Prawo dla monitoringu wizyjnego cz. 4. na przykładzie Wielkiej Brytanii

Waldemar Więckowski
Polska Izba Systemów Alarmowych,
doradca Zarządu

Kompromis pomiędzy zapewnieniem bezpieczeństwa a ochroną danych osobowych powinien być wypracowany również w przypadku dozoru wizyjnego. O takiej potrzebie może świadczyć choćby sposób pojmowania tego, jaki zapis wizyjny umożliwia identyfikację osoby. Wg branży dozoru wizyjnego muszą być spełnione ściśle określone wymagania dotyczące kadru; wg odpowiedzialnych za ochronę danych osobowych – każde nagranie wizyjne.

W artykule posłużę się przykładem kompromisowych rozwiązań przyjętych w Wielkiej Brytanii. Bardzo podoba mi się wydawanie kodeksów dobrych praktyk przez brytyjskie urzędy państwowe. Nie mogę jednak powiedzieć, że opisane rozwiązanie jest modelowe, bo nie znam rozwiązań przyjętych w innych państwach. A z przyczyn oczywistych – nie jestem prawnikiem – nie odnoszę się do tego, jak opisane rozwiązanie ma się do legislacji w Polsce. Ponieważ warto czerpać z doświadczeń innych państw, ten artykuł jest zachętą – powtórzoną za RPO – do tego w przypadku „prawa dla monitoringu".

DLACZEGO WIELKA BRYTANIA JAKO PRZYKŁAD

W październiku ub.r. w biurze Rzecznika Praw Obywatelskich odbyło się seminarium *„Kto na nas patrzy? Obywatel pod obserwacją kamer"*. [1] Wśród materiałów przygotowanych przez organizatorów znalazła się *Rekomendacja Rzecznika Praw Obywatelskich w kwestii prawnej regulacji funkcjonowania monitoringu wizyjnego w Polsce.* [2] Jej punkt drugi dotyczy czerpania z doświadczeń innych państw:

W niektórych państwach funkcjonowanie monitoringu wizyjnego zostało już uregulowane w instrumentach prawnych (Wielka Brytania, Holandia, Szwecja). ***Analiza funkcjonowania przyjętych w innych krajach rozwiązań może być dla polskiego ustawodawcy pomocna w opracowywaniu kształtu polskiej regulacji, jak również może służyć jako źródło dobrych praktyk.***

Nie wiem, bo tego nie wyjaśniono, dlaczego prof. Irena Lipowicz – rzecznik praw obywatelskich – wymieniła akurat te trzy kraje i z jakiego powodu Wielka Brytania znalazła się na pierwszym miejscu. Być może bez szczególnego.

Wielka Brytania pojawia się również w przygotowanym na to seminarium materiale fundacji Panoptykon *Regulacje prawne monitoringu wizyjnego – zarys rozwiązań przyjętych w różnych państwach.* [3] Tym razem jako jedno z sześciu państw, ale nadal na pierwszym miejscu, łamiąc porządek alfabetyczny, podobnie jak w materiale RPO. Autorzy notki o tym kraju odnotowali następujące cechy charakterystyczne uregulowań prawnych dotyczących dozoru CCTV:

Wielka Brytania – szerokie obowiązki informacyjne

- *Prawo: Ustawa o ochronie danych z 1998 r., Rozporządzenie o uprawnieniach organów śledczych z 2000 r., CCTV Code of Practice z 2008 r., Code of Practice on Covert Surveillance and Property Interference z 2000 r.*
- *Obowiązek* ***informowania o obecności kamer*** *(np. za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych). Takie informacje muszą być* ***widoczne i czytelne*** *oraz zawierać* ***dane operatora systemu monitoringu****, w tym kontakt do osoby, która może odpowiedzieć na ewentualne pytania lub dostarczyć szczegółowych informacji. Znaki muszą być stosowane przez wszystkie podmioty korzystające z monitoringu.*
- *Gdy osobę uchwyconą przez monitoring da się zidentyfikować, nagranie traktowane jest jak dane osobowe. W takiej sytuacji przetwarzanie danych musi być zgodne z zasadami wyrażonymi w ustawie o ochronie danych i służyć jednemu z wymienionych w niej celów.*
- *W 2012 r. w Wielkiej Brytanii powołano* ***pierwszego komisarza ds. CCTV,*** *który ma zachęcać operatorów do przestrzegania przepisów, reprezentować interesy społeczeństwa, a także składać roczny raport przed parlamentem.*

Powyższa charakterystyka już sama w sobie jest wystarczająco zachęcająca, aby przyjrzeć się uregulowaniom brytyjskim. Gdyby jednak ktoś z branży dozoru wizyjnego nie czuł się jeszcze przekonany, to przesądzającym, choć pośrednim, argumentem może być przywołanie przygotowanych przez brytyjską policję wytycznych stosowania systemów dozorowych CCTV, które we fragmentach wykorzystano później w przygotowaniu arkusza 7. normy europejskiej EN 50132.

Skoro brytyjskie uregulowania standaryzacyjne i normalizacyjne dotyczące dozoru CCTV są na tak wysokim poziomie, to zapewne na co najmniej takim samym poziomie będą uregulowania legislacyjne dotyczące stosowania tego dozoru.

DATA PROTECTION ACT 1998 (USTAWA O OCHRONIE DANYCH Z 1998)

W tej brytyjskiej ustawie nie ma słowa o CCTV czy o dozorze wizyjnym *(CCTV surveillance)*. Ale nie wspomina ich też polska ustawa o ochronie danych osobowych. Co więcej, nie pojawia się w niej pojęcie *image*, tak jak w polskiej ustawie nie pojawiają się słowa *wizerunek* czy *obraz*.

Obie ustawy – brytyjska i polska – przewidują powołanie urzędu Generalnego Inspektora (w Wielkiej Brytanii *Data Protection Commissioner* – komisarz ds. ochrony danych) i określają jego obowiązki. Obie ustawy w żaden sposób nie ukierunkowują inspektora (komisarza) na zajęcie się zagadnieniem uregulowania dozoru CCTV.

W cztery miesiące po wejściu w życie ustawy *Data Protection Act 1998* brytyjski komisarz ds. ochrony danych publikuje *CCTV Code of Practice* (Kodeks praktyk CCTV).

CCTV CODE OF PRACTICE (KODEKS PRAKTYK CCTV)

***CCTV Code of Practice* jest dokumentem brytyjskiego komisarza ds. ochrony danych!** Zazwyczaj pomija się ten fakt, a ma on przecież istotne znaczenie dla zawartości dokumentu. Kodeks jest przewodnikiem takiego planowania dozoru CCTV, które ma zapewnić zgodność (dozoru) z wymaganiami ustawy o ochronie danych. Żadne inne (!) aspekty nie są w tym kodeksie w zasadzie uwzględnione.

Ciekawe jest to, co we wstępie do pierwszej edycji (z 2000 r.) kodeksu napisano o jego powstaniu (tłumaczenie własne):

(…) Do 1 marca 2000 r., kiedy zaczęła obowiązywać ustawa o ochronie danych, nie istniała ustawowa baza systematycznej kontroli prawnej dozoru CCTV w obszarach publicznych. Definicje w nowej ustawie są szersze niż znajdujące się w ustawie o ochronie danych z 1984 i dlatego łatwiej objąć nimi przetwarzanie obrazów osób uchwyconych przez kamery CCTV, niż w przypadku poprzedniej legislacji dot. ochrony danych. Te same prawnie obowiązujące normy postępowania z informacjami, które poprzednio odnosiły się do przetwarzania danych osobowych na komputerach, teraz obejmują CCTV. Ważną nową cechą ostatniej legislacji jest przyznanie uprawnień do wydania przez komisarza kodeksu praktyk (…) ustanawiającego przewodnik postępowania zgodnego z dobrą praktyką.

Kodeks praktyk CCTV jest pierwszym kodeksem wydanym przez komisarza ds. ochrony danych w ramach uprawnień przyznanych mu ustawą o ochronie danych z 1998. Ustawa zaczęła obowiązywać 1 marca 2000 r., a kodeks wydano już w lipcu tego samego roku.

Status prawny CCTV Code of Practice

Najlepiej status prawny tego kodeksu oddają dwa dokumenty: sam *CCTV Code of Practice* w pierwszym wydaniu z 2000 r. oraz odpowiedź komisarza ds. informacji z maja 2011 r. [4] na konsultacje Home Office dotyczące opracowania kodeksu praktyk dozoru wizyjnego. [5]

We wstępie do *CCTV Code of Practice* znajduje się następujący fragment:

(…) Istnieją normy opracowane przez reprezentantów operatorów systemów CCTV, a także, w szczególności, przez Brytyjski Instytut Normalizacyjny (BSI – odpowiednik Polskiego Komitetu Normalizacyjnego). I chociaż tego typu normy są użyteczne, to nie mogą one być prawnie obowiązujące. Zmiany w legislacji dotyczącej ochrony danych oznaczają, że po raz pierwszy prawnie obowiązujące normy będą dotyczyć pozyskiwania i przetwarzania obrazów powiązanych z osobami.

(...)

Niniejszy kodeks praktyk ma podwójne zadanie: wspomóc operatorów systemów CCTV w zrozumieniu swoich obowiązków prawnych, równocześnie upewniając ogół o ochronie, która powinna być zapewniona. Kodeks ustanawia przedsięwzięcia, które muszą być podjęte, aby uzyskać zgodność z postanowieniami Data Protection Act 1998 (ustawy o ochronie danych z 1998), a także idzie dalej, wprowadzając przewodnik postępowania zgodnego z dobrą praktyką ochrony danych. Kodeks jasno określa standardy, które muszą być spełnione, aby zapewnić zgodność z Data Protection Act 1998, a następnie wskazuje te, które nie są ścisłym wymaganiem prawnym, ale reprezentują postępowanie zgodne z dobrą praktyką.

Z kolei komisarz ds. informacji (następca komisarza ds. ochrony danych) [4] na konsultacje Home Office dotyczące opracowywanego kodeksu praktyk dozoru wizyjnego [5] odpowiedział:

(...) Kodeks praktyk CCTV opracowany przez komisarza ds. informacji jest przeznaczony do pomocy operatorom CCTV w spełnieniu ich zobowiązań prawnych i nie jest tylko czymś skierowanym do tych prawomyślnych, którzy chcą stosować dobrą praktykę. Kodeks zawiera zalecenia komisarza ds. informacji, jak można spełnić wymagania prawne ustawy o ochronie danych, a zalecenia te są oparte na prawnie obowiązujących zasadach ochrony danych. Jak jasno stwierdza kodeks komisarza ds. informacji, operatorzy mogą stosować alternatywne metody spełnienia wymagań prawnych, lecz jeśli nie zrobią niczego, ryzykują naruszenie prawa. (...)

W uzupełnieniu wątku statusu prawnego *CCTV Code of Practice* przytoczyłbym jeszcze zapis *Data Protection Act 1998* (ustawy o ochronie danych z 1998) dotyczący inicjatywy (decyzji) o przygotowywaniu kodeksów. Znajduje się on w we fragmencie dotyczącym obowiązków komisarza ds. ochrony danych (podpunkt 3 punktu 51 ustawy):

W przypadku, kiedy
(a) sekretarz stanu wskaże to, wydając nakaz, lub
(b) komisarz uzna za właściwe to uczynić,
komisarz powinien, po konsultacjach z izbami gospodarczymi, podmiotami danych lub z osobami reprezentującymi podmioty danych, jak wyda się mu to właściwe, przygotować i rozpowszechnić wśród osób, które uzna za właściwe kodeksy praktyk służące za przewodniki po dobrych praktykach.

W moim rozumieniu zacytowane fragmenty świadczą o tym, że *CCTV Code of Practice* nie jest dokumentem obligatoryjnym – zawiera natomiast zbiór metod (jednych z wielu) umożliwiających spełnienie wymagań ustawy o ochronie danych, czego zaniechanie oznacza ryzyko naruszenia prawa.

CCTV Code of Practice jest przewodnikiem pomocnym przy realizacji zapisów ustawy o ochronie danych. Czy istnieją inne kodeksy przydatne przy realizacji wymagań, związanych np. z zapewnieniem bezpieczeństwa czy też z ochroną osób i mienia? Odpowiedzi na to pytanie należy szukać w innej ustawie – *Protection of Freedoms Act 2012* (ustawie o ochronie swobód z 2012).

Domaganie się, aby w przypadku dozoru wizyjnego jedną ustawą uregulować zagadnienia zapewnienia bezpieczeństwa i ochrony danych osobowych, jest jak domaganie się, aby pogodzić ogień z wodą. Tę sprzeczność doskonale zrozumieli Brytyjczycy, którzy kierując się nadrzędną zasadą ochrony swobód obywatelskich, zachowali jednak odrębność uregulowań szczegółowych tych zagadnień w odniesieniu do dozoru wizyjnego.

PROTECTION OF FREEDOMS ACT 2012 (USTAWA O OCHRONIE SWOBÓD Z 2012)

Zgodnie z tą ustawą ma zostać wydany kodeks praktyk systemów dozoru wizyjnego *(code of practice about surveillance camera systems)* oraz mianowany komisarz ds. dozoru wizyjnego *(Surveillance Camera Commissioner)*. Tym zadaniem zostało „obarczone" Home Office (brytyjskie MSW).

Różnice pomiędzy przywołanymi kodeksami praktyk – CCTV i dozoru wizyjnego – zaczynają się już od trybu stanowienia obu dokumentów.

Data Protection Act 1998 (ustawa o ochronie danych z 1998) nadaje brytyjskiemu komisarzowi ds. ochrony danych uprawnienia do wydania kodeksów praktyk, nie nakładając jednak na niego obowiązku wydania kodeksu dedykowanego konkretnej dziedzinie. Jedynym przypadkiem, gdy komisarz musi ustanowić kodeks, jest bezpośredni nakaz sekretarza stanu, który też nie jest zobligowany do jego wydania.

Natomiast *Protection of Freedoms Act 2012* (ustawa o ochronie swobód z 2012) nakazuje wprost (sekretarzowi stanu) wydanie kodeksu praktyk systemów dozoru wizyjnego (rozdział 29, punkt 1): Sekretarz Stanu musi przygotować kodeks praktyk zawierający porady dotyczące systemów dozoru wizyjnego.

SURVEILLANCE CAMERA CODE OF PRACTICE (KODEKS PRAKTYK DOZORU WIZYJNEGO)

Zakres tego kodeksu został określony w Rozdziale 29 Ustawy o ochronie swobód z 2012:

(2) Kodeks musi zawierać porady dotyczące jednej lub kilku spośród następujących (czynności):
(a) opracowywania lub stosowania systemów dozoru wizyjnego,
(b) wykorzystywania lub przetwarzania obrazów lub innych informacji uzyskanych dzięki takim systemom.
(3) Kodeks może, w szczególności, zawierać klauzule dotyczące:
(a) rozważań, czy zastosować systemy dozoru wizyjnego,
(b) typu systemów lub urządzeń,
(c) norm (standardów) technicznych na systemy lub urządzenia.
(d) lokalizacji systemów lub urządzeń,
(e) publikacji informacji o systemach lub urządzeniach,
(f) norm (standardów) dotyczących osób korzystających z lub utrzymujących w ruchu systemy lub urządzenia,
(g) norm (standardów) dotyczących osób korzystających z lub przetwarzających informacje uzyskane za pomocą systemów,
(h) dostępu do uzyskanych informacji lub ich udostępniania,
(i) procedur zażaleń i konsultacji.
(…)
(6) W niniejszym rozdziale określenie „systemy dozoru wizyjnego" oznacza:
(a) systemy telewizji w obwodzie zamkniętym lub systemy automatycznego rozpoznawania tablic rejestracyjnych,
(b) jakiekolwiek inne systemy do nagrywania lub przeglądu obrazów wizyjnych dla celów dozoru,
(c) jakiekolwiek systemy do przechowywania, odbioru, transmisji, przetwarzania lub kontroli obrazów lub informacji uzyskanych za pomocą systemów określonych w punktach (a) lub (b) wyżej, lub
(d) jakiekolwiek inne systemy związane lub inaczej połączone z systemami określonymi w punktach (a), (b) lub (c) wyżej.

Status prawny Surveillance Camera Code of Practice

Wydaje się że, najlepiej opisuje go punkt 2. w rozdziale 33. Ustawy o ochronie swobód z 2012:

Zaniechanie ze strony jakiejkolwiek osoby działania zgodnego z którąkolwiek klauzulą kodeksu dozoru wizyjnego samo w sobie nie powoduje, że ta osoba podlega postępowaniu karnemu lub cywilnemu.

a także punkt 2. w rozdziale 34. określający obowiązki komisarza ds. dozoru wizyjnego w odniesieniu do kodeksu:

Komisarz powinien pełnić następujące funkcje:
(a) propagować zgodność z kodeksem dozoru wizyjnego,
(b) prowadzić przegląd funkcjonowania kodeksu oraz
(c) udzielać porad w sprawach kodeksu (włącznie ze zmianami lub odstępstwami).

PODZIAŁ KOMPETENCJI (ZADAŃ) POMIĘDZY KOMISARZAMI DS. INFORMACJI I DS. DOZORU WIZYJNEGO

Istotę tego podziału najlepiej oddaje odpowiedź [4] komisarza ds. informacji na konsultacje Home Office dotyczące kodeksu praktyk dozoru wizyjnego. [5]

Komisarz ds. informacji jest odpowiedzialny za propagowanie oraz wprowadzenie w życie ustawy o ochronie danych z 1998 (Data Protection Act 1998, DPA) *oraz ustawy o swobodzie dostępu do informacji 2000* (Freedom of Information Act 2000, FOIA). *Komisarz jest niezależny od rządu i podtrzymuje prawo do informacji w interesie publicznym, propagując otwartość ciał publicznych oraz prywatność danych osób fizycznych. (…)*

W rozdziale poświęconym ocenie podejścia rządu do regulacji w zakresie dozoru wizyjnego komisarz ds. informacji nawiązuje do wydanego przez siebie kodeksu praktyk CCTV:

Komisarz ds. informacji jest zainteresowany istnieniem skutecznej regulacji systemów CCTV oraz automatycznego rozpoznawania tablic rejestracyjnych (ANPR), a także innych pojawiających się technologii kamerowych. Zapewnienie, że dozór wizyjny jest przedmiotem skutecznej kontroli, jest sprawą zasadniczą i dlatego komisarz wspiera propozycje rządowe podniesienia standardów oraz dalszych uregulowań w tym ważnym obszarze. Aby pomóc zapewnić, że kamery CCTV są stosowane odpowiedzialnie i wesprzeć operatorów CCTV w przestrzeganiu legislacji o ochronie danych, komisarz ds. informacji opublikował w roku 2000 Kodeks praktyk CCTV, zrewidowany w roku 2008. Ustawa o ochronie danych z 1998 będzie nadal obowiązywać tam, gdzie wchodzą w grę obrazy osób fizycznych, we wszystkich sektorach w Zjednoczonym Królestwie. Jest ważne, aby kodeks praktyk dozoru wizyjnego Home Secretary (MSW) był spójny z jej wymaganiami, wzmacniał ochronę oraz nie prowadził do nieporozumień odnośnie do zobowiązań prawnych.

Komisarz ds. informacji podkreśliwszy, że wydany przez niego kodeks praktyk CCTV jest poradnikiem zorientowanym na zagadnienia ochrony danych, zwraca uwagę na swoją wyłączną odpowiedzialność za te zagadnienia.

(…) z zadowoleniem przyjmuje się wyjaśnienie rządu, że nic w projekcie ustawy o ochronie swobód (Protection of Freedoms Bill), co dotyczy uregulowań w zakresie systemów dozoru wizyjnego, nie będzie kolidować z obecną rolą i odpowiedzialnością komisarza ds. informacji i że będzie on nadal posiadał prymat i wyłączną odpowiedzialność w zakresie ochrony danych.

Postawiwszy jasno sprawę nienaruszalności i odrębności swoich kompetencji, komisarz ds. informacji:

• odnosi się do roli nowego komisarza ds. dozoru wizyjnego:

Rząd jasno stwierdził, że rola i odpowiedzialność nowego komisarza ds. dozoru wizyjnego, chociaż różna będzie komplementarna do roli i odpowiedzialności komisarza ds. informacji a także, że w dużym stopniu będzie istniał wspólny interes. (…)

• wyraża swoją opinię odnośnie kodeksu dozoru wizyjnego:

Pomocne dla rządu może być rozważenie, czy kodeks Home Secretary (MSW) nie powinien być poświęcony przede wszystkim ustanowieniu standardów w kwestiach technicznych i użytkowych.

• a także proponuje wprowadzeń wzajemnych odwołań w obu kodeksach:

Byłoby możliwe ustanowienie w kodeksie dozoru wizyjnego odwołań do kodeksu wydanego przez komisarza ds. informacji; a w zamian dokonanie w tym drugim zmian zawierających odwołania do kodeksu Home Office, tak jak obecnie zawiera on odwołania do wytycznych dostarczonych przez Home Office's Scientific Development Branch (HOSDB – Ośrodek Naukowo-Rozwojowy Ministerstwa Spraw Wewnętrznych). Ponieważ oba kodeksy będą musiały koegzystować, ważne, aby były one komplementarne, a nie przeciwstawne.

PODSUMOWANIE

W publicznej dyskusji o uregulowniach prawnych monitoringu wizyjnego w Polsce zagadnienia dotyczące zapewnienia bezpieczeństwa, a zwłaszcza ochrony osób i mienia (zabezpieczenia) zostały zdominowane przez zagadnienia ochrony prywatności i danych osobowych. Chociaż są one jak dwie strony tej samej monety, domaganie się przez prominentnych uczestników publicznej dyskusji, aby uregulować je jedną ustawą, jest jak domaganie się, by pogodzić ogień z wodą.

Ta sprzeczność nie jest widoczna, bo debatom ton nadają rzecznicy ochrony prywatności i danych – GIODO, RPO oraz fundacja Panoptykon. To niewątpliwie cena, jaką MSW płaci za brak uczestnictwa w dyskusji. Nie zmienia to jednak istoty rzeczy, że zadania związane z ochroną danych osobowych (informacji) i dozorem wizyjnym (zapewnieniem bezpieczeństwa) są z natury różne.

Przedstawiony w artykule przykład Wielkiej Brytanii jest doskonałym dowodem na to, że warto rozważyć ich odrębne uregulowanie.

I co w tym przykładzie równie istotne, ten rozdział kompetencji inicjatywą skorelowania kodeksów praktyk wspiera brytyjski komisarz ds. informacji. Być może czyni to również dlatego, że jego urząd ustanowiono co najmniej 12 lat wcześniej niż urząd komisarza odpowiedzialnego za dozór wizyjny, ma więc spore doświadczenie i znajomość specyfiki dozoru wizyjnego.

Literatura:

[1] *Kto na nas patrzy? Obywatel pod obserwacją kamer,* seminarium RPO, GIODO i Fundacji Panoptykon, 11 października 2012 r.

[2] *Rekomendacja Rzecznika Praw Obywatelskich w kwestii prawnej regulacji funkcjonowania monitoringu wizyjnego w Polsce,* seminarium RPO, GIODO i Fundacji Panoptykon, 11 października 2012 r.

[3] *Regulacje prawne monitoringu wizyjnego – zarys rozwiązań przyjętych w różnych państwach,* Fundacja Panoptykon, seminarium RPO, GIODO i Fundacji Panoptykon, 11 października 2012 r.

[4] *Consultation On A Code Of Practice Relating To Surveillance Cameras, Home Office,* ISBN: 978-1-84987-433-5.

[5] *The Information Commissioner's response to the Home Office consultation on a code of practice relating to surveillance camera, Information Commissioner's Office,* 24.05.2011.