KIEDY STRUŚ WŁOŻY GŁOWĘ W PIASEK, CZYLI CO WIDAĆ, GDY PATRZYMY W OKO KAMERY WIDEOMONITORINGU

SEMINARIUM
„KTO NA NAS PATRZY? OBYWATEL POD OBSERWACJĄ KAMER”
zorganizowane przez Rzecznika Praw Obywatelskich,
Generalnego Inspektora Ochrony Danych Osobowych
oraz Fundację Panoptykon

Dr WOJCIECH WIEWIÓROWSKI
Generalny Inspektor Ochrony Danych Osobowych / WPiA Uniwersytet Gdański

Warszawa, 11 października 2012 r.
Biuro Rzecznika Praw Obywatelskich

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ (art. 51)

1. *Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.*
2. *Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.*
3. *Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.*
4. *Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.*
5. *Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.*

GIODO
Generalny Inspektor Ochrony Danych Osobowych

KILKA PODSTAWOWYCH POJĘĆ

Art. 6. 1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

KILKA PODSTAWOWYCH POJĘĆ

Art. 7. Ilekroć w ustawie jest mowa o:

1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

2) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych, (…)

4) administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę (…) decydujące o celach i środkach przetwarzania danych osobowych,

5) zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie,

NAGRANIE Z MONITORINGU JAKO ZBIÓR DANYCH OSOBOWYCH

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

KODEKS PRACY

Art. 22[1]. § 1. Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:

1) imię (imiona) i nazwisko,

2) imiona rodziców,

3) datę urodzenia,

4) miejsce zamieszkania (adres do korespondencji),

5) wykształcenie,

6) przebieg dotychczasowego zatrudnienia.

§ 2. Pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, także:

1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,

2) numeru PESEL (…).

§ 4. Pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

§ 5. W zakresie nieuregulowanym w § 1-4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych.

ADEKWATNOSC

Art. 26. 1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem,

2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2,

3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

ADEKWATNOSC

Obowiązek badania adekwatności przetwarzania danych osobowych wynika nie tylko z przepisów ustawy o ochronie danych osobowych, ale także z Dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (95/46/WE). Zgodnie z art. 6 ust. 1 lit. c/ Dyrektywy, państwa członkowskie mają obowiązek dopilnowania, żeby dane osobowe były nie nadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone

ADEKWATNOSC

Stosowność – czy zastosowany środek jest stosowny i odpowiedni do celów, które mają zostać osiągnięte

Konieczność - czy zastosowany środek jest konieczny do celów, które mają zostać osiągnięte

Proporcjonalność *senso stricto* – czy zastosowany środek nie ingeruje w prywatność bardziej niż jest to konieczne

Szerzej o adekwatności i zgodzie: L.A.Bygrave, D.W.Schartum: *Consent, Proportionality and Collective Power* [w:] S.Gutwirth, Y.Poullet, P.De Hert, C.de Tervangne, S.Nouwt [red.] *Reinventing Data Protection,* Springer 2009, s. 157

MONITORING

Przestrzeń publiczna

Przestrzeń prywatna dostępna dla nieokreślonej liczby osób

Przestrzeń prywatna dostępna dla określonych osób

Przestrzeń prywatna

Monitoring pracowników

Monitoring „*quasi*-pracowników”

Monitoring w miejscach szczególnych ze względu na prywatność

Monitoring w miejscach szczególnych ze względów bezpieczeństwa

Systemy łączące różne rodzaje danych w tym dane z monitoringu

Systemy inteligentne (i samouczące się) korzystające z danych z monitoringu

…

CELE MONONITORINGU JAKO CELE PRZETWARZANIA DANYCH

- **Kamery do bieżącej obserwacji**
  - poszerzenie pola widzenia osoby, sprawującej nadzór nad powierzonym terenem,
  - promocja miejsc turystycznych, takich jak plaże, stoki narciarskie,
  - pokazanie zjawisk przyrodniczych lub naukowych
- **Obserwacja i zapis obrazu na elektronicznych nośnikach informacji**
  - oprócz doraźnego celu, jakim jest obserwacja, istnieją inne cele np. zapamiętanie obrazu dla celów dowodowych, lub zapewnienie możliwości ponownej jego obserwacji w celu przyjrzenia się jego szczegółom.
- **Zapisywanie obrazu w celu zapewnienia możliwości jego odtworzenia w przyszłości**
  - rejestracja obrazu służy głównie celom dowodowym i prewencyjnym tj. zniechęcającym do popełnienia zabronionych czynów na skutek łatwych możliwości ich wykrycia, a równoległa obserwacja i zapamiętywanie wiązałoby się z niewspółmiernie wielkimi kosztami.

CELE MONONITORINGU JAKO CELE PRZETWARZANIA DANYCH

...

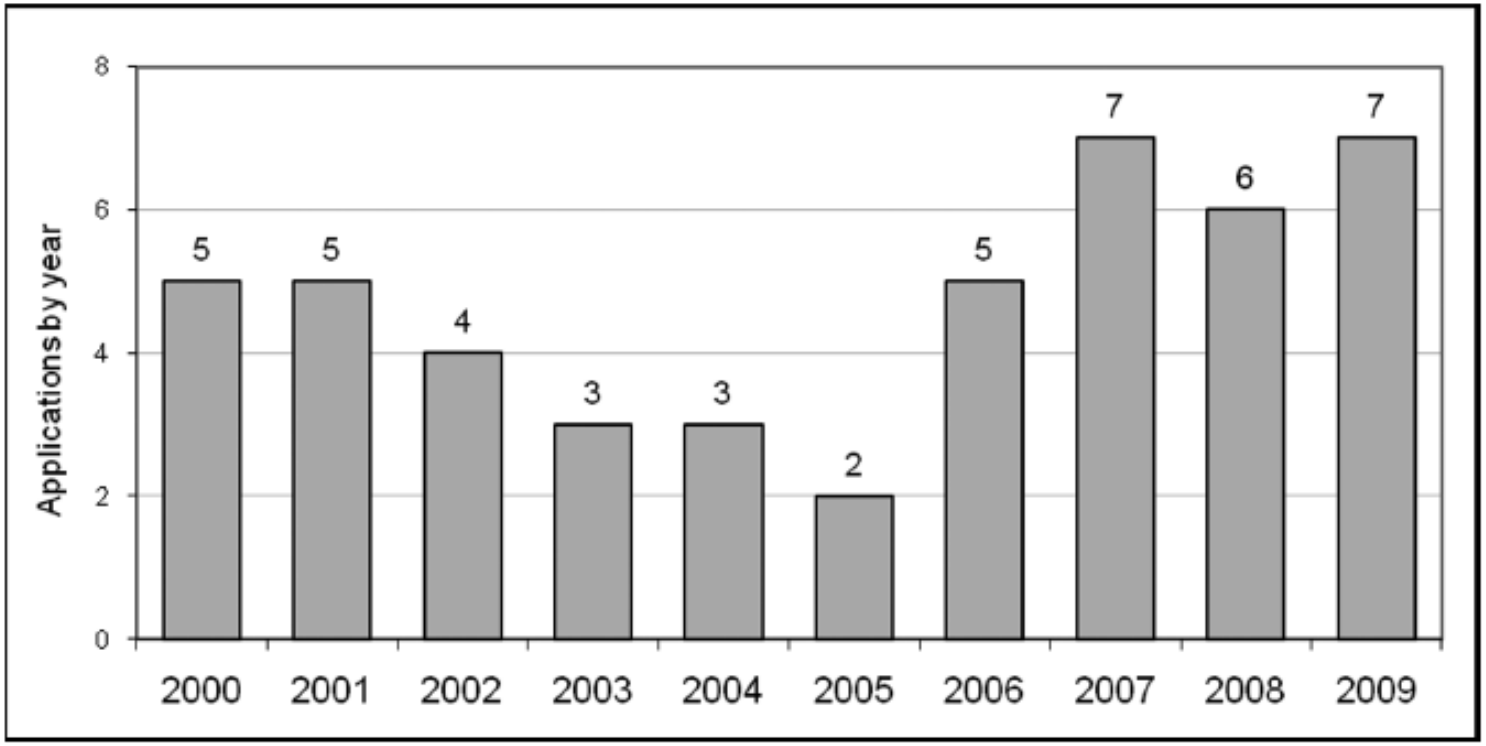

Fig. 10. Number of requests for CCTV to the CCDVC by year (2000–2009).

Gemma Galdon Clavell, *Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia*, Information Polity 16 (2011) 334

CELE MONONITORINGU JAKO CELE

Table 3
CCTV files (not cameras) registered with AEPD until 31/05/10

Year of registration	Private CCTV	Public CCTV	CCTV total
1994	8	2	10
1995	4	0	4
1996	1	0	1
1997	0	0	0
1998	0	0	0
1999	3	0	3
2000	13	0	13
2001	17	0	17
2002	32	0	32
2003	90	0	90
2004	118	3	121
2005	250	0	250
2006	433	14	447
2007	4,776	89	4,865
2008	9,212	184	9,396
2009	21,973	285	22,258
2010	13,818	403	14,221

Gemma Galdon Clavell, *CCTV in Spain: An empirical account of the deployment of video-surveillance in a southern-european country*, Information Polity 16 (2011) p. 6

CELE MONONITORINGU JAKO CELE PRZETWARZANIA DANYCH

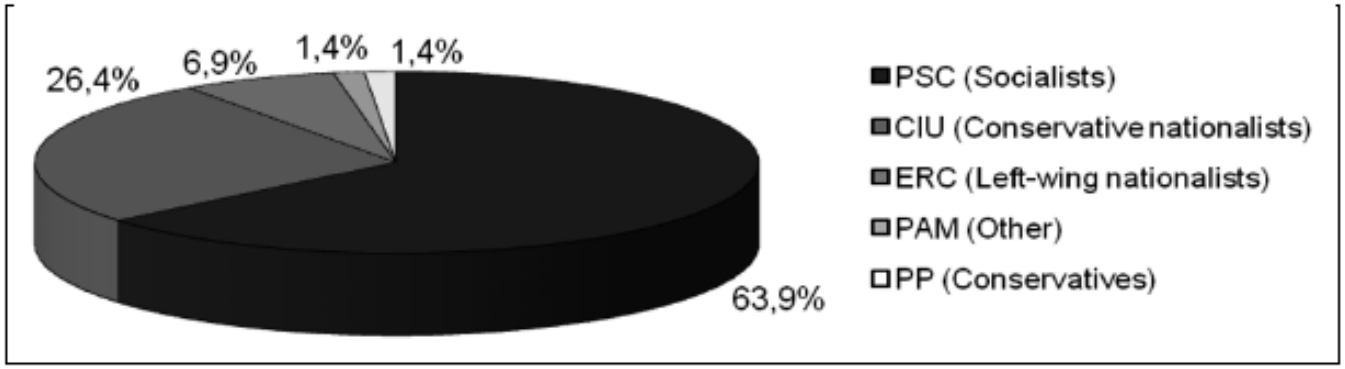

Fig. 8. Political affiliation of local community safety councilors at the time of first request for CCTV.

Gemma Galdon Clavell, *Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia*, Information Polity 16 (2011) 326

DANE OSOBOWE W SYSTEMACH WIDEONADZORU

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

- Opinia Grupy Roboczej art. 29,
- pojęcie danych osobowych obejmuje informacje dostępne w jakiejkolwiek formie, na przykład alfabetycznej, liczbowej, graficznej, fotograficznej lub akustycznej
- danymi osobowymi są zatem również wizerunki osób fizycznych, jak również profile otaczających je przedmiotów ułatwiających często ich identyfikację
- Dyrektywa: „jeżeli w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, niniejsza dyrektywa powinna mieć zastosowanie do przetwarzania takich danych".

DANE OSOBOWE W SYSTEMACH WIDEONADZORU

- przetwarzanie takich danych jest objęte dyrektywą 95/46, ale tylko wtedy, gdy jest ono zautomatyzowane lub jeśli dane te zawarte są lub przeznaczone do umieszczenia w zbiorze danych zorganizowanym według określonych kryteriów dotyczących osób fizycznych w celu zapewnienia łatwego dostępu do nich.
- kryterium dotyczące automatyzacji przetwarzania, w przypadku wideofilmowania jest na ogół spełnione.
- Niezależnie od zastosowanej metody analizy rejestrowanych obrazów, każdy przypadek, gdzie obraz rejestrowany jest automatycznie należy uznać jako czynność zautomatyzowaną, a więc jako czynność objętą dyrektywą 95/46.

DANE OSOBOWE W SYSTEMACH WIDEONADZORU

- Należy przyjąć, iż zarówno dane wizualne jak i dźwiękowe będą uznane za dane osobowe, **jeżeli umożliwiają identyfikację osoby, której dotyczą lub też istnieje duże prawdopodobieństwo jej identyfikacji**.
- Będą nimi w szczególności wtedy, **gdy nastąpi powiązanie z innymi danymi umożliwiającymi identyfikację**, przy czym dodatkowe dane nie muszą się znajdować w dyspozycji tego samego administratora ale mogą być przechowywane przez osoby trzecie. Ewolucja dostępnych technologii, w tym systemów głębokiej analizy danych (data mining) niewątpliwie zwiększają możliwości identyfikacji osoby, której dane aktualnie mogą nie mieć statusu danych osobowych. Biorąc pod uwagę koncentrację informacji o charakterze osobowym i nieosobowym w sieci Internet, możliwości ich łączenia ze sobą, zestawiania i tworzenia w ten informacji o nowej jakości, Grupa Robocza art. 29 zwraca uwagę na konieczność globalnie selektywnego i systematycznego podejścia do tego tematu.

DANE OSOBOWE W SYSTEMACH WIDEONADZORU

- **Grupa Robocza art. 29 -** należy traktować dane jako dane osobowe:
- *„a) nawet jeżeli obrazy używane są w obwodzie zamkniętym, nawet jeżeli nie są połączone z danymi identyfikacyjnymi danej osoby,*
- *b) nawet jeżeli nie dotyczą osób, których twarze zostały sfilmowane, lecz zawierają inne informacje (np. tablica rejestracyjna samochodu lub numer PIN – otrzymany w wyniku nadzorowania urządzenia do automatycznego pobierania pieniędzy),*
- *c) niezależnie od nośnika informacji używanego przy przetwarzaniu (np. systemy video stałe lub przenośne, takie jak przenośne odtwarzacze video, obrazy kolorowe i/lub czarno-białe), od stosowanej techniki (urządzenia kablowe, urządzenia światłowodowe), typu aparatu (stałe, rotacyjne, przenośne), sposobu filmowania (ciągły lub nieciągły, np. obrazy uzyskiwane w przypadku przekraczania dozwolonej prędkości; inaczej jest w przypadku zapisu obrazu uzyskanego w sposób okazjonalny i odosobniony), jak również komunikacji (połączenie z „centrum" rozpo-wsze-chnia-nia obrazów do zdalnych terminali; itd.)*."

DANE OSOBOWE W SYSTEMACH WIDEONADZORU

Dyrektywa 95/46/WE nie obejmuje operacji przetwarzania danych w zakresie współpracy policyjnej i sądowej w sprawach karnych oraz „przetwarzania związanego z bezpieczeństwem publicznym, obronnością, bezpieczeństwem państwa (łącznie ze stanem gospodarki państwa, kiedy przetwarzanie danych dotyczy bezpieczeństwa państwa) oraz z działalnością państwa w dziedzinach prawa karnego".

Ograniczenie to znajduje również odzwierciedlenie w motywie 16 preambuły do ww. dyrektywy, który stanowi, że *„przetwarzanie danych dźwiękowych i obrazowych, np. w przypadku nadzoru kamer wideo, nie wchodzi w zakres niniejszej dyrektywy, jeśli dokonywane jest dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub też w trakcie działań organów państwowych w dziedzinie prawa karnego lub innych działań nie wchodzących w zakres prawa Wspólnoty"*.

DANE OSOBOWE W SYSTEMACH WIDEONADZORU

- Nadmienić również należy, że dyrektywa 95/46/WE nie jest jedynym aktem prawnym dotyczącym ochrony danych osobowych, który ma zastosowanie do przetwarzania danych osobowych w związku ze stosowanie systemów wideo nadzoru.
- Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych

  „Konwencja ma na celu zagwarantowanie, na terytorium każdej ze Stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowanie jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych (ochrona danych)”.

DANE OSOBOWE W SYSTEMACH WIDEONADZORU

O znaczeniu, jakie ma monitoring dla ochrony prywatności osoby fizycznej w świetle ochrony prywatności, o której mowa w Konwencji Nr 108 świadczy raport dotyczący zasad jakie w celu ochrony prywatności powinny być stosowane przy pozyskiwaniu i przetwarzaniu danych za pomocą środków monitoringu wizyjnego opracowany przez Grupę Projektową w zakresie Ochrony Danych Osobowych (CJ-PD) przyjęty przez Europejski Komitet ds. Współpracy Prawnej (CDCJ) na 78 spotkaniu w dniach 20-23 maja 2003 r. czy też raport Komisji Weneckiej Rady Europy na temat „Wideonadzoru Miejsc Publicznych Przez Władzę oraz Ochrony Praw Człowieka" z marca 2007 r.

WIDEONADZÓ R W PROJEKCIE NOWYCH RAM PRAWNYCH OCHRONY DANYCH W UE - rozporządzenie

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Artykuł 33 ***Ocena skutków w zakresie ochrony danych***

1. Jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych.

WIDEONADZÓ R W PROJEKCIE NOWYCH RAM PRAWNYCH OCHRONY DANYCH W UE - rozporządzenie

Artykuł 33 ***Ocena skutków w zakresie ochrony danych*** […]

2. Szczególne ryzyko, o którym mowa w ust. 1, stwarzają w szczególności następujące operacje przetwarzania:

a) systematyczna i kompleksowa ocena aspektów osobowych osoby fizycznej bądź operacje przetwarzania mające na celu analizę lub przewidzenie w szczególności […] miejsca pobytu, stanu zdrowia, preferencji osobistych, […] lub zachowania osoby fizycznej, która opiera się na automatycznym przetwarzaniu, i na której opierają się środki, które wywołują skutki prawne dotyczące danej osoby lub mają na nią istotny wpływ; […]

c) **monitorowanie publicznie dostępnych miejsc, zwłaszcza przy wykorzystaniu urządzeń optyczno-elektronicznych (wideonadzór) na szeroką skalę;** […]

3. Ocena obejmuje przynajmniej ogólny opis przewidywanych operacji przetwarzania, ocenę ryzyk dla praw i wolności podmiotów danych, środki przewidywane w celu sprostania ryzykom, gwarancje, środki i mechanizmy bezpieczeństwa mające zagwarantować ochronę danych osobowych oraz wykazać zgodność z niniejszym rozporządzeniem, uwzględniając prawa i słuszne interesy podmiotów danych i innych zainteresowanych osób.

WIDEONADZÓ R W PROJEKCIE NOWYCH RAM PRAWNYCH OCHRONY DANYCH W UE - rozporządzenie

Artykuł 33 ***Ocena skutków w zakresie ochrony danych*** […]

4. Administrator zwraca się o opinie do podmiotów danych lub ich przedstawicieli w zakresie planowanego przetwarzania, bez uszczerbku dla ochrony handlowych lub publicznych interesów lub bezpieczeństwa operacji przetwarzania.
5. Jeśli administrator jest organem lub podmiotem publicznym i jeśli przetwarzanie wynika z obowiązku prawnego na mocy art. 6 ust. 1 lit. c) przewidującego zasady i procedury operacji przetwarzania przewidziane przez prawo Unii, ust. 1-4 nie stosuje się, chyba że państwa członkowskie uznają przeprowadzenie takiej oceny przed przetwarzaniem za niezbędne.
6. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i warunków operacji przetwarzania mogących stwarzać szczególne ryzyko, o którym mowa w ust. 1 i 2 oraz wymogów w zakresie oceny, o których mowa w ust. 3, w tym warunków skalowalności, weryfikowalności i sprawdzenia. Wykonując to uprawnienie, Komisja rozważa szczególne środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.
7. Komisja może określić standardy i procedury przeprowadzania, weryfikowania i kontroli oceny, o której mowa w 3. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

POTRZEBA ODRĘBNEJ REGULACJI

- Istnieje potrzeba odrębnej ustawowej regulacji dotyczącej stosowania wideonadzoru, albowiem w wielu sytuacjach dochodzi tam do przetwarzania danych osobowych i następuje ingerencja w prywatność osoby, która chroniona jest Konstytucją RP
- Także, biorąc pod uwagę regulacje u.o.d.o, w praktyce problemem może być m. in. wykonywanie przez administratora wielu obowiązków wynikających z przepisów o ochronie danych osobowych np. obowiązku informacyjnego, o którym mowa w art. 24 u.o.d.o, czy też zapewnienie realizacji uprawnień kontrolnych osobie, której dane dotyczą (art. 32 i art. 33 u.o.d.o).

POTRZEBA ODRĘBNEJ REGULACJI

- Wskazać warto na opinię (nr 4/2004) Grupy Roboczej Artykułu 29, w której zwrócono uwagę m. in. na konieczność respektowania zasady proporcjonalności (dane muszą być adekwatne i istotne dla celów przetwarzania) przy posługiwaniu się monitoringiem, który oznacza przede wszystkim to, że urządzenia służące do takiego monitoringu mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie.
- Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, nie wymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania dla realizacji powyższych prawnie uzasadnionych celów Ta sama zasada dotyczy również wyboru odpowiedniej technologii, kryteriów wykorzystywania urządzeń w konkretnych sytuacjach oraz ustaleń dotyczących przetwarzania danych, odnoszących się także do zasad dostępu i okresu przechowywania. Ponadto, w opinii tej wskazano, iż osoby, których dane dotyczą powinny być świadome faktu prowadzenia tego rodzaju monitoringu, a w szczególności posiadać szczegółowe informacje odnośnie miejsc objętych takim systemem.

SPRAWDZIMY JAK SIĘ MAJĄ ZBIORY DANYCH Z WIDEOMONITORINGU. ZACZNIEMY OD …

SPRAWDZIMY JAK SIĘ MAJĄ ZBIORY DANYCH Z WIDEOMONITORINGU. ZACZNIEMY OD …

CEL I ZAKRES POŻĄDANYCH REGULACJI

Regulacje dotyczące monitoringu powinny w szczególności określić

- miejsca i okoliczności, w jakich stosowanie monitoringu jest dopuszczalne,
- prawa i obowiązki podmiotu prowadzącego monitoring,
- prawa osób objętych monitoringiem,
- zasady dotyczące wykorzystywania danych zebranych w procesie monitoringu. .

Określone w tych regulacjach warunki prawne stosowania monitoringu powinny zapewnić równowagę między uzasadnionymi potrzebami podmiotów stosujących monitoring i prawem do prywatności osób, które zostały objęte monitoringiem.

CEL I ZAKRES POŻĄDANYCH REGULACJI

- monitoring wizyjny, który jest stosowany **w celu wspomagania kontroli dostępu i zapewnienia bezpieczeństwa** siedzib i mienia oraz znajdujących się w nich ludzi i informacji.
  - poprawa bezpieczeństwa poprzez zapobieganie wszelkiego rodzaju incydentom.
  - zabezpieczenie dowodów, jeśli takie incydenty wystąpią
- systemy monitoringu, które mogą pełnić funkcję czynnika automatyzującego określone procesy
  - udostępnianie miejsc parkingowych i rozliczanie opłat parkingowych, pobieranie opłat z korzystanie z autostrad, tuneli czy promów}
  - zbieranie informacji w celu optymalizacji np. sygnalizacji świetlnej na drogach w zależności od natężenia ruchu, do sterowanie procesami technologicznymi itp.
- W zakres przedmiotowy regulacji dotyczącej stosowania monitoringu powinny wchodzić również zastosowania monitoringu prowadzonego w innych celach niż wymienione wyżej np.: monitoring na potrzeby reklamy miejsc turystycznych, promocji określonych imprez oraz inne nie uregulowane w ramach odrębnych przepisów szczególnych jego zastosowania.

CEL I ZAKRES POŻĄDANYCH REGULACJI

W ramach warunków stosowania monitoringu przedmiotem regulacji powinno być:

1. określenie zasad, warunków i okoliczności w jakich monitoring może być stosowany, w tym **wskazanie organu lub organów odpowiedzialnych** za kontrolę legalności jego stosowania oraz wydawanie zgód i zezwoleń na jego zastosowanie;
2. wskazanie przestrzeni na której monitoring może być stosowany oraz przestrzeni lub jej fragmentów, wobec których monitoringu nie należy stosować oraz sposobu jej oznaczenia;
3. wskazanie technicznych i organizacyjnych warunków jakie musi spełniać podmiot przed wprowadzeniem monitoringu, w czasie jego stosowania oraz podczas jego usuwania;
4. określenie praw i obowiązków podmiotów stosujących monitoring;
5. określenie praw osób, których wizerunki znalazły się w systemie monitoringu;
6. określenie odpowiedzialności karnej za naruszenie zasad i warunków stosowania monitoringu.

NOTYFIKACJA ZBIORÓW I SYSTEMÓW - MOŻLIWE ROZWIĄZANIA

1. zgłaszanie projektów systemu monitoringu, do akceptacji przez GIODO lub inny urząd w przypadku, gdy w systemie stosowane są elementy automatycznego przetwarzania obrazu mające na celu rozpoznanie osób, identyfikację określonego typu ich zachowań, określenie intencji ich postępowania, lub inne mechanizmy wprowadzające indeksację zarejestrowanych obrazów z danymi osobowymi.
2. obowiązek zgłaszania zbiorów danych osobowych tworzonych w wyniku stosowania monitoringu (należałoby dokładnie określić warunki klasyfikacji powstałego w wyniku monitoringu nagrania do danych osobowych);
3. połączenie obydwu rozwiązań tj. wprowadzenie obowiązku zgłoszenia, o którym mowa (1) oraz zgłoszenia zbioru (2);
4. obowiązek rejestracji lub notyfikacji systemów monitoringu, w których są lub mogą być przetwarzane dane osobowe niezależnie od stopnia ich technologicznego zaawansowania i automatycznie wykonywanych czynności przetwarzania danych.

NOTYFIKACJA ZBIORÓW I SYSTEMÓW - MOŻLIWE ROZWIĄZANIA

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

NOTYFIKACJA ZBIORÓW I SYSTEMÓW - MOŻLIWE ROZWIĄZANIA

Hiszpania [ustawa strukturalna nr 4/1997 z 4 sierpnia 1997 r. dotycząca korzystania z kamer wideo przez służby zajmujące się bezpieczeństwem w miejscach publicznych]

- zainstalowanie kamer (innego urządzenia nagrywającego) wymaga uzyskania zezwolenia Komisji, której przewodniczy sędzia,
- podobne przepisy w Hiszpanii odnoszą się również do sektora prywatnego.

Belgia [ustawa z dnia 21 marca 2007 r. regulująca instalowanie i użytkowanie kamer monitorujących]

- podmiot, który zamierza wprowadzić monitoring musi uzyskać pozytywną opinię rady gminy
- Notyfikacja systemu do Komisji Ochrony Życia Prywatnego

Włochy [ustawa o przetwarzaniu danych osobowych]

- Zgłoszenie do Urzędu Rzecznika Ochrony Danych Osobowych jest obligatoryjne tylko w okolicznościach kiedy z uwagi na zastosowane technologie mogą zaistnieć szczególne zagrożenia dla ochrony danych osobowych.
- Zgłoszenie takie jest bezwzględnie wymagane jeśli system nadzoru wizyjnego stosuje się w połączeniu z zastosowaniem biometrii lub w połaczeniu z systemem rozpoznawania twarzy w celu np. identyfikacji osób lub ich intencji czy nastroju.

OZNACZENIE OBSZARU MONITOROWANEGO

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

DOKUMENTACJA SYSTEMU MONITORINGU

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

DOKUMENTACJA SYSTEMU MONITORINGU

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

POLITYKA BEZPIECZEŃSTWA DANYCH PRZETWARZANYCH W SYSTEMIE MONITORINGU

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Opis zabezpieczenia infrastruktury systemu monitoringu przed nieautoryzowaną ingerencją w ustawienia systemu, o których mowa w dokumentacji projektowej;
2. Opis zabezpieczeń przed nieuprawnionymi działaniami, które mogą spowodować nieuprawniony dostęp lub zakłócanie obrazów przekazywanych przez kamery;
3. Opis zabezpieczeń przed nieuprawnionym dostępem, przejęciem lub zniszczeniem nagrań zarejestrowanych przez system;
4. Opis środków i procedur zapewniających rozliczalność wszelkich działań związanych z zarządzaniem systemem monitoringu, w tym udostępnianiem wglądu w nagrania upoważnionym osobom oraz wykonywaniem i udostępnianiem kopii nagrań wideo lub audiowideo zawierających zarejestrowane przez poszczególne kamery zdarzenia;
5. Opis środków i procedur dotyczących przekazywania kopii zarejestrowanych przez poszczególne kamery nagrań uprawnionym podmiotom zewnętrznym, w tym agencjom ochrony, policji, prokuraturze, sądom i innym oraz sposobu dokumentowania tych czynności;

POLITYKA BEZPIECZEŃSTWA DANYCH PRZETWARZANYCH W SYSTEMIE MONITORINGU

6. Procedury dotyczące wykonywania i przekazywania kopii nagrań zawierających dowody zaistnienia określonych zdarzeń;
7. Informacje o zastosowanych w systemie wideonadzoru mechanizmów automatycznej analizy obrazu, takich jak identyfikacja określonych zdarzeń typu pojawienie się w nadzorowanej przestrzeni człowieka lub innego zaliczanego do określonej kategorii obiektu np. pies, kot, samochód, itp.;
8. Informacje o zastosowanych w systemie monitoringu mechanizmach zaawansowanej analizy obrazu umożliwiające rozpoznawanie osób i lub ich intencji w zakresie określonego typu działań, np. działanie maskujące (skradanie się), przemoc fizyczna wobec innych osób, itp.

OBSZARY OBJĘTE SZCZEGÓLNĄ OCHRONĄ PRYWATNOŚCI

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

KORELACJA POMIĘDZY SYSTEMAMI MONITORINGU. ZINTEGROWANE SYSTEMY MONITORINGU

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

ZASAD STOSOWANIA INTELIGENTNYCH SYSTEMÓW AUTOMATYCZNEGO ROZPOZNAWANIA OKREŚLONYCH ZDARZEŃ

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Wprowadzenie „inteligentnych narzędzi monitoringu" powinno być dopuszczalne jedynie po przeprowadzeniu oceny wpływu ich zastosowania na ochronę danych i prywatności oraz po przeprowadzeniu kontroli wstępnej. GIODO po indywidualnej analizie każdego przypadku powinien oceniać dopuszczalność zastosowania danej techniki i w razie konieczności nakazać stosowanie dodatkowych zabezpieczeń.
2. Do kategorii systemów których zastosowanie wymaga szczególnej analizy należą systemy w których zastosowano jedno lub kilka z niżej wymienionych narzędzi lub narzędzia o zbliżonych funkcjonalnościach:
3. Połączenie systemu monitoringu wizualnego z danymi biometrycznymi (np. odciskami palców stosowanymi w kontroli dostępu) lub innymi bazami danych (np. bazą danych podejrzanych wykorzystywaną do rozpoznawania twarzy);
4. Indeksowanie danych na obrazach pozwalające na zautomatyzowane wyszukiwanie i alerty (np. w celu śledzenia osób);

ZASAD STOSOWANIA INTELIGENTNYCH SYSTEMÓW AUTOMATYCZNEGO ROZPOZNAWANIA OKREŚLONYCH ZDARZEŃ

GIODO
Generalny Inspektor Ochrony Danych Osobowych

5. Systemy rozpoznawania twarzy bądź chodu;
6. Wszelkiego rodzaju nadzór dynamiczno-prewencyjny (np. zastosowanie oprogramowania do automatycznej analizy zachowań w celu stworzenia zautomatyzowanych alertów opartych na ustalonych definicjach podejrzanego zachowania, ruchów, stroju i gestów);
7. Sieć kamer z oprogramowaniem umożliwiającym śledzenie poruszających się osób lub przedmiotów na całym monitorowanym obszarze;
8. Systemy alarmowe audio (w których alarm wywoływany jest zmianami w strukturze dźwięków, np. nagłym krzykiem);
9. Kamery na podczerwień i podobne, urządzenia termowizyjne i inne kamery szczególnego zastosowania, które mogą nagrywać obrazy w ciemnościach lub przy niewielkiej ilości światła oraz „widzieć” przez ściany i ubrania;
10. Kamery szczególnego zastosowania o zwiększonych możliwościach powiększenia optycznego i cyfrowego.

SKUTECZNOŚĆ MONONITORINGU

- Wg danych London Evening Standard z września 2007 r. wynika np., że w miejscach o dużej koncentracji kamer nie odnotowano większej wykrywalności przestępstw niż w miejscach, gdzie ich nie było w ogóle. Podobnie, jeśli chodzi o liczbę przestępstw, obecność kamer nie wpłynęła na zmniejszenie ich liczby

Justin Davenport, Evening Standard; *„Tens of thousands of CCTV cameras, yet 80% of crime unsolved”*; http://www.thisislondon.co.uk/news/article-23412867-details/Tens+of+thousands+of+CCTV+cameras%2C+yet+80%25+of+crime+unsolved/article.do

Paweł Wittach, „niewielki Brat”; Akademia Monitoringu Wizyjnego Newsletter nr 3, maj-czerwiec 2009; http://www.specialisedprojects.com.pl/aktualnosci.php?czytaj=70n

GIODO
Generalny Inspektor Ochrony Danych Osobowych

DZIĘKUJĘ ZA UWAGĘ

desiwm@giodo.gov.pl
http://edugiodo.giodo.gov.pl