

Piotr Mączyński*
Renata Płaszowska**

Prawo do prywatności oraz ochrona danych osobowych osób monitorowanych przez systemy monitoringu wizyjnego funkcjonujące w celu zapewniania bezpieczeństwa i porządku publicznego

W niniejszej pracy autorzy poruszają tematykę związaną z prawem do prywatności oraz ochroną osób monitorowanych objętych oglądem kamer systemów monitoringu wizyjnego funkcjonujących w celu zapewniania bezpieczeństwa i porządku publicznego. Wykorzystywanie systemów monitoringu wizyjnego, jako narzędzia usprawniającego wykonywanie zadań z zakresu zapewniania bezpieczeństwa i porządku, ma miejsce w związku z działalnością szeregu podmiotów publicznych. Z tego powodu, celem autorów jest przybliżenie czytelnikowi istniejących uregulowań stanowiących na poziomie międzynarodowym oraz konstytucyjnym. Z uwagi na konflikt, jaki zachodzi pomiędzy zapewnianiem bezpieczeństwa z wykorzystaniem kamer monitoringu wizyjnego a prawem do prywatności jednostek, a także okoliczność coraz powszechniejszego wykorzystywania tego rodzaju narzędzia, autorzy analizują również poziom doprecyzowania prawa do prywatności oraz ochrony danych osobowych na poziomie ustaw oraz aktów wykonawczych oraz podejmują próby oceny gwarancji tych praw. Ponadto, autorzy przybliżają czytelnikowi perspektywy dalszego rozwoju omawianych praw oraz ich gwarancji.

* Doktorant w Katedrze Socjologii Prawa Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego.

** Absolwentka administracji na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego.

1. Wstęp

Wraz z coraz szerszym zastosowaniem rozwijającej się technologii, nieuchronnie spotykamy się z problemem możliwie pełnej realizacji prawa do prywatności oraz ochrony danych osobowych. Problem ten autorzy pragną przedstawić na przykładzie osób monitorowanych przez systemy monitoringu wizyjnego, które funkcjonują w celu zapewnienia bezpieczeństwa i porządku publicznego. Mianem systemu monitoringu wizyjnego określa się system umożliwiający rejestrację i obserwację zdarzeń z odległości, za pomocą kamer, z których obraz jest transmitowany do centrum odbiorczego (w którym może następować wyłącznie rejestracja obrazu, jak również bieżący jego ogląd przez operatora)¹. Takie określenie przedmiotu analizy uzasadnione może być co najmniej kilkoma przyczynami. Przede wszystkim, zwraca się uwagę, że w przypadku prawie 90% polskich miast wykorzystywane są kamery służące obserwacji lub rejestracji obrazu; jednocześnie w znakomitej większości są to kamery zintegrowane w ramach systemów monitoringu wizyjnego². Rosnąca popularność systemów monitoringu wizyjnego spowodowana może być przede wszystkim zmniejszającymi się kosztami instalacji kamer, przy jednoczesnej poprawie ich parametrów technicznych. Ponadto, nie ulega wątpliwości, że – abstrahując od aspektów prewencyjnych – zgromadzony za pośrednictwem kamer materiał może ułatwiać pracę służbom i strażom. Warto jednocześnie zauważyć, że wraz z postępem technologicznym zwiększają się także możliwości wykorzystywania monitoringu wizyjnego do innych celów. Integrowanie wielu funkcjonalności w ramach jednego systemu może być czynnikiem, mającym istotny wpływ na decyzję o budowie nowych lub rozbudowie istniejących systemów.

¹ Szerzej na temat możliwości definiowania systemów monitoringu wizyjnego i historii ich zastosowania w Polsce: P. Waszkiewicz, *Wielki brat. Rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne*.

² Fundacja Panoptykon, *Monitoring w polskich miastach w oczach społeczeństwa*, wyniki analiz danych dotyczących miejskiego monitoringu wizyjnego otrzymanych od 335 miast w efekcie wniosków o udostępnienie informacji publicznej, s. 1. Dane na rok 2012.

Wykorzystywanie systemów monitoringu wizyjnego, jako narzędzia usprawniającego wykonywanie zadań z zakresu zapewniania bezpieczeństwa i porządku publicznego, ma miejsce w związku z działalnością szeregu podmiotów – mniej lub bardziej wyspecjalizowanych. Nie chcąc koncentrować rozważań na opisie i analizie istniejących definicji bezpieczeństwa i porządku publicznego, a także demarkacji różnych rodzajów bezpieczeństwa, na potrzeby niniejszego rozdziału autorzy przyjmują definicję nawiązującą do zadań podmiotów, które monitoring wykorzystują.

Analizując krajowe regulacje na poziomie ustawowym i podustawowym przyjąć pragniemy, iż rozważania na temat ochrony danych osobowych obejmować będą okres od momentu rejestracji obrazu, poprzez cały proces dalszego przetwarzania danych, do momentu ich zniszczenia. Warto jednocześnie zauważyć, że mówiąc o ochronie prawa do prywatności, pod uwagę – oprócz wskazanych wyżej – należy wziąć także procesy wcześniejsze, związane chociażby ze sposobem instalacji i lokalizacją kamer, a także z realizacją obowiązków informacyjnych, mających na celu uświadomienie osób monitorowanych o przebywaniu w zasięgu oglądu kamer oraz celów, dla jakich one funkcjonują

Wykorzystywanie systemów monitoringu wizyjnego w celu zapewniania bezpieczeństwa i porządku publicznego będzie miało miejsce w każdym wypadku, w którym jest to dokonywane w związku z ustawowo określonymi zadaniami, których realizacja ma – w zamierzeniu podmiotu wykonującego – sprzyjać poprawie stanu bezpieczeństwa i porządku publicznego.

Niemniej, w związku z coraz powszechniejszym wykorzystywaniem systemów monitoringu wizyjnego pojawia się jednak szereg zagrożeń. Czy bowiem jednostki monitorowane w imię bezpieczeństwa nie są pozbawiane prywatności? Czy osoby takie zawsze są świadome tego, że znajdują się w zasięgu oglądu kamery?

W niniejszej pracy, przedmiotem zainteresowania autorów nie jest ocena woli korzystania przez jednostki z prawa do prywatności, a co za tym idzie z ochrony danych osobowych. Naszym zadaniem jest określenie zakresu regulacji (międzynarodowych oraz konstytucyjnych, a także ustaw i aktów wykonawczych stanowiących na ich podstawie) relevant-

nych dla określenia zakresu uprawnień oraz oceny rzeczywistych gwarancji ich zastosowania. Oceniając obowiązujący porządek prawny skupić należy się analizie, na ile deklaracje zawarte w prawie międzynarodowym i Konstytucji RP są realizowane na poziomie ustaw i rozporządzeń. Innymi słowy, ocenić trzeba czy obecnie istniejące regulacje w wystarczającym stopniu realizują postawione przed nimi cele. Dokonanie tego zabiegu pozwoli na podjęcie próby zarysowania perspektyw dla dalszego rozwoju gwarancji poszanowania tych praw. Wydaje się bowiem, że w obowiązującym porządku prawnym brak jest wystarczających gwarancji - czy to materialnoprawnych, czy też proceduralnych - dla skutecznego korzystania z prawa do prywatności oraz ochrony danych osobowych przez osoby objęte oglądem kamer wchodzących w skład systemów monitoringu wizyjnego.

2. Regulacje międzynarodowe

Najstarszym i najbardziej ogólnym aktem o zasięgu międzynarodowym, poruszającym kwestię prawa do prywatności jest Konwencja Rady Europy o Ochronie Praw Człowieka i Podstawowych Wolności, która weszła w życie w 1953 roku³. Konwencja ta jest w rzeczywistości umową międzynarodową, której podpisanie jest przesłanką warunkującą członkostwo w Radzie Europy. Konwencja wymienia szeroki katalog praw i wolności, których państwa podpisujące umowę zobowiązują się przestrzegać i chronić. Z owych praw i wolności mogą korzystać wszystkie osoby pozostające pod jurysdykcją państw, które Konwencję podpisały, a więc nie tylko ich obywatele. Fakt ten jest szczególnie istotny dla rozważań na temat ochrony prywatności osób w związku zastosowaniem monitoringu wizyjnego, gdyż oznacza to, że postanowienia konwencji chronią na równi prawa wszystkich osób znajdujących się „pod okiem” monitoringu wizyjnego w danym kraju bez względu na ich obywatelstwo.

Choć Konwencja jest aktem raczej o charakterze kompleksowym, katalog praw i wolności w niej zawarty nie jest wyczerpujący (proces jej

³ Konwencja o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r., Dz.U. z 1993 r., Nr 61, poz. 284 z późn. zm.

uzupełniania poprzez tworzenie dodatkowych protokołów ciągle trwa) a jej przepisy, choć obowiązują bezpośrednio, choćby ze względu na swój ogólny charakter dla swej skuteczności wymagają wdrożenia do prawa krajowego przez uchwalenie konkretnych regulacji ustawowych. Konwencja jest aktem wyróżniającym się spośród innych źródeł prawa międzynarodowego nie tylko z tego powodu, że jej postanowienia dotyczą najistotniejszych praw i wolności człowieka, ale przede wszystkim ze względu na to że ustanawia unikalną procedurę kontroli, w postaci skargi międzypaństwowej i skargi indywidualnej, pozwalającą na żądanie zaprzestania naruszania praw, przywrócenia stanu zgodnego z nimi, a także przyznanie odpowiedniego zadośćuczynienia finansowego osobom poszkodowanym, co stanowi gwarancję ochrony przestrzegania postanowień konwencji.

W odniesieniu do kwestii związanych ochroną prywatności w związku zastosowaniem monitoringu wizyjnego najistotniejsze znaczenie ma przepis art. 8 Konwencji, zgodnie z którym każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji, a wszelkie przypadki ingerencji władzy publicznej w korzystanie z tego prawa muszą być określone przepisami o randze ustawowej i uzasadnione koniecznością warunkowaną bezpieczeństwem państwowym, bezpieczeństwem publicznym lub dobrobytem gospodarczym kraju, ochroną porządku i zapobieganiem przestępstwom, ochroną zdrowia lub moralności lub ochroną praw i wolności innych osób⁴. Jak widać regulacja ta jest pełną pojęć nieostrych, nie stanowi ona konkretnego źródła praw i obowiązków, a jedynie wytyczną wyznaczającą kierunek w jakim ma się udać ustawodawca tworząc prawo krajowe.

Spośród międzynarodowych konwencji, aktem o bardziej konkretnym znaczeniu w sprawie ochrony danych osobowych jest Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób

⁴ Szerzej na temat ingerencji władz publicznych w korzystanie z prawa do prywatności: P. Hofmański, *Prawo do poszanowania prywatności a rozwiązania polskiego prawa karnego materialnego i procesowego*, [w:] J. Skupiński (red.), *Standardy praw człowieka a polskie prawo karne*, wyd. SCHOLAR, Warszawa 1995, s. 253-254.

w Związku z Automatycznym Przetwarzaniem Danych Osobowych⁵. Nie ulega wątpliwości, iż jej przepisy powinny mieć zastosowanie w odniesieniu do regulacji dotyczących monitoringu wizyjnego, co znajduje potwierdzenie w opinii Komitetu Doradczego (powołanego na podstawie przepisów Konwencji), zgodnie z którą za dane osobowe uznaje się rejestr głosu i obrazu, który nawet niebezpośrednio pozwala na identyfikację osoby figurującej w rejestrze. Konwencja ta, podobnie jak Konwencja Rady Europy o Ochronie Praw Człowieka i Podstawowych Wolności, nie zawiera bezpośrednich instrumentów i regulacji chroniących dane osobowe, ale ustala wytyczne w jakim kierunku powinno zmierzać ustawodawstwo krajów członkowskich. Konwencja ta również, tak samo jak poprzednio omawiany akt, koncentruje się nie tylko na prawach obywateli krajów podlegających jej przepisom, ale na prawach każdego, kto przebywa na terenie tych państw niezależnie od obywatelstwa.

Przepisy tej Konwencji nakładają na kraje członkowskie wprost obowiązek stworzenia ustawodawstwa w zakresie ochrony danych osobowych oraz określa zasady na jakich ta ochrona powinna się odbywać. Odnoszą się one głównie do rzetelnego i zgodnego z prawem pozyskiwania i przetwarzania danych osobowych, wykorzystywania ich wyłącznie do uzasadnionych celów, a także gromadzenia ich przez tylko taki okres, który jest konieczny ze względu na cel, w jakim są one gromadzone. Postanowienia konwencji kładą też nacisk na wymóg ochrony zgromadzonych danych przed dostępem do nich osób nieupoważnionych oraz zapobieżenia ich zniszczeniu. Ponadto Konwencja w odniesieniu do pewnych wyjątkowo wrażliwych danych, takich jak na przykład stan zdrowia, czy pochodzenie rasowe, wprowadza środki szczególnej ochrony, ustanawiając zakaz przetwarzania tych danych w sposób automatyczny, jeśli prawo wewnętrzne nie zapewnia im odpowiedniej ochrony.

Konwencja nakazuje krajom członkowskim nadanie pewnych szczególnych uprawnień osobom, których dane gromadzi. Mianowicie, zgodnie z przepisami Konwencji osoby, których dane figurują w zbiorach mu-

⁵ Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r., Dz.U. z 2003 r., Nr 3, poz. 25.

szą mieć zagwarantowane prawo uzyskania informacji o istnieniu takiego zbioru oraz możliwość wglądu do danych zebranych na ich temat, a w przypadku gdy dane zostały przetworzone z naruszeniem prawa, sprostowania ich lub usunięcia. Osobie której odmówiono realizacji wyżej wymienionych uprawnień, zgodnie z konwencją przysługuje prawo do złożenia skargi.

Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych zawiera tylko podstawowe normy i zasady ochrony przed nadużyciami ze strony podmiotów gromadzących dane, jakimi kierować ma się ustawodawca krajowy tworząc regulacje prawne w tej dziedzinie. Na skutek tego na przestrzeni lat doszło do znacznych rozbieżności w ustawodawstwach państw członkowskich UE. W celu ich ujednoczenia 24 października 1995 roku została wydana Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych⁶. Dyrektywa ta narzuca konkretne rozwiązania dotyczące przetwarzania danych osobowych, które mają zapewnić podstawowy, jednolity dla państw członkowskich poziom ochrony gromadzonych danych osobowych oraz zapewnienie swobodnego ich przepływu pomiędzy krajami członkowskimi.

Jednym z ważniejszych postanowień Dyrektywy jest wprowadzenie zamkniętego katalogu kryteriów legalności przetwarzanych danych. Do przypadków stanowiących podstawę do zgodnego z prawem przetwarzania danych należą sytuacje, gdy osoba, której dane dotyczą jednoznacznie wyraziła na to zgodę lub sytuacje, w których przetwarzanie danych jest konieczne dla:

- realizacji umowy, której stroną jest osoba, której dane dotyczą lub w celu podjęcia działań na życzenie osoby, której dane dotyczą przed zawarciem umowy lub
- zgodności z zobowiązaniem prawnym, któremu administrator danych podlega lub
- ochrony żywotnych interesów osoby, której dane dotyczą lub

⁶ Dyrektywa Parlamentu Europejskiego i Rady (95/46/WE) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych, Dz. Urz. WE L 281, z 23 listopada 1995 r., z późn. zm.

- realizacji zadania wykonywanego w interesie publicznym lub dla sprawowania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane lub
- potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, przed którą ujawnia się dane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą.

Jak wynika z powyższych przetwarzanie danych jest legalne jeśli osoba której dane dotyczą wyrazi na to zgodę lub gdy występuje taka konieczność ze względu na ochronę jedynie dóbr i interesów wysokiej wartości takich jak interes publiczny, zobowiązanie prawne, żywotne interesy osoby, której dane dotyczą.

W odniesieniu do monitoringu wizyjnego istotne znaczenie ma regulacja, zgodnie z którą postanowienia Dyrektywy obowiązują jedynie w zakresie, w jakim nie dotyczą przetwarzania danych w formie dźwięku i obrazu, wykonywanego dla celów bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego. Dziedziny te nie wchodzą bowiem w zakres zastosowania prawa wspólnotowego. Warto zauważyć, iż nie stoi to na przeszkodzie aby polski ustawodawca implementując przepisy dyrektywy zastosował zasady w niej zawarte również w odniesieniu do nagrań sporządzonych za pomocą monitoringu wizyjnego również w celach bezpieczeństwa i porządku publicznego.

Omawiając przepisy Dyrektywy Parlamentu Europejskiego i Rady (95/46/WE) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych, nie można pominąć przepisu art. 29 tej Dyrektywy, na mocy którego została utworzona Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, złożona z przedstawicieli organów nadzorczych, powołanych przez każde z Państw Członkowskich, przedstawiciela organu lub organów ustanowionych dla instytucji i organów wspólnotowych oraz przedstawiciela Komisji, powoływanych przez instytucję, organ lub organy, które reprezentuje. Do zadań Grupy należy między innymi badanie kwestii dotyczących stosowania krajowych środków przyjętych na mocy omawianej dyrektywy, w celu przyczynienia się do

jednolitego stosowania tych środków i wydawanie opinii w sprawie istniejącego poziomu ochrony danych osobowych w krajach wspólnoty jak i poza Unią, postulowanie Komisji potrzebnych zmian w przepisach Dyrektywy lub dodatkowych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych, a wreszcie wydawanie, z własnej inicjatywy, zaleceń we wszystkich sprawach dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych we Wspólnocie.

Nie ulega wątpliwości jak duże znaczenie w dobie tak dynamicznie rozwijających się możliwości technicznych ma istnienie niezależnego organu doradczego Komisji zajmującego zagadnieniami związanymi z ochroną danych osobowych mającego możliwość bieżącego badania stanu prawnego i postulowania dostosowywania przepisów prawa do zmieniających się warunków. Rola sukcesywnego uaktualniania stanu prawnego w odpowiedzi na zmieniającą się rzeczywistość jest szczególnie istotna przede wszystkim w dziedzinach, w których rozwój technologiczny ma podstawowe znaczenie, do których bez wątpienia należy kwestia monitoringu wizyjnego.

W odniesieniu do zagadnień związanych z monitoringiem wizyjnym, pośród aktów prawa międzynarodowego nie można również pominąć Karty Praw Podstawowych Unii Europejskiej⁷. Postanowienia Karty w zakresie ochrony danych osobowych powielają regulacje zawarte w powyżej omawianych aktach, ale także nieco je precyzują. Zgodnie treścią przepisów Karty każdy ma prawo do ochrony danych osobowych, które go dotyczą. Ochrona ta ma polegać między innymi na tym, iż dane muszą być przetwarzane rzetelnie i w określonych celach oraz za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Ponadto każda osoba (więc znów nie tylko obywatele krajów członkowskich, ale każdy człowiek) ma prawo do dostępu do zebranych danych, które go dotyczą, i prawo do dokonywania ich sprostowania. Przestrzeganie powyższych wytycznych powinno podlegać kontroli niezależnego organu. Ponadto Karta podkreśla, istnienie prawa należnego każdemu do poszanowania życia prywatnego i rodzinnego, domu i ko-

⁷ Karta Praw Podstawowych Unii Europejskiej (2012/C 326/02), Dz. Urz. UE C z 26 października 2012 r.

munikowania się. W tym miejscu warto zauważyć tendencję do wychodzenia na przeciw zmianom, jakie przynoszą nowe technologie, której przykładem jest zastąpienie pojawiającego się w starszych aktach słowa „korespondencja” pojęciem szerszym „komunikowanie się”.

Zgodnie z obowiązującą hierarchią źródeł prawa, polski ustawodawca, tworząc prawo o randze ustawy lub implementując przepisy unijne, oprócz regulacji międzynarodowych musi brać pod uwagę również brzmienie przepisów Ustawy Zasadniczej.

Prawo do prywatności jest silnie związane z jedną z podstawowych wartości chronionych konstytucyjnie, a mianowicie z wolnością człowieka. Art. 31 Konstytucji RP uznaje wolność człowieka za wartość podlegającą ochronie prawnej, co oznacza, że w świetle prawa każdy jest zobowiązany szanować wolności i prawa innych. Z literalnego brzmienia przepisu wynika, iż nakaz poszanowania wolności człowieka, dotyczy zarówno innych osób jak i organów i instytucji państwowych. Oczywistym jest, iż fakt że wolność człowieka podlega ochronie konstytucyjnej, nie oznacza, iż nie może ona mieć żadnych limitów. Ograniczenia wolności mogą być ustanawiane tylko w drodze ustawy i tylko z przyczyn wskazanych w omawianym przepisie, ponadto nie mogą naruszać istoty wolności i praw, co z resztą wynika ze słownikowej definicji użytego przez ustawodawcę określenia „ograniczenie”, w kontraście np. do pojęcia „pozbawienie”. W myśl art. 31 § 3 dopuszczalne jest ograniczenie wolności, wtedy kiedy jest to 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 zasadzie każda z powyższych przesłanek może mieć zastosowanie dla zagadnień związanych z monitoringiem wizyjnym. Warto zwrócić jednak uwagę na użycie przez ustawodawcę sformułowania „gdy są konieczne”, oznacza to wprowadzenie zasady proporcjonalności, która nakazuje organom państwowym użycie jedynie takich środków, które są niezbędne dla osiągnięcia konkretnego celu. Oznacza to, że organy państwowe mają osiągać cel, który służy społeczeństwu, jak najmniejszym kosztem dla poszczególnych jednostek (jak i całego społeczeństwa). Zasada proporcjonalności w tym przypadku zakazuje nadmiernej ingerencji państwa w wolność człowieka.

Samo prawo do prywatności jest również jednym z podstawowych praw obywatela, podlega zatem ochronie konstytucyjnej. Zgodnie z brzmieniem art. 47 Konstytucji każdy ma prawo do prawnej ochrony życia prywatnego, rodzinnego czci i dobrego imienia oraz do decydowania o swoim życiu. Nie sposób nie zwrócić uwagi na to, do jak wysokiej rangi podniesiona zostaje ochrona życia prywatnego, poprzez postawienie jej w jednym przepisie z wartościami nadrzędnymi dla godności ludzkiej jak ochrona czci i dobrego imienia. Kwestia ochrony prywatności pojawia się również w treści przepisu art. 51 Konstytucji, zgodnie z którym władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać informacji o obywatelach innych niż te niezbędne w demokratycznym państwie prawnym. A zasady i tryb ich gromadzenia określać ma ustawa. Każdy ma prawo do dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, a jedyne ograniczenie tego prawa może nastąpić tylko drogą ustawową. Ponadto każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych i zebranych w sposób sprzeczny z ustawą. Jak widać postanowienia Konstytucji odpowiadają najważniejszym postanowieniom aktów prawa europejskiego w tej dziedzinie.

Jak już zostało kilkakrotnie podkreślane, adresatami prawa do prywatności w świetle przepisów unijnych jest każdy człowiek. Nasza Konstytucja, poza jednym wyjątkiem nie odbiega o tej zasady. Zawarty w art. 47 zakaz gromadzenia i udostępniania informacji innych niż te niezbędne w demokratycznym państwie prawnym przez władze publiczne dotyczy tylko danych obywateli, natomiast kolejne przepisy komentowanego artykułu odnoszą się już do wszystkich, o czym świadczy użycie pojęcia „każdy”. Wprowadzenie takiego odróżnienia jest co najmniej zastanawiające. Zdaniem autorów, w związku z treścią przedstawianych wcześniej aktów prawa międzynarodowego oraz z dopuszczalnością stosowania rozszerzającej interpretacji zasad konstytucyjnych, tworząc regulacje ustawowe w oparciu o omawiany przepis należy odnosić zawarte w nim wytyczne nie tylko do obywateli, ale do wszystkich podmiotów prawa. Za przyjęciem takiego stanowiska przemawia również nieostrość pojęcia „informacje niezbędne w demokratycznym państwie prawnym”, w połączeniu z ogólną zasadą subsydiarności wyrażoną w Preambule do

Konstytucji, zgodnie z którą organy władzy państwowej powinny działać tylko wtedy gdy są niezbędne. Taka wykładnia zdaje się szczególnie zasadna w odniesieniu do zagadnień związanych prawem do prywatności osób monitorowanych za pomocą systemu monitoringu wizyjnego.

Przed przystąpieniem do analizy konkretnych regulacji ustawowych odnośnie prawa do prywatności i ochrony danych osobowych osób monitorowanych, warto skupić uwagę na jeszcze jednym akcie o charakterze ogólnym, a mianowicie na Karcie Demokratycznego Zastosowania Monitoringu Wizyjnego⁸, opracowanej przez Europejskie Forum Bezpieczeństwa Miast (European Forum for Urban Security). Karta ta nie jest aktem prawa powszechnie obowiązującego, jest adresowana przede wszystkim do władz publicznych prowadzących systemy monitoringu wizyjnego, ale jej przepisy są jednak na tyle uniwersalne, iż z powodzeniem wytycznymi w niej zawartymi mogą się kierować się zarówno podmioty prywatne wdrażające system monitoringu wizyjnego, jak i ustawodawca krajowy w procesie tworzenia prawa. Karta przedstawia siedem uniwersalnych zasad spośród których każdą w pewnym stopniu można odnieść do ochrony prywatności i ochrony danych osobowych. W świetle przepisów Karty zasady demokratycznego zastosowania monitoringu wizyjnego są następujące:

- Zasada legalności, zgodnie z którą projektowanie i rozwój systemów monitoringu powinny przebiegać zgodnie z obowiązującym prawem. Jako źródła owego prawa Karta w szczególności wymienia wszystkie akty prawa międzynarodowego omawiane w niniejszej pracy, stąd też oczywiste jest, że odnosi się również do przytoczonych przepisów chroniących prywatność i dane osobowe.
- Zasada niezbędności, według której tak silna ingerencja w prywatność jednostek jak zastosowanie monitoringu wizyjnego powinna być dopuszczalna wyłącznie w sytuacjach w których efektywna realizacja zamierzonego celu nie jest możliwa z wykorzystaniem innych środków.

⁸ Karta została opracowana w ramach projektu *Obywatele, miasta i monitoring wizyjny*. Całość jej postanowień w polskim przekładzie znaleźć można na stronie: http://www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_PL.pdf. Dostęp: 30 sierpnia 2015 r.

- Zasada proporcjonalności, zgodnie z którą zakładany system monitoringu wizyjnego powinien odbywać się wyłącznie na skalę nie szerszą niż adekwatna do potrzeb.
- Zasada przejrzystości – moim zdaniem jedna z najbardziej interesujących zasad, która została poruszona już w Karcie Podstawowych Praw Unii Europejskiej. Zgodnie z nią akcja wprowadzania monitoringu miejskiego powinna być połączona z akcją informacyjną. Mieszkańcy powinni być informowani co do celów systemu, jego kosztów, ale też (co w przedmiocie ochrony prywatności ma znaczenie szczególnie istotne) co do obszarów objętych monitoringiem, sposobie ochrony zapisanych nagrań i przede wszystkim prawa dostępu do nagrań. W świetle wcześniejszych rozważań uznać należy, iż istotne jest aby postulat informowania rozszerzyć z grona mieszkańców, na wszystkich wkraczających w obszar obserwacji monitoringu wizyjnego.
- Zasada odpowiedzialności – ograniczająca prawo do prowadzenia obserwacji i rejestracji obrazu w przestrzeni publicznej za pomocą systemu monitoringu wizyjnego dla ściśle określonych podmiotów.
- Zasada niezależnej kontroli – sugeruje konieczność przeprowadzania kontroli przez niezależny i wyspecjalizowany podmiot, posiadający wykwalifikowanych pracowników. Zdaniem autorów, jest to druga spośród szczególnie interesujących zasad, ze względu na to, iż postuluje również udział w przeprowadzaniu kontroli również dla przedstawicieli mieszkańców.
- Zasada udziału obywateli – zasada rozszerza powyższy postulat sugerując konieczność umożliwienia mieszkańcom wyrażenia stanowiska w sprawie monitoringu wizyjnego poprzez różne formy konsultacji a nawet partycypacji w podejmowanych decyzjach.

3. Regulacje krajowe

Przesądzenie, czy obraz zarejestrowany przez kamerę monitoringu wizyjnego może stanowić dane osobowe wymaga kilku słów komentarza. Zgodnie bowiem z art. 6 ustawy o ochronie danych osobowych⁹, za dane osobowe poczytuje się wszelkie informacje dotyczące osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania, tj. takiej 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. Jednocześnie zwrócić należy uwagę na – wprowadzone w 2001 r. - wyłączenie wyrażone w ust. 3 komentowanego przepisu, które stanowi, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Przesłanki te mają charakter nieostry, co podkreśla się w doktrynie wskazując, że jej rzeczywiste znaczenie zostanie dopiero ukształtowane przez rozstrzygnięcia Generalnego Inspektora Ochrony Danych Osobowych dotyczące konkretnych spraw¹⁰. Jednocześnie należy mieć świadomość, iż odnośnienie się do ustawy o ochronie danych osobowych w przypadku systemów monitoringu wizyjnego może sprawiać problemy z uwagi na konieczność odpowiedniego stosowania jej przepisów do specyficznego rodzaju danych, jakim jest zapis obrazu.

Na korzyść stanowiska uznającego obrazy zarejestrowane przez systemy monitoringu wizyjnego za dane osobowe przemawiają także rozstrzygnięcia sądów i trybunałów. Wojewódzki Sąd Administracyjny w Warszawie wprost stwierdził, że system monitoringu wizyjnego, pozwalając na identyfikację osób, jest zbiorem danych osobowych i podlega przepisom ustawy o ochronie danych¹¹. W podobnym tonie wypowie-

⁹ Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2014 r., poz. 1182.

¹⁰ J. Barta, *Komentarz do art. 6 ustawy o ochronie danych osobowych*, w: J. Barta, P. Fajgielski, R. Markiewicz (red.), *Ochrona danych osobowych. Komentarz*, LEX, Warszawa 2011.

¹¹ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 9 lipca 2014 r., sygn. II SA/Wa 2393/13, *Rzeczposp. PCD 2014/159/1*.

dział się Trybunał Sprawiedliwości wskazując, że możliwa do zidentyfikowania osoba w rozumieniu Dyrektywy 95/46 to „osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na [...] jeden bądź kilka szczególnych czynników określających jej fizyczną [...] tożsamość”, wobec czego obraz osoby zarejestrowany przez kamerę monitoringu wizyjnego stanowi dane osobowe w rozumieniu Dyrektywy, o ile pozwala on na ustalenie tożsamości danej osoby¹².

Uznanie obrazu zarejestrowanego przez kamerę funkcjonującą w systemie monitoringu wizyjnego za dane osobowe niesie za sobą daleko idące konsekwencje. Wiąże się to z jednej strony z szeregiem obowiązków administratorów systemów monitoringu wizyjnego wynikających z faktu przetwarzania danych osobowych, wyrażonych w ustawie o ochronie danych osobowych, a także – na co warto zwrócić uwagę – w rozporządzeniu Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych¹³. Ponadto, związane jest to także z szerokimi uprawnieniami osób, których dane są przetwarzane. W grę wchodzi zatem przede wszystkim uprawnienie do kontroli przetwarzanych danych wyrażone w art. 32 ust. 1 ustawy o ochronie danych osobowych, tj. m.in.:

- prawo do uzyskania informacji dot. istnienia takiego zbioru oraz danych jego administratora;
- prawo do uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w zbiorze danych.

Ponadto, przepis ten stanowi uprawnienie takiej osoby do uzyskania „w powszechnie zrozumiałej formie treści tych danych”. W związku ze wspomnianą już koniecznością odpowiedniego stosowania ustawy o ochronie danych osobowych do systemów monitoringu wizyjnego, należy poważnie zastanowić się, w jaki sposób administrator miałby realizować ten obowiązek. Albowiem w obowiązującym porządku prawnym

¹² Wyrok Trybunału Sprawiedliwości z 11 grudnia 2014 r., sygn. C-212/13, LEX nr 1551850.

¹³ Rozporządzenie Parlamentu Europejskiego i Rady z 12 marca 2014 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

brak jest przepisów szczególnych, które regulowałyby dostęp osób monitorowanych do ich danych przetwarzanych w ramach systemów monitoringu wizyjnego. Pozwala to zatem przyjąć, iż uprawnienie takiej osoby istnieje w przypadku funkcjonowania każdego systemu, który pozwala na jej zidentyfikowanie. Korzystanie z tego uprawnienia następuje zatem w oparciu o odpowiednio stosowaną ustawę o ochronie danych osobowych.

Niewątpliwie, biorąc pod uwagę coraz częstsze zastosowanie systemów monitoringu wizyjnego, szerokie zastosowanie ustawy o ochronie danych osobowych wobec administratorów tych systemów jest pożądane. Postulat ten jest również związany z niedostatkiem (a *de facto* brakiem) regulacji szczegółowych, które dopuszczając wykorzystywanie zdalnej rejestracji i obserwacji obrazów przez poszczególne podmioty publiczne, jednocześnie zapewniałyby pełną realizację praw jednostki.

Warto w tym miejscu zasygnalizować, iż wizerunek osoby podlega ochronie również na gruncie Kodeksu cywilnego. Art. 23 przywołanej ustawy stanowi, że dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Warto jednak zaznaczyć, iż z perspektywy funkcjonowania instytucji publicznych prowadzących monitoring wizyjny, gwarancje wyrażone w art. 23 Kodeksu cywilnego (doprecyzowane w art. 24), a także w art. 81 ustawy o prawie autorskim i prawach pokrewnych¹⁴ (traktującym o ochronie przed nieuprawnionym rozpowszechnianiem wizerunku osoby) wydają się być dalece niewystarczające. Albowiem od podmiotów publicznych, w tym także tych, które podejmują działania w celu zapewniania bezpieczeństwa i porządku publicznego, oczekuje się szczególnej dbałości o realizację konstytucyjnie gwarantowanych praw jednostki.

Z tego też powodu elementem niezwykle istotnym dla analizy krajowych gwarancji dla realizacji prawa do prywatności oraz ochrony da-

¹⁴ Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U. z 2006 r., Nr 90, poz. 631 z późn. zm.

nych osobowych osób monitorowanych przez systemy monitoringu wizyjnego funkcjonujące w celu zapewniania bezpieczeństwa i porządku publicznego jest określenie podstaw prawnych, z których wywodzone są uprawnienia organów publicznych do prowadzenia monitoringu wizyjnego. Zgodnie z wyrażoną w art. 7 Konstytucji zasadą praworządności, organy władzy publicznej mogą działać tylko tam i o tyle, o ile prawo je do tego upoważnia, co jest z kolei zgodne z wymogami wynikającymi z zasady demokratycznego państwa prawnego¹⁵. Oznacza to, iż podmiot publiczny wykorzystujący system monitoringu wizyjnego powinien mieć ku temu odpowiednie umocowanie. Niedopuszczalne jest bowiem domniemanie kompetencji władzy publicznej w zakresie ingerencji w wolność jednostki, w tym także w jej prawo do prywatności¹⁶.

Expressis verbis uprawnienie do prowadzenia monitoringu wizyjnego – a więc do obserwacji i rejestracji obrazów za pomocą środków technicznych – przewidziano w przypadku regulacji dotyczących działalności szeregu służb i straży¹⁷. W każdym z tych przypadków, ustawodawca zdecydował się na delegację uprawnienia do doprecyzowania tych regulacji przez właściwego ministra, bądź Radę Ministrów w drodze rozporządzenia. Regulacje te w dużej mierze odnoszą się do zagadnień związanych z przechowywaniem, niszczeniem oraz udostępnianiem zapisanych nagrań uprawnionym podmiotom. Spośród wspomnianych wcześniej aktów wykonawczych, pragniemy bliżej skupić się na dwóch z nich – dotyczących Policji oraz straży gminnych – z uwagi na fakt, iż są to

¹⁵ W. Skrzydło, *Komentarz do art. 7 Konstytucji*, [w:] W. Skrzydło (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, LEX, Warszawa 2013.

¹⁶ Wyrok Trybunału Konstytucyjnego z 30 lipca 2014 r., Sygn. akt K 23/11. W orzeczeniu tym Trybunał za niekonstytucyjne uznał przepisy umożliwiające m.in. Policji posługiwaniem się retencją danych komunikacyjnych, nie gwarantujące jednocześnie niezależnej kontroli ich udostępniania, a także nie regulujące niezwłocznego, komisijnego i protokolarnego zniszczenia wszelkich materiałów, które zawierają informacje objęte zakazami dowodowymi.

¹⁷ Są to przede wszystkim: ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz.U. z 2015 r., poz. 355; ustawa z dnia 12 października 1990 r. o Straży Granicznej, Dz.U. z 2014 r., poz. 1402; ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych, Dz.U. z 2013 r., poz. 1383; ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, Dz.U. z 2010 r., Nr. 29, poz. 154; ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. z 2014 r., poz. 253; ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz.U. z 2014 r., poz. 1411.

podmioty wykorzystujące monitoring wizyjny w relatywnie największym zakresie.

Zgodnie z art. 15 ust. 1 pkt 5a, Policja wykonując czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe ma prawo obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych podejmowanych na podstawie ustawy - także i dźwięku towarzyszącego tym zdarzeniom. Zwrócić należy jednocześnie uwagę, iż możliwość rejestracji obrazu może być rozszerzona o rejestrację dźwięku, co w znaczący sposób może ingerować w prywatność osób obserwowanych. Ponadto, możliwość rejestracji i archiwizowania dźwięku wydaje się powodować, iż taki system nie mieści się w przyjętej definicji systemu monitoringu wizyjnego (należy w tym miejscu poczynić zastrzeżenie, iż istnieją systemy aktywowane akustycznie – jednakże nie służą one archiwizacji zarejestrowanego dźwięku). W związku z powyższymi okolicznościami, dużego znaczenia w tej materii nabiera analiza rozporządzenia, którego delegację przewidziano w ust. 8 komentowanego artykułu. Albowiem zgodnie z dyspozycją tego przepisu, Rada Ministrów zobowiązana została do określenia sposobu postępowania przy wykonywaniu tego uprawnienia, z uwzględnieniem m.in. poszanowania praw osób, wobec których działania te są podejmowane. Rozporządzenie¹⁸ dotyczące prowadzenia obserwacji i rejestracji obrazu w miejscach publicznych, wydane na podstawie art. 15 ust. 8 ustawy o Policji, nie nawiązuje jednak w pełni do dyspozycji zawartej w przepisie ustawy. Albowiem w zakresie uprawnienia dotyczącego możliwości obserwacji i rejestracji obrazu w miejscach publicznych wskazano w nim jedynie na sposoby wykorzystywania tej możliwości (bezpośredni lub zdalny) oraz obowiązek dokumentacji tych czynności przez policjanta. Nie odniesiono się jednak do części dyspozycji przepisu ustawowego dotyczącej

¹⁸ Rozporządzenie Rady Ministrów z 26 lipca 2005 r. r w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów. Dz.U. z 2005 r., Nr 141, poz. 1186.

sposobu prowadzenia obserwacji lub rejestracji obrazu przy uwzględnieniu poszanowania praw osób, wobec których działania te są podejmowane¹⁹.

W analogiczny sposób przedstawia się regulacja uprawnień straży gminnych, które w związku z realizacją swoich zadań mają prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych w przypadku, gdy czynności te są niezbędne do wykonywania zadań oraz w celu utrwalania dowodów popełnienia przestępstwa lub wykroczenia, przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych, a także ochrony obiektów komunalnych i urządzeń użyteczności publicznej²⁰. Zwrócić należy jednak uwagę, iż w tym przypadku potencjalne możliwości ingerencji w prywatność za pośrednictwem takiego systemu są ograniczone poprzez brak możliwości rejestracji dźwięku. Z drugiej jednak strony, zauważyć trzeba, że z perspektywy funkcjonowania miejskich systemów monitoringu wizyjnego, w chwili obecnej to właśnie uregulowania ustawy o strażach gminnych mają największe znaczenie. Związane jest to z faktem, iż straże gminne (miejskie) są podmiotami, którym relatywnie najczęściej powierzane jest zadanie prowadzenia miejskich systemów monitoringu wizyjnego²¹. Tym bardziej na aprobatę zasługuje fakt, iż w wyrażonej w ust. 3 komentowanego przepisu delegacji wskazano na konieczność uwzględnienia w rozporządzeniu potrzeby respektowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka w trakcie obserwowania i rejestrowania obrazów w miejscach publicznych przy użyciu środków technicznych.

Niestety, podobnie jak miało to miejsce w przypadku omawianym wcześniej, także i rozporządzenie w sprawie sposobu obserwowania i re-

¹⁹ Szerzej na temat podmiotowych i przedmiotowych braków m.in. ustawy o Policji w tym zakresie: D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, wyd. Lexis Nexis, Warszawa 2012, s. 306-309.

²⁰ Art. 11 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych, Dz.U. z 2013 r., poz. 1383.

²¹ Informacja z kontroli NIK *Funkcjonowanie miejskiego monitoringu wizyjnego*, nr ewid. 181/2013/P/13/154/LLU, s. 9

jestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną²² nie czyni zadość wskazaniom ustawodawcy. Oprócz wskazania – podobnie jak w rozporządzeniu odnoszącym się do uprawnienia Policji – możliwości prowadzenia obserwacji i rejestracji obrazu w sposób zdalny i bezpośredni, a także obowiązku odpowiedniego dokumentowania tych czynności, określono także minimalny i maksymalny termin przechowywania nagrań, statuując jednocześnie obowiązek sporządzania notatki służbowej ze zniszczenia nagrań. Brak jest jednak w rozporządzeniu odniesienia do respektowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka w trakcie obserwowania i rejestrowania obrazów w miejscach publicznych przy użyciu środków technicznych. W szczególności nie wskazano, w jaki sposób należy prowadzić obserwację lub rejestrację obrazu, aby nie dochodziło do naruszenia tych praw. Po raz wtóry stwierdzić należy, iż gwarancje prawa do prywatności oraz ochrony danych osobowych na gruncie ustaw i aktów wykonawczych dotyczących funkcjonowania poszczególnych służb i straży w zasadzie nie istnieją. I to pomimo faktu, iż ustawodawca sygnalizował potrzebę ich regulacji na poziomie rozporządzeń.

Za najważniejsze braki w przywołanych wyżej regulacjach postrzegamy brak wymogu określenia szczegółowych celów, dla których może być prowadzona rejestracja i obserwacja obrazów, a także brak określenia kategorii przestrzeni, w których rejestracja i obserwacja obrazu nie powinna być prowadzone w ogóle – ze względu na podwyższony poziom poczucia prywatności jednostki. Ponadto, warto również rozważyć uzależnienie możliwości wykorzystywania monitoringu wizyjnego od pozytywnych wyników przeprowadzanych w tym celu analiz, bądź też konsultacji z innymi podmiotami. Należy bowiem pamiętać, iż jego wykorzystanie niewątpliwie stanowić może ingerencję w prywatność jednostek, nie koniecznie musi jednak sprzyjać realizacji stawianych przed nim celów. Z tego też powodu, decyzja o budowie lub rozbudowie systemu monitoringu wizyjnego (pociągająca za sobą także niemałe koszty

²² Rozporządzenie RM z 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. z 2009 r., Nr 220, poz. 1720.

– zarówno sprzętu oraz jego instalacji, jak również koszty osobowe, dotyczące w szczególności operatorów kamer) powinna być zawsze należyście uzasadniona.

Uregulowania dotyczące możliwości obserwowania i rejestracji obrazu zostały również przewidziane w ustawach o bezpieczeństwie imprez masowych²³ oraz o grach hazardowych²⁴, niemniej regulacje te nie odnoszą się w sposób bezpośredni do podmiotów publicznych. Ponadto, zwrócić należy uwagę, iż stanowione na podstawie tych ustaw akty wykonawcze zawierają dość szczegółowe regulacje dotyczące parametrów technicznych i rozmieszczenia kamer, pomijając jednocześnie elementy relewantne z perspektywy niniejszej pracy.

Warto jednocześnie zwrócić uwagę, iż szereg podmiotów publicznych wykorzystuje systemy monitoringu w związku z wykonywaniem zadań dotyczących chociażby pośrednio zapewniania bezpieczeństwa i porządku. Odbywa się to jednak bez wyrażonego *expressis verbis* w przepisach prawa powszechnie obowiązującego uprawnienia do obserwacji i rejestracji obrazu. Oczywiście nie można oczekiwać, ażeby ustawodawca za każdym razem w sposób szczegółowy konkretyzował uprawnienia wszystkich kategorii podmiotów publicznych. Niemniej zwrócić należy uwagę, iż może to powodować *de facto* brak możliwości weryfikacji sposobu administrowania takimi systemami, w szczególności w odniesieniu do ochrony danych osobowych.

4. Projekt założeń do projektu ustawy o monitoringu wizyjnym

Wobec fragmentaryczności regulacji dotyczących możliwości wykorzystywania systemów monitoringu wizyjnego, na co zwróciła uwagę w przywoływanym wcześniej raporcie Najwyższa Izba Kontroli, pozytyw-

²³ Ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, Dz.U. z 2013 r., poz.611, wraz z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 10 stycznia 2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej Dz.U. z 2011 r. poz. 73.

²⁴ Ustawa z dnia 19 listopada 2009 r. o grach hazardowych, Dz.U. z 2009 r. poz. 1540, wraz z rozporządzeniem Ministra Finansów z dnia 6 kwietnia 2012 r. w sprawie audiowizyjnego systemu kontroli gier w kasynie gry Dz. U. z 2012 r. poz.416.

nie należy ocenić podjęte przez Ministerstwo Spraw Wewnętrznych starania, mające na celu przygotowanie projektu ustawy o monitoringu wizyjnym²⁵. Niestety, od czasu ukazania się i skierowania do konsultacji drugiej wersji projektu założeń, brak jest oficjalnych wiadomości na temat dalszych prac nad projektem.

Niemniej uważamy, iż warto poświęcić kilka słów komentarza projektowi założeń do projektu ustawy, gdyż – co należy wyraźnie podkreślić – regulacja ta wydaje się być niezwykle pożądana, zwłaszcza biorąc pod uwagę fakt, iż wykorzystywanie kamer funkcjonujących w systemach monitoringu wizyjnego ma miejsce na coraz większą skalę. Z tej perspektywy niezwykle interesująco rysuje się określenie przez projektodawcę głównego celu regulacji, jakim ma być zapewnienie istnienia gwarancji przestrzegania praw i wolności konstytucyjnych – w szczególności tych, które wiążą się z prawem do prywatności jednostki. Stanowi to dość klarowny sygnał ze strony MSW, iż obecne uregulowania w tym zakresie są dalece niewystarczające. Zapewnienie istnienia gwarancji przestrzegania praw i wolności konstytucyjnych ma nastąpić w szczególności poprzez unormowanie zasad prowadzenia monitoringu wizyjnego oraz określenie praw osób, których wizerunki są obserwowane, rejestrowane lub przetwarzane w sposób umożliwiający identyfikację ich tożsamości. Zaś efektem regulacji wskazano na być instrumentów służących gwarancji przestrzegania konstytucyjnych praw i wolności.

Projektowana regulacja zawierać miałaby zbiór generalnych zasad, uszczegóławianych w dalszych jej przepisach, wedle których miałyby być prowadzony monitoring wizyjny we wszystkich przestrzeniach publicznych (w zamiarze projektodawcy przestrzeń publiczną dzielić miałyby się na: otwartą przestrzeń publiczną i zamkniętą przestrzeń przeznaczoną do użytku publicznego; w odniesieniu do tych dwóch kategorii zakłada się zróżnicowanie obowiązków administratorów oraz warunków prowadzenia monitoringu wizyjnego). Projektowana regulacja miałaby mieć charakter ogólny względem obecnie istniejących regulacji szczegółowych, traktujących o działalności poszczególnych służb, inspekcji i straży.

²⁵ Przebieg prac MSW można śledzić w Biuletynie Informacji Publicznej MSW, <http://www.bip.msw.gov.pl/bip/projekty-aktow-prawnyc/2013/22768,Projekt-za-lozen-do-projektu-ustawy-o-monitoringu-wizyjnym.html>, dostęp: 13.08.2015.

Z perspektywy niniejszego opracowania, szczególną uwagę należy poświęcić zasadzie informowania. Pomimo faktu, iż nie została ona wprost wyrażona przez projektodawcę, a jedynie wywiedziona na podstawie obowiązków administratorów, ma ona niebagatelne znaczenie dla realizacji prawa do prywatności jednostki.

Zgodnie z projektem założeń, w przypadku systemów monitoringu wizyjnego funkcjonujących w otwartej przestrzeni publicznej, administratorzy zobowiązani będą do informowania osób o objęciu monitoringiem wizyjnym, poprzez oznaczenie miejsc usytuowania kamer wchodzących w skład systemu. Oznaczenie to następować ma poprzez umieszczenie - w obszarze objętym ich oglądem - tablic informacyjnych, które zawierać mają, oprócz odpowiedniego piktogramu, wskazanie również danych administratora systemu oraz danych umożliwiających kontakt z nim. Proponowane przez projektodawcę rozwiązanie uznać należy za niewątpliwie słuszne, gdyż sprzyja ono transparentności funkcjonowania całego systemu.

Wśród społeczności lokalnych zauważalny jest również brak świadomości o funkcjonowaniu w poszczególnych przestrzeniach kamer wchodzących w skład systemów monitoringu wizyjnego. Przeprowadzone w Krakowie badania wskazują, że blisko 10% respondentów twierdzi, iż nigdy nie znalazło się w sytuacji, w której byłyby obserwowane przez kamerę monitoringu wizyjnego²⁶. Wydaje się to nieprawdopodobne, gdyż zwrócić należy uwagę, że w rzeczywistości z obecnością kamer mamy do czynienia w zasadzie permanentnie – począwszy od systemów monitoringu miejskiego, poprzez kamery funkcjonujące w związku z działalnością komunikacji miejskiej, skończywszy na kamerach instalowanych np. w sklepach. Ponadto, badania przeprowadzone zostały w dużym mieście, w którym obecność kamer (wchodzących w skład systemów publicznych i – przede wszystkim prywatnych) jest wyraźnie zauważalna. Z tego powodu, jako uzasadnione postrzegamy uświadamianie osób znajdujących się w zasięgu oglądu kamery o tym fakcie.

Niemniej, dla możliwie pełnej realizacji omawianej zasady, celowym byłoby także rozwinięcie obowiązku informacyjnego o wskazanie celu,

²⁶ Raport z badania ilościowego zrealizowanego dla Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Miasta Krakowa, *Monitoring w Krakowie*, marzec 2015 r., s. 45.

dla którego w poszczególnych przestrzeniach prowadzony jest monitoring. Ponadto postulujemy zawarcie informacji o tym, czy obraz z danej kamery jest objęty bieżącym oglądem operatora, czy też funkcjonuje on wyłącznie w celu rejestracji obrazów. Świadomość wymienionych wyżej okoliczności może bowiem w sposób zasadniczy wpływać na zachowania osób monitorowanych w sytuacji zaistnienia zdarzenia powodującego zagrożenie.

Oprócz omawianych wyżej, fizycznych oznaczeń w miejscach funkcjonowania kamer, administrator systemu funkcjonującego w otwartej przestrzeni publicznej będzie również zobowiązany do zamieszczania - na powszechnie dostępnej stronie internetowej, a także w swojej siedzibie - informacji na temat przybliżonego zasięgu administrowanego przez siebie systemu. Nawiązując do badań z 2012 r., w aż 42% miast brak jest jakichkolwiek informacji o obecności kamer miejskich systemów monitoringu wizyjnego²⁷. Z tego powodu – uznając za zasadne powyższe uwagi - nie powinno ulegać wątpliwości, że wprowadzenie szerokiego obowiązku informacyjnego jest zasadne.

Z perspektywy rzetelnej realizacji obowiązku informacyjnego, pozytywnie należy ocenić również zakaz stosowania atrap kamer (które stosowane są w ponad 15% miast²⁸) w otwartych przestrzeniach publicznych. Tym samym, projektodawca słusznie zwraca uwagę, iż prowadzenie monitoringu wizyjnego jest jednym z przejawów ingerencji w prawa i wolności konstytucyjne. Z jednej bowiem strony, atrapy kamer powodować mogą poczucie ingerencji w prywatność jednostki, z drugiej zaś mogą stwarzać jednocześnie mylne poczucie zwiększonego poziomu bezpieczeństwa. Pragniemy jednocześnie zaznaczyć, że plany zastosowania tego zakazu wyłącznie do otwartych przestrzeni publicznych stanowić mogą nieuzasadnioną dysproporcję pomiędzy regulacją prowadzenia monitoringu wizyjnego w dwóch kategoriach przestrzeni publicznych (otwartej przestrzeni publicznej oraz zamkniętej przestrzeni prze-

²⁷ Fundacja Panoptykon, *Monitoring w polskich miastach w oczach społeczeństwa*, wyniki analiz danych dotyczących miejskiego monitoringu wizyjnego otrzymanych od 335 miast w efekcie wniosków o udostępnienie informacji publicznej. Dane na rok 2012, s. 2.

²⁸ *Ibidem*.

znaczonych do użytku publicznego), negującą możliwość efektywnej realizacji głównego celu projektowanej ustawy, jakim jest ochrona prywatności jednostki.

W odniesieniu do wszystkich kategorii przestrzeni, zabronione ma być prowadzenie monitoringu wizyjnego połączonego z przekazywaniem lub rejestracją dźwięku (z wyłączeniem systemów wykorzystujących aktywację akustyczną), a także w miejscach, w których mogłoby prowadzić do naruszenia godności człowieka, a więc takich, w których zwiększone jest poczucie prywatności, jak np. w toaletach czy przebieralniach.

Projektodawca wskazał wprost, że w stosunku do obrazu zarejestrowanego w systemach monitoringu wizyjnego nie będzie przysługiwać uprawnienie wynikające z art. 32 i 33 ustawy o ochronie danych osobowych. Uprawnienia te odnoszą się do dostępu przez osobę objętą monitoringiem do jej danych. Projektodawca wyłączenie to uzasadnia możliwością znaczącego utrudnienia funkcjonowania systemów monitoringu wizyjnego poprzez nadmierne i wielokrotne wykorzystywanie tego uprawnienia przez osoby monitorowane. Na bezzasadność tego wyłączenia uwagę zwrócił Generalny Inspektor Ochrony Danych Osobowych, wskazując iż „wyłączenie praw kontrolnych wynikających z art. 32 i 33 u.o.d.o. stanowi nieproporcjonalne naruszenie konstytucyjnych zasad wyrażonych w art. 51 ust. 3-4 Konstytucji. Zewnętrzna kontrola – także przez obywatela – stanowi mechanizm weryfikujący prawidłowość działania systemu, w którym dochodzi do przetwarzania danych osobowych, wizerunków osób fizycznych i innych dóbr chronionych prawem”²⁹. Zaproponowane przez projektodawcę wyłączenie uznać należy nie tylko za ograniczenie uprawnień osoby monitorowanej wynikających z projektowanej ustawy o monitoringu wizyjnym. W rzeczywistości bowiem, wyłączenie to będzie obejmować również uprawnienia, które *de facto* mogą istnieć w obowiązującym obecnie porządku prawnym. Uchwalenie ustawy, zawierającej przepisy przewidujące brak możliwości wykorzystywania uprawnień wynikających z art. 32 i 33 u.o.d.o. będzie zatem dla ochrony prywatności jednostki istotnym krokiem wstecz – w kierunku

²⁹ Uwagi do projektu założeń do projektu ustawy o monitoringu wizyjnym zgłoszone przez GIODO, s. 6.

przeciwnym dla realizacji jednego z fundamentalnych celów projektowanej regulacji. Na korzyść przedstawionej wcześniej argumentacji, iż obraz zarejestrowany przez kamerę monitoringu wizyjnego stanowić może dane osobowe przemawia również potwierdzenie uprawnienia do wizerunku, jakiego w wyroku z 12 marca 2014 r. dokonał Trybunał Konstytucyjny³⁰. Wyrok ten dotyczył wskazania sprawcy wykroczenia drogowego, bez możliwości dostępu do obrazu zarejestrowanego przez fotoradar.

Wyłączenie proponowane przez projektodawcę wynika bowiem z błędnego – zdaniem autorów – założenia, iż „obraz z monitoringu przedstawiający osobę, lecz będący jedynie podglądem danego miejsca w przestrzeni publicznej, nie stanowi danych osobowych, a danymi osobowymi jest *dopiero* obraz utrwalony na nośnikach danych”. Projektodawca wydaje się pomijać regulację art. 6 u.o.d.o., myląc jednocześnie wskazane w tej ustawie definicje danych osobowych z ich przetwarzaniem. Ponadto, przytoczona przez projektodawcę argumentacja, iż przyznanie osobom monitorowanym uprawnień przewidzianych w art. 32 i 33 u.o.d.o. może destabilizować pracę systemów, pociągając za sobą wysokie koszty, wydaje się być nietrafna. Co więcej, rozwiązanie takie jest zdaniem autorów sprzeczne z Konwencją o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych stanowiącą, iż osoby, których dane figurują w zbiorach muszą mieć zagwarantowane prawo uzyskania informacji o istnieniu takiego zbioru, a także możliwość wglądu do danych ich dotyczących, a w przypadku przetwarzania tych danych z naruszeniem prawa – do ich sprostowania lub usunięcia.

5. Podsumowanie

Podsumowując powyższe rozważania, autorzy pragną zwrócić uwagę, iż w obowiązującym stanie prawnym uwidaczniają się – wraz z coraz powszechniejszym wykorzystywaniem technologii – niedostatki, które powodują szereg zagrożeń zarówno dla prywatności jednostek, jak i dla ochrony ich danych osobowych. W rozważanej perspektywie, związane jest to przede wszystkim z brakiem odpowiedniej, kompleksowej

³⁰ Sygn. P 27/13.

regulacji traktującej o zasadach wykorzystywania systemów monitoringu wizyjnego oraz o przetwarzaniu pozyskiwanych przez nie danych osobowych.

Odpowiedź na pytanie, na ile deklaracje zawarte w prawie międzynarodowym i Konstytucji RP w zakresie prawa do prywatności i ochrony danych osobowych są realizowane na poziomie ustaw i rozporządzeń, powinna być złożona. O ile bowiem polskie ustawodawstwo w zakresie tradycyjnie pojmowanych danych osobowych realizuje standardy wyznaczone m.in. przez Europejską Konwencję Praw Człowieka, o tyle rozwiązania dotyczące monitoringu wizyjnego obarczone są w tym względzie znaczącymi niedoskonałościami. Związane jest to z faktem, iż przetwarzane w ich ramach dane – zarejestrowane obrazy – mają dość specyficzny charakter. Początkowo istniały nawet wątpliwości, czy takie obrazy mogą stanowić dane osobowe. Niemniej w chwili obecnej nie ulega to wątpliwości, co zostało ugruntowane przez orzecznictwo. Odpowiednie stosowanie ustawy o ochronie danych osobowych do danych przetwarzanych w systemach monitoringu wizyjnego wydaje się być niewystarczające – w szczególności w zakresie umożliwienia osobom monitorowanym dostępu do ich danych, a także nadzoru sprawowanego nad administrowaniem tymi systemami.

Ponadto, szczegółowe regulacje przyznające uprawnienie do prowadzenia monitoringu nie są wystarczające, gdyż sposobu prowadzenia monitoringu (który w najmniejszym stopniu ingerowałby w prywatność jednostki) nie regulują w ogóle, fragmentarycznie odnosząc się również do sposobu administrowania tymi danymi. Co istotne, akty wykonawcze stanowione na podstawie tych ustaw nie realizują w pełni dyspozycji przepisów ustawowych. W związku z powyższym, pozytywnie należy ocenić podjęte starania mające na celu objęcie regulacją całości.

Mając na uwadze powyższe, niewątpliwie pozytywnie ocenić należy podjęte przez Ministerstwo Spraw Wewnętrznych starania, mające na celu uregulowanie tej materii. Na aprobatę zasługuje również uwzględnienie w projekcie założeń do projektu ustawy o monitoringu wizyjnym regulacji europejskich – nie tylko w sposób powodujący zgodność z nimi projektowanej regulacji, ale także dalsze ich pogłębianie. Zwrócić należy jednak uwagę, iż głównym celem projektodawcy powinno być przede wszystkim zapewnienie ochrony prywatności oraz danych osobowych

jednostek, gdyż to właśnie te prawa stają się coraz bardziej zagrożone. W związku z powyższym, postuluje się uwzględnienie na etapie projektowania kompleksowej ustawy o monitoringu wizyjnym, także dokumentów nie mających co prawda mocy prawnej, ale uwzględniających w szczególności właśnie ochronę prywatności jednostek – m.in. Kartę Demokratycznego Zastosowania Monitoringu Wizyjnego. Co więcej, w celu objęcia należytą ochroną danych osobowych gromadzonych i przetwarzanych w związku z funkcjonowaniem systemów monitoringu wizyjnego, warto również rozważyć ustanowienie przepisów szczególnych - względem ustawy o ochronie danych osobowych – w ustawie o monitoringu wizyjnym. Celem tych przepisów powinno być względne uelastycznienie u.o.d.o., które pozwoliłoby na możliwie najpełniejsze jej zastosowanie do rodzaju danych, gromadzonych i przetwarzanych w systemach monitoringu wizyjnego. Z drugiej jednak strony, pozostawienie obecnych uregulowań w niezmiennym kształcie (w formie przepisów szczególnych), w przypadku braku stosownych przepisów regulujących przetwarzanie danych osobowych w ramach systemów monitoringu wizyjnego, spowodować może, iż obecnie istniejące wątpliwości nie zostaną rozwiązane.

Warto również zauważyć, iż starania podjęte przez MSW doprowadzić mają do precyzyjnego ustalenia, które podmioty publiczne i dla realizacji jakich celów będą mogły prowadzić monitoring wizyjny w przestrzeniach publicznych. Jest to o tyle istotne, iż w obecnym stanie prawnym bardzo często uprawnienia te są przez podmioty publiczne wywodzone z ogólnych regulacji dotyczących zakresów ich zadań. Na aprobatę zasługują również dążenia do precyzyjnego uregulowania katalogu podmiotów uprawnionych do wykorzystywania zarejestrowanych nagrań, a także sposobu i terminów ich archiwizowania oraz udostępniania uprawnionym podmiotom. Niewątpliwie dyskusja w temacie ochrony prywatności oraz ochrony danych osobowych osób monitorowanych przez systemy monitoringu wizyjnego jest otwarta – a wraz z intensyfikacją prac mających za cel uchwalenie ustawy o monitoringu wizyjnym, będzie się coraz bardziej nasilać.

Personal data protection and the right to privacy of the persons monitored by video-surveillance systems operating in order to ensure safety and public order

In this paper, the authors are dealing with issues related to the right to privacy and personal data protection of persons monitored by video-surveillance cameras operating in order to ensure safety and public order. The use of video monitoring systems, as a useful tool to streamline execution of the tasks of providing security and order, takes place in connection with the activities of a number of public entities. For this reason, important aim is to acquaint the reader with existing rules made at international and constitutional level. Due to the conflict which exists between providing security with the use of video-surveillance cameras and the right to privacy of individuals, and increasingly widespread use of such tools, the authors also point to clarify the right to privacy and personal data protection at the level of laws and by-laws and attempt to assess the guarantees of these rights. In addition, the authors are presenting closer discussed prospects for further development of rights and its warranties.