przez skrzydło otwartych drzwi, zasłoniętym przez inne tablice informacyjne, zbyt nisko lub zbyt wysoko itp.

Biorąc pod uwagę, że informacja tekstowa zawarta na stosownej tablicy informacyjnej będzie zrozumiała wyłącznie dla osób znających język polski, niezbędne jest, aby niezależnie od informacji w formie tekstowej umieszczony był piktogram kamery, który jest graficznym znakiem informującym o stosowaniu monitoringu w danej przestrzeni. Informacja w postaci piktogramu powinna być stosowana niezależnie od informacji tekstowej. Proponuje się do rozważenia użycie następujących piktogramów:




Odnośnie do informowania o przestrzeni objętej monitoringiem – nie wydaje się celowe, aby w treści przepisu szczegółowo i wyczerpująco normować przedmiotowy zakres monitoringu, mając na uwadze różnorodność miejsc, do których niniejsze regulacje mogą mieć zastosowanie. Miejscami tymi mogą być zarówno stadiony, parkingi publiczne, przejścia podziemne, jak i miejsca zamknięte – typu wnętrze autobusu, kabina przedziału kolejowego czy dźwigu osobowego. Ważne jest jednak, aby określenie obszaru objętego monitoringiem było takie, by został osiągnięty oczekiwany skutek. W projektowanej regulacji proponuje się przyjąć, że w przypadku gdy informacja na tablicy informacyjnej nie wskazuje (nie określa) szczegółowo nazwy monitorowanego obszaru, wówczas zasięg informacyjny tablicy dotyczy tylko jej najbliższego otoczenia, tj. placu, hali kasowej w banku, przestrzeni hali sklepowej w supermarkecie, przejścia podziemnego, peronu kolejowego itp. W przypadku wejścia w inną strefę, oddzieloną od strefy oznaczonej jako monitorowana, wymagać należy odnowienia informacji o monitorowaniu.

Ponadto o ile przedmiotowe regulacje zezwalać będą na stosowanie monitoringu przez osoby prywatne, a nie tylko przez podmioty publiczne oraz prowadzące działalność gospodarczą, to w stosownym komunikacie informacyjnym powinny zostać wskazane – w miejscu danych identyfikujących podmiot – dane identyfikujące taką osobę: jej imię, nazwisko i adres.

4. Prawa osób objętych monitoringiem oraz obowiązki podmiotu stosującego monitoring wobec tych osób

Wydaje się w pełni uzasadnione, aby osobom objętych monitoringiem przysługiwały takie same prawa jak osobom, których dane osobowe są przetwarzane. Uprawnienia tych ostatnich określone zostały w art. 32–35 u.o.d.o. Jedyne różnice, jakie mogą w tym obszarze

wystąpić, powinny być uzasadnione specyficznymi właściwościami stosowanej w systemach monitoringu technologii. Wspomniana w rozdziale 2. hiszpańska ustawa strukturalna 4/1997, określająca zasady korzystania z kamer wideo przez służby zajmujące się bezpieczeństwem w miejscach publicznych mówi wprost, że „każda osoba zainteresowana, która została nagrana, ma prawo wglądu do nagrań i żądania ich usunięcia".

Podobnie w odniesieniu do obowiązków podmiotów stosujących monitoring – ich obowiązki powinny być nie mniejsze niż obowiązki administratorów danych przetwarzających dane osobowe. Inny może być jedynie sposób realizacji niektórych obowiązków, usprawiedliwiony specyfiką systemów monitoringu, których ogólną cechą jest to, że dane identyfikacyjne osób objętych monitoringiem nie są na ogół znane administratorowi systemu, i to, że systemy takie bardzo często pracują w trybie bezobsługowym, to znaczy pracują autonomicznie, bez udziału człowieka, który mógłby np. określony obowiązek informacyjny przekazać słownie. Okoliczności te sprawiają, że takie obowiązki jak np. obowiązek informacyjny – nie mogą być wykonane imiennie. Z tych samych względów nie jest również możliwe uzyskanie zgody od osób objętych monitoringiem – na identycznych zasadach jak w przypadku przetwarzania danych osobowych. Uzasadnione jest zatem przyjęcie zasady, że wejście osoby w wyraźnie oznaczoną strefę objętą systemem monitoringu równoznaczne jest z wyrażeniem przez tę osobę zgody na przetwarzanie jej danych w zakresie wizerunku i wykonywanych czynności, jakie zostaną zarejestrowane przez kamery tego systemu.

4.1. Prawo do informacji

Osoba, której wizerunek został zarejestrowany w systemie monitoringu, powinna mieć prawo do uzyskania informacji dotyczących operacji przetwarzania danych jej dotyczących. Wydaje się jednak uzasadnione, aby w przepisie prawa ustanawiającym to uprawnienie szczegółowo dookreślić możliwe do wykonania przez administratora systemu monitoringu sposoby jego wykonania. Należy rozważyć, w jaki sposób powinien być wykonywany obowiązek informacyjny, np. prawo do wglądu w nagranie, aby wykonując ten obowiązek wobec jednej osoby nie naruszać jednocześnie prawa innej osoby. Może się bowiem zdażyć, że w danym nagraniu, oprócz wizerunku osoby składającej żądanie udostępnienia danych znalazł się również wizerunek innej osoby, która znalazła się w tym samym czasie i miejscu w chwili dokonywania nagrania.

Należy w szczególności rozważyć, czy prawa osoby do wglądu w nagranie systemu monitoringu nie należałoby ograniczyć – do uzasadnionych przypadków, tak by prawo to, mając na uwadze duże nakłady pracy ze strony administratora systemu w celu jego wykonania, nie było nadużywane w sposób nieuzasadniony.

Prawa wglądu w dane dotyczące nagrania, w którym występuje wizerunek składającej wniosek osoby, nie należy z całą pewnością ograniczać wobec osób, które znalazły się w obszarze objętym monitoringiem i w obszarze tym stały się obiektem ataku ze strony innych osób lub w inny sposób uczestniczyły aktywnie w zdarzeniu. Osoby takie powinny uzyskiwać nie tylko prawo wglądu w nagranie, na którym się znalazły, ale również prawo do uzyskania informacji w zakresie czy i jakie działania zostały podjęte przez administratora systemu w związku z zaistniałym zdarzeniem. Równolegle do rozważanego uprawnienia należy rozważyć wprowadzenie dla administratora danych obowiązku ich przekazania do organów ścigania, jeśli w wyniku realizacji nagrania udokumentowane zostało przestępstwo karalne z urzędu.

4.2. Prawo do żądania korekty lub usunięcia danych zarejestrowanych w systemie monitoringu

W odniesieniu do zakresu i sposobu realizacji praw odnoszących się do operacji usuwania danych z obrazu zarejestrowanego przez system monitoringu – należy uwzględnić specyfikę danych rejestrowanych przez kamery systemu monitoringu, a w szczególności ograniczone możliwości poprawiania zarejestrowanych danych. Należy mieć na uwadze, że w przeciwieństwie do danych tekstowych przetwarzanych w bazach danych, w zbiorze stanowiącym nagranie z systemu monitoringu nie ma selektywnego dostępu do określonych danych. Nie jest w związku z tym łatwa operacja usunięcia z nagrania, które przedstawia wizerunki kilkunastu osób, tylko wizerunku jednej osoby lub kilku z nich. Ponadto usunięcie określonego fragmentu z nagrania na wniosek osoby składającej wniosek jest ingerencją w treść nagrania, a to powinno być odpowiednio uzasadnione i udokumentowane. Nie można bowiem wówczas mówić, że kamera zarejestrowała coś inaczej niż to miało miejsce w rzeczywistości. W związku z powyższym w zakresie dotyczącym usuwania danych – w odniesieniu do nagrań z systemu monitoringu należy rozważyć jedynie operację „zamazywania” wizerunku czy też innych części obrazu nagrania, nie zaś operację ich usuwania.

W związku z powyższym sugeruje się rozważenie ograniczenia lub modyfikacji praw do żądania korekty lub usunięcia danych wobec osób objętych monitoringiem – w porównaniu z uprawnieniami w tym zakresie zawartymi w u.o.d.o. Proponuje się między innymi, aby:

1) rozważyć stosowanie operacji „zakrywania" wizerunku skarżącej się osoby, w przypadku gdy osoba składająca żądanie jest uczestnikiem zdarzenia zarejestrowanego przez kamerę, ale nie bierze w nim aktywnego udziału (tzn. tylko wtedy, gdy jest przypadkowym uczestnikiem zdarzenia);
2) odmawiać wykonania operacji kasowania danych, w przypadku gdy zarejestrowany obraz jest przechowywany tylko przez określony okres, np. 2–4 tygodni, i z uwagi na brak incydentów, w czasie jaki obejmowało nagranie, nie jest przewidywane poddawanie go żadnym operacjom przetwarzania, z jego zastosowania wyjątkiem operacji jego przechowywania.

5. Warunki, jakie powinny spełniać podmioty przed wprowadzeniem monitoringu

Regulacja odnosząca się do zasad i warunków stosowania monitoringu powinna nakazywać, aby podmiot, który zamierza wprowadzić monitoring, wykazał zasadność jego stosowania, w tym proporcjonalność stosowania tego środka do celu, jakiemu ma służyć. Wprowadzenie monitoringu powinno być poprzedzone analizą w zakresie możliwości zastosowania innych, mniej ingerujących w prywatność, środków dla osiągnięcia zamierzonego celu. Nadmierne rozpowszechnianie systemów pozyskiwania obrazu w miejscach publicznych i prywatnych nie może prowadzić bowiem do nieuzasadnionego ograniczenia podstawowych praw i wolności obywateli. Należy mieć na uwadze, że obecność monitoringu zmusza obywateli do podporządkowania się i ogranicza ich prywatność.

W związku z powyższym na podmioty, które decydują się na zastosowanie monitoringu, przedmiotowa regulacja powinna nakładać obowiązek stosowania pewnych zasad, które stanowią kompromis między prawem do prywatności i prawem do ochrony swojego mienia, czy też optymalizacji wykonywania obowiązków w zakresie zapewnienia bezpieczeństwa i porządku publicznego. Przykładem takiego kompromisu może być np. zakaz stosowania monitoringu w takich miejscach jak przebieralnie, przymierzalnie czy toalety.

W ramach przedmiotowej regulacji niezbędne jest zatem wskazania tych przypadków i okoliczności, które powinny stanowić bezwzględne granice do stosowania monitoringu.

W przepisach przedmiotowych regulacji poza wymienionymi już przypadkami bezwzględnego zakazu stosowania monitoringu w przymierzalniach i toaletach, odnoszącymi się do ogólnych zasad poszanowania prywatności człowieka, powinny znaleźć się również zakazy odnoszące się do zasad stosowania monitoringu w określonych sektorach. W sektorze hotelarskim np. powinien być wprowadzony zakaz stosowania lub ograniczenia w stosowaniu monitoringu w odniesieniu do łazienek i pokoi hotelowych. Obszarów takich, gdzie pewne ograniczenia dla zachowania równowagi między podstawowymi prawami człowieka a interesem administratora systemu monitoringu jest bardzo dużo. Szczególna uwaga powinna być zwrócona np. na takie miejsca jak szpitale, przychodnie, kawiarnie, wydzielone boksy w tych kawiarniach, restauracje, biura, zakłady pracy, kabiny telefoniczne, kabiny wind i inne.

Ważnym elementem wstępnej analizy dotyczącej stosowania monitoringu jest określenie przez podmiot jego możliwości w zakresie wypełnienia związanych z wprowadzeniem monitoringu zobowiązań. Należy w szczególności przeanalizować możliwości w zakresie:

1) zapewnienia nadzoru eksploatacyjnego nad przyszłą instalacją;
2) zapewnienia bezpieczeństwa fizycznego urządzeń i oprogramowania tworzącego system monitoringu;
3) zapewnienia szkoleń dla personelu zarządzającego systemem monitoringu;
4) zapewnienia narzędzi i środków do bezpiecznego przechowywania nagrań z monitoringu i ich obróbki, np. w celu przygotowania materiału na żądanie policji, prokuratury czy organów sądowniczych.

Przedmiotowa regulacja powinna zezwalać na stosowanie instalacji monitoringu tylko wtedy, jeżeli podmiot ją wprowadzający jest w stanie zapewnić wszystkie wyżej wymienione wymagania w zakresie bezpieczeństwa i nadzoru eksploatacyjnego. Regulacja ta powinna obejmować również, jak wcześniej wskazano, obowiązki w zakresie uzyskania zezwolenia na stosowanie monitoringu oraz zgłoszenia do odpowiednich organów kontroli, jeśli takie będą wymagane.

6. Sposób prowadzenia dokumentacji dla systemu monitoringu

Dokumentacja systemu wideofilmowania, która powinna składać się z 3 części, obejmuje:

1) Projekt systemu monitoringu – zawierający rozmieszczenie poszczególnych kamer oraz podstawowe informacje o ich parametrach, wykaz pomieszczeń lub ich części, w których przetwarzane są dane zarejestrowane przez kamery systemu, wykaz zbiorów zawierających dane zebrane w systemie, wykaz powiązań między nimi oraz wykaz programów i procedur służących do przetwarzania danych.
2) Politykę bezpieczeństwa danych przetwarzanych w systemie monitoringu.
3) Instrukcję zarządzania systemem monitoringu używanym do przetwarzania danych zawartych w zarejestrowanych nagraniach i/lub danych bieżących, tj. danych, które reprezentują obraz obserwowanego przez kamery terenu.

6.1. Projekt systemu monitoringu

Projekt systemu monitoringu powinien zawierać informacje dotyczące ilości, rodzaju i ustawień zainstalowanych w systemie kamer. W przypadku gdy kamery skierowane są na poszczególne punkty operacyjne, np. drzwi wejściowe, okienka kasowe, kasy itp., w projekcie powinno być wyraźnie to wskazane. W przypadku gdy pole widzenia kamery obejmuje miejsca przeznaczone do wykonywania czynności klasyfikowanych jako intymne lub poufne, miejsca te powinny być wyłączone z pola obserwacji kamer – poprzez odpowiednie ich ustawienie lub zastosowanie odpowiednich środków technicznych. W projekcie tym powinny się znaleźć również informacje dotyczące szczegółowych parametrów technicznych kamer, takie jak:

1) rozdzielczość rejestrowanego obrazu,
2) głębia koloru obrazu,
3) format i sposób przekazywania danych,
4) zastosowane metody kompresji,
5) wbudowane w kamery mechanizmy wstępnego przetwarzania danych, typu wykrywanie obiektów żywych w monitorowanym obszarze, identyfikacja kierunku przemieszczanie się obiektu,
6) wbudowane mechanizmy przekazywania informacji o zidentyfikowanym poruszającym się obiekcie – do innych kamer, w zależności od kierunku poruszania się itp.

W odniesieniu do poszczególnych punktów pobierania danych (kamer) należy określić charakter rejestrowanych danych w co najmniej ogólnych kategoriach, takich jak: obraz ogólny monitorowanej przestrzeni, obraz twarzy osób wchodzących do danego

pomieszczenia, obraz źrenicy oka, obraz kształtu dłoni, linii papilarnych itp. Projekt ten powinien w szczególności określać zasoby informacyjne gromadzone w ramach danego systemu monitoringu i przedstawiać powiązania pomiędzy nimi. Powiązanie takie może być realizowane np. poprzez rejestrowanie czasu określonego zdarzenia. Dla systemu, w którym np. w jednym module rejestrowane są w formie nagrań wideo wizerunki osób wchodzących/wychodzących z budynku, oraz w innym wydzielonym funkcjonalnie module – dane identyfikacyjne typu imię, nazwisko, nr dokumentu tożsamości, elementem takiego powiązania może być czas rejestracji tych dwóch zdarzeń.

W projekcie należy wskazać wszelkie automatyczne powiązania, jakie występują pomiędzy danymi rejestrowanymi w systemie monitoringu i danymi w innych systemach, np. niezależnej od danego systemu bazie danych osób poszukiwanych, zaginionych, uprzywilejowanych itp., jak również powiązania, które mogą nastąpić na skutek manualnego wykonania określonych czynności porównawczych.

Jeżeli np. w instytucji zainstalowany jest system monitoringu składający się z takich modułów, jak:

1) system monitoringu wizyjnego,
2) system zawierający wizerunki osób, którym wstęp na teren instytucji został zabroniony/dozwolony, oraz
3) system analizy danych rejestrowanych w systemie monitoringu, porównujący wizerunki osób wchodzących do instytucji z wizerunkami zawartymi w bazie danych osób, którym wstęp na teren instytucji został zabroniony/dozwolony, w celu otwarcia/zamknięcia dostępu do określonego miejsca lub zaalarmowania służb ochrony o zaistniałym zdarzeniu,

to należy uznać, że pomiędzy wymienionymi systemami – modułami systemu monitoringu – następuje przepływ danych.

Rozważanie aspektów przepływu danych nie jest możliwe bez szczegółowej wiedzy na temat właściwości poszczególnych systemów, w tym struktur przetwarzanych informacji. Nie bez znaczenia w takiej sytuacji będzie również przyjęta klasyfikacja wszystkich przetwarzanych przez danego administratora zestawów danych i stosowanych narzędzi programowych. Może się bowiem okazać, że jeden administrator zakwalifikuje dane rozwiązanie jako jeden zintegrowany system, w którym przetwarzane są zarówno dane dotyczące bieżącego strumienia danych wizualnych przekazywanych przez kamery, jak również dane dotyczące osób niepożądanych. Inny zaś administrator – w podobnej sytuacji –

uzna, że są to dwa odrębne systemy. Niezależnie od powyższego w dokumentacji projektu systemu przetwarzania, jaką zobowiązany jest posiadać administrator danych, powinny być zagadnienia te szczegółowo wyjaśnione.

Projekt powinien zawierać również informacje o zastosowanych środkach technicznych służących do zarządzania systemem, monitorowania jego pracy oraz środkach służących do wykonywania kopii z wskazanych odcinków zarejestrowanych nagrań.

6.2. Polityka bezpieczeństwa danych przetwarzanych w systemie monitoringu

Na politykę bezpieczeństwa danych przetwarzanych w systemie monitoringu powinny składać się w szczególności:

1) opis zabezpieczenia infrastruktury systemu monitoringu przed nieautoryzowaną ingerencją w ustawienia systemu, o których mowa w dokumentacji projektowej;
2) opis zabezpieczeń przed nieuprawnionymi działaniami, które mogą spowodować nieuprawniony dostęp lub zakłócanie obrazów przekazywanych przez kamery;
3) opis zabezpieczeń przed nieuprawnionym dostępem, przejęciem lub zniszczeniem nagrań zarejestrowanych przez system;
4) opis środków i procedur zapewniających rozliczalność wszelkich działań związanych z zarządzaniem systemem monitoringu, w tym udostępnianiem wglądu w nagrania upoważnionym osobom oraz wykonywaniem i udostępnianiem kopii nagrań wideo lub audiowideo zawierających zarejestrowane przez poszczególne kamery zdarzenia;
5) opis środków i procedur dotyczących przekazywania kopii zarejestrowanych przez poszczególne kamery nagrań uprawnionym podmiotom zewnętrznym, w tym agencjom ochrony, policji, prokuraturze, sądom i innym podmiotom oraz sposobu dokumentowania tych czynności;
6) procedury dotyczące wykonywania i przekazywania kopii nagrań zawierających dowody zaistnienia określonych zdarzeń;
7) informacje o zastosowanych w systemie wideonadzoru mechanizmach automatycznej analizy obrazu, takich jak identyfikacja określonych zdarzeń – typu pojawienie się w nadzorowanej przestrzeni człowieka lub innego zaliczanego do określonej kategorii obiektu, jak np. pies, kot, samochód itp.;

8) informacje o zastosowanych w systemie monitoringu mechanizmach zaawansowanej analizy obrazu, umożliwiających rozpoznawanie osób i/lub ich intencji w zakresie określonego typu działań, np. działanie maskujące (skradanie się), przemoc fizyczna wobec innych osób itp.

Przewidziane w polityce bezpieczeństwa środki mają służyć zapewnieniu poufności danych przetwarzanych w systemie monitoringu. Dostęp do rejestrowanych przez kamery systemu obrazów, jak również zarejestrowanych nagrań powinien być możliwy tylko dla upoważnionych przez administratora systemu osób. Środki w zakresie bezpieczeństwa systemu monitoringu powinny zabezpieczać przed możliwością przejęcia rejestrowanego przez kamery obrazu na skutek np. korzystania przez inne podmioty z tej samej infrastruktury, np. kabli operatora telewizji przewodowej, lub innego podmiotu.

6.3. Instrukcja zarządzania systemem monitoringu

Instrukcja zarządzania systemem monitoringu powinna zawierać opis czynności związanych z utrzymaniem systemu monitoringu oraz procedury dotyczące zarządzania systemem. W szczególności instrukcja powinna zawierać:

1) wykaz operatorów systemu i osób administrujących systemem,
2) procedury nadawania uprawnień dostępu do systemu,
3) procedury dotyczące kopiowania i przekazywania nagrań z systemu monitoringu oraz procedury sporządzania dokumentacji tych czynności i jej przechowywania.

Ze względu na uwarunkowania organizacyjne, które mogą być różne u każdego z podmiotów, w ramach tworzonej regulacji powinny zostać wskazane instrukcje/plan zarządzania systemem monitoringu, mając na względzie zapewnienie bezpieczeństwa przekazywanych danych oraz zakres i rodzaj działalności wykonywanej przez rejestrującego system monitoringu.

7. Obowiązki administratora systemu monitoringu wobec GIODO i innych organów kontroli

Zgodnie z obowiązującymi przepisami dotyczącymi ochrony danych osobowych stosowanie monitoringu może pod pewnymi warunkami prowadzić do powstania zbioru danych osobowych, który podlega obowiązkowi zgłoszenia do rejestracji GIODO.

Stosownie bowiem do przepisu art. 40 ustawy o ochronie danych osobowych „administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu

Inspektorowi", chyba że zachodzi jedna z przesłanek zwalniających go z tego obowiązku, określonych w art. 43 ust. 1 tej ustawy.

Przez zbiór danych, zgodnie z definicją zawartą w art. 7 pkt 1 u.o.d.o., rozumie się „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie".

Cechą wyróżniającą zbiór danych osobowych od innego zestawu danych jest zatem struktura, czyli takie uporządkowanie, które daje możliwość wyszukania konkretnych danych według określonego kryterium. Aby jakikolwiek zestaw danych zaklasyfikować jako zbiór danych w rozumieniu przepisów ustawy, wystarczające jest kryterium umożliwiające odnalezienie danych osobowych w zestawie. Możliwość wyszukania według jakiegokolwiek kryterium osobowego (np. imię, nazwisko, data urodzenia, PESEL) lub nieosobowego (np. data, kolejność zamieszczenia danych w zbiorze) przesądza o uporządkowanym charakterze zestawu i tym samym umożliwia zakwalifikowanie go jako zbioru danych w rozumieniu art. 7 pkt 1 ustawy.

Zbiór danych osobowych może powstać m.in. w związku ze stosowaniem systemów monitoringu. Na potrzeby określenia, w jakich przypadkach może dojść do powstania zbioru danych osobowych w związku ze stosowaniem monitoringu, należy wyróżnić następujące sytuacje:

1) monitoring w czasie rzeczywistym bez dokonywania zapisu – nie dochodzi do powstania jakiegokolwiek zestawu danych osobowych, a tym samym brak potrzeby rozważania tego przypadku na gruncie art. 7 ust 1 u.o.d.o.;

2) dokonanie zapisu obrazu lub dźwięku w wyniku monitoringu – powstaje zestaw danych osobowych, który przy spełnieniu określonych warunków może być zbiorem danych w rozumieniu art. 7 pkt 1 u.o.d.o.;

3) dokonanie zapisu obrazu lub dźwięku w wyniku monitoringu – powstaje zestaw danych osobowych, który nie jest zbiorem danych w rozumieniu art. 7 pkt 1 u.o.d.o.

W przypadku gdy obraz lub dźwięk w wyniku zastosowania monitoringu zostanie utrwalony w postaci zapisu, a tym samym dojdzie do powstania zestawu danych osobowych, rozważenia wymaga kwestia, czy zestaw ten spełnia warunki definicji zbioru danych osobowych z art. 7 ust 1 u.o.d.o., tj. czy zestaw posiada określoną strukturę (uporządkowanie)

oraz czy istnieje możliwość dotarcia do danych konkretnej osoby (obrazu twarzy, sylwetki, zapisanej wypowiedzi itp.) za pomocą jakiegokolwiek kryterium.

Należy uznać, że każde nagranie dokonane w wyniku monitoringu posiada strukturę (uporządkowanie) – z uwagi na fakt, iż dotyczy sekwencji zdarzeń następujących w określonym czasie, zarejestrowanych przez urządzenie służące do monitoringu. Jednakże nie w każdym przypadku będzie możliwe dotarcie do danych konkretnej osoby, bez konieczności manualnego przeglądania całego nagrania lub jego obszernego fragmentu.

Przykłady sytuacji, gdy nagranie z monitoringu może być uznane za zbiór danych osobowych:

1) zestaw danych został poddany opracowaniu (skatalogowaniu), w wyniku którego utworzono indeksy umożliwiające dotarcie do zapisu danych konkretnej osoby;
2) system informatyczny stosowany w związku z monitoringiem wyposażony został w mechanizmy umożliwiające automatyczne wyszukanie w zarejestrowanych nagraniach danych dotyczących konkretnej osoby (np. mechanizm rozpoznawania kształtu twarzy, sylwetki, głosu);
3) dotarcie do danych konkretnej osoby jest możliwe na podstawie innego zbioru danych osobowych, w którym rejestrowane są w sposób tradycyjny zdarzenia z udziałem konkretnej osoby, zarejestrowane równocześnie w zapisie z monitoringu (np. w kasynach gry, gdzie monitoring stosowany przy wejściu do budynku połączony jest z tradycyjną księgą wejść/wyjść).

W związku z powyższym w ramach regulacji monitoringu należałoby sprecyzować, kiedy nagranie z monitoringu tworzy zbiór danych osobowych, ewentualnie rozważyć koncepcję, w której zdefiniowanie tej kwestii nie byłoby niezbędne bez szkody dla ochrony danych osób, które mogą być objęte monitoringiem. Uznanie zapisu z monitoringu za zbiór danych osobowych pociąga za sobą bowiem wynikający z ustawy o ochronie danych osobowych obowiązek zgłoszenia przez administratora danych tego zbioru do rejestracji GIODO. Zbiory danych osobowych tworzone w związku ze stosowaniem monitoringu, tak jak inne zbiory danych osobowych, co do zasady podlegają bowiem obowiązkowi rejestracji. Biorąc to pod uwagę, zauważyć jednakże należy, iż wobec tego że większość utworzonych w wyniku stosowania monitoringu zapisów nie spełnia warunków definicji zbioru danych osobowych, nie podlegają one zgłoszeniu do rejestracji, nie ma więc możliwości sprawowania nadzoru nad przetwarzanymi w ten sposób danymi. Rozwiązaniem tej kwestii mogłoby być

zobowiązanie administratorów danych, aby w zgłoszeniu systemu monitorowania skierowanym do GIODO zawarli część informacji przewidzianych w art. 41 ust. 1 u.o.d.o., w szczególności informacje dotyczące administratora danych, podstawy prawnej i celu przetwarzania, ale także np. informacje na temat sposobu udostępniania danych oraz określenie kategorii odbiorców danych. Należałoby wówczas do katalogu zwolnień z obowiązku rejestracji zbiorów danych zawartego w art. 43 ust. 1 u.o.d.o. dopisać przepis zawierający stosowne zwolnienie dotyczące danych przetwarzanych w zbiorach tworzonych na skutek rejestracji obrazu w systemie monitoringu wizyjnego.

Zakres informacji zawartych w zgłoszeniu skierowanym do GIODO oraz sposób postępowania powinny być skorelowane z ewentualnymi obowiązkami innych podmiotów (organów samorządu terytorialnego – np. gmin) w zakresie sprawowania nadzoru nad przypadkami stosowania monitoringu na terenie należącym do ich właściwości miejscowej. W związku z zadaniami oraz umiejscowieniem GIODO w systemie organów publicznych, należałoby także rozważyć zasadność stworzenia takich unormowań, by osoby, które są lub mogą być objęte monitoringiem, mogły z łatwością uzyskać informacje o stosowaniu tej formy przetwarzania danych osobowych przez konkretne podmioty oraz uzyskać informacje, o których mowa w art. 41 u.o.d.o. Można zatem rozważyć utworzenie jawnego i ogólnopolskiego rejestru, w którym te informacje by się znalazły.

Kolejną kwestią, którą należałoby uregulować inaczej niż w dotychczas obowiązujących przepisach, jest kwestia przetwarzania danych szczególnie chronionych.

Zgodnie bowiem z art. 46 ust. 2 u.o.d.o. administrator tzw. danych szczególnie chronionych (wskazanych w art. 27 ust. 1 u.o.d.o.) może rozpocząć ich przetwarzanie dopiero po zarejestrowaniu zbioru, chyba że ustawa zwalnia go z obowiązku zgłoszenia zbioru do rejestracji. Oznacza to, że warunkiem koniecznym do zgodnego z prawem przetwarzania danych szczególnie chronionych jest rejestrowanie przez GIODO zbioru przed rozpoczęciem przetwarzania tych danych.

W związku z powyższym podkreślić należy, iż co do zasady celem monitoringu nie jest gromadzenie danych szczególnie chronionych, jednakże dokonane w wyniku stosowania monitoringu zapisy mogą wskazywać na dane szczególnie chronione osób podlegających takiemu monitoringowi. Na przykład niektóre cechy danej osoby, w szczególności jej wyglądu, mogą być źródłem informacji na temat jej stanu zdrowia lub przynależności wyznaniowej. W przypadku przyjęcia koncepcji zgłaszania do GIODO, w ramach specjalnej procedury, informacji o stosowaniu monitoringu, w wyniku którego powstają zapisy

niestanowiące zbioru danych osobowych, ale mogące zawierać lub zawierające, w związku ze swą specyfiką, dane szczególnie chronione, należałoby rozważyć potrzebę szczególnego sposobu postępowania organu ochrony danych osobowych w takich przypadkach – biorąc pod uwagę założenie rezygnacji z kontroli wstępnej zbiorów danych pochodzących z monitoringu.

8. Ogólne zasady stosowania monitoringu

8.1. Szczególne kategorie danych

System monitoringu nie powinien mieć na celu nagrywania (np. poprzez zbliżenie lub ukierunkowanie kamery) lub innego rodzaju przetwarzania (np. indeksowanie, profilowanie wskazano) obrazów ujawniających tzw. szczególne kategorie danych – o pochodzeniu rasowym lub etnicznym, poglądach politycznych, religijnych lub filozoficznych, przynależności do związków zawodowych, zdrowiu i życiu seksualnym. Nie należy również monitorować obszarów, w których istnieje zwiększone prawdopodobieństwo nagrania obrazów ujawniających szczególne kategorie danych, nawet jeśli nie ma się zamiaru zbierać tego typu danych.

Gdy podmiot monitorujący zamierza odejść od wyżej wymienionych zasad, musi przeprowadzić ocenę swego wpływu na ochronę danych i prywatności, a monitoring może być prowadzony jedynie po zastosowaniu dodatkowych zabezpieczeń. W przypadku np. monitoringu mającego na celu zapewnienie bezpieczeństwa podczas demonstracji, można zastosować m.in. następujące dodatkowe zabezpieczenia:

1) Nadzór nad wszelkiego rodzaju pokojowymi protestami może być sprawowany jedynie w wypadku wykazania takiej konieczności ze względów bezpieczeństwa;
2) Kamery nie powinny być skierowane na twarze obywateli i nie należy prowadzić prób identyfikacji, o ile nie dojdzie do bezpośredniego zagrożenia bezpieczeństwa publicznego lub agresywnych zachowań przestępczych (np. wandalizmu lub napaści);
3) W przypadku niewystąpienia incydentów dotyczących bezpieczeństwa należy usunąć nagrania z pokojowych demonstracji w ciągu określonego czasu, np. 2 godzin od zakończenia protestu (lub rozważyć prowadzenie monitoringu jedynie na bieżąco);
4) Odpowiednie przeszkolenie operatorów systemu wideonadzoru w celu zapewnienia, że prywatność i inne prawa podstawowe uczestników

zarejestrowanych przez kamery, a w szczególności ich prawo do zgromadzeń, nie są w nieproporcjonalny sposób naruszane.

8.2. Obszary objęte szczególną ochroną prywatności

Obszary objęte szczególną ochroną prywatności nie powinny być monitorowane. Zwykle są to: biura (w tym pokoje biurowe dzielone przez dwie lub więcej osób i duże otwarte biura z boksami), obszary wypoczynku (stołówki, kafejki, bary, aneksy kuchenne, jadalnie, salony, poczekalnie itp.), toalety, prysznice i szatnie. W przypadku gdy podmiot prowadzący monitoring zamierza odejść od wyżej wymienionych zasad, musi przeprowadzić ocenę wpływu systemu monitorowania na ochronę danych i prywatności, i zgłosić projekt wprowadzenia takiego systemu do kontroli wstępnej przez GIODO.

8.3. Korelacja pomiędzy systemami monitoringu. Zintegrowane systemy monitoringu

Korelacja systemu monitoringu danego podmiotu z podobnym systemem innego podmiotu lub strony trzeciej powinna być poprzedzona oceną ich wpływu na ochronę danych i prywatności. Ocena taka powinna być również wymagana w przypadku, gdy jeden podmiot prowadzi kilka oddzielnych systemów monitoringu (np. w różnych miastach lub w tym samym miejscu, ale wykorzystywanych do różnych celów) i chce je ze sobą skorelować. Warunkiem zezwalającym na wykonanie powyższego rodzaju korelacji powinno być poprzedzenie jej odpowiednim zgłoszeniem do kontroli wstępnej.

8.4. Nagrywanie dźwięku w systemie monitoringu

Ze względu na swój inwazyjny charakter nagrywanie dźwięku, co do zasady, w systemach monitoringu nie powinno być stosowane. Wyjątek mogą stanowić przypadki wykorzystania nagrywania dźwięków jako zapasowych systemów kontroli dostępu poza godzinami pracy biura (jako wideofonu pozwalającego skontaktować się na odległość z ochroną w celu uzyskania dostępu).

Jeśli system monitoringu wykorzystywany jest również jako zapasowy system kontroli dostępu, należy wyraźnie o tym poinformować, a kamery mogą przekazywać bądź nagrywać dźwięk jedynie po uaktywnienie funkcji przekazywania, nagrywania dźwięku przez daną osobę, która stara się uzyskać dostęp do systemu lub po określonej liczbie nieudanych prób uzyskania dostępu.

Inne proponowane wyjątki muszą być odpowiednio uzasadnione oraz podlegać powinny ocenie wpływu na ochronę danych i prywatności. Ich stosowanie może być dozwolony tylko po zgłoszeniu do wstępnej kontroli.

8.5. Szkolenia w zakresie ochrony danych

Wszyscy pracownicy posiadający prawo dostępu do systemu, w tym wykonujący codzienne działania w zakresie wideonadzoru lub sprawujący nadzór techniczny nad systemem monitoringu, powinni przejść szkolenia w zakresie ochrony danych i zapoznać się z przepisami o ochronie danych osobowych i wytycznymi w zakresie nadzorowania systemu, w tym zabezpieczania, kopiowania i udostępniania danych, w takim stopniu, w jakim są one potrzebne dla wykonywanych przez nich zadań. Podczas szkolenia należy zwrócić szczególną uwagę na unikanie ujawniania nagrań z wideonadzoru komukolwiek poza osobami upoważnionymi.

Szkolenia powinny odbywać się po zainstalowaniu nowego systemu lub wprowadzeniu znaczących zmian w już istniejącym, po objęciu obowiązków przez nowego pracownika, a także okresowo, w regularnych odstępach czasu.

8.6. Zobowiązania w zakresie poufności

Wszyscy pracownicy posiadający prawo dostępu do systemu, w tym podwykonawcy wykonujący codzienne działania w zakresie wideonadzoru lub sprawujący nadzór techniczny nad systemem, muszą podpisać zobowiązania do zachowania poufności, w których oświadczą, że nie będą przekazywać, pokazywać lub w inny sposób ujawniać treści nagrań z wideonadzoru – nikomu, kto nie ma prawa dostępu (czyli zwykle nikomu poza ochroną danej instytucji).

9. Warunki i szczegółowe zasady stosowania inteligentnych systemów automatycznego rozpoznawania określonych zdarzeń

Wprowadzenie „supernowoczesnych inteligentnych narzędzi monitoringu” powinno być dopuszczalne jedynie po przeprowadzeniu oceny wpływu ich zastosowania na ochronę danych i prywatności oraz po przeprowadzeniu kontroli wstępnej. GIODO po indywidualnej analizie każdego przypadku powinien oceniać dopuszczalność zastosowania danej techniki i w razie konieczności nakazać stosowanie dodatkowych zabezpieczeń.

Do kategorii systemów, których zastosowanie wymaga szczególnej analizy, należą systemy, gdzie zastosowano jedno lub kilka z niżej wymienionych narzędzi, lub narzędzia o zbliżonych funkcjonalnościach:

1) połączenie systemu monitoringu wizualnego z danymi biometrycznymi (np. odciskami palców stosowanymi w kontroli dostępu) lub innymi bazami danych (np. bazą danych podejrzanych – wykorzystywaną do rozpoznawania twarzy);
2) indeksowanie danych na obrazach, pozwalające na zautomatyzowane wyszukiwanie i tzw. alerty (np. w celu śledzenia osób);
3) systemy rozpoznawania twarzy bądź chodu;
4) wszelkiego rodzaju nadzór dynamiczno-prewencyjny (np. zastosowanie oprogramowania do automatycznej analizy zachowań – w celu stworzenia zautomatyzowanych alertów opartych na ustalonych definicjach podejrzanego zachowania, ruchów, stroju i gestów);
5) sieć kamer z oprogramowaniem umożliwiającym śledzenie poruszających się osób lub przedmiotów na całym monitorowanym obszarze;
6) systemy alarmowe audio (w których alarm wywoływany jest zmianami w strukturze dźwięków, np. nagłym krzykiem);
7) kamery na podczerwień i tym podobne, urządzenia termowizyjne i inne kamery szczególnego zastosowania, które mogą nagrywać obraz w ciemnościach lub przy niewielkiej ilości światła oraz „widzieć" przez ściany i ubrania;
8) kamery szczególnego zastosowania o zwiększonych możliwościach powiększenia optycznego i cyfrowego.

10. Retencja danych w systemach monitoringu

Dla każdego systemu monitoringu powinien być określony okres przechowywania danych, po którym zarejestrowane dane powinny być usuwane. Okres ten nie powinien być dłuższy niż 7 do 30 dni[8]; w przypadkach szczególnie uzasadnionych może on zostać wydłużony. Dane zarejestrowane w systemie monitoringu mogą być przechowywane przez okres dłuższy niż został ustalony jedynie w przypadkach, kiedy jest to niezbędne do wykonania kopii wymaganych dla celów dowodowych w postępowaniach prowadzonych przez sąd lub policję.

[8] Regulacje włoskie dopuszczają maksymalnie 7-dniowy okres przechowywania danych z systemu monitoringu przez władze miejskie, jeśli jego celem było zapewnienie bezpieczeństwa publicznego. Przedłużenie tego okresu wymaga złożenia odpowiedniego wniosku do włoskiego organu ochrony danych.