ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3994
PRZEGLĄD PRAWA I ADMINISTRACJI CXXII
WROCŁAW 2020

https://doi.org/10.19195/0137-1134.122.19

DARIUSZ WASIAK
ORCID: 0000-0001-6057-7475
Wyższa Szkoła Bankowa we Wrocławiu

MONITORING WIZYJNY W DZIAŁALNOŚCI STRAŻY GMINNYCH. ZARYS PROBLEMATYKI

Abstrakt: Represyjny charakter działań straży gminnych sprawia, że te parapolicyjne formacje zostały wyposażone w instrumenty prawne oraz narzędzia techniczne umożliwiające ingerencję w dobra i wolności zawarte w Konstytucji RP. Jednym z takich narzędzi jest środek techniczny umożliwiający obserwację i rejestrację obrazu zdarzeń w miejscach publicznych. Mowa tu o monitoringu wizyjnym, którego wykorzystanie wymaga jednak spełnienia przez straże gminne kilku ustawowych obostrzeń. Niniejszy artykuł traktuje w związku z tym o aktualnych obowiązkach komendantów straży gminnych w zakresie stosowania monitoringu wizyjnego oraz ich zgodności z konstytucyjną zasadą proporcjonalności.

Słowa kluczowe: monitoring wizyjny, straż gminna, dane osobowe, ochrona danych, RODO, Konstytucja RP, drony

UWAGI WPROWADZAJĄCE

Straże gminne (dalej: straż lub straże) na mocy przepisów ustawy z dnia 29 sierpnia 1997 roku o strażach gminnych[1] mają prawo realizować powierzone im zadania z wykorzystaniem środków technicznych umożliwiających obserwację i rejestrację obrazu zdarzeń w miejscach publicznych (dalej: monitoring wizyjny). Mowa tu o możliwości monitorowania przez straż gminną zachowań ludzkich występujących wyłącznie w strefie publicznej za pośrednictwem oznaczonych (widzialnych) urządzeń rejestrujących, które utrwalają wizerunek osoby fizycznej objętej ich zasięgiem[2].

Straż gminna jako podmiot odpowiedzialny za stan porządku publicznego na terenie swojego działania nie może zatem prowadzić obserwacji osób w miejscu ich zamieszkania czy też wykonywania pracy, choć niewątpliwie działania

[1] Dz.U. z 1997 r. Nr 123, poz. 779 ze zm. (dalej: ustawa o strażach).
[2] Wyrok WSA w Warszawie z dnia 9 kwietnia 2013 roku, sygn. II SA/Wa 211/13.

straży przy wykorzystaniu urządzeń rejestrujących mogą prowadzić do ustalenia tożsamości każdej osoby fizycznej, a dokładniej jej cech, na podstawie których można ustalić, kim dana osoba jest i czym się różni od innych osób w określonym otoczeniu[3].

Treść przepisu art. 10a ust. 1 ustawy o strażach stanowi, że straże w celu realizacji ustawowych zadań mogą przetwarzać dane osobowe bez wiedzy i zgody osoby, której te dane dotyczą. Wskazane uprawnienie odnosi się wyłącznie do przetwarzania danych uzyskanych: (1) w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia; (2) z rejestrów, ewidencji i zbiorów, do których straż ma dostęp na podstawie odrębnych przepisów, w celu zidentyfikowania sprawcy naruszenia obowiązujących przepisów, lecz poza danymi ujawniającymi pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak też danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, które mogą być przetwarzane wyłącznie po uzyskaniu zgody osoby, której dane dotyczą.

1. ZGODA JAKO PRZYCZYNA NIEPRAWIDŁOWOŚCI

Odebranie zgody od osoby, której dane dotyczą, lecz bez wykazania przez straż niezbędności przetwarzania tej kategorii danych, może skutkować uznaniem przez Urząd Ochrony Danych Osobowych[4] za przetwarzanie danych w zakresie ponadmiarowym z jednoczesnym stwierdzeniem naruszenia zasad przetwarzania danych[5]. Przepis art. 10 ust. 1 ustawy o strażach ogranicza bowiem strażom prawo do przetwarzania danych osobowych zebranych bez wiedzy i zgody osoby, której te dane dotyczą, do innych celów niż te, które zostały określone we wskazanym przepisie. Dlatego też należy przyjąć, że aby straż mogła przetwarzać dane osobowe bez wiedzy i zgody osoby, której te dane dotyczą, obowiązana jest ona do wykazania podjęcia czynności dających podstawę do tego, aby określony czyn, a tym samym określone zachowanie człowieka, można było uznać za wykroczenie z art. 1 ustawy z dnia 20 maja 1971 roku Kodeks wykroczeń[6], w którym do zmiennych klasyfikujących czyn jako zabroniony zalicza się:

1. społeczną szkodliwość czynu, której stopień szkodliwości jest uzależniony od uzewnętrznionego zachowania człowieka (działania lub zaniechania), będącego przejawem woli tego człowieka — w związku z tym niewykazanie szkodliwości czynu przekreśla byt wykroczenia;

[3] Wyrok WSA w Warszawie z dnia 3 marca 2009 roku, sygn. II SA/Wa 1495/08.
[4] https://www.uodo.gov.pl/pl (dostęp: 2.01.2020).
[5] https://www.uodo.gov.pl/pl/138/701 (dostęp: 2.01.2020).
[6] Dz.U. z 1971 r. Nr 12, poz. 114 ze zm. (dalej: kodeks wykroczeń).

2. bezprawność, która wiąże się z tym, że określony czyn musi być zabroniony ustawą obowiązującą w czasie jego popełnienia pod groźbą kary aresztu, ograniczenia wolności, grzywny do 5000 złotych lub nagany;

3. zawinienie, które wymusza niezbędność przypisania dokonania czynu zabronionego konkretnemu człowiekowi w określonym czasie bądź dokonania ustaleń, że możliwość nieprzypisania winy konkretnemu człowiekowi we wskazanym czasie jest wykluczona z punktu widzenia przeciętnie roztropnego człowieka. Do katalogu tego należy również zaliczyć zachowanie człowieka w określonym stadium popełniania czynu z uwzględnieniem: (a) zamiaru, (b) przygotowania, (c) usiłowania, (d) dokonania, a każda postać stadialna objęta jest karalnością tylko wówczas, gdy ustawa tak stanowi.

Dopiero po spełnieniu tych warunków straże mogą w zgodzie z przepisami prawa przetwarzać dane zawarte w rejestrach, ewidencjach i zbiorach, do których mają dostęp na podstawie odrębnych przepisów, bez wiedzy i zgody osoby, której dane dotyczą. Dlatego też każde inne przetwarzanie danych przez straż bez wiedzy i zgody osoby, której dane dotyczą, należy uznać za naruszenie przepisu art. 107 ust. 1 lub 2 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych[7] w zw. z art. 231 § 1 ustawy z dnia 6 czerwca 1997 roku — Kodeks karny[8], gdyż czyn ten jest przestępstwem bezskutkowym, do którego dochodzi w następstwie działania funkcjonariusza publicznego na szkodę interesu publicznego lub prywatnego w związku z przekroczeniem uprawnień lub niedopełnieniem obowiązków. Do zaistnienia znamion przestępstwa nie jest konieczne, aby wystąpił jakikolwiek uszczerbek w dobrach chronionych prawem, ponieważ przedmiotem ochrony jest prawidłowe funkcjonowanie instytucji państwowych i samorządu terytorialnego, a także wynikający z tego ich autorytet. Dlatego też źródłem naruszeń tego typu mogą być zarówno normy prawne regulujące obowiązki komendanta, jak i polecenia służbowe wydane przez wójta, o ile ich zakres mieści się w granicach posiadanych uprawnień, a niebezpieczeństwo będzie rzeczywiste i skonkretyzowane[9].

Przytoczone uwagi odnoszą się do wszystkich czynności procesowych będących w szczególności następstwem wykorzystania danych z monitoringu wizyjnego, gdyż wykazanie niedopełnienia obowiązków służbowych, których efektem będzie na przykład wystąpienie samego zagrożenia naruszenia zasad ochrony danych osobowych (nie musi zatem wystąpić naruszenie ochrony danych osobowych), może skutkować wszczęciem przez Prezesa Urzędu Ochrony Danych Osobowych postępowania w celu nałożenia na komendanta kary administracyjnej, o której mowa w art. 102 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych. Samo bowiem nieoznaczenie strefy objętej monitoringiem wizyjnym

[7] Dz.U. z 2018 r. poz. 1000 ze zm.

[8] Dz.U. z 1997 r. Nr 88, poz. 553 ze zm. (dalej: kodeks karny).

[9] Uchwała 7 sędziów SN z dnia 24 października 2014 roku, sygn. I KZP 24/12; oraz uchwała SN z dnia 11 czerwca 2019 roku, sygn. I DO 11/19.

należy zakwalifikować jako niedopełnienie obowiązku prawnego, gdyż niebezpieczeństwo naruszenia normy prawnej jest w takim wypadku rzeczywiste i skonkretyzowane. Straże nie mają przecież prawa do niejawnego działania za pośrednictwem monitoringu wizyjnego w pełnym zakresie. Wskazane w art. 10 ust. 1 ustawy o strażach przesłanki legitymizujące możliwość przetwarzania danych bez wiedzy i zgody osoby, której dane dotyczą, oznaczone są zakresowo i wskazują na kryterium czasu. Innymi słowy straże mogą przetwarzać dane bez wiedzy i zgody osoby, której dane dotyczą, dopiero po wykazaniu, że zachodzą przesłanki uzasadniające prowadzenie dalszych czynności wobec konkretnej, a nie jakiejkolwiek osoby fizycznej, w celu jej identyfikacji, utrwalania zachowań przestępczych czy też zastosowania kary, w tym środków karnych. W tym przepisie nie ma zatem mowy o możliwości prowadzenia przez straże inwigilacji wszystkich osób objętych zasięgiem monitoringu wizyjnego. Wynika to także z przepisów ustawy z dnia 24 sierpnia 2001 roku — Kodeks postępowania w sprawach o wykroczenia[10] oraz ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[11].

Niemniej jednak nie oznacza to, że poprawnie skonstruowana zależność ustawowa przekłada się na zgodność działania straży z tymi zasadami. Innymi słowy nie oznacza to, że w strażach nie może dochodzić do naruszenia zasad ochrony danych, w szczególności z uwagi na marginalizowanie prawnie narzuconych obowiązków lub zbyt swobodną interpretację przepisów, co w konsekwencji może skutkować naruszeniem przez straż, reprezentowaną przez jej komendanta, konstytucyjnie gwarantowanych praw i wolności osób objętych zasięgiem monitoringu wizyjnego. O tym w zarysie mowa w dalszej części artykułu przez pryzmat obowiązków[12], o których mowa w art. 13 i art. 24 ogólnego rozporządzenia o ochronie danych 679/2016[13] i art. 22 i 31 ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przy uwzględnieniu między innymi wytycznych Prezesa Urzędu Ochrony Danych Osobowych (dalej: PUODO)[14].

2. USTAWOWE WARUNKI WYKORZYSTANIA MONITORINGU WIZYJNEGO

Jak już podniesiono, realizacja powierzonych strażom zadań może być wspomagana użyciem monitoringu wizyjnego na mocy treści przepisu art. 11 ust. 2

[10] Dz.U. z 2001 r. Nr 106, poz. 1148 ze zm. (dalej: kodeks postępowania w sprawach o wykroczenia).

[11] Dz.U. z 2019 r. poz. 125.

[12] https://uodo.gov.pl/pl/225/1214 (dostęp: 2.01.2020).

[13] Dz.Urz. UE L z 2016 r. Nr 119/1.

[14] https://uodo.gov.pl/pl/383/354 (dostęp: 2.01.2020).

ustawy o strażach w określonym ustawą zakresie, czyli tylko wówczas, gdy straże wykażą niezbędność zastosowania tych urządzeń technicznych do realizacji następujących celów:

1. utrwalanie dowodów popełnienia przestępstwa lub wykroczenia;

2. przeciwdziałanie przypadkom naruszania spokoju i porządku w miejscach publicznych;

3. ochronę obiektów komunalnych i urządzeń użyteczności publicznej — z tym że określone zadania muszą być dodatkowo dookreślone zakresowo i czasowo, a prowadzenie obserwacji prewencyjnych przy wykorzystaniu monitoringu wizyjnego nie może tworzyć samoistnej przesłanki legitymizującej takie działania.

Gdy straże już wykażą niezbędność prowadzenia ustawowo nakreślonych działań z wykorzystaniem monitoringu wizyjnego, są one obowiązane do:

1. cyklicznego potwierdzania skuteczności prowadzonych obserwacji;

2. rejestrowania utrwalonych zdarzeń;

3. rozróżniania danych na dane:

— osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony;

— osób skazanych za czyn zabroniony;

— pokrzywdzonych czynem zabronionym lub osób, w których wypadku określone fakty wskazują, że mogą stać się ofiarami czynu zabronionego;

— innych osób związanych z czynem zabronionym, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w sprawie czynu zabronionego lub na dalszych etapach postępowania, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w pkt 1 i 2;

4. rozróżniania danych na dane mające swoje źródło w:

— faktach,

— indywidualnych ocenach (o ile będzie to możliwe lub nie będzie dalece utrudnione ze względu na dane osobowe);

5. ewidencjonowania operacji przetwarzania danych polegających w szczególności na:

— zbieraniu,

— modyfikowaniu,

— przeglądaniu,

— ujawnianiu wraz z przekazywaniem,

— łączeniu,

— usuwaniu;

6. ewidencjonowania operacji przetwarzania danych, opierając się na:

— dacie i godzinie operacji;

— tożsamości osoby, która przeglądała lub ujawniła dane osobowe — w miarę możliwości;

— tożsamości odbiorców danych osobowych — w miarę możliwości;

— zasadności operacji — dla ewidencji prowadzonych w sposób niezautomatyzowany;

z tym, że:

a) ewidencje winny być przeznaczone wyłącznie:

— do weryfikowania zgodności przetwarzania danych z prawem,

— do monitorowania własnej działalności,

— do zapewnienia integralności i bezpieczeństwa danych osobowych,

— na potrzeby prowadzonych postępowań;

b) prowadzenie rozróżnienia oraz ewidencjonowania wymagane jest od 6 lutego 2020 roku, chyba że straż była w stanie wykazać, iż wprowadzenie takiego zautomatyzowanego systemu informatycznego w celu dostosowania go do wdrożonych i funkcjonujących już w straży środków technicznych i organizacyjnych wymagało niewspółmiernego wysiłku lub nakładów, co nie może być jednak utożsamiane wyłącznie z wielkością wydatków, które musiałyby zostać poniesione[15]. Wówczas obowiązek wprowadzenia automatycznego rozróżnienia oraz ewidencjonowania wymagany będzie dopiero od 6 maja 2023 roku. Wyjątek ten nie przekłada się na obowiązek prowadzenia od 6 lutego 2020 roku przez straż rozróżnienia oraz ewidencjonowania w wersji tradycyjnej (papierowej), o ile dokonanie takiego rozróżnienia będzie możliwe lub nie będzie dalece utrudnione.

Ponadto straże obowiązane są do bezwzględnego respektowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka, czyli między innymi prawa do prywatności, prawa do ochrony danych osobowych i innych praw wynikających z Konstytucji RP[16]. Respektując przynależne każdemu człowiekowi prawa, straże nie mogą zapominać, że informacje, które bez nadzwyczajnego wysiłku, czyli bez nieproporcjonalnie dużych nakładów, dają się „powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, również zalicza się do kategorii danych osobowych[17]. Z tego względu model prowadzenia działań z wykorzystaniem monitoringu wizyjnego musi uwzględniać obowiązek:

1. respektowania przez straż zasady proporcjonalności osadzonej w art. 31 ust. 3 Konstytucji RP jako normy gwarancyjnej, której celem jest ochrona praw i wolności każdej jednostki przed nadmierną ingerencją straży, a także obowiązek działania straży bez oderwania od aktualnie obowiązującego porządku prawnego, w szczególności działania na rzecz ochrony przetwarzanych danych przed ich szkodliwym dla jednostki wykorzystywaniem, o czym mowa w art. 51 Konstytucji RP;

2. przestrzegania przepisów Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[18], notabene

[15] Wyrok NSA z dnia 4 marca 2002 roku, sygn. II SA 3144/01.

[16] Dz.U. z 1997 r. Nr 78, poz. 483 ze zm. (dalej: Konstytucja RP).

[17] Wyrok NSA z dnia 19 maja 2011 roku, sygn. II SA/Wa 1086/10.

[18] Dz.U. z 2003 r. Nr 3, poz. 25.

obecnie aktualizowanej, gdy dane będą przetwarzane w całości lub części w sposób zautomatyzowany. Innymi słowy operacje zachodzące w ramach procesu przetwarzania danych z wykorzystaniem systemu monitoringu, które są wykonywane bądź będą wykonywane w całości lub części z zastosowaniem metod zautomatyzowanych, muszą zostać ocenione pod kątem ich zgodności z wymogami przepisów konwencji. Ocena taka winna zostać dokonana w szczególności, gdy dane są rejestrowane, modyfikowane, usuwane, odzyskiwane lub rozpowszechnianie w całości lub części w sposób zautomatyzowany.

W związku z tym dyskrecjonalność, a dokładniej brak delimitacji zbędności wspierania przez monitoring wizyjny wykonywania ustawowo nakreślonych działań straży, sprawia, że strażom, a raczej ich komendantom, można przypisać zachowanie skutkujące naruszeniem normy w zakresie określonym przez art. 231 kodeksu karnego. Praktyka zawodowa podpowiada, że niezbędność wspomagania działań straży przy zastosowaniu monitoringu wizyjnego może być legitymowana w szczególności:

1. przyjętą przez radę gminy metodyką działań straży, choćby z uwagi na specyfikę i architekturę urządzeń i budynków usytuowanych na terenie gminy;
2. niewspółmiernością liczby strażników do powierzchni i specyfiki ochranianego terenu;
3. czasem wykonywania przez strażników powierzonych zadań straży;
4. czasem, miejscem i rodzajem występowania naruszeń prawa;
5. strukturą organizacyjną straży;
6. czy też brakiem odpowiednich środków transportu.

Jest to o tyle istotne, że każda jednostka objęta zasięgiem monitoringu wizyjnego uzbrojona jest w konstytucyjne prawo do poszanowania swojego życia prywatnego i rodzinnego, o czym mówi wprost art. 47 Konstytucji RP, a każdy organ władzy publicznej może działać wyłącznie na podstawie i w granicach prawa, o czym stanowi art. 7 Konstytucji RP. Dlatego też straże, a dokładniej ich komendanci, obowiązani są do projektowania działań z wykorzystaniem monitoringu wizyjnego, biorąc zawsze za wyznacznik, że:

1. wizerunek osoby, który zostanie utrwalony przez system monitoringu wizyjnego, należy do danych osobowych mieszczących w sobie zarówno wizerunek twarzy, jak i poszczególne elementy charakteryzujące konkretną osobę, takie jak jej zachowanie, chód, gestykulacja, fryzura, ubiór, a nawet indywidualne połączenia kolorystyczne, czyli elementy dostrzegalne — zewnętrzne, które mogą indywidualizować każdą jednostkę w grupie i być znakiem ją identyfikującym zaliczanym do kategorii danych osobopoznawczych[19];
2. wizerunkiem jest każda podobizna bez względu na technikę wykonania, czyli także za pośrednictwem aparatu fotograficznego znajdującego się w telefonie komórkowym, który nie może być uznany za część systemu monitoringu wizyjnego[20].

[19] Wyrok NSA z dnia 28 listopada 2002 roku, sygn. II SA/Wa 3389/01.
[20] Wyrok SA w Katowicach z 28 maja 2015 roku, sygn. I ACa 158/15.

3. WPŁYW NOWYCH REGULACJI NA DOTYCHCZASOWE WARUNKI WYKORZYSTANIA MONITORINGU WIZYJNEGO

Polski ustawodawca jeszcze pod rządami ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych określił szczegółowo warunki, sposoby, możliwości oraz podstawy i wymagania prawne dla monitoringu wizyjnego wykorzystywanego przez straże, które nadal obowiązują i nie kolidują między innymi z przepisami:

1. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

2. ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych;

3. dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW[21];

4. czy też ustawy ją implementującej, którą jest już wskazywana ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Innymi słowy należy przyjąć, że realizowanie obowiązków wynikających z podanych przepisów, lecz bez wypełniania przez komendanta obowiązków prawnych określonych w ustawie wraz z aktem wykonawczym w zakresie odnoszącym się do monitoringu wizyjnego nie będzie mogło być uznane za wypełnienie wymogów prawnych w tym zakresie. Dopiero wypełnienie przez straż wszystkich wskazanych w niniejszym artykule obligatoryjnych wymagań prawnych uposaża ją w prawo do legalnego przetwarzania danych osobowych z wykorzystaniem monitoringu wizyjnego. Dlatego też na przykład sama techniczna, organizacyjna i finansowa koncepcja budowy sieci monitoringu wizyjnego, będąca w ocenie wójta podstawą do legalnego wykorzystywania monitoringu wizyjnego przez straż, nie może zostać uznana za element wypełniający wymienione warunki prawne

Ponadto brakuje w obecnie obowiązującym wykazie Prezesa Urzędu Ochrony Danych Osobowych wymogu dokonania przez straże oceny skutków względem ochrony danych dla operacji przetwarzania danych w związku z wykorzystaniem monitoringu wizyjnego[22], którego podstawę wykorzystania dookreśla przepis pra-

[21] Dz.Urz. UE L z 2016 r. Nr 119/89.

[22] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 roku w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. z 2019 r. poz. 666), http://monitorpolski.gov.pl/MP/2019/666 (dostęp: 2.01.2020).

wa niezwalniający komendantów z obowiązku dokonania analizy tych procesów pod kątem ich zgodności z innymi wymaganiami prawnymi. W związku z tym każdy komendant, w szczególności komendant straży ulokowanej w strukturach organizacyjnych urzędu gminy jako wydział, w celu ochrony przed wykazaniem naruszeń prawa obowiązany jest do przeanalizowania wszystkich występujących procesów, w ramach których dochodzi do przetwarzania danych osobowych w związku z realizowaniem ustawowych zadań.

Dlatego też niewykazanie przez komendanta spełnienia wymienionych wymogów prawnych może skutkować wskazaniem naruszenia zasad ochrony danych osobowych, a tym samym możliwością nałożenia kary administracyjnej oraz odpowiedzialnością karną, o której mowa w ustawie z 10 maja 2018 roku o ochronie danych osobowych i ustawie z dnia 6 czerwca 1997 roku — Kodeks karny, w wyniku niedopełnienia obowiązków służbowych.

4. MONITORING WIZYJNY BEZPOŚREDNI

Przepisy rozporządzenia Rady Ministrów z dnia 16 grudnia 2009 roku w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską)[23] uposażają straż w prawo do obserwowania i rejestrowania zdarzeń w sposób zarówno zdalny, jak i bezpośredni, czyli na przykład przy wykorzystaniu kamer osobistych (służbowych) umiejscowionych na ubiorze służbowym, które nieintencjonalnie mogą zarejestrować zachowania niezwiązane z przeprowadzaną interwencją. Należy w związku z tym stwierdzić, że:

1. w przypadku wykorzystywania przez strażników monitoringu wizyjnego w sposób bezpośredni w miejscu publicznym, czyli w miejscu ogólnodostępnym, które w swojej istocie może być ograniczone barierami technicznymi lub fizycznymi, takimi jak na przykład ogrodzenie, których pokonanie nie wymaga uzyskania zwolnień ustawowych lub pochodnych wydanych przez organy prawnie umocowane, nie zwalania strażników z obowiązku poszanowania praw osób niepowiązanych z interwencją, czyli takich, których zachowanie nie kwalifikuje ich do kategorii osób rozróżnionych na mocy przepisu art. 19 ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Dlatego też należy uznać, że działania patrolowe strażnika z wykorzystaniem kamer osobistych powinny być realizowane wyłącznie w celu utrwalania dowodów popełnienia przestępstwa lub wykroczenia, nie zaś do przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych lub też ochrony obiektów komunalnych i urządzeń użyteczności publicznej, co może sugerować treść art. 11 ust 2 ustawy o strażach, gdyż rolę tę od-

[23] Dz.U. z 2009 r. Nr 220, poz. 1720.

grywa strażnik. Nie ma więc uzasadnienia niezbędności wspomagania takich działań patrolowych stale włączonym rejestratorem obrazu umiejscowionym w klapie ubioru służbowego strażnika tylko na kanwie samej przesłanki wskazującej na „przeciwdziałanie". Trzeba bowiem rozróżnić niezbędność stosowania monitoringu pośredniego i bezpośredniego. Dlatego też w tym przypadku powoływanie się przez straż na samą przesłankę „przeciwdziałania" jest argumentacją niepełną. Bez wykazania elementu niezbędności, który będzie dopełnieniem przesłanki ogólnej: przeciwdziałanie, działania strażników przy wykorzystaniu stale włączonego rejestratora osobistego, należy uznać za nadużycie. Innymi słowy wymóg niezbędności można próbować uzasadnić między innymi na podstawie przesłanek zawartych w art. 226 § 1 kodeksu karnego, czyli w sklasyfikowanych w zarysie wytycznych, które mogą zagrażać autorytetowi funkcjonariusza publicznego;

2. nie każde zarejestrowane za pomocą rejestratora obrazu umiejscowionego w klapie ubioru służbowego strażnika zachowanie osoby fizycznej jest następstwem naruszenia przez nią przepisów osadzonych przede wszystkim w prawie wykroczeń, na podstawie których straż może stosować także przepisy prawa karnego. Jednakże w okolicznościach uzasadniający podejrzenie popełnienia czynu karalnego bądź zgłoszenie oparte na przykład na treści przepisu art. 304 § 2 ustawy z dnia z dnia 6 czerwca 1997 roku Kodeks postępowania karnego[24] należy tę przesłankę uznać za wystarczającą dla straży gminnych w zakresie ich działania z użyciem rejestratora obrazu umiejscowionego na klapie ubrania roboczego strażnika, który zarejestruje także osoby postronne. W takim przypadku nie można przypisać straży nadużyć, o ile rzecz jasna nośniki danych będą stosownie zabezpieczone i chronione, a okres retencji danych oraz ich usuwania poprawnie określony. Dotyczy to także udostępniania przez straż danych w celu ich dalszego upubliczniania, gdyż podmiot zamierzający dokonać publikacji nie ma własnego, samodzielnego uprawnienia do oceny, że publikacja danych osobowych osoby, przeciwko której toczy się postępowanie przygotowawcze lub sądowe, jest dopuszczalna ze względu na interes społeczny[25].

Innymi słowy na zgodność przetwarzania danych w strażach może wpływać poziom posiadanych kompetencji i umiejętności odczytywania oraz stosowania norm prawnych przez komendanta oraz poszczególnych strażników.

WNIOSKI

W ramach końcowej analizy zakresu badawczego należy stwierdzić, że ustawowo sprofilowany dla straży model dostępu do danych, przetwarzania danych

[24] Dz.U. z 1997 r. Nr 88, poz. 555 ze zm.

[25] Wyrok SN z dnia 18 marca 2008 roku, sygn. IV CSK 474/07.

oraz ich zakres ochrony i zapewnienia bezpieczeństwa i wyłączeń jest czytelny i dobrze umiejscowiony w systemie prawnym.

Zależności te wskazują, że ustawowo wyznaczony zakres możliwości gromadzenia danych osobowych przez straże został ukształtowany prawidłowo. Z tej właśnie przyczyny na potrzeby dalszych rozważań można wstępnie przyjąć, że model dostępu do danych, a zarazem możliwość ich przetwarzania przez straże jest prawidłowy i realizowany z poszanowaniem zasady wyrażonej w art 51 Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku oraz z uwzględnieniem zasady proporcjonalności, o której mowa w art. 31 ust. 3 Konstytucji RP w kontekście niezbędności zapewnienia ochrony konstytucyjnych praw i wolności osób.

Na tym polu nie doszukamy się tu zbyt wielu luk, które mogą prowadzić do bezpośredniego wskazania naruszeń w zakresie niekonstytucyjnego działania lub niedbałości o prawa i wolności osób objętych monitoringiem wizyjnym. Nie oznacza to jednak, że straże nie borykają się z problemami prawnymi, technicznymi, obiektowymi, kadrowymi i organizacyjnymi, co może skutkować tym, że w każdej chwili może dojść między innymi do przekroczenia niestabilnej granicy, którą wyznacza zasada proporcjonalności, a tym samym zakres możliwości działania straży. Może zatem w każdej chwili dojść do naruszenia konstytucyjnie gwarantowanych praw i wolności w kontekście działań na rzecz zapewnienia porządku i bezpieczeństwa w ramach czynności z wykorzystaniem monitoringu wizyjnego z uwagi na zły nadzór czy lekceważenie obowiązków. Innymi słowy może się to zdarzyć wskutek przekroczenia lub niedopełnienia obowiązków czy też w następstwie niepewności działania.

Takim przejawem budowania niepewności u komendantów może być chociażby stanowisko PUODO z 2 marca 2020 roku w zakresie realizowania obowiązku informacyjnego przy zastosowaniu fotopułapek. Organ wskazał, że:

> straże gminne […] nie są zobowiązane do spełnienia obowiązku informacyjnego (przysługuje im bowiem uprawnienie do obserwowania i rejestrowania bez wiedzy i zgody osoby, której dane te dotyczą). Natomiast gmina — zgodnie z wyżej przytoczonymi zasadami — musiałaby spełnić obowiązek informacyjny w miejscu umieszczenia fotopułapki[26].

W tych okolicznościach należy jednak przyjąć, że PUODO najwyraźniej w swoim stanowisku nie wziął pod uwagę, że:

1. fotopułapka może rejestrować zdarzenia tylko z miejsc publicznie dostępnych;
2. fotopułapka rejestruje także inne zdarzania i osoby;
3. polski system prawny klasyfikuje określone formy stadialne wykroczenia lub przestępstwa;
4. ustawa o strażach wskazuje czas wyłączenia jawności;
5. wykładnia celowościowa wskazuje cel i zakres wyłączania tej jawności;

[26] https://uodo.gov.pl/pl/225/1447 (dostęp: 2.01.2020).

6. straż obowiązana jest wykazać niezbędność prowadzenia takich działań przy użyciu fotopułapki, a wprowadzanie wyłączeń z realizacji obowiązku informacyjnego jest już prawnie dookreślone w przepisach ogólnego rozporządzenia o ochronie danych 679/2016 i ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Innymi słowy, stosując wykładnię prezentowaną przez PUODO, można dojść do konkluzji, że każda straż pod pretekstem i przy wykazaniu niezbędności nieustannego poszukiwania sprawcy[27] na przykład zaśmiecania ulicy nie będzie obowiązana do realizowania obowiązku informacyjnego, stanowiącego element gwarancji autonomii informacyjnej podmiotu praw, czyli każdego człowieka przebywającego w tym przypadku na terenie Rzeczypospolitej Polskiej. To z kolei narzuca wniosek, że PUODO dopuszcza prowadzenie przez straże niejawnego nadzoru w każdej przestrzeni publicznej i to przy wykorzystywaniu ukrytych narzędzi rejestrujących obraz zdarzeń. To kłóci się jednak z promowanym dotychczas stanowiskiem PUODO prezentowanym podczas szkoleń dla inspektorów ochrony danych organizowanych w 2019 roku[28], między innymi w zakresie realizacji obowiązku informacyjnego.

Analizując to stanowisko PUODO, należy jednak wziąć pod uwagę, że nie jest ono bezwarunkowo wiążące, a do obowiązków komendantów należy jego ocena oraz podjęcie działań organizacyjnych i technicznych w takim zakresie, aby wszystkie procesy przetwarzania danych były realizowane w sposób zgodny z literą prawa. Dlatego też warto zasygnalizować również to, że każdy komendant straży obowiązany był do 6 lutego 2019 roku do sprawdzenia i efektywnego obudowania wszystkich występujących w straży procedur, w ramach których dochodzi do zarówno przetwarzania danych w samej straży, jak i wymiany informacji pomiędzy komendantem a innymi administratorami, w celu między innymi:

1. oceny wszystkich zachodzących procesów, a tym samym przeprowadzenia próby sfalsyfikowania poprawności wdrożonej dokumentacji z zakresu ochrony danych w straży i urzędzie gminy z uwagi na obowiązywanie przepisów ustawy z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, a tym samym zaistnieniem nowej relacji między komendantem a innymi administratorami, w tym wójtem, w obszarze przetwarzania danych osobowych;

2. wykazania w każdym czasie, że ochrona danych osobowych w ramach zidentyfikowanych procesów przetwarzania danych jest realizowana bez naruszenia obowiązujących zasad ochrony danych osobowych. Celem takich działań jest także wyłonienie procesów, w ramach których może dochodzić do współadministrowania danymi osobowymi, które winny zostać określone w umowie o współadministrowaniu, co niestety nie jest regułą; czy też wyłonienia procesów

[27] Tak jak w wizjach Paula Michela Foucaulta.

[28] https://www.uodo.gov.pl/pl/p/iod/zakonczone-szkolenia (dostęp: 2.01.2020).

opartych na powierzaniu przetwarzania danych mających swoje umocowanie formalne nie w umowie powierzenia, lecz w innych instrumentach prawnych, do których należy zaliczyć uchwały rady gminy lub zarządzenia wójta. Realizując wskazane wymogi prawne, komendant musi mieć jednak na uwadze, że wójt nie ma nieograniczonej legitymacji do przetwarzania danych będących w zasobach straży, niezależnie od jej ulokowania w strukturach gminy. Jest to o tyle istotne, że przywołane tutaj zmienne mają bezpośredni wpływ zarówno na treść samej klauzuli informacyjnej oraz regulaminu monitoringu wizyjnego, jak i legalność działań straży;

3. prowadzenia rozróżnienia danych i ewidencjonowania operacji przetwarzania danych w formie papierowej lub elektronicznej z zastrzeżeniem, o którym była mowa wcześniej.

VIDEO SURVEILLANCE IN THE ACTIVITIES OF THE MUNICIPAL POLICE: OUTLINE OF THE PROBLEM

Summary

The activities of the municipal police are of a repressive nature which enables these para-policy formations to use legal instruments and technical tools which permit the interference with the rights and freedoms embedded in the Polish Constitution. One of these tools is video surveillance — serving to observe and record events in public places. However, using video surveillance requires the fulfilment of several statutory restrictions by the municipal police. The article addresses the current duties of municipal police commanders in this field in the context of the principle of proportionality embodied in the Constitution.

Keywords: video surveillance, municipal police, personal data, data protection, GRDP, Constitution, drones

BIBLIOGRAFIA

LITERATURA

Guidelines 3/2019 on processing of personal data through video devices. Version 2.0, Adopted on 29.01.2020.

Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego z 15 czerwca 2018 roku.

WYKAZY

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. UE L z 1995 r. Nr 281/31).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L z 2016 r. Nr 119/89).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 roku w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii (Dz.U. UE L z 2019 r. Nr 305/17).

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 roku w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. z 2019 r. poz. 666).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.).

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

Rozporządzenie Delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 roku w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich (Dz.U. UE L z 2019 r. Nr 152/1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L z 2016 r. Nr 119/1).

Rozporządzenie Rady Ministrów z dnia 16 grudnia 2009 roku 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).

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526).

Rozporządzenie Wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 roku w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz.U. UE L z 2019 r. Nr 152/45).

Ustawa z dnia 20 maja 1971 roku Kodeks wykroczeń (Dz.U. z 1971 r. Nr 12, poz. 114 ze zm.).

Ustawa z dnia 26 czerwca 1974 roku Kodeks pracy (Dz.U. z 1974 r. Nr 24, poz. 141 ze zm.).

Ustawa z dnia 6 czerwca 1997 roku — Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 ze zm.).

Ustawa z dnia 6 czerwca 1997 roku Kodeks postępowania karnego (Dz.U. z 1997 r. Nr 88, poz. 555 ze zm.).

Ustawa z dnia 29 sierpnia 1997 roku o strażach gminnych (Dz.U. z 1997 r. Nr 123, poz. 779 ze zm.).

Ustawa z dnia 24 sierpnia 2001 roku — Kodeks postępowania w sprawach o wykroczenia (Dz.U. z 2001 r. Nr 106, poz. 1148 ze zm.).

Ustawa z dnia 6 września 2001 roku o dostępie do informacji publicznej (Dz.U. z 2001 r. Nr 112, poz. 1198 ze zm.).

Ustawa z dnia 3 lipca 2002 roku Prawo lotnicze (Dz.U. z 2002 r. Nr 130, poz. 1112 ze zm.).

Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.).

Ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125).

ORZECZENIA

Rozstrzygnięcie Wielkiej Izby Europejskiego Trybunału Sprawiedliwości z dnia 17 października 2019 roku w sprawie *López Libard i inni przeciwko Hiszpanii*.
Uchwała 7 sędziów SN z dnia 24 października 2014 roku, sygn. I KZP 24/12.
Uchwała SN z dnia 11 czerwca 2019 roku, sygn. I DO 11/19.
Wyrok NSA z dnia 28 listopada 2002 roku, sygn. II SA/Wa 3389/01.
Wyrok NSA z dnia 19 maja 2011 roku, sygn. II SA/Wa 1086/10.
Wyrok SA w Katowicach z 28 maja 2015 roku, sygn. I ACa 158/15.
Wyrok SN z dnia 18 marca 2008 roku, sygn. IV CSK 474/07.
Wyrok WSA w Warszawie z dnia 3 marca 2009 roku, sygn. II SA/Wa 1495/08.
Wyrok WSA w Warszawie z dnia 9 kwietnia 2013 roku, sygn. II SA/Wa 211/13.

INNE

Technologia informacyjna — Techniki bezpieczeństwa — Praktyczne zasady postępowania w zakresie ochrony danych osobowych, ISO/EOC 29151:2017.
Technika informatyczna — Techniki bezpieczeństwa — Praktyczne zasady zabezpieczania informacji, ISO/EOC 27002:2013.
Technologia informacyjna — Techniki bezpieczeństwa — Wytyczne dotyczące oceny wpływu na prywatność, ISO/EOC 29134:2017.
Technika informatyczna — Techniki bezpieczeństwa — Zarządzanie ryzykiem w bezpieczeństwie informacji, ISO/EOC 27005:2013.
Zarządzanie bezpieczeństwem informacji, ISO/EOC 27001:2017.