MATERIAŁY DYDAKTYCZNE 42

Monitoring wizyjny – część III

Aspekty prawne

KATOWICE 2017

podinsp. Jacek Wróbel
nadkom. w st. spocz. Piotr Podsiedlik
Zakład Prewencji i Ruchu Drogowego

Monitoring wizyjny – cz. III

Aspekty prawne

Katowice 2017

Redakcja:
mł. insp. Dariusz Walczak

Redakcja techniczna i korekta:
Paweł Mięsiak

Spis treści

Wstęp

Przypadło nam żyć i pracować w czasach ogromnego i bardzo szybkiego rozwoju techniki i informatyki, które we wszystkich dziedzinach życia służą człowiekowi. Dynamiczny rozwój cyfryzacji świata niesie za sobą jednak wiele zagrożeń, związanych z wykorzystaniem dobrodziejstw współczesności do celów własnych i niekoniecznie zgodnych z prawem. W związku z tym szeroko pojęte instytucje i organizacje powołane do walki z przestępczością nie mogą pozostawać w tyle w tym swoistym wyścigu cyfrowych zbrojeń.

Powyższa publikacja dotyka tylko maleńkiego fragmentu jednej z dziedzin walki z przestępczością za pomocą techniki informatycznej, a mianowicie wykorzystania **monitoringu wizyjnego**.

W tej 3-częściowej pracy przybliżone zostały podstawowe aspekty wykorzystania przez organy ścigania bardzo skutecznego środka do walki z przestępczością jakim jest właśnie monitoring wizyjny. Każda z części publikacji odnosi się do innej problematyki, jednakże są ze sobą powiązane tematyką wykorzystania monitoringu wizyjnego w pracy współczesnej Policji.

Publikacja w swoim zamyśle nie ma stanowić kompendium wiedzy na temat tej dynamicznie rozwijającej się problematyki. Lektura skryptu daje jednak solidny fundament do przyswojenia wiedzy w zakresie praktycznego wykorzystania monitoringu wizyjnego w codziennej służbie Policji, ale i innych służb. Skrypt powinien być szeroko wykorzystywany zarówno w procesie dydaktycznym szkoleń podstawowych, jak i kursów specjalistycznych.

Rozdział 1.
Typologia regulacji prawnych

Nie budzi zdziwienia fakt, iż systemy monitoringu wizyjnego obecnie są coraz częściej wykorzystywane, a ich fundamentalne zadanie, którym jest zapewnienie bezpieczeństwa powoduje powstawanie szeregu pytań dotyczących właśnie wykorzystania owego środka. Spore zainteresowanie budzi aspekt prawny wykorzystania monitoringu wizyjnego, szczególnie określenia miejsc, przestrzeni, która może być poddana nadzorowi z wykorzystaniem kamer, a w szczególności możliwości ingerencji w prywatne życie osób znajdujących się na obszarze objętym ich zasięgiem. Istotną kwestią pozostaje również ustalenie jakim podmiotom oraz w jakim zakresie przysługuje kompetencja do wykorzystania tego środka i pochodzących z niego nagrań. W zakresie uregulowań wykorzystania systemów monitoringu wizyjnego można wyróżnić trzy stanowiska ustawodawców[1]:

1) brak regulacji,
2) regulacje rozproszone w różnych aktach prawnych,
3) oddzielny akt regulujący wykorzystanie systemów CCTV (czasem obok innych ustaw, które mogą obejmować tę problematykę).

	Brak regulacji	**Regulacje rozproszone**	**Oddzielny akt regulujący wykorzystanie systemów CCTV**
Państwa	Stany Zjednoczone	Holandia, Kanada, Niemcy, Norwegia, Polska, Szwajcaria, Węgry, Wielka Brytania	Belgia, Dania, Francja, Hiszpania, Szwecja

Tab. 1. Umiejscowienie regulacji dotyczących używania systemów CCTV[2].

[1] P. Waszkiewicz, *Wielki Brat. Rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne,* Warszawa 2011, s. 67.

[2] Tamże.

Najczęstszym przypadkiem jest brak regulacji obejmujących całościowo funkcjonowanie systemów monitoringu wizyjnego w jednym akcie prawnym. Bywa tak, że rozproszone regulacje prawne są stosunkowo dokładne. Najczęstszym aktem, w którym można znaleźć tego typu regulacje są ustawy dotyczące ochrony danych osobowych – w większości z wymienionych krajów: Holandii, Kanadzie, Niemczech, Norwegii, Szwajcarii, Wielkiej Brytanii i na Węgrzech – to właśnie te ustawy obejmują również wykorzystanie systemów monitoringu wizyjnego. Dane monitoringu wizyjnego są wymienione obok innych danych albo definicja danych osobowych obejmuje prawo do wizerunku, a powody jego ograniczenia są ściśle określone.

Rozdział 2.
Akty prawne w ujęciu prawnoporównawczym

W granicach dwóch państw o ustroju federalnym – Niemiec i Szwajcarii – istnieją różnice w regulacjach prawnych tego przedmiotu. W **Niemczech** na poziomie federalnym wykorzystanie systemów CCTV reguluje ustawa o ochronie danych osobowych z 14 stycznia 2003 r. Jej art. 6 b stanowi, że w miejscach publicznych wykorzystanie monitoringu wizyjnego jest możliwe jedynie w przypadkach wypełniania zadań przez upoważnione do tego organy publiczne, w celu zagwarantowania miru domowego lub realizacji uprawnionych interesów, przy czym musi to być interes proporcjonalny do naruszenia prawa do prywatności. Teren objęty działaniem systemów telewizji dozorowanej musi być wyraźnie oznaczony wraz ze wskazaniem administratora systemu. Prawo do korzystania z inwigilacji za pomocą kamer (również ukrytych) przysługuje Federalnej Policji Kryminalnej. Z kolei zapewnienie bezpieczeństwa na terenie krajów związkowych podlega prawu policyjnemu, które każdy z 16 landów może regulować w odmienny sposób. Np. w Nadrenii-Westfalii art. 15 ustawy *o Policji* z 8 lipca 2003 r. stanowi, że w celu zapobiegania przestępstwom w miejscach publicznych, w których często do nich dochodzi, można zainstalować kamery, a o ich pracy trzeba poinformować w wyraźny sposób. Nagrania, o ile nie są niezbędne do prowadzonych postępowań, należy wykasować po upływie 14 dni[3].

W **Szwajcarii** brak jest specjalnej ustawy regulującej korzystanie z systemów CCTV. Przyjęte w tym kraju rozwiązania sytuują się pomiędzy regulacjami niemieckimi a brytyjskimi. W szwajcarskiej ustawie federalnej o ochronie danych osobowych z 19 czerwca 1992 r. nie pojawiają się przepisy odnoszące się bezpośrednio do monitoringu. Mieszkańcy w drodze referendów decydują, czy na terenie ich społeczności będzie możliwy nadzór przestrzeni publicznej za pomocą kamer. Przyjmowane

[3] Tamże, s. 68.

na poziomie regionalnym regulacje są w miarę podobne – określają miejsca, w których można instalować kamery, typy oznaczeń oraz czas przechowywania danych[4].

Najdokładniejsze i zarazem zebrane w jednym akcie są regulacje **hiszpańskie**. Ustawa regulująca używanie kamer wideo w miejscach publicznych przez siły i organy bezpieczeństwa została uchwalona 4 sierpnia 1997 r., czyli kiedy gwałtowny rozwój systemów CCTV w innych krajach dopiero się rozpoczynał. Zakres ustawy obejmuje nagrywanie obrazów i dźwięków za pomocą systemów stacjonarnych i mobilnych w otwartych, jak i zamkniętych miejscach publicznych, czyli również budynkach, do których dostęp jest wolny. Art. 6 wprowadza zakaz obejmowania nadzorem kamer wnętrza mieszkań i klatek schodowych, z wyjątkiem sytuacji, w których zostaje wydany nakaz sądowy. Kolejne wyłączenie możliwości nagrywania obejmuje miejsca publiczne, jeżeli w rażący sposób naruszano by prywatność osób tam się znajdujących. Jeżeli przez przypadek dojdzie do nagrania tego typu, należy je natychmiast skasować. Cele wykorzystania kamer zostały zidentyfikowane, jako: zwiększenie bezpieczeństwa, podwyższenie komfortu korzystania z przestrzeni publicznej, prewencja popełniania przestępstw i wykroczeń, przy czym ograniczenia praw i wolności, które wymagają poszanowania, muszą być zminimalizowane, adekwatne i proporcjonalne. Art. 3 określa zasady podejmowania decyzji o instalacji systemu CCTV. Wymaga ona w każdym przypadku wniosku samorządu terytorialnego, po uzyskaniu wcześniejszej, pozytywnej opinii lokalnej Komisji Sprawiedliwości pod przewodnictwem prezesa sądu okręgowego. Ustawa wprowadza obowiązek niszczenia nagrań po upływie miesiąca, chyba, że są niezbędne do prowadzonego postępowania, wprowadza też możliwość oglądania nagrań przez osoby, które zostaną zarejestrowane. Ustawa w sposób kompleksowy reguluje wykorzystanie systemów CCTV – od określenia warunków jego montażu – przez określenie granic ingerencji w prywatność obywateli – aż do zagwarantowania im prawa do informacji i kontroli[5].

[4] Tamże, s. 68-69.

[5] Tamże, s. 69-70.

Francja jest kolejnym przykładem państwa, gdzie oprócz standardowych regulacji obowiązuje odrębna ustawa. Jej postanowienia są zbliżone do hiszpańskich. Określa ona miejsca jako otwarte dla publiczności, czyli poza otwartą przestrzenią publiczną, także restauracje, apteki oraz sklepy. Wybór miejsca, w którym zostaną zainstalowane kamery, jest ograniczony do takich, gdzie występuje szczególne ryzyko napaści lub kradzieży, a montaż wymaga zgody prefekta policji, po uprzednim zasięgnięciu opinii Rady Departamentu pod przewodnictwem sędziego. Statuuje też obowiązek informowania osób, które wchodzą na teren objęty pracą kamer – dotyczy to także personelu pracującego w takich miejscach[6].

Specjalna ustawa dotycząca funkcjonowania monitoringu w przestrzeni publicznej w **Szwecji** uchwalona została niewiele później niż regulacje hiszpańska i francuska. Ustawa o telewizji przemysłowej w przestrzeni publicznej weszła w życie 1 lipca 1998 r. Podobnie do innych regulacji wykorzystanie systemów CCTV zawiera obowiązek uzyskania zezwolenia na instalację kamer, którego w Szwecji udziela zarząd powiatu, prowadzący też rejestr systemów i nadzór nad przestrzeganiem warunków ich obsługi. Zostały określone warunki instalacji systemów, jak i przechowania nagrań. Wprowadzono też obowiązek widocznego informowania o prowadzeniu monitoringu[7].

W **Belgii** zgodnie z ustawą z dnia 21 marca 2007 r., która reguluje instalowanie i użytkowanie kamer monitorujących, przyjęte zostały zasady wymagające od podmiotu, który zamierza wprowadzić monitoring, uzyskania pozytywnej opinii rady gminy, w której znajduje się monitorowane miejsce i notyfikację tego systemu do Komisji Ochrony Życia Prywatnego. W związku z tym, podmiot, który ma zamiar wprowadzić stosowanie monitoringu, jest zobowiązany 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

[6] Tamże, s. 70.

[7] Tamże.

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[8].

We **Włoszech** zasady stosowania monitoringu uregulowane są w ustawie dotyczącej przetwarzania danych osobowych. Osoba, która zamierza uruchomić system monitoringu zgłasza ów system do Urzędu Rzecznika Ochrony Danych Osobowych. Zgłoszenie to 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 inwencji czy nastroju[9].

Wielka Brytania jest krajem o największej bezwzględnej liczbie kamer i największej ich liczbie w przeliczeniu na liczbę mieszkańców. Do 2000 roku brak było nie tylko aktu prawnego obejmującego w sposób kompleksowy korzystanie z systemów CCTV, ale kwestia monitoringu wizyjnego nie została uregulowana w ramach żadnego z aktów prawnych związanych z szeroko rozumianym bezpieczeństwem. Ustawa o ochronie danych osobowych stanowiła podstawę do wydania swego rodzaju wykładni przepisów regulujących korzystanie z systemów CCTV. *CCTV Code of Practice* – Wytyczne postępowania dotyczące systemów CCTV lub Kodeks praktyki CCTV – jest to poradnik wydany przez brytyjskiego odpowiednika Inspektora Ochrony Danych Osobowych w 2000 roku. Zawiera wytyczne dla administratorów systemów CCTV dotyczące wykorzystania, eksploatacji, nadzoru nad systemami oraz gwarancje prawa do prywatności dla osób objętych inwigilacją za ich pomocą. CCTV COP zwraca uwagę na racjonalne przesłanki, którymi należy kierować się na etapie rozważania wykorzystania systemu CCTV – jeżeli oczekiwane efekty, np. poprawa

[8] GIODO, *Wymagania w zakresie regulacji monitoringu*, s. 14, http://www.atosochrona.pl/wgrane_pliki/monitoring.pdf, 26.01.2015.

[9] Tamże.

bezpieczeństwa, można osiągnąć w inny sposób, który nie będzie ingerował w sferę praw i wolności obywatelskich, wówczas należy go wybrać. Obszar, który będzie objęty zasięgiem pracy kamer musi zostać tak wybrany, aby sprostać stawianym zadaniom, a zarazem nie może naruszać innych obszarów, m.in. stanowiących własność osób fizycznych. Rozróżniane są cztery kategorie celów systemów CCTV:

1) monitorowanie – np. nadzór sprawowany nad ruchem drogowym, do realizacji którego nie potrzeba dokładnych zbliżeń twarzy, numerów rejestracyjnych;
2) wykrywanie – potwierdzanie czy dana osoba znajduje się w obszarze pracy kamer;
3) rozpoznawanie – stwierdzenie, że dana osoba jest znana (poszukiwana lub nie);
4) identyfikacja – zagwarantowanie zapisu o jakości pozwalającej w trakcie procesu potwierdzić czyjąś tożsamość.

Wymagane jest jasne oznaczenie terenu, który kamery obejmują swoim zasięgiem – proponowane jest wykorzystanie znaków odpowiedniej wielkości, ale dopuszczalna jest możliwość ogłoszeń emitowanych przez głośniki. Na znakach powinny znaleźć się informacje o celu, w jakim został zainstalowany konkretny system, np. zapobieganie przestępczości oraz o administratorze systemu wraz z danymi kontaktowymi. Z obowiązku tego zwolnieni są właściciele małych systemów w sklepach i placówkach handlowych, którzy je administrują samodzielnie. Każda osoba, która została nagrana, ma prawo do zgłoszenia się do administratora w celu zapoznania się z nagraniem ją przedstawiającym[10].

Podobne do brytyjskiego rozwiązanie przyjęto w **Kanadzie**. Działalność na szczeblu federalnym Inspektora Ochrony Danych Osobowych Kanady jest wspierana i uzupełniana w każdej prowincji przez miejscowych Inspektorów Ochrony Danych Osobowych. Wydają oni, na podstawie ustaw o ochronie danych osobowych oraz aktów prawa lokalnego, dyrektywy dotyczące wykorzystania systemów CCTV zarówno

[10] P. Waszkiewicz, dz. cyt., s. 71-73.

przez podmioty publiczne, jak i prywatne. Zgodnie z nimi system wideo nadzoru powinien być rozważany tylko, jeżeli inne środki ochrony bezpieczeństwa publicznego, wykrywania lub zapobiegania przestępstwom lub prowadzenia dochodzenia w ich sprawie zostały rozpatrzone i odrzucone, jako niewykonalne. Wideonadzór powinien być wykorzystany, kiedy konwencjonalne środki (np. patrole piesze) do osiągnięcia tych samych celów organów ścigania i zapewnienia bezpieczeństwa publicznego są znacząco mniej efektywne albo niemożliwe do wprowadzenia, a korzyści z nadzoru znacząco przeważają zmniejszenie prywatności nierozłącznie związane ze zbieraniem danych osobowych za pomocą systemu wideo nadzoru. Użycie każdej kamery systemu wideo nadzoru powinno być uzasadnione weryfikowalnymi danymi o przestępczości oraz istotnymi obawami o bezpieczeństwo. Jednym ze wskazań jest to, aby ograniczyć operatorom możliwość obejmowania zasięgiem kamer obszaru poza wyznaczony teren, w tym zaglądania przez okna do wnętrza budynków. Inne wymagają jasnego poinformowania za pomocą czytelnych znaków o granicach obszaru objętego nadzorem systemu, jak i ograniczenia dostępu do obrazu przekazywanego przez kamery.

Zarówno brytyjskie, jak i kanadyjskie rozwiązania w szerokim zakresie wyczerpują postulaty obrońców praw obywatelskich sprzeciwiających się upowszechnianiu monitoringu. Sformułowane przez nich podstawowe reguły, to:

1. Obowiązkowe informowanie obywateli o obszarze objętym monitoringiem.
2. Monitoring nie może wykraczać poza oznaczony obszar.
3. Wszystkie nagrania dokonane przez kamery muszą być niszczone w krótkim czasie po nagraniu, chyba że są nieodzowne do prowadzonych przez policję postępowań.
4. Obywatele muszą mieć dostęp do nagrań z ich udziałem[11].

Ten krótki przegląd uwidocznia różnice w podejściach poszczególnych ustawodawców do problematyki systemów monitoringu wizyjnego. W niektórych krajach stosunek do tego środka technicznego jest bardziej liberalny, w innych mniej. Rodzi

[11] Tamże, s. 73-75.

się pytanie, które z podejść jest właściwe? Odpowiedź wydaje się prosta – jest to obszar, na którym regulacje prawne stanowią gwarancję praw i wolności obywateli. Ustawodawca stojący na ich straży jasno reguluje kwestie związane z funkcjonowaniem systemów CCTV. Na pewno zebranie przepisów w jednym miejscu ułatwia ich wdrażanie, jednak trudno przesądzić, czy konieczna jest całkowicie nowa ustawa. Wydaje się, że ustawa o ochronie danych osobowych jest odpowiednim miejscem.

Rozdział 3.
Polskie akty prawne

Zatem, jak na tym tle wygląda prawne umocowanie monitoringu wizyjnego w Polsce? Polska jest krajem, gdzie nie uchwalono osobnej ustawy, która regulowałaby zagadnienie monitoringu wizyjnego. W prawodawstwie polskim funkcjonuje wiele aktów prawnych, które w mniejszym lub większym stopniu regulują pośrednio lub bezpośrednio zagadnienia związane z monitoringiem wizyjnym. Brak jest jednak w polskim systemie regulacji prawnej, która w sposób kompleksowy określałaby problematykę funkcjonowania systemów monitoringu wizyjnego, a przyznać należy, iż istniejące regulacje są w tym temacie dość fragmentaryczne.

W naszym kraju obowiązuje zamknięty katalog źródeł prawa określony w art. 87 *Konstytucji Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 r.[12] Do źródeł obowiązującego prawa konstytucja zalicza: ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia oraz akty prawa miejscowego, ustalając tym samych hierarchię owych aktów, z małym wyjątkiem, albowiem umowa międzynarodowa ratyfikowana za uprzednią zgodą wyrażoną w ustawie ma pierwszeństwo przed ustawą, jeżeli ustawy tej nie da się pogodzić z umową (art. 91, ust. 2).

Jedynym aktem wspólnotowym dotyczącym omawianej problematyki jest, jak do tej pory, dyrektywa 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*[13]. Wymóg dostosowania prawodawstwa polskiego do prawodawstwa unijnego doprowadził do uchwalenia ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*[14]. Istotne jest ograniczenie stosowania przedmiotowej dyrektywy ustanowione w jej wstępie (pkt

[12] Dz.U. Nr 78, poz. 483, z późn. zm.

[13] Dz.Urz.WE L 281 z 23.11.1995, s. 31.

[14] Dz.U. z 2014 r. poz. 1182.

16): „*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 działań państwowych w dziedzinie prawa karnego lub innych działań niewchodzących w zakres prawa wspólnotowego*". W prawie wspólnotowym brak jest innych regulacji wykorzystania systemów monitoringu wizyjnego.

Często zwracano uwagę, że użycie systemów monitoringu wizyjnego stwarza realne zagrożenie dla praw i wolności osób fizycznych. Owe prawa i wolności osobiste zdefiniowane są w rozdziale II Konstytucji RP. Dla systemu monitoringu wizyjnego najistotniejsze są praktycznie cztery artykuły.

Art. 47. *Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym*. – Zapewniający prawo do ochrony życia prywatnego.

Art. 49. *Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony*. – Można go odnieść do systemów CCTV, w których przekazowi obrazu będzie towarzyszyć fonia lub jakość nagrań pozwala na odczytanie słów z ruchu warg.

Art. 50. *Zapewnia się nienaruszalność mieszkania. Przeszukanie mieszkania, pomieszczenia lub pojazdu może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony*. – Ogranicza wykorzystanie systemów kamer telewizji dozorowanej. Nie mogą one, poza przypadkami określonymi w ustawie, rejestrować tego, co odbywa się w obrębie mieszkania.

Art. 51. ust. 2. *Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym*. **–** Dotyczy również informacji pozyskiwanych w drodze używania różnych środków technicznych, w tym systemów monitoringu wizyjnego.

Podkreślić należy, że w żadnym z artykułów Konstytucji RP nie ma mowy o monitoringu wizyjnym, ale też trzeba zauważyć, iż nie ma takiej potrzeby. Wystarczy zatem wyszczególnienie praw i wolności człowieka i obywatela w połączeniu z **art.**

7 Konstytucji RP, który stanowi: *Organy władzy publicznej działają na podstawie i w granicach prawa*. Oznacza to, że organy władzy publicznej potrzebują wyraźnego upoważnienia prawnego dla swoich działań, również w szeroko rozumianym obszarze zapewnienia bezpieczeństwa.

Umowy międzynarodowe, które w pewnym zakresie dotyczą kwestii związanych z systemami CCTV, to przede wszystkim – *Powszechna Deklaracja Praw Człowieka* ONZ z 10.12.1948 r., *Międzynarodowy Pakt Praw Obywatelskich i Politycznych* – ratyfikowany przez Polskę 18.03.1977 r.[15] oraz *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* – ratyfikowana przez Polskę 19.01.1993 r.[16]

Art. 12. Powszechnej Deklaracji Praw Człowieka stanowi: *Nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu*.

Art. 17 ust. 1 i 2. Międzynarodowego Paktu Praw Obywatelskich i Politycznych stanowi: *Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami*.

Art. 8. Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności stanowi: *Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób*.

[15] Dz.U. Nr 38, poz. 167.

[16] Dz.U. Nr 61, poz. 284.

W podobnym tonie brzmi również **art. 7** *Karty Praw Podstawowych Unii Europejskiej*[17], który stanowi, że: *każdy ma prawo po poszanowania życia prywatnego i rodzinnego, domu i komunikowania się*. Natomiast **art. 8** dotyczący ochrony danych osobowych stanowi, iż: *każdy ma prawo do ochrony danych osobowych, które go dotyczą*.

Są to regulacje, które znalazły swoje odzwierciedlenie również w Konstytucji RP. Innych umów międzynarodowych, które w sposób bezpośredni odnosiłyby się do problematyki systemów monitoringu wizyjnego obecnie nie ma.

W przywołanej już ustawie z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych,* nie pojawia się monitoring wizyjny, jako źródło danych osobowych. **Art. 6.** ustawy stanowi jednak, że: *1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne*.

Pytanie, czy w myśl tej definicji specyficznym czynnikiem będzie np. zdjęcie takiej osoby lub nagranie ją przedstawiające? Niewątpliwie, jeżeli jest ono odpowiedniej jakości, na jego podstawie można określić cechy fizyczne konkretnej osoby, czyli jest takim specyficznym czynnikiem. Wydaje się, że **art. 6 ust. 3.** ustawy będzie adekwatny tylko w sytuacjach nagrań w miejscach publicznych, gdzie rotacja ludzi jest duża, a nagrania niewyraźne. Wówczas nagrań tych nie będzie można uznać za podlegające regulacjom ustawy, albowiem: *Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań*.

Ustawodawcy nie przewidzieli jednak lawinowego wręcz wzrostu liczby kamer monitoringu wizyjnego w Polsce na początku XXI w. Zdanie Generalnego Inspektora Ochrony Danych Osobowych (GIODO) dotyczące nagrań z systemów monitoringu wizyjnego, jest co najmniej dwuznaczne: *Ważne jest natomiast, by podczas rejestrowania*

[17] Dz.Urz.UE z 30.3.2010 r. nr 2010/C 83/02.

obrazu nie dochodziło do naruszenia praw i wolności obywateli. A ponieważ nadzór wideo ogranicza naszą prywatność, na terenach, na których jest on wprowadzony, powinny być umieszczone tablice informujące o jego istnieniu. Administratorzy systemów dozoru wizyjnego powinni zaś dbać o zgodne z prawem, w tym z ustawą o ochronie danych osobowych, postępowanie z zarejestrowanymi obrazami. Ważne jest przede wszystkim zadbanie o bezpieczne gromadzenie i przechowywanie zapisów z kamer, tak by nie dostały się one w ręce osób nieuprawnionych. W niektórych przypadkach zarejestrowane obrazy możemy bowiem uznać za dane osobowe. O ile bez dodatkowych informacji trudno byłoby zidentyfikować tysiące osób przewijających się po ulicach pod okiem kamery, to już w przypadku obrazów ludzi siedzących w samochodach, które można powiązać z numerami rejestracyjnymi aut, można mówić o danych osobowych[18].

W obecnej sytuacji, kiedy brak jest odrębnych regulacji prawnych, należy stosować istniejące, w tym przede wszystkim właśnie ustawę *o ochronie danych osobowych*. Docelowo jednak systemy CCTV powinny doczekać się regulacji prawnej przystającej do rzeczywistości społecznej i rozwoju techniki w tym zakresie, co pozwoliłoby również na ograniczenie możliwości interpretacji zawężających pojęcie danych osobowych. Na podobnym stanowisku stoi również Generalny Inspektor Ochrony Danych Osobowych: *trzeba stworzyć odrębną regulację ustawową, która określi zasady i warunki dopuszczalności stosowania monitoringu, czy wideonadzoru. Musi być wiadomo w jakich sytuacjach nadzór taki jest możliwy do zastosowania, a także przez jaki okres można przechowywać nagrania. Trzeba jasno określić podmioty, które mogą wykorzystywać systemy monitoringu, jak również unormować prawa, jakie przysługują osobie, której taki nadzór może dotyczyć*[19].

---

[18] M. Kosiarski, *Ostrożnie udostępniajmy informacje o sobie*. Rozmowa z Michałem Serzyckim – GIODO. „Rzeczpospolita" z 10.11.2008. http://www.rp.pl/artykul/117341,217181-Ostroznie-udostepniajmy-informacje-o-sobie.html, , 26.01.2015.

[19] A. Makosz, *Informacje z ulicznych kamer poza kontrolą.* „Dziennik Gazeta Prawna" z 11.06.2010 r., http://prawo.gazetaprawna.pl/artykuly/427743,informacje_z_ulicznych_kamer_poza_kontrola.html, 26.01.2015.

Rozdział 4.
Organy uprawnione do korzystania z systemów monitoringu wizyjnego

Prawo do korzystania z systemów CCTV polski ustawodawca przyznaje m.in. **Policji** w ustawie z dnia 6 kwietnia 1990 r. *o Policji*[20]. Pozwala na obserwowanie i rejestrowanie przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych na podstawie ustawy – także i dźwięku towarzyszącego tym zdarzeniom (art. 15 ust. 1 pkt 5a). Prawo to przysługuje również innym służbom wyposażonym w uprawnienia policyjne, jak np.: Żandarmeria Wojskowa, Agencja Bezpieczeństwa Wewnętrznego, Straż Graniczna, Centralne Biuro Antykorupcyjne czy Straż Ochrony Kolei. Prawne regulacje dotyczące korzystania przez Policję z systemów CCTV zawiera rozporządzenie Rady Ministrów z dnia 26 lipca 2005 r. *w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów*[21], w rozdziale VI **§ 19:** *Policjant podczas czynności służbowych wykonuje uprawnienie do obserwowania i rejestrowania obrazu lub dźwięku zdarzeń, planowo lub doraźnie oraz w sposób – bezpośredni – w przypadku obecności policjantów w miejscu prowadzenia obserwacji i rejestracji obrazu lub dźwięku zdarzeń; – zdalny – przy użyciu urządzeń teleinformatycznych przekazujących obraz lub dźwięk zdarzeń na odległość; – jawny lub przy użyciu metod uniemożliwiających osobom nieupoważnionym ustalenie faktu prowadzenia obserwacji i rejestracji.*

§ 20. *Policjant dokumentuje czynności służbowe, o których mowa w § 19, stosownie do okoliczności i wyników obserwacji oraz dyspozycji podmiotu decydującego o podjęciu obserwacji, w notatniku służbowym, notatce służbowej, notatce urzędowej,*

[20] Dz.U. z 2011 r. Nr 287, poz. 1687 z późn. zm.

[21] Dz.U. Nr 141, poz. 1186.

komunikacie, meldunku lub na odpowiednim nośniku technicznym, określając miejsce i czas ich rozpoczęcia i zakończenia oraz rodzaj użytych środków technicznych.

Zaznaczyć w tym miejscu należy, że brak jest regulacji dotyczących przechowywania nagrań w sytuacji, kiedy nie są one wykorzystywane procesowo. Kwestie związane z rejestracją obrazu dla celów procesowych reguluje rozporządzenie Ministra Sprawiedliwości z dnia 14 września 2012 r. *w sprawie rodzaju urządzeń i środków technicznych służących do utrwalania obrazu lub dźwięku dla celów procesowych oraz sposobu przechowywania, odtwarzania i kopiowania zapisów*[22]. Zakres stosowania rozporządzenia określony jest w § 1 ust. 1: *Do utrwalania obrazu lub dźwięku dla celów procesowych używa się urządzeń typu analogowego lub cyfrowego.* Obraz lub dźwięk jest utrwalany w formie zapisu na środkach technicznych umożliwiających przechowywanie danych przez okres niezbędny dla prawidłowego przeprowadzenia postępowania karnego. Zapisem cyfrowym jest taki, dla którego można wygenerować funkcję skrótu. Zapisem analogowym jest zapis niebędący zapisem cyfrowym. Nośnikiem cyfrowym jest taki, na którym utrwalono zapis cyfrowy, w szczególności płyta CD, płyta DVD, karta pamięci, dysk twardy lub inny wyposażony w pamięć środek techniczny. Nośnikiem analogowym jest nośnik, na którym utrwalono zapis analogowy, w szczególności kaseta magnetofonowa, kaseta magnetowidowa, minikaseta DV lub fotograficzny materiał światłoczuły.

Częściej niż rejestrować czynności procesowe systemy monitoringu wizyjnego mogą pozwolić utrwalić zdarzenia, których przebieg jest istotny dla postępowania sądowego. Wówczas nagrania takie mogą stanowić dowody w późniejszym postępowaniu. W związku z tym, iż systemy CCTV w Polsce są najczęściej prowadzone przez **straże gminne**, a nie przez Policję, dużą rolę odgrywają regulacje dotyczące funkcjonowania tej właśnie formacji. W zakresie realizowania obowiązków, które wynikają z ustawy z dnia 29 sierpnia 1997 r. *o strażach gminnych*[23] prawo wykorzystywania

[22] Dz.U. z 2012 r., poz. 1090.

[23] Dz.U. z 2013 r., poz. 1383 z późn. zm.

systemów CCTV przysługuje również strażom gminnym. Art. 11 ust. 2 przedmiotowej ustawy stanowi, że w związku z realizowanymi zadaniami określonymi w art. 1 ust. 10, straży przysługuje prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, w przypadku, gdy czynności te są niezbędne do wykonywania zadań w celu:

1) utrwalania dowodów popełnienia przestępstwa lub wykroczenia,
2) przeciwdziałania przypadkom naruszenia spokoju i porządku w miejscu publicznym,
3) ochrony obiektów komunalnych i urządzeń użyteczności publicznej.

Rozporządzenie Rady Ministrów z dnia 16 grudnia 2009 r. *w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską*[24]*)* określa dwa sposoby prowadzenia obserwacji:

1) zdalny – przy użyciu urządzeń umożliwiających przekazywanie obrazu zdarzeń na odległość,
2) bezpośredni – w przypadku prowadzenia przez strażnika gminnego (miejskiego) obserwacji i rejestracji obrazu w miejscu zdarzenia.

Podkreślić należy, iż zadaniem straży gminnych nie jest potajemne gromadzenie informacji o obywatelu, ani prowadzenie skomplikowanych czynności operacyjnych, między innymi z wykorzystaniem systemów CCTV. Dlatego dziwić może chociażby brak obowiązku wyraźnego oznaczania przestrzeni znajdującej się pod nadzorem kamer.

Oprócz instytucji publicznych powołanych do zapewnienia bezpieczeństwa funkcjonują również prywatne **służby ochrony osób i mienia**, których działanie reguluje ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia*[25]. Przedmiotowa ustawa stanowi, iż ochrona osób i mienia realizowana jest w formie bezpośredniej ochrony fizycznej i zabezpieczenia technicznego. Ochrona realizowana w formie za-

[24] Dz.U. Nr 220, poz. 1720.

[25] Dz.U. z 2014 r., poz. 1099.

bezpieczenia technicznego polega na montażu elektronicznych urządzeń i systemów alarmowych sygnalizujących zagrożenie chronionych osób i mienia oraz eksploatacji, konserwacji i naprawach w miejscach ich zainstalowania, a także montażu urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatacji, konserwacji, naprawach i awaryjnym otwieraniu w miejscach zainstalowania.

Stosowanie systemów monitoringu wizyjnego w ochronie osób i mienia zalicza się niewątpliwie do zabezpieczenia technicznego. Zwrócić należy uwagę na cel prowadzenia tych działań, tj. sygnalizowanie zagrożeń chronionych osób i mienia, a nie monitorowanie zachowań, które nie spełniają tego warunku. Zatem służby ochrony osób i mienia nie zostały upoważnione do prowadzenia obserwacji i rejestracji zdarzeń w miejscach publicznych. Nie można zgodzić się ze stwierdzeniem, że obserwacja jest dozwolona bez ograniczeń. Należy też rozróżnić miejsce publiczne od przestrzeni prywatnej, np. placówek handlowych, do których dostęp ma nieograniczona liczba klientów. Jest to sfera nieuregulowana prawnie, co nie oznacza przyznania nieograniczonych praw agencjom ochrony osób i mienia. Szczególnie, kiedy mogłyby one naruszyć konstytucyjnie zagwarantowane prawa i wolności. Praktyka działania służb ochrony osób i mienia bywa różna, należy zatem stanowczo zaakcentować, że w żadnym razie nie można stosować interpretacji rozszerzającej, która uprawniałaby te służby do monitorowania miejsc publicznych. Praktyka życia codziennego wskazuje, że kwestia wykorzystania systemów CCTV przez prywatne służby ochrony osób i mienia wymaga uregulowania, które rozwiałoby wszelkie wątpliwości w tym zakresie.

Należy też wspomnieć o ograniczeniach wiążących się z rozpowszechnianiem wizerunku wynikających z ustawy z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych*[26], gdzie art. 81 wprost stanowi, że *rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie*.

[26] Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.

Ustawodawca wymienia również przypadki niewymagające zezwolenia, które ograniczają się do osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych, a także osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

W sytuacjach, z którymi zazwyczaj się spotykamy w przypadku nagrań pochodzących z systemów CCTV, nikt nie pyta osoby przedstawionej na nagraniach o zezwolenie ani nie otrzymuje ona z tego tytułu zapłaty. Najczęściej osoby przedstawione na takich nagraniach nie są osobami powszechnie znanymi (przynajmniej do czasu publikacji owych nagrań). W świetle przepisów *Konstytucji RP*, *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności* oraz przytoczonego artykułu ustawy, praktyka przekazywania mediom nagrań z systemów CCTV okazuje się nie mieć oparcia w obowiązujących przepisach, a co więcej, stoi w sprzeczności z tymi aktami prawnymi. Można w tym miejscu przytoczyć przepisy art. 13 ust. 2 ustawy z dnia 26 stycznia 1984 r. *o prawie prasowym*[27], który stanowi, że nie wolno publikować w prasie danych osobowych i wizerunku osób, przeciwko którym toczy się postępowanie przygotowawcze lub sądowe, jak również danych osobowych i wizerunku świadków, pokrzywdzonych i poszkodowanych, chyba że osoby te wyrażą na to zgodę. Zatem jeżeli nie wolno publikować wizerunku osób, przeciwko którym toczy się postępowanie, to tym bardziej ochrona ta dotyczy innych osób – takich, przeciwko którym nie jest prowadzone ani postępowanie przygotowawcze, ani sądowe.

Bezpośrednio do systemów telewizji dozorowanej odnosi się Polska Norma na Systemy Alarmowe – Systemy Dozorowane CCTV, stosowana w zabezpieczeniach – część 7: Wytyczne stosowania (PN-EN 50132-7: 2003 – PNCCTV). Należy jednak przypomnieć, iż zgodnie z przepisami ustawy z dnia 12 września 2002 r. *o normalizacji*[28] od 1.01.2003 r. stosowanie norm jest całkowicie dobrowolne. We wprowadzeniu

[27] Dz.U. Nr 5, poz. 24 z późn. zm.

[28] Dz.U. Nr 169, poz. 1386 z późn. zm.

do normy wyrażone jest jej przesłanie, w którym możemy wyczytać, iż skuteczność systemu CCTV zależy od aktywnego udziału użytkownika w realizacji zalecanych w niniejszej normie procedur postępowania w procesie inwestycyjnym. Przedmiotowa norma określa procedury związane z projektowaniem systemów oraz parametry techniczne wykorzystywanego sprzętu w zależności od zdefiniowanego celu. Zalecana procedura projektowania systemu składa się z następujących etapów:

1) opracowanie wymagań użytkowych,

2) zaprojektowanie systemu,

3) uzgodnienie wyboru urządzeń,

4) zainstalowanie i uruchomienie systemu,

5) przekazanie systemu,

6) konserwacja (utrzymanie w ruchu).

Nie zagłębiając się zbytnio w czysto techniczne specyfikacje, warto w tym miejscu zwrócić uwagę jedynie na określenie wymogów związanych z celem systemu. Jeżeli celem jest kontrola tłumu, wówczas wystarcza, kiedy obiekt (osoba) zajmuje przynajmniej 5% wysokości ekranu (przy rozdzielczości ponad 400 linii telewizyjnych). Detekcja intruza wymaga już przekroczenia 10% wysokości ekranu, natomiast rozpoznanie jest możliwe przy przekroczeniu 50% wysokości ekranu. Z kolei do potrzeb identyfikacji – obserwowana osoba powinna zajmować przynajmniej 120% wysokości ekranu.

Polski ustawodawca w dwóch przypadkach wprowadził ustawowy obowiązek prowadzenia monitoringu wizyjnego – w zakładach karnych oraz podczas imprez masowych. Przepisy dotyczące monitoringu aresztów i zakładów karnych zostały zmienione pod wpływem opinii publicznej poruszonej serią samobójstw skazanych, którzy odbywali kary pozbawienia wolności za zabójstwo Krzysztofa Olewnika[29]. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny wykonawczy*[30] nakłada obowiązek stałego

[29] M. Kryszkiewicz, *Zero prywatności dla niebezpiecznych więźniów*. „Gazeta Prawna" z 26.02.2009 r.

[30] Dz.U. Nr 90, poz. 557 z późn. zm.

monitorowania skazanych i tymczasowo aresztowanych zaliczonych do kategorii tzw. niebezpiecznych.

Ustawa z dnia 20 marca 2009 r. *o bezpieczeństwie imprez masowych*[31] uprawnia **organizatora** do utrwalania przebiegu każdej **imprezy masowej**, a w szczególności zachowania osób w niej uczestniczących za pomocą urządzeń rejestrujących obraz i dźwięk (art. 11 ust. 1). Natomiast w art. 11 ust. 4 wprowadza obowiązek utrwalania przebiegu imprez masowych odbywających się w jednym z miejsc z wykazu sporządzonego przez wojewodę. Wykaz takich stadionów, obiektów i terenów powstaje w uzgodnieniu z komendantem wojewódzkim (stołecznym) Policji i z komendantem wojewódzkim Państwowej Straży Pożarnej oraz po zasięgnięciu opinii właściwego miejscowo polskiego związku sportowego. Przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10 stycznia 2011 r. *w sprawie sposobu utrwalania przebiegu imprezy masowej*[32] określają miejsca podlegające obowiązkowej rejestracji obrazu i dźwięku (§ 4):

1) kasy biletowe na terenie imprezy masowej – w przypadku imprezy odpłatnej;
2) bramy, furtki i inne miejsca przeznaczone do wejścia uczestników na teren imprezy masowej;
3) drogi dla służb ratowniczych, drogi ewakuacyjne oraz ciągi komunikacyjne na terenie imprezy masowej z wyłączeniem klatek schodowych;
4) parkingi zorganizowane na terenie imprezy masowej;
5) sektory dla uczestników imprezy masowej;
6) płyta boiska lub scena.

Przy czym kasy biletowe, bramy, furtki i inne miejsca przeznaczone do wejścia uczestników na teren imprezy masowej, drogi dla służb ratowniczych, drogi ewakuacyjne oraz ciągi komunikacyjne oraz parkingi powinny znajdować się w zasięgu co najmniej jednego urządzenia rejestrującego obraz. Natomiast sektory dla

[31] Dz.U. z 2013 r., poz. 611 z późn. zm.

[32] Dz.U. Nr 16, poz. 73.

uczestników i płyta boiska lub scena, w polu widzenia co najmniej dwóch urządzeń rejestrujących obraz. Warto podkreślić, że dla Stadionu Narodowego w Warszawie zaprojektowano instalację 900 kamer[33]. Liczbę kamer monitoringu wizyjnego instalowanych na poszczególnych stadionach (w tym również planowanych) obrazuje poniższa tabela.

Stadion	Liczba kamer
Stadion Narodowy w Warszawie	900 (planowana)
Stadion Miejski w Poznaniu	673 (planowana)
Stadion Miejski we Wrocławiu	553 (planowana)
Stadion Piłkarski w Gdańsku	500 (planowana)
Stadion Piłkarski w Krakowie	600 (planowana)
Stadion Piłkarski w Chorzowie	350 (planowana)
Magdeburg	16
Norymberga	24
Hamburg	32
Alianz Arena Monachium	92
Reading	30
Amsterdam Arena	95
Wiedeń (EURO 2008)	40
Arsenal	140
Liverpool	56
System monitoringu miejskiego w Warszawie (największy w Polsce)	ok. 300

Tab. 2. Kamery monitoringu wizyjnego na stadionach piłkarskich Europy
Źródło: http://www.systemyalarmowe.com.pl/index.php/pl/reportae-i-felietony/159,29.01.2015.

Przedstawiając prace polskiego ustawodawcy w zakresie wykorzystania systemów monitoringu wizyjnego, nie sposób pominąć dwóch kolejnych przedsięwzięć, które

[33] http://www.systemyalarmowe.com.pl/index.php/pl/reportae-i-felietony/159.

dotyczą **szkół** i **sklepów monopolowych**. W dniu 6 marca 2007 r. Rada Ministrów przyjęła program poprawy stanu bezpieczeństwa w szkołach i placówkach oświatowych pt. „Zero tolerancji dla przemocy w szkole" (uchwała nr 28/2007). Program ten zakładał wprowadzenie monitoringu wizyjnego szkół oraz placówek oświatowych. Rozporządzenie Rady Ministrów z dnia 6 września 2007 r. *w sprawie form i zakresu finansowego wspierania organów prowadzących w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w publicznych szkołach i placówkach*[34] określiło zasady sfinansowania organom prowadzącym kosztów zakupu i instalacji oraz modernizacji lub rozszerzenia zestawów do monitoringu wizyjnego.

W kwietniu 2009 roku Państwowa Agencja Rozwiązywania Problemów Alkoholowych podczas prac nad zmianą ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi zaproponowała Komisji Nadzwyczajnej „Przyjazne Państwo" do spraw związanych z ograniczaniem biurokracji, aby przedsiębiorca prowadzący punkt sprzedaży albo podawania napojów alkoholowych miał obowiązek wykonywania nadzoru polegającego m.in. na rejestracji zdarzeń w takich miejscach za pomocą kamer. Pomysł spotkał się z akceptacją, jednakże do chwili obecnej nie został wprowadzony w życie w formie obowiązującego nakazu. Systemy CCTV będą zatem instalowane w tych sklepach monopolowych, których właściciele uznają to za potrzebne, a nadzór nad zakresem monitoringu i rejestrowanym materiałem będzie spoczywał tylko w ich rękach[35].

Porównanie zaprezentowanych polskich regulacji prawnych monitoringu wizyjnego z obowiązującymi w innych państwach europejskich uświadamia dzielący te ustawodawstwa dystans. Może to świadczyć o pewnej niefrasobliwości polskiego ustawodawcy, niepodejmującego tej tematyki. Nie można się zgodzić z poglądami, że każda osoba wkraczając w miejsce publiczne, musi się liczyć z tym, że jest widziana[36].

---

[34] Dz.U. Nr 163, poz. 1155 z późn. zm.

[35] P. Waszkiewicz, dz. cyt., s. 93.

[36] M. Ordysińska, *Aspekty prawne funkcjonowania systemów monitoringu wizyjnego w Polsce. Cz. II. Konwencje prawne funkcjonowania systemów monitoringu*. „Systemy Alarmowe" nr 5/2006, s. 84.

Uprawnienia do dokonywania nagrań w przestrzeni publicznej zostały przyznane Policji, innym służbom mundurowym oraz strażnikom gminnym, które są instytucjami mającymi stać na straży bezpieczeństwa i porządku publicznego. Istnieje tu jednak pole do nadużyć nie tylko ze strony służb publicznych, ale także prywatnych firm i ich pracowników, faktycznie nie podlegających żadnej kontroli.

Przypadek CCTV jest szczególny i dlatego wymaga regulacji przez ustawodawcę – systemy takie dają możliwość ingerencji w prawa obywateli i nie jest to tylko zagrożenie potencjalne. Dlatego niezbędna jest gwarancja praw i wolności ustanowionych w aktach wyższego rzędu. Niezbędne kwestie, które wymagają regulacji, to:

1) określenie miejsc i sytuacji, w których mogą być wykorzystane systemy CCTV;
2) wytyczne przechowywania danych i dostępu do nich;
3) określenie przypadków, kiedy nagrania mogą zostać przekazane mediom;
4) wymagania stawiane pracownikom centrów odbiorczych (mogą oni stanowić najsłabsze ogniwo systemu);
5) sposób wyraźnego informowania osób obserwowanych o tym fakcie (oznaczenie wizualne, komunikaty nadawane przez głośniki).

Odrębną kwestią jest unormowanie sposobu wydawania zezwoleń na obsługę systemów monitoringu wizyjnego. Rozwiązania francuskie czy hiszpańskie, które wymagają opinii specjalnej komisji na poziomie lokalnym, stanowią bardzo dobry przykład do naśladowania. Przejrzystość postępowania jest jedną z podstaw państwa prawa. Swoista moda na instalowanie kamer prowadzi do tego, że coraz mniejsza liczba miejsc jest ich pozbawiona. Poddanie systemów pewnej kontroli mogłoby ograniczyć ten zagrażający prawom i wolnościom trend i zagwarantować ich respektowanie.

Rozpowszechnienie wykorzystania systemów CCTV powoduje oswojenie się z nimi przez wszystkich obywateli bez względu na wiek, ale nie zwiększa faktycznej wiedzy o możliwościach wykorzystania oraz, co wydaje się najważniejsze, stopnia realizacji stawianych zadań – przewidywanych korzyściach ich zastosowania.

Omawiając prawne aspekty monitoringu wizyjnego, warto również w tym miejscu przypomnieć wymagania, które zgodnie z obowiązującymi przepisami powinny spełniać instalacje systemów CCTV.

Instalacja telewizji dozorowej wymaga najwyższej kultury technicznej oraz zdolności przewidywania nawet mało prawdopodobnych zjawisk. W systemach związanych z zabezpieczeniami każdy instalator i użytkownik, musi mieć świadomość, iż urządzenia o zbyt słabych parametrach w stosunku do powierzonych im zadań, mogą w przyszłości nieść zagrożenie mienia, a nawet życia. Skutkuje to także problemami z awaryjnością.

Wykonywanie instalacji telewizji dozorowej wymaga uzyskania wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego, którego dokonuje właściwy miejscowo komendant wojewódzki Policji (art. 27 ust. 1 ustawy o ochronie osób i mienia). Wpis na listę kwalifikowanych pracowników zabezpieczenia technicznego uprawnia do wykonywania czynności związanych z montażem elektronicznych urządzeń i systemów alarmowych, sygnalizujących zagrożenie chronionych osób i mienia oraz eksploatacją, konserwacją i naprawami w miejscach ich zainstalowania, a także czynności związanych z montażem urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatacją, konserwacją, naprawami i awaryjnym otwieraniem w miejscach zainstalowania.

Na listę kwalifikowanych pracowników zabezpieczenia technicznego wpisuje się osobę, która ukończyła 18 lat; posiada obywatelstwo polskie lub obywatelstwo innego państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej lub państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym; ma pełną zdolność do czynności prawnych; nie była skazana prawomocnym wyrokiem za przestępstwo umyślne i nie toczy się przeciwko niej postępowanie karne o takie przestępstwo; posiada nienaganną opinię wydaną przez właściwego ze względu na jej miejsce zamieszkania komendanta powiatowego (rejonowego, miejskiego) Policji, sporządzoną na podstawie aktualnie posiadanych przez Policję informacji albo – w przypadku obywatela innego państwa

członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej lub państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym oraz obywatela polskiego zamieszkałego na terenie tych państw – przez organ odpowiedniego szczebla i kompetencji tych państw, właściwy ze względu na miejsce zamieszkania tej osoby; posiada zdolność fizyczną i psychiczną do pracy stwierdzoną orzeczeniem lekarskim, wydanym przez lekarza uprawnionego do przeprowadzania badań, o którym mowa w przepisach wydanych na podstawie art. 229 § 8 ustawy z dnia 26 czerwca 1974 r. – *Kodeks pracy* (Dz.U. z 1998 r. Nr 21, poz. 94, z późn. zm.); posiada wykształcenie co najmniej zawodowe techniczne o specjalności elektronicznej, elektrycznej, łączności, mechanicznej, informatycznej lub ukończyła kurs pracownika zabezpieczenia technicznego albo została przyuczona do wymienionych zawodów na podstawie przepisów ustawy z dnia 22 marca 1989 r. *o rzemiośle* (Dz.U. z 2002 r. Nr 112, poz. 979, z późn. zm.). Na listę kwalifikowanych pracowników zabezpieczenia technicznego wpisuje się również osobę, której uznano kwalifikacje do wykonywania zawodu pracownika zabezpieczenia technicznego na podstawie ustawy z dnia 18 marca 2008 r. *o zasadach uznawania kwalifikacji zawodowych nabytych w państwach członkowskich Unii Europejskiej*.

Osoba wpisana na listę kwalifikowanych pracowników zabezpieczenia technicznego jest uprawniona do opracowywania planu ochrony w zakresie montażu elektronicznych urządzeń i systemów alarmowych, sygnalizujących zagrożenie chronionych osób i mienia oraz eksploatacji, konserwacji i naprawach w miejscach ich zainstalowania, a także montażu urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatacji, konserwacji, naprawach i awaryjnym otwieraniu w miejscach zainstalowania, jak również organizowania i kierowania zespołami pracowników zabezpieczenia technicznego.

Koncesję na działalność gospodarczą w zakresie świadczenia usług zabezpieczenia technicznego musi posiadać tylko ta firma, która świadczy usługi w zakresie zabezpieczania obiektów podlegających obowiązkowej ochronie. Sposób uzyskania koncesji oraz listę obiektów podlegających obowiązkowej ochronie zawiera ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia* (art. 5 ust. 5).

Rozdział 5.
Zasady stosowania monitoringu wizyjnego

Oprócz regulacji prawnych, które regulują funkcjonowanie systemów monitoringu wizyjnego, obowiązują również pewne zasady, którymi powinniśmy kierować się podczas wykorzystania monitoringu wizyjnego. Zasady wykorzystania monitoringu wizyjnego są następujące:

1. Monitoring musi zostać wykonany na podstawie szczegółowych, profesjonalnie przygotowanych założeń i bez naruszenia praw człowieka.
2. Projektant systemu musi posiadać doświadczenie, zarówno praktyczne, jak i teoretyczne (to warunek, aby zbudowany system spełniał pokładane w nim nadzieje).
3. Monitoring musi być wykonany zgodnie z wymaganiami obowiązujących przepisów prawa i konwencji.
4. Monitoring musi być wykonany w sposób profesjonalny, zgodnie z wymaganiami obowiązujących norm.
5. Inwestorzy, projektanci i wykonawcy muszą realizować system monitoringu, wykorzystując sprzęt o wysokiej jakości, niezawodności i trwałości, a odrzucać sprzęt awaryjny o niskiej jakości.
6. Sprzęt musi posiadać stosowne atesty i certyfikaty.
7. Monitoring musi być obsługiwany przez osoby profesjonalnie przeszkolone – również w zakresie praw człowieka.
8. Osoby znajdujące się w obszarze monitorowanym muszą mieć świadomość przebywania w takim obszarze.
9. Osoby znajdujące się w obszarze monitorowanym muszą mieć poczucie bezpieczeństwa.

10. Działanie monitoringu musi podlegać analizom, mającym na celu określenie, czy zamierzony cel został osiągnięty[37].

Szczególnie istotnym, a lekceważonym przez inwestorów i instalatorów elementem budowy systemu monitoringu wizyjnego jest wizualna informacja o instalacji monitoringu, jej odstraszające znaczenie może mieć istotny wpływ w ochronie obiektu.

Opracowanie precyzyjnych wymagań użytkowych jeszcze przed rozpoczęciem inwestycji pozwoli na prawidłowe jej zaprojektowanie oraz optymalny dobór sprzętu uwzględniający wymagania i koszty. Z jednej strony firma podejmująca się wykonania instalacji powinna, z własnej inicjatywy oczekiwać odpowiedzi na poniższe pytania, z drugiej strony inwestor może być pewny, że bez przekazania tych informacji odpowiedzialny wykonawca nie powinien podejmować się żadnych prac. Funkcjonuje 12 pytań do planującego wykonanie instalacji telewizji dozorowej, których zadaniem jest ułatwienie formułowania wymagań użytkowych:

1. Jakiego rodzaju zagrożenia mają być monitorowane?
2. Jaki obszar ma być monitorowany?
3. Jaki jest cel monitorowania poszczególnych stref?
4. Jaki ma być stopień automatyzacji?
5. Jaka powinna być reakcja systemu na naruszenia poszczególnych stref?
6. Jaki powinien być czas reakcji systemu?
7. W jakich warunkach środowiska mają funkcjonować urządzenia?
8. Jaki ma być sposób sterowania systemem?
9. Ile jednoczesnych zdarzeń powinien obsłużyć system?
10. Jaki ma być zasięg i bezpieczeństwo transmisji sygnału?
11. Jaka powinna być forma przeszkolenia pracowników obsługujących?
12. W jakiej formie i przez kogo ma być prowadzona konserwacja systemu?

Powyższe pytania opracowane zostały na podstawie wymagań użytkowych zawartych w normie: *Systemy dozorowe CCTV w zastosowaniach dotyczących zabezpieczenia EN 50132-7*.

[37] T. Malinowski, *Aspekty prawne a prawa dziecka w świetle zastosowania systemów monitoringu wizyjnego*, „Zabezpieczenia" nr 4/2011, s. 19.

Rozdział 6.
Monitoring wizyjny a ochrona wizerunku osoby i prawo do prywatności

Podkreślić należy, iż przepisy zarówno ustawy z dnia 23 kwietnia 1964 r. *Kodeks cywilny*[38], jak również powoływana już ustawa z dnia 4 lutego *1994 r. o ochronie praw autorskich i prawach pokrewnych*, nie zawierają normatywnej definicji wizerunku. S. Ritterman uważa, że **wizerunek** danej osoby obejmuje głowę, jak i całą postać indywidualizującą tę osobę jako jednostkę fizyczną[39]. Zdaniem T. Grzeszak wizerunek to skonkretyzowane ustalenie obrazu fizycznego człowieka, zdatne do zwielokrotnienia i do rozpowszechniania. T. Grzeszak, uważa, że to wizerunek jest przedmiotem obrotu, a jego synonimem jest podobizna. Odróżnia ona od wizerunku obraz fizyczny człowieka (wygląd), będący atrybutem tożsamości, stanowiący jego dobro osobiste, portret (utwór o tematyce portretowej), będący przedmiotem obrotu autorskiego i praw autorskich osobistych, oraz materialny egzemplarz, w którym wizerunek (a często i portret), będący przedmiotem prawa własności jest utrwalony[40]. Natomiast S. Grzybowski za wizerunek uważa obraz fizyczny osoby[41]. Szerzej na temat prawnego pojęcia wizerunku pisze W. Danilewicz[42].

Prywatność to z kolei 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.

[38] Dz.U. z 2014 r., poz. 121 z późn. zm.

[39] S. Ritterman, *Komentarz do ustawy o prawie autorskim*, Kraków 1937, s. 120.

[40] W. Danilewicz, *Prawne pojęcie wizerunku,* „Edukacja Prawnicza" nr 6 (117)/2010.

[41] S. Grzybowski, *Ochrona dóbr osobistych według przepisów ogólnych Kodeksu cywilnego*, Warszawa 1957, s. 96.

[42] W. Danilewicz, dz. cyt.

Niewątpliwie wszelkie nagrania obrazu i/lub dźwięku przedstawiające wizerunek/wypowiedź osoby fizycznej są danymi ujawniającymi jej zachowania[43].

Kodeks cywilny w **art. 23** wymienia dobra osobiste człowieka, do których zalicza w szczególności: zdrowie, wolność, cześć, swobodę sumienia, nazwisko lub pseudonim, **wizerunek**, tajemnicę korespondencji, nietykalność mieszkania, twórczość naukową, artystyczną, wynalazczą i racjonalizatorska. Pozostają one pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Jak już wspominano wcześniej, ustawodawca nie definiuje, co rozumie pod pojęciem wizerunku osoby.

W rozumieniu przywoływanej już ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych,* za **dane osobowe** uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 6 ust. 1). Natomiast za możliwą do zidentyfikowania uważa się osobę, której tożsamość można określić bezpośrednio lub pośrednio, powołując się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2). Jak łatwo można się zorientować, katalog informacji stanowiących dane osobowe jest bardzo szeroki, a tym samym nie jest proste określenie, które informacje są danymi osobowymi, a które nimi nie są. Niemniej jednak zakwalifikowanie wizerunku osoby do katalogu danych osobowych nie powinno być kłopotliwe. W przypadku monitoringu miejsca pracy, obraz z kamer pozwala pracodawcy na jednoznaczne i bezpośrednie zidentyfikowanie osób, których wizerunek jest rejestrowany. O takiej identyfikacji możemy mówić także w przypadku, gdy np. osoba z zewnątrz wchodząca do instytucji rejestrowana jest w księdze wejść i wyjść. W obu tych przypadkach, mając na uwadze warunek, jakim jest identyfikacja osoby, przyjąć należy bezwzględnie, że zarejestrowany przez system monitoringu wizyjnego wizerunek jest częścią katalogu danych osobowych określonych przez ustawodawcę.

[43] GIODO, *Wymagania w...,* dz. cyt., s. 6.

Co zatem w przypadku, gdy niemożliwe lub znacznie utrudnione jest powiązanie wizerunku osób utrwalonych przez monitoring z innymi danymi pozwalającymi na chociażby pośrednią ich identyfikację? Należy uznać, że nie stanowi on danych osobowych podlegających ustawowej ochronie. Twierdzenie to należy wywieść z wyjątku określonego w ustawie, mówiącego, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań (art. 6 ust. 3).

Niezależny europejski organ doradczy Komisji Europejskiej – Grupa robocza ds. ochrony danych[44] w sprawie pojęcia danych osobowych[45] wskazuje, że obrazy osób zarejestrowane przez systemy nadzoru wideo mogą stanowić dane osobowe, jeżeli można rozpoznać te osoby. Tak więc możliwość identyfikacji tych osób nie jest tu w ogóle brana pod uwagę, gdyż jak stwierdzono w dalszej części, identyfikacja osób jest jednym z głównych celów nadzoru wideo i wszystkie wizerunki należy uznać za dane dotyczące osób możliwych do zidentyfikowania, nawet jeżeli niektóre zarejestrowane osoby nie są możliwe do zidentyfikowania w praktyce.

Z danymi osobowymi ściśle wiąże się pojęcie **przetwarzania danych**, za które ustawodawca w ustawie *o ochronie danych osobowych* rozumie: *jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.*

Dopuszczalność przetwarzania danych osobowych zależy od ich rodzaju, tj. wrażliwości opisywanych przez nie sfer prywatności (intymności) jednostki. Na tym tle ustawodawca podzielił katalog informacji stanowiących dane osobowe na tzw. „zwykłe" i „wrażliwe" (sensytywne). Pierwsza grupa powstaje w wyniku tzw. selekcji negatywnej, tzn. są to informacje niemieszczące się w zamkniętym katalogu „danych

[44] Grupa robocza ds. ochrony danych powołana na mocy art. 29 Dyrektywy 95/46/WE niezależny organ doradczy w zakresie ochrony danych i prywatności, mieszcząca się przy Dyrekcji Komisji Europejskiej – Sądownictwo Cywilne, Prawa Podstawowe i Obywatelstwo.

[45] Opinia nr 4/2007 z dnia 20.06.2007 r. w sprawie pojęcia danych osobowych (01248/07/PL. WP 136).

wrażliwych", za które uważa się informacje ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, stan zdrowia, kod genetyczny, nałogi, życie seksualne oraz dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, postępowań sądowych lub administracyjnych (art. 27 ust. 1). Tak więc, za „dane zwykłe" uważa się wszelkie „podstawowe" informacje o osobie, tj. imię, nazwisko, data urodzenia, miejsce zamieszkania itp.[46]

Pozornie mogłoby się wydawać, że wizerunek osób zarejestrowanych przez system monitoringu nie należy do kategorii danych osobowych o charakterze wrażliwym, nic jednak bardziej mylnego. Należy tu jednocześnie uświadomić sobie, że operator systemu monitoringu wizyjnego nie ma żadnej możliwości ograniczenia rejestrowania obrazu lub inaczej mówiąc decydowania o jego zawartości, nie mając wpływu czy i jakie „wrażliwe" cechy osób znajdujących się w jego obszarze zostaną zarejestrowane.

Ustalenie ponad wszelką wątpliwość, że wizerunek osoby stanowi dane osobowe, nie musi automatycznie oznaczać, że systemy monitoringu wizyjnego rejestrujące wizerunki osób podlegają rygorom ustawy o ochronie danych osobowych, zgodnie z którą dane osobowe podlegają ochronie przewidziane w ustawie tylko wtedy, gdy są lub mogą być przetwarzane w zbiorach danych (art. 2 ust. 1). Przetwarzanie to jakakolwiek operacja wykonywana na danych osobowych, taka jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach teleinformatycznych (art. 7 pkt 2). Tak, więc poza zmienianiem, każda z wymienionych czynności wykonywana jest przez systemy monitoringu, coraz częściej stanowiących już systemy informatyczne[47].

O ile pojęcie „przetwarzania danych osobowych" nie budzi wątpliwości w odniesieniu do czynności obserwowania, przesyłania czy archiwizowania obrazu z kamer

[46] Ł. Kister, *Prawne aspekty dopuszczalności monitoringu wizyjnego – ochrona wizerunku osób,* „Ochrona Mienia i Informacji" nr 6/2010, s. 29.

[47] Tamże, s. 29.

monitoringu, o tyle nie jest już takie proste zakwalifikowanie tego zapisu jako zbioru danych. Zgodnie z ustawą o ochronie danych osobowych za zbiór danych uważany jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie (art. 7 pkt 1). W przypadku nagrania monitoringu, bez względu na technikę i nośnik, możemy mówić o jakiejś formie zbioru różnego rodzaju informacji w formie sekwencji obrazów, ale czy jest to zbiór danych osobowych? Przede wszystkim informacje w tym zbiorze nie są podzielone z uwagi na zarejestrowane wizerunki osób, a raczej z uwagi na czas rzeczywisty lub długość nagrania, co powoduje, że w tej samej jednostce czasu zarejestrowane mogą być wizerunki osób lub nie. Poza tym, trudno mówić o kryteriach pozwalających na dostęp do określonych danych osobowych, czyli wizerunku konkretnej osoby lub nawet grupy osób. Nie oznacza to jednak możliwości jednoznacznego uznania monitoringu za system gromadzenia danych osobowych nieobjęty ochroną ustawową[48].

Zarejestrowany przez kamery monitoringu materiał w pewnych okolicznościach może być postrzegany jako baza danych. W ten sposób należy traktować zarejestrowany obraz w systemach wyposażonych w rozwiązania umożliwiające automatyczne rozpoznawanie numerów rejestracyjnych pojazdów (ARPR) czy też gromadzące automatycznie dane umożliwiające rozpoznawanie twarzy. Każdorazowo zastosowanie takich systemów musi znajdować uzasadnienie w opracowanych celach wdrożenia systemu monitoringu wizyjnego i być poddawane szczegółowemu badaniu pod kątem konstytucyjności[49].

O złożoności problemu i jego trudnościach interpretacyjnych świadczą także dwie zupełnie odmienne od siebie opinie GIODO. W pierwszej, że film z monitoringu wideo nie ma charakteru zbioru danych osobowych w rozumieniu ustawy[50], by w kolejnej stwierdzić, iż zestaw kaset magnetycznych z zapisem obrazu monitoringu

[48] Tamże, s. 30.

[49] M. Ordysińska, *Aspekty prawne funkcjonowania…*, s. 85.

[50] Sprawozdanie z działalności GIODO za rok 2000, s. 12. http://www.giodo.gov.pl.

stanowi zbiór danych osobowych[51]. Należy jednak stwierdzić, że żadna z tych opinii nie znajduje racjonalnego poparcia jako oparte na błędnych założeniach i braku kompleksowej analizy.

W tym momencie należy zasygnalizować, że uznając system monitoringu za przetwarzający dane osobowe, jego administrator zobowiązany będzie do realizacji obowiązków organizacyjno-technicznych określonych w ustawie o ochronie danych osobowych i rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy służące do przetwarzania danych osobowych*[52]. Zaznaczyć w tym miejscu należy, iż co najmniej problematyczne wydaje się spełnienie niektórych z regulacji przedmiotowego rozporządzenia – np. wygenerowanie raportu o konkretnej osobie, której wizerunek został zarejestrowany.

Bez względu na to czy uznamy system monitoringu wizyjnego za podlegający rygorom ustawy o ochronie danych osobowych czy też nie, to jednak musimy mieć świadomość ochrony jakiej podlega wizerunek każdego z nas, wynikający z konstytucyjnego prawa jednostki do prywatności. W związku z tym należy zastanowić się nad przesłankami prawnymi i faktycznymi dopuszczającymi stosowanie monitoringu wizyjnego, którego celem jest nadzór wizyjny nad osobami znajdującymi się w jego zasięgu. Do podstawowych z nich należy zaliczyć[53]:

1. Realizacja przepisu prawa rangi ustawy nakazującego obowiązkową rejestrację obrazu określonych obiektów lub wydarzeń, np. kasyna, imprezy masowe.
2. Szczególnie ważny, usprawiedliwiony cel podmiotu publicznego lub prywatnego (art. 23 ust. 1, pkt 5), np. polegający na zapewnieniu właściwego poziomu bezpieczeństwa samego obiektu, a także osób w nim przebywających.

[51] Sprawozdanie z działalności GIODO za rok 2003, s. 175.

[52] Dz.U. Nr 100, poz. 1024.

[53] Ł. Kister, *Prawne aspekty..., dz. cyt.*, s. 30.

3. Realizacja określonych prawem zadań dla dobra publicznego (art. 23 ust. 1, pkt 4), np. monitoring miejski przez służby powołane do zwalczania i zapobiegania działań sprzecznych z prawem.

Jednocześnie wydaje się, że nie możemy odwoływać się tutaj do głównej zasady dopuszczalności przetwarzania danych osobowych, jaką jest zgoda osoby, której dane dotyczą, gdyż w przypadku danych wrażliwych oświadczenie woli musi zachować formę pisemną i nie może być domniemane z treści innej deklaracji.

Jednak za najważniejszy obowiązek instytucji prowadzącej nadzór nad obszarem lub obiektem jest jednoznaczne poinformowanie (uświadomienie) osób, że przebywają na terenie objętym monitoringiem wizyjnym (wchodzą do niego), wraz z informacją, kto jest jego administratorem. A dodatkowo należy bezwzględnie respektować zasadę proporcjonalności, która oznacza, że stosowanie systemów wideonadzoru jest dopuszczalne, gdy inne środki prewencyjne i ochrona o charakterze fizycznym, niewymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania dla realizacji prawnie uzasadnionych celów.

W aspekcie legalności stosowanego wideonadzoru należy zastanowić się także, kto jest administratorem danych osobowych (wizerunków) zarejestrowanych przez kamery monitoringu, czyli kto w praktyce ponosi odpowiedzialność za zgodne z prawem ich przetwarzanie. Czy jest to agencja ochrony, której powierzono monitorowanie, czy może właściciel monitorowanego obiektu? W ustawie o ochronie danych osobowych jest mowa, że **administrator danych** to organ, jednostka organizacyjna, podmiot lub osoba, decydująca o cechach i środkach przetwarzania danych osobowych (art. 7 pkt 4). W każdym przypadku stosowania monitoringu administratorem danych z niego pochodzących jest właściciel monitorowanego obiektu lub zlecający monitoring. Agencja ochrony jest jedynie przetwarzającym, wykonującym czynności na zlecenie, nie decydując o celach i środkach przetwarzania. Nie wyklucza to jednak odpowiedzialności samej agencji i jej pracowników za niezgodne z prawem działania

lub zaniechania naruszające bezpieczeństwo przetwarzanych danych osobowych (wizerunków osób)[54].

Omawiając przepisy ustawy *o ochronie danych osobowych*, należy podkreślić, iż ustawodawca w art. 23 precyzuje zasady przetwarzania danych osobowych, które dopuszczalne jest tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,
4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

[54] Tamże, s. 31.

Pamiętać również należy, iż każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a w szczególności prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna – jej miejsca zamieszkania oraz imienia i nazwiska,
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej,
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Nie sposób pominąć przepisów rozdziału 8 ustawy *o ochronie danych osobowych*, który zawiera przepisy karne. A mianowicie:

Art. 49 – ***1.*** *Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

2. *Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność*

wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 51 – ***1.*** *Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

2. *Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

Art. 52 – *Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

Art. 53 – *Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

Art. 54 – *Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*

Art. 54a – *Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

Reasumując, podkreślić należy, iż prawo do prywatności nie ma absolutnego charakteru i podobnie jak inne prawa i wolności jednostki, może podlegać ograniczeniom. Ograniczenia te jednak muszą być sformułowane w sposób czyniący zadość wymaganiom konstytucyjnym, czyli ograniczenie praw jednostki może nastąpić tylko wówczas, gdy przemawia za tym norma, zasada lub wartość konstytucyjna, a stopień tego ograniczenia musi pozostać w odpowiedniej proporcji do rangi interesu, któremu ograniczenie to ma służyć[55].

[55] Zob. Orzeczenie Trybunału Konstytucyjnego z 24.06.1997 r. Sygn. akt K. 21/96

Rozdział 7.
Propozycje rozwiązań prawnych

Nie sposób, omawiając aspekty prawne związane z monitoringiem wizyjnym, nie przywołać w tym miejscu *Karty Demokratycznego Zastosowania Monitoringu Wizyjnego*, który to dokument, opracowany przez Europejskie Forum na Rzecz Bezpieczeństwa Miejskiego (*European Forum for Urban Security*), które jest organizacją pozarządową powstałą w 1987 z inicjatywy władz kilku miast europejskich. W chwili obecnej forum zrzesza ok. 300 europejskich miast, również polskich. Karta próbuje określić regulacje projektowania, wykorzystywania i rozwoju publicznych (miejskich) systemów monitoringu wizyjnego. Autorzy dokumentu podkreślają, że zaproponowane przez nich zasady są gwarancją demokratycznego stosowania systemów CCTV, a których zadaniem jest przeciwdziałanie tzw. dzikiemu rozwojowi monitoringu. Oto owe zasady:

1. Zasada legalizmu – projektowanie i rozwój systemu monitoringu wizyjnego może następować tylko w zgodzie z obowiązującym prawem i przepisami.
2. Zasada niezbędności – instalacja systemu monitoringu wizyjnego musi być uzasadniona.
3. Zasada proporcjonalności – projekt, instalacja, obsługa i późniejszy rozwój systemów monitoringu wizyjnego musi odbywać się rozsądnie i stosownie do potrzeb.
4. Zasada przejrzystości – władze, które wprowadzają miejski system monitoringu wizyjnego muszą mieć jasną i spójną strategię jego działania.
5. Zasada odpowiedzialności – prawo do prowadzenia obserwacji i rejestracji obrazu w przestrzeni publicznej za pomocą systemu monitoringu wizyjnego jest zarezerwowane dla wąskiej grupy, ściśle określonych podmiotów. Są one odpowiedzialne za systemy instalowane w ich imieniu.

6. Zasada niezależnej kontroli – aby utrzymać skuteczne działanie systemu monitoringu wizyjnego, należy wprowadzić wskaźniki skuteczności oraz kontrole (audyt).
7. Zasada udziału obywateli – należy dołożyć wszelkich starań, aby zachęcić obywateli do angażowania się w każdy etap funkcjonowania systemu monitoringu wizyjnego.

Według opinii GIODO przedstawionej w *Wymaganiach w zakresie regulacji monitoringu* 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 wizyjnego 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 *o ochronie danych osobowych* reguluje w sposób bardzo 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 wizyjnego. 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 *Konstytucji Rzeczypospolitej Polskiej.*

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.

GIODO stoi na stanowisku, iż 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.

Zakres przedmiotowy regulacji 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 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.

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.

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.

Literatura

Akty prawne

- Ustawa z dnia 23 kwietnia 1964 r. *Kodeks cywilny*, Dz.U. z 2014 r., poz. 121 z późn. zm.
- *Międzynarodowy Pakt Praw Obywatelskich i Politycznych*, ratyfikowany przez Polskę 18.03.1977 r., Dz.U. Nr 38, poz. 167.
- Ustawa z dnia 26 stycznia 1984 r. *o prawie prasowym,* Dz.U. Nr 5, poz. 24 z późn. zm.
- Ustawa z dnia 6 kwietnia 1990 r. *o Policji*, Dz.U. z 2011 r. Nr 287, poz. 1687 z późn. zm.
- *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* – ratyfikowana przez Polskę 19.01.1993 r., Dz.U. Nr 61, poz. 284.
- Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych*, Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. *w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*, Dz.U. L 281 z 23.11.1995.
- *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* Dz.U. Nr 78, poz. 483, z późn. zm.
- Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny wykonawczy*, Dz.U. Nr 90, poz. 557 z późn. zm.
- Ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia*, Dz.U. z 2014 r., poz. 1099.
- Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*, Dz.U. z 2014 r., poz. 1182.
- Ustawa z dnia 29 sierpnia 1997 r. *o strażach gminnych*, Dz.U. z 2013 r., poz. 1383 z późn. zm.
- Ustawa z dnia 12 września 2002 r. *o normalizacji*, Dz.U. Nr 169, poz. 1386 z późn. zm.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków*

technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy służące do przetwarzania danych osobowych, Dz.U. Nr 100, poz. 1024.
- Rozporządzenie Rady Ministrów z dnia 26 lipca 2005 r. *w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów,* Dz.U. Nr 141, poz. 1186.
- Rozporządzenie Rady Ministrów z dnia 6 września 2007 r. *w sprawie w sprawie form i zakresu finansowego wspierania organów prowadzących w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w publicznych szkołach i placówkach,* Dz.U. Nr 163, poz. 1155 z późn. zm.
- Ustawa z dnia 20 marca 2009 r. *o bezpieczeństwie imprez masowych*, Dz.U. z 2013 r., poz. 611 z późn. zm.
- Rozporządzenie Rady Ministrów z dnia 16 grudnia 2009 r. *w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską),* Dz.U. Nr 220, poz. 1720.
- *Karty Praw Podstawowych Unii Europejskiej*, Dz.U.UE z 30.3.2010 r. nr 2010/C 83/02.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 stycznia 2011 r. *w sprawie sposobu utrwalania przebiegu imprezy masowej,* Dz.U. Nr 16, poz. 73.
- Rozporządzenie Ministra Sprawiedliwości z dnia 14 września 2012 r. *w sprawie rodzaju urządzeń i środków technicznych służących do utrwalania obrazu lub dźwięku dla celów procesowych oraz sposobu przechowywania, odtwarzania i kopiowania zapisów*, Dz.U. z 2012 r., poz. 1090.
- Orzeczenie Trybunału Konstytucyjnego z 24.06.1997 r. Sygn. akt K. 21/96.
- Wyrok Trybunału Konstytucyjnego z dnia 20.04.2004 r. – K 45/02.

Publikacje zwarte

- Danilewicz W., *Prawne pojęcie wizerunku*, „Edukacja Prawnicza" nr 6 (117)/2010.
- GIODO, *Wymagania w zakresie regulacji monitoringu,* http://www.atosochrona.pl/wgrane_pliki/monitoring.pdf.

- Grzybowski S., *Ochrona dóbr osobistych według przepisów ogólnych Kodeksu cywilnego,* Warszawa 1957.
- Kister Ł., *Prawne aspekty dopuszczalności monitoringu wizyjnego – ochrona wizerunku osób,* „Ochrona Mienia i Informacji" nr 6/2010.
- Kosiarski M., *Ostrożnie udostępniajmy informacje o sobie. Rozmowa z Michałem Serzyckim* – GIODO, „Rzeczpospolita" z 10.11.2008.
- Kryszkiewicz M., *Zero prywatności dla niebezpiecznych więźniów*, „Gazeta Prawna" z 26.02.2009 r.
- Makosz A., *Informacje z ulicznych kamer poza kontrolą,* „Dziennik Gazeta Prawna" z 11.06.2010 r.
- Malinowski T., *Aspekty prawne a prawa dziecka w świetle zastosowania systemów monitoringu wizyjnego,* „Zabezpieczenia" nr 4/2011.
- Ordysińska M., *Aspekty prawne funkcjonowania systemów monitoringu wizyjnego w Polsce.* Cz. II. *Konwencje prawne funkcjonowania systemów monitoringu.* „Systemy Alarmowe" nr 5/2006.
- Ritterman S., *Komentarz do ustawy o prawie autorskim*, Kraków 1937.
- Waszkiewicz P., Wielki Brat. Rok 2010. *Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne,* Warszawa 2011.
- Sprawozdanie z działalności GIODO za rok 2000.
- Sprawozdanie z działalności GIODO za rok 2003.

Zakład Prewencji i Ruchu Drogowego

podinsp. Jacek Wróbel
nadkom. w st. spocz. Piotr Podsiedlik

Szkoła Policji w Katowicach
ul. gen. Jankego 276
40-684 Katowice-Piotrowice
www.katowice.szkolapolicji.gov.pl