

**Opinia 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem
kamer video**

Przyjęta 11 lutego 2004 r.

Grupa robocza została powołana artykułem 29 dyrektywy 95/46/WE. Jest to niezależny organ konsultacyjny Unii Europejskiej do spraw ochrony danych i prywatności. Jej zadania są określone w art. 30 dyrektywy 95/46/WE i w art. 14 dyrektywy 97/66WE.

Sekretariat:

Komisja Europejska, Generalna Dyrekcja „Rynek Wewnętrzny”, dział E (Usługi, własność intelektualna i przemysłowa, media i ochrona danych). B-1049 Bruksela, Belgia, biuro nr C100-6/136.

Strona internetowa: www.europa.eu.int/comm/privacy

GRUPA ROBOCZA DO SPRAW OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH powołana dyrektywą 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995¹,
uwzględniając art. 29 i 30 ust. 1 pkt a) oraz ust. 3 wyżej wymienionej dyrektywy,
uwzględniając swój regulamin wewnętrzny, a w szczególności jego art. 12 i 14,

przyjęła niniejszą opinię:

1. WSTĘP

Od kilku lat instytucje publiczne i prywatne w Europie coraz częściej posługują się systemami pozyskiwania obrazów. To zjawisko spowodowało żywe dyskusje, zarówno na poziomie wspólnotowym, jak i w Państwach Członkowskich, mające na celu określenie warunków i ograniczeń, jakie można zastosować przy instalowaniu urządzeń pozwalających na prowadzenie nadzoru z użyciem kamer, jak również koniecznych zabezpieczeń dla osób, których dane dotyczą.

Doświadczenie tych ostatnich lat, które nastąpiło po implementacji w Państwach Członkowskich dyrektywy 95/46/WE, uwidoczniło ogromne rozpowszechnienie systemów w obwodzie zamkniętym, kamer i innych bardziej wyrafinowanych środków w najprzeróżniejszych sektorach.

Ewolucja dostępnych technologii, informatyzacja i miniaturyzacja znacznie zwiększają możliwości oferowane przez środki zapisu obrazu i dźwięku, a zwłaszcza ich zastosowanie w sieciach Intranet i Internet.

Poza kontekstem publicznych i prywatnych miejsc pracy, który był już analizowany przez grupę w szczegółowym dokumencie (opinia 8/2001 w sprawie przetwarzania danych osobowych w miejscu pracy²), coraz większe rozpowszechnienie technik video-nadzoru jest

¹ Dziennik Urzędowy L 281 z 23.11.1995, p.31, dostępny pod następującym adresem:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

² WP 48, przyjęta 13 września 2001, dostępna na stronie:
http://europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm

dobrze znanej opinii publicznej. Wzrasta również tendencja w kierunku łączenia ze sobą systemów video-nadzoru.

Pobieżna analiza podstawowych aplikacji wykazuje, że cele video-nadzoru mogą być bardzo zróżnicowane³, ale można je jednak podzielić na pewne kategorie:

- 1) ochrona osób
- 2) ochrona dóbr
- 3) dobro publiczne
- 4) wykrywanie, zapobieganie i ściganie czynów przestępczych
- 5) udostępnianie dowodów
- 6) inne legalne cele.

Warunki dopuszczenia instalowania kamer video i podobnych urządzeń również są zróżnicowane.

W niektórych przypadkach używanie systemów rejestracji obrazu może być obowiązkowe zgodnie ze specyficznymi przepisami jakiegoś Państwa Członkowskiego (na przykład w niektórych kasynach); w innych przypadkach jest zgodne ze szczególnie ważnym celem członków rodziny zainteresowanej osoby (np. poszukiwanie zaginionych nieletnich i osób

³ Różne systemy video-nadzoru są instalowane:

- a) wewnątrz i w pobliżu instytucji publicznych i/lub w pobliżu budynków otwartych dla publiczności, aby przeciwdziałać czynom nielegalnym i drobnym aktom wandalizmu;
- b) wewnątrz stadionów i urządzeń sportowych, zwłaszcza z okazji szczególnych imprez;
- c) w sektorze transportu i w związku z ruchem drogowym, w celu nadzorowania ruchu na autostradach i drogach o dużym natężeniu ruchu, lub w celu wykrywania wykroczeń polegających na przekroczeniu dozwolonej prędkości lub przepisów dotyczących ruchu w centrum miasta, lub w celu kontrolowania podziemnych dróg dostępu do metra, stacji benzynowych, jak również wewnątrz taksówek;
- d) w celu przeciwdziałania i/lub wykrywania nielegalnych zachowań w pobliżu szkół, zwłaszcza w odniesieniu do napastowania nieletnich;
- e) wewnątrz budynków służby zdrowia, w czasie operacji chirurgicznych, lub, na przykład, w celu nadzorowania i kontrolowania na odległość pacjentów na oddziale intensywnej opieki, lub w sektorach zarezerwowanych dla ciężko chorych lub izolowanych od otoczenia;
- f) na lotniskach, na pokładach statków i w pobliżu granic, w celu nadzorowania nielegalnej imigracji lub w celu poszukiwania osób lub nieletnich zaginionych;
- g) przez prywatnych detektywów;
- h) wewnątrz i w pobliżu supermarketów i sklepów z luksusowymi artykułami, w celu pozyskania dowodów w przypadku wykroczenia, jak również w celu wprowadzania do handlu produktów i analizowania zachowań konsumentów;
- i) wewnątrz i w pobliżu prywatnych rezydencji, dla celów bezpieczeństwa osobistego i pozyskania dowodów w przypadku wykroczenia;
- j) dla celów prasowych i reklamowych obserwowanych on line za pomocą kamer internetowych (web-cam) lub kamer on line używanych dla celów promocji turystyki lub reklamowych, zainstalowanych na niektórych plażach lub w lokalach nocnych, gdzie przewidziane jest filmowanie klientów i gości bez uprzedzenia, w regularnych odstępach czasu.

dorosłych). Można również przytoczyć przykłady wyjątkowe – zwłaszcza w krajach trzecich – gdzie wprowadzono systemy automatycznego rozpoznawania rysów twarzy, aby uniemożliwić bigamię (w wersji franc.: fałszywe śluby); lub gdy policja lokalna decyduje o podawaniu do wiadomości publicznej (wersja franc: rozpowszechnianiu ciągłym i publicznym) obrazów o ciężkich warunkach życia więźniów, bez ich zgody.

O ile w niektórych przypadkach video-nadzór daje się usprawiedliwić, w innych mamy do czynienia z impulsywnym sięganiem po techniki ochrony z użyciem kamer, bez odpowiedniego zastanowienia się nad warunkami i sposobami ich użycia. Niekiedy przyczyny należy szukać w korzyściach ekonomicznych przyznawanych na dużą skalę przez organy publiczne lub w korzystnych warunkach ubezpieczenia w przypadku stosowania systemu video-nadzoru.

Video-nadzór ma również skutki psychologiczne – czasami uważany jest (błędnie bądź nie) przez opinię publiczną za „nieocenione narzędzie” z uwagi na fakt, iż był przydatny w wykrywaniu przestępstw.

Mamy więc do czynienia z sektorem złożonym, stale zmieniającym się, w którym dostępne są już różnorakie techniki.

Niniejszy dokument przedstawia pierwszą analizę, która przyjęła za punkt wyjścia istnienie częściowo różniących się przepisów, jak również zbyt szczegółowych przepisów w wewnętrznym ustawodawstwie każdego kraju, co wymaga bardziej systematycznego i zharmonizowanego podejścia.

Dokument dotyczy nadzoru w celu zdalnej kontroli wydarzeń, sytuacji i faktów specyficznych, nie zajmuje się bezpośrednio innymi przypadkami dotyczącymi reklamy okazjonalnej i/lub ewentualnych relacji wydarzeń, na przykład w związku z przejrzystością działania przedstawicielskich organów parlamentarnych lub władz lokalnych.

Każdy z operatorów będzie mógł następnie szczegółowo rozwinąć wskazówki otrzymane przy tej okazji, nie tylko w swoim sektorze działalności, lecz również w nawiązaniu do rozwoju przyszłych technologii, które grupa zamierza zbadać.

Zasady, które zostaną tu przeanalizowane, są zresztą związane z pozyskiwaniem obrazu, ewentualnie w połączeniu z dźwiękami i/lub z danymi biometrycznymi takimi jak odciski palców⁴.

Zasady te mogą, tam gdzie mają konkretne zastosowanie, być również rozpatrywane pod względem ewentualnego przetwarzania danych osobowych realizowanego za pomocą nie urządzeń video, lecz za pomocą innych form nadzoru, to znaczy zdalnej kontroli – tak jest na przykład w przypadku systemów nawigacji satelitarnej GPS.

Niniejszy dokument ma za zadanie po pierwsze zwrócić uwagę na szeroki wachlarz kryteriów oceny legalnego i odpowiedniego charakteru instalacji systemów video-nadzoru.

Jednakże, zostały również wzięte pod uwagę następujące aspekty:

- a) konieczność ogólnej oceny systemu video-nadzoru przez odpowiednie instytucje Państw Członkowskich, aby zachęcić do globalnie selektywnego i systematycznego podejścia do tego tematu. Nadmierne rozpowszechnianie systemów pozyskiwania obrazu w miejscach publicznych i prywatnych nie może spowodować nieuzasadnionego ograniczenia podstawowych praw i wolności obywateli, w przeciwnym razie mogliby być zmuszeni podporządkować się w nieproporcjonalny sposób procedurom gromadzenia danych, które czyniłyby ich masowo identyfikowalnymi w dużej liczbie miejsc publicznych i prywatnych.
- b) przydatność oceny kierunków ewolucji technik video-nadzoru, tak, aby rozwój aplikacji informatycznych opierających się na rozpoznawaniu twarzy osób i na badaniu i przewidywaniu zachowań ludzkich zarejestrowanych na obrazie nie spowodował masowego i nierozważnego przechodzenia na nadzór dynamiczno-prewencyjny, w przeciwieństwie do najpowszechniejszej formy nadzoru statycznego, którego zadaniem jest informowanie o specyficznych zdarzeniach i ich uczestnikach. Ta nowa forma nadzoru opiera się na zautomatyzowanym pobieraniu rysów twarzy osób fizycznych i ich „anormalnych” zachowań; przewiduje również możliwość wysyłania automatycznych sygnałów alarmu i wezwania do interwencji, które mogłoby spowodować ryzyko dyskryminacji.

⁴ Bardziej ogólne zagadnienie stosowania dyrektywy 95/46/WE w dziedzinie biometrii będzie omówione przez grupę roboczą w odrębnym dokumencie.

2. MIĘDZYNARODOWE INSTRUMENTY PRAWNE

a) Konwencja praw człowieka i podstawowych wolności.

Ochrona życia prywatnego zapewniona jest w artykule 8 Konwencji praw człowieka.

b) Konwencja Nr 108/1981 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.

Zakres stosowania tej Konwencji nie ogranicza się, tak jak w przypadku dyrektywy, do działalności z pierwszego filaru (patrz niżej). Działania związane z video-nadzorem zawierające przetwarzanie danych osobowych podlegają zakresowi stosowania tej Konwencji. Według Komitetu Konsultacyjnego powołanego tą Konwencją, głos i obraz muszą być traktowane jako dane osobowe, o ile dostarczają informacji o osobie czyniąc ją identyfikowalną, nawet pośrednio.

Rada Europy dopracowuje całość zasad w sprawie ochrony osób wobec gromadzenia i przetwarzania danych przy pomocy video-nadzoru. Zasady te będą musiały zresztą szczegółowo określać sposoby ochrony mające zastosowanie wobec osób, których dane dotyczą, zawarte w postanowieniach instrumentalnych Rady Europy.

c) Karta podstawowych praw Unii Europejskiej

Karta podstawowych praw Unii Europejskiej przewiduje w art. 17 ochronę życia prywatnego i rodzinnego, domu i komunikacji oraz, w art. 8, ochronę danych osobowych.

3. NADZÓR W ROZUMIENIU DYREKTYWY 95/46/WE

Specyficzny charakter przetwarzania danych zawierającego dźwięk i obraz został podkreślony w dyrektywie 95/46/WE (zwanej dalej „dyrektywą”), do którego odnosi się wyraźnie w wielu punktach.

Dyrektywa zapewnia ochronę prywatności i życia prywatnego oraz większą ochronę danych osobowych w odniesieniu do podstawowych praw i wolności osób fizycznych (art. 1 ust. 1) [wersja franc.: Państwa Członkowskie zapewniają, zgodnie z tą dyrektywą, ochronę wolności i podstawowych praw osób fizycznych, w szczególności ich życia prywatnego, wobec przetwarzania danych osobowych (art. 1 ust. 1)].

Podmiotem wielu informacji gromadzonych za pomocą systemów video-nadzoru są osoby zidentyfikowane lub identyfikowalne, które zostały sfilmowane w miejscach publicznych lub publicznie dostępnych. Osoby przechodzące w tych miejscach spodziewają się z pewnością ograniczonej ochrony życia prywatnego, jednak nie przewidują całkowitego pozbawienia ich praw i wolności w odniesieniu do ich życia prywatnego i ich wizerunku.

Szczególną uwagę należy zwrócić na prawo do swobodnego przemieszczania się osób, które znajdują się legalnie na terytorium Państwa; to prawo zapewnione jest w Dodatkowym Protokole Nr 4, art. 2 do Europejskiej Konwencji praw człowieka i podstawowych wolności.

Swoboda przemieszczania może być ograniczona tylko ograniczeniami niezbędnymi w społeczeństwie demokratycznym i proporcjonalnymi do osiągnięcia określonych celów. Zainteresowane osoby mają prawo korzystać ze swobody poruszania się bez nadmiernego uwarunkowania psychologicznego dotyczącego ich poruszania się i zachowania. Nie mogą również być poddawane szczegółowej kontroli, na przykład pozwalającej na śledzenie ich przemieszczania się i/lub wywołanie „alarmu” w oparciu o oprogramowanie, które automatycznie „interpretuje” przypuszczalnie podejrzane zachowanie osoby bez interwencji człowieka – ze względu na nieproporcjonalne wykorzystywanie video-nadzoru przez różne instytucje w szeregu miejsc publicznych i/lub publicznie dostępnych.

Specyficzny i delikatny charakter przetwarzania danych w formie dźwięku i obrazu dotyczących osób fizycznych podkreślany jest w preambule dyrektywy i w niektórych artykułach. Poza stwierdzeniami sformułowanymi poniżej w kwestii zakresu stosowania, preambuła i odpowiednie artykuły mówią, że:

- a) dyrektywa ma z zasady zastosowanie do tej kwestii, z uwzględnieniem również stałej ewolucji technik umożliwiających pozyskiwanie, manipulowanie i posługiwanie się w inny sposób specyficzną kategorią danych osobowych, które zostały w ten sposób zgromadzone (punkt 14 preambuły);
- b) zasady dyrektywy w kwestii ochrony mają zastosowanie do wszelkiej informacji, również w formie dźwięku lub obrazu, dotyczącej osoby zidentyfikowanej lub identyfikowalnej, z uwzględnieniem całości środków, jakie mogą być racjonalnie użyte przez administratora danych lub przez inne osoby w celu zidentyfikowania tej osoby (art. 2 punkt a), punkt 26 preambuły).

Poza wyżej wymienionymi specyficznymi odniesieniami, oczywiście dyrektywa ma zastosowanie w ramach odnośnych postanowień, dotyczących zwłaszcza:

1. *Jakość danych.* Obrazy muszą być przetwarzane rzetelnie i legalnie, dla określonych, wyraźnych i legalnych celów. Obrazy muszą być używane zgodnie z zasadą, według której dane muszą być stosowne, istotne i niezbyt obszerne, nie mogą być dalej przetwarzane w sposób niezgodny z celem, dla którego zostały zgromadzone, muszą być przechowywane przez określony okres, itd. (art. 6);
2. *Kryteria legalności przetwarzania danych.* Wymagają, aby przetwarzanie danych osobowych za pomocą video-nadzoru było obowiązkowo oparte na przynajmniej jednym z warunków, o których mowa w art. 7 (jednoznaczna zgoda, konieczność zobowiązań umownych, poszanowanie obowiązku prawnego, ochrona żywotnych interesów osoby, której dane dotyczą, realizacja zadania wykonywanego dla dobra publicznego lub wynikającego z uprawnień władzy publicznej, równowaga interesów);
3. Przetwarzanie szczególnych kategorii danych, podlegające środkom zabezpieczającym, mającym zastosowanie w przypadku posługiwania się, w ramach video-nadzoru, danymi sensytywnymi (szczególnie chronionymi) lub dotyczącymi wykroczeń (art. 8);
4. Informowanie osób, których dane dotyczą (art. 10 i 11);
5. Prawa osób, których dane dotyczą, zwłaszcza prawo dostępu i prawo sprzeciwu z ważnych i legalnych powodów (art. 12 i 14);
6. Środki zabezpieczające mające zastosowanie w przypadku indywidualnych decyzji zautomatyzowanych (art. 15);
7. Bezpieczeństwo operacji przetwarzania (art. 17);
8. Zgłaszanie przetwarzania zbiorów (art. 18 i 19);
9. Kontrola wstępna przetwarzania stanowiącego szczególne zagrożenie dla praw i wolności osób, których dane dotyczą (art. 20); oraz
10. Przekazywanie danych do krajów trzecich (art. 25 i następne).

Szczególny i delikatny charakter przetwarzania dźwięków i obrazów podkreślony jest w ostatnim artykule dyrektywy, który zobowiązuje Komisję do przeanalizowania przestrzegania dyrektywy w tej kwestii i przedstawienia ewentualnych odpowiednich propozycji, z

uwzględnieniem technologii informacji i postępu, jaki dokonuje się w z informatyzowanym społeczeństwie (art. 33).

4. USTAWODAWSTWO KRAJOWE DOTYCZĄCE VIDEO-NADZORU

W kilku Państwach Członkowskich istnieją już badania w sprawie video-nadzoru, opierające się na normach konstytucyjnych⁵ albo na specyficznych postanowieniach ustawodawczych, przepisach lub innych decyzjach pochodzących od właściwych władz krajowych⁶.

W kilku państwach istnieją również szczególne przepisy, mające zastosowanie niezależnie od tego, czy video-nadzór zawiera przetwarzanie danych osobowych czy nie. Przepisy te mówią również, że instalacja i stosowanie systemów CCTV (telewizji przemysłowej) i innych podobnych systemów nadzoru podlegają wcześniejszej zgodzie ze strony władz administracyjnych, które mogą być w części lub w całości reprezentowane przez krajowy organ ochrony danych. Przepisy mogą być zróżnicowane w zależności od charakteru publicznego lub prywatnego osoby odpowiedzialnej za działanie określonego systemu.

W innych krajach video-nadzór nie jest obecnie objęty specyficznymi przepisami prawa; jednakże organy ochrony danych osobowych zadziałały w celu zapewnienia odpowiedniego stosowania ogólnych zasad ochrony danych za pomocą opinii, wytycznych lub kodeksów zachowań, które już zostały przyjęte (Zjednoczone Królestwo), lub są w trakcie opracowania (Włochy).

| | |
|--------|--|
| Belgia | Opinie Organu Ochrony Danych, zwłaszcza opinia 34/99 z 13 grudnia 1999 w sprawie przetwarzania obrazów zwłaszcza z użyciem systemów video-nadzoru; Opinia 3/2000 z 10 stycznia 2000 w sprawie używania systemów video-nadzoru w wejściach do apartamentowców |
|--------|--|

⁵ Patrz decyzja portugalskiego Trybunału Konstytucyjnego nr 255/2002. Trybunał postanowił, że „używanie elektronicznych urządzeń do nadzorowania i kontrolowania obywateli przez prywatne organy bezpieczeństwa stanowią ograniczenie lub uszczuplenie prawa do ochrony życia prywatnego, przyznanego artykułem 26 Konstytucji”.

⁶ Co najmniej w jednym państwie (sprawa Belgia – Gaia), nie poszanowanie ustawodawstwa w kwestii ochrony danych w ramach gromadzenia obrazów doprowadziło do odrzucenia dowodów przed sądem.

| | |
|-----------|--|
| Dania | <p>Tekst jednolity ustawy Nr 76 z 1 lutego 2000 w sprawie zakazu stosowania video-nadzoru. Ustawa ta generalnie zakazuje podmiotom prywatnym prowadzenia video-nadzoru publicznych ulic, dróg, placów lub podobnych obszarów wykorzystywanych do powszechnego podróżowania. Istnieją jednakże określone zwolnienia od tego zakazu.</p> <p>Decyzja Organu Ochrony Danych z 3 czerwca 2002 w sprawie video-nadzoru prowadzonego przez dużą grupę supermarketów oraz transmisji z pubu prowadzonej na żywo w Internecie.</p> <p>Decyzja Organu Ochrony Danych z 1 lipca 2003 stanowiąca, że video-nadzór prowadzony w prywatnie zarządzanych środkach transportu publicznego musi być proporcjonalny i zgodny z zasadami zawartymi w Duńskiej Ustawie o Ochronie Danych.</p> <p>Decyzje Organu Ochrony Danych z 13 listopada 2003 nakładające określone ograniczenia na video-nadzór prowadzony przez organy publiczne.</p> |
| Finlandia | <p>W Finlandii nie istnieje szczególne ustawodawstwo dotyczące video-nadzoru, ale istnieją przepisy dotyczące video-nadzoru i innego technicznego nadzoru, obserwacji lub monitorowania w wielu różnych ustawach.</p> <p>Często zadawane są pytania odnośnie video-nadzoru i nagrywania rozmów i mieliśmy kilka związanych z tym spraw.</p> <p>Na przykład Rzecznik Ochrony Danych wydał opinię na temat nagrywania rozmów telefonicznych w obsłudze klienta oraz w pracy (numery ref.: 1061/45/2000 oraz 5125/45/2000)</p> <p>Nasze Biuro opublikowało broszurę „Prywatność w przypadku video-nadzoru” (Asiaa tietosuoja 4/2001 Yksityisyyden suoja kamervallonnassa http://www.tietosuoja.fi/uploads/03wamgvxuybt4ti.rtf).</p> |

| | |
|----------|--|
| Francja | <p>Ustawa Nr 78-17 z 6 stycznia 1978 o przetwarzaniu, zbiorach i o wolnościach;</p> <p>Zalecenie organu ochrony danych Nr 94-056 z 21 czerwca 1994;</p> <p>Poradnik organu ochrony danych dotyczący video-nadzoru w miejscu pracy: http://www.cnil.fr/thematic/index.htm i innych spraw (np. kamery internetowe)⁷</p> <p>Ustawa w sprawie video-nadzoru dla celów bezpieczeństwa w miejscach publicznych: ustawa Nr 95-73 z 21 stycznia 1995 w sprawie bezpieczeństwa (zmieniona postanowieniem 2000-916 z 19 września 2000).</p> <p>Dekret Nr 96-926 z 17 października 1996 i okólnik z 22 października 1996 w sprawie wejścia w życie ustawy 95-73.</p> |
| Grecja | <p>1) Pismo nr 390 z 28 stycznia 2000 w sprawie instalacji telewizji przemysłowej w metrze w Atenach</p> <p>2) Dyrektywa nr 1122 z 26 września 2000 w sprawie telewizji przemysłowej</p> <p>3) Decyzja nr 84/2002 w sprawie telewizji przemysłowej w hotelach</p> |
| Niemcy | <p>Art. 6 punkt b ustawy federalnej 2001.</p> <p>Art. 25 Prawo o ochronie granic.</p> <p>Dalsze uregulowania w kwestii video-nadzoru prowadzonego przez policję w ustawach o policji poszczególnych landów.</p> <p>W Parlamencie prowadzone są dyskusje na temat projektu ustawy zakazującej ukrytego video-nadzoru.</p> |
| Irlandia | <p>Ustawa o ochronie danych z 1998 i 2003 r.</p> <p>Casus Nr 14/1996 (wykorzystywanie telewizji przemysłowej)</p> |

⁷ Porównaj roczne sprawozdania Krajowej Komisji Francuskiej do Spraw Informatyki i Wolności (CNIL).

| | |
|------------|--|
| Włochy | <p>Art. 134 Kodeksu o ochronie danych osobowych (rozporządzenie nr 196 z 30 czerwca 2003, przewidujące przyjęcie kodeksu postępowania).</p> <p>Decyzje organu nadzoru Garante nr 2 z 10 kwietnia 2002 roku (propagujące przyjęcie kodeksów postępowania), 28 września 2001 (biometria i techniki rozpoznawania twarzy wdrożone przez banki) oraz 29 listopada 2000 (tzw. „dekalog video-nadzoru)</p> <p>Dekret prezydencki Nr 250 z 22 czerwca 1999 (regulujący dostęp pojazdów do centrów miast i stref ograniczonego ruchu)</p> <p>Dekret Nr 433 z 14 listopada 1992 i ustawa Nr 4/1993 (mająca zastosowanie wobec muzeów, bibliotek i archiwów państwowych)</p> <p>Dekret legislacyjny Nr 45 z 4 lutego 2000 (statki pasażerskie na szlakach krajowych)</p> <p>Art. 4 ustawy Nr 300 z 20 maja 1970 (Statut pracowników)</p> |
| Luksemburg | <p>Art. 10 i 11 ustawy z 2 sierpnia 2002 w sprawie ochrony osób wobec przetwarzania danych osobowych</p> |

| | |
|------------|---|
| Holandia | <p>Sprawozdanie organu ochrony danych opublikowane w 1997 zawiera wytyczne dotyczące video-nadzoru, zwłaszcza w związku z ochroną osób i mienia w miejscach publicznych. Aktualizacja wytycznych opracowana w 1997 r. będzie dostępna w 2004 r.</p> <p>Badanie w zakresie nadzoru przy użyciu kamer video we wszystkich holenderskich miastach w 2003 r.</p> <p>Zmiana w Kodeksie Karnym, która wejdzie w życie 1 stycznia 2004, która rozszerzy zakres przestępstwa karnego polegającego na fotografowaniu miejsc dostępnych publicznie bez informowania tych osób, została ostatnio zatwierdzona przez niższą izbę parlamentu.</p> <p>Rząd proponuje, aby zmienić ustawę o samorządzie lokalnym, wyraźnie przyznając radom miejskim i burmistrzom kompetencje do wykorzystywania systemów video-nadzoru w sferze publicznej do celów publicznych na pewnych warunkach (np. obowiązek okresowej oceny skuteczności video-nadzoru).</p> |
| Portugalia | <p>Dekret z mocą ustawy Nr 231/98 z 22 lipca 1998 (prywatna działalność ochrony i systemy samo-ochrony)</p> <p>Ustawa Nr 38/98 z 4 sierpnia 1998 (środki zapobiegawcze w przypadku przemocy połączonej z imprezami sportowymi)</p> <p>Dekret z mocą ustawy Nr 263/01 z 28 września 2001 (dyskoteki)</p> <p>Dekret z mocą ustawy Nr 94/2002 z 12 kwietnia 2002 (imprezy sportowe)</p> |
| Hiszpania | <p>Ustawa organiczna Nr 4/1997 (video-nadzór prowadzony przez organy bezpieczeństwa w miejscach publicznych)</p> <p>Dekret królewski Nr 596/1999 wprowadzający ustawę Nr 4/1997</p> |

| | |
|-----------------------|--|
| Szwecja | <p>Video-nadzór jest określony szczególną ustawą (1998:150) w sprawie ogólnego video-nadzoru i ustawą (1995:1506) w sprawie tajnego video-nadzoru (w śledztwach kryminalnych)⁸.</p> <p>Ogólny video-nadzór zazwyczaj wymaga zezwolenia organu administracyjnego hrabstwa. Jednakże np. nadzór w urzędach pocztowych, bankach i sklepach nie wymaga zezwolenia. Tajny video-nadzór musi być dopuszczony przez sąd. Decyzje organu administracyjnego hrabstwa może uchylić Minister Sprawiedliwości.</p> <p>Nagrywanie przy pomocy kamer video z wykorzystaniem techniki cyfrowej postrzegane jest jako przetwarzanie danych osobowych i podlega nadzorowi ze strony organu ochrony danych (Data Inspection Board) w takim zakresie, w jakim nie jest szczególnie uregulowany w ustawie o ogólnym video-nadzorze.</p> <p>Komisja śledcza opublikowała raport dotyczący video-nadzoru (SOU 2002:110)</p> |
| Zjednoczone Królestwo | Kodeks postępowania dotyczący telewizji przemysłowej 2000 (Rzecznik Informacji), obecnie w trakcie nowelizacji. |

Inne warte przytoczenia instrumenty zostały również przyjęte w Islandii (art. 4, ustawa Nr 77/2000, Norwegii (tytuł VII ustawy Nr 31 z 14 kwietnia 2000), Szwajcarii (zalecenie Rzecznika Federalnego) i Węgier (zalecenie organu ochrony danych z 20 grudnia 2000).

5. SEKTORY, W KTÓRYCH DYREKTYWA 95/46/WE NIE MA CZĘŚCIOWO LUB CAŁKOWICIE ZASTOSOWANIA

Dyrektywa nie ma zastosowania do przetwarzania danych w formie dźwięków i obrazów prowadzonego dla celów dotyczących bezpieczeństwa publicznego, obronności, bezpieczeństwa Państwa lub wykonywania czynności Państwa w dziedzinie prawa karnego

⁸ W Szwecji video-nadzór ogólny w zasadzie wymaga zezwolenia organu administracyjnego hrabstwa, chociaż istnieje pewna liczba wyjątków, na przykład dotyczących urzędów pocztowych, banków i sklepów. Tajny video-nadzór musi być dopuszczony przez sąd. Minister sprawiedliwości może uchylić decyzję organu administracyjnego hrabstwa podjętą zgodnie z ustawą w sprawie video-nadzoru dla ochrony interesów dobra publicznego. Zapis video za pomocą kamer cyfrowych traktowany jest jako przetwarzanie danych osobowych w myśl szwedzkiej ustawy o ochronie danych osobowych, podlega więc nadzorowi organu ochrony danych. Komisja śledcza bada obecnie stosowanie video-nadzoru w zapobieganiu przestępczości. Komisja oceni między innymi ustawę dotyczącą ogólnego video-nadzoru pod kątem konieczności wprowadzenia zmian. Komisja śledcza przeanalizuje również zakres stosowania szwedzkiej ustawy o ochronie danych osobowych w dziedzinie video-nadzoru, jak również ewentualną potrzebę szczególnego ustawodawstwa w sprawie przetwarzania danych osobowych w związku z video-nadzorem.

i/lub innych czynności, nie wchodzących w zakres obowiązywania prawa wspólnotowego⁹. Jednakże wiele Państw Członkowskich, implementujących dyrektywę 95/46/WE, objęło te aspekty ogólnie, przewidując, jednak, szczególne wyjątki.

A. W kilku państwach, przetwarzanie prowadzone dla wyżej wymienionych celów musi zapewniać w każdym przypadku pewne gwarancje, zgodnie z Konwencją Nr 108/1981 i z odnośnymi zaleceniami Rady Europy, jak również zgodnie z określonymi krajowymi postanowieniami ustawodawczymi (art. 3 ust. 2 oraz punkt 16 preambuły dyrektywy Nr 95/46/WE). Ze względu na specyficzny charakter, jak również ze względu na istnienie szczególnych przepisów powiązanych dotyczących czynności śledczych prowadzonych przez służby policyjne i/lub sądowe, jak również dla celów bezpieczeństwa państwa¹⁰ (które mogą zawierać „ukryty” video-nadzór, to znaczy nie zawierający żadnych danych o nadzorowanych miejscach), ta kategoria przetwarzania nie jest analizowana w niniejszym dokumencie.

Jednakże grupa robocza podkreśla, że konieczne jest, podobnie jak w przypadku innych procesów przetwarzania danych osobowych, które również nie wchodzą w zakres stosowania dyrektywy, aby video-nadzór uzasadniony rzeczywistymi wymogami bezpieczeństwa publicznego lub wykrywaniem, zapobieganiem i ściganiem wykroczeń, spełniał warunki określone w art. 8 Konwencji praw człowieka i podstawowych wolności. Między innymi musi być przewidziany w szczegółowych przepisach znanych opinii publicznej i być związany i przystosowany do zapobiegania *konkretnym* zagrożeniom i *szczególnym* wykroczeniom (na przykład miejsca narażone na takie zagrożenia lub w przypadku wydarzeń publicznych, przy których istnieje racjonalne zagrożenie aktami przestępczymi)¹¹. Skutki wywołane przez systemy video-nadzoru muszą być brane pod uwagę (na przykład, przeniesienie działań przestępczych do innych miejsc lub sektorów); administrator danych zawsze

⁹ Patrz punkt 16 preambuły

¹⁰ Można tu przywołać zasady przywołane przez Europejski Trybunał Praw Człowieka w sprawie Rotaru/Rumunia z 4 maja 2000, wyżej wymieniony.

¹¹ Francuski okólnik z 22 października 1996 wymieniał miejsca odizolowane lub sklepy otwarte do późnych godzin nocnych.

powinien być wyraźnie wskazany, aby umożliwić osobom, których dane dotyczą, realizację ich praw.

Ta konieczność istnieje również ze względu na fakt, że systemy video-nadzoru są coraz częściej instalowane przez policję i inne służby publiczne (na przykład samorządy) i/lub przez instytucje prywatne (banki, stowarzyszenia sportowe, przedsiębiorstwa przewozowe), co stwarza ryzyko pewnego pomieszania ról i odpowiedzialności indywidualnej dotyczącej zadań, które mają być realizowane¹².

- B. Po drugie, dyrektywa nie ma zastosowania do przetwarzania zbiorów prowadzonego przez osobę fizyczną dla celów wyłącznie osobistych lub domowych (art. 3 ust 2 i punkt 12 preambuły).

Na przykład fakt instalowania systemów video-nadzoru w celu zdalnego nadzorowania wyłącznie wewnątrz prywatnego mieszkania (w celu przeciwdziałania kradzieżom lub w ramach zarządzania tzw. e-rodziną), całkowicie różni się od sytuacji, gdy video-nadzór zainstalowany jest w pobliżu prywatnego domu w celu ochrony nieruchomości/lub zagwarantowania bezpieczeństwa.

W tych przypadkach możliwe jest, że system zainstalowany jest nie przez właściciela według jego własnego wyboru ochrony wejścia (drzwi) do jego własności, lecz przez kilku właścicieli, którzy to uzgodnili między sobą lub przez spółdzielnię lub wspólnotę mieszkaniową, w celu kontrolowania wejść i innych stref wspólnych, co pozwala na zastosowanie dyrektywy do tego działania.

Podobnie, kiedy system zarządzany jest na rzecz jednej rodziny i poprzez filmowanie jednych drzwi, podestu czy garażu itp., fakt, że dyrektywa nie ma

¹² Znaczącym przykładem w tej sprawie jest działalność prowadzona przez włoskie władze miejskie w celu kontrolowania, za pomocą video-nadzoru, stref publicznych gdzie zbierają się w nocy prostytutki. Niektóre władze stwierdziły w przeszłości, że są właściwe do kontrolowania tego zjawiska, podczas gdy inne zdecydowały się na stosowanie przepisów, zakazujących zatrzymywania lub przejazdu samochodów klientów

tu zastosowania ze względu na użytek wyłącznie osobisty i brak możliwości dostępu osób trzecich do informacji, nie zwalnia administratora z obowiązku poszanowania praw i legalnych interesów sąsiadów i innych przechodzących osób. Te prawa i interesy są w każdym razie chronione w Państwach Członkowskich, nie tylko przepisami ustawy o ochronie danych, lecz również przepisami prawa cywilnego o charakterze ogólnym, gwarantującymi prawa osobiste, ochronę wizerunku, życia rodzinnego i życia prywatnego (wystarczy pomyśleć, na przykład, o kamerze szerokokątnej zainstalowanej przed wejściem do mieszkania prywatnego, która systematycznie rejestruje klientów gabinetu lekarskiego lub kancelarii adwokackiej na tym samym piętrze, naruszając w ten sposób tajemnicę zawodową).

Szczególną uwagę należy zwrócić na ukierunkowanie urządzeń video, na konieczność umieszczania tablic informacyjnych i na szybkie kasowanie nagrań (po kilku godzinach), jeżeli nie zostało popełnione żadne włamanie ani wykroczenie.

- C. Na koniec, art. 9 dyrektywy stanowi, że Państwa Członkowskie przewidzą wyjątki lub wyłączenia niektórych postanowień w nim zawartych, jeżeli przetwarzanie realizowane jest wyłącznie dla celów dziennikarskich, wyrazu literackiego lub artystycznego, zwłaszcza w dziedzinie audiowizualnej (punkt 17 preambuły). Trzeba przewidzieć wyłącznie wyjątki pozwalające pogodzić prawo do życia prywatnego z przepisami regulującymi swobodę wypowiedzi¹³. Należy tu zachować szczególne środki ostrożności, zwłaszcza gdy instalowane są kamery internetowe lub kamery on line, aby uniknąć wad i luk w kwestii ochrony danych osób podlegających video-nadzorowi, dla celów, które czasem mogą być natury czysto reklamowej lub promocji turystycznej¹⁴.

6. VIDEO-NADZÓR I PRZETWARZANIE DANYCH OSOBOWYCH

prostytutek, grożąc przesłaniem do domu zdjęcia. Organ włoski wydał decyzję w celu wyjaśnienia kwestii dotyczących oskarżenia o naruszenie właściwych przepisów.

¹³ Patrz Zalecenie 1/97 grupy roboczej o ustawie o ochronie danych i środkach komunikacji.

¹⁴ Kamera internetowa, która została zainstalowana potajemnie przy schodach koło jednego z wyjść z metra w Mediolanie, przekazywała bezpośrednio do sieci części intymne przechodzących kobiet, dla celów najwyraźniej związanych z działalnością dziennikarską. Niemożność rozpoznania tożsamości przechodzących nie pozwoliła interweniować krajowemu organowi ochrony danych.

Uwzględniając różnorodność sytuacji, grupa robocza uważa za konieczne zwrócenie uwagi, że dyrektywa 95/46/WE ma zastosowanie do przetwarzania danych osobowych włącznie z obrazami i dźwiękami gromadzonymi za pomocą systemu telewizji przemysłowej i innych systemów video-nadzoru, zautomatyzowanych w całości lub w części, jak również do nieautomatyzowanego przetwarzania danych osobowych znajdujących się lub mających się znaleźć w zbiorze.

Obrazy i dźwięki odnoszące się do zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych są traktowane 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 one osób, których twarze zostały sfilmowane, lecz zawierają inne informacje (na przykład tablica rejestracyjna samochodu lub numer PIN – otrzymany w wyniku nadzorowania urządzenia do automatycznego pobierania pieniędzy),
- c) niezależnie od nośnika informacji używanego przy przetwarzaniu, (na przykład 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, na przykład obrazy uzyskane w przypadku przekraczania dozwolonej prędkości; inaczej jest w przypadku zapisu obrazu uzyskanego w sposób okazjonalny i odosobniony), jak również komunikacji (połączenie z „centrum” rozpowszechniania obrazów do zdalnych terminali; itd.)

Identyfikacja może być wynikiem, w granicach określonych dyrektywą, połączenia danych z informacjami przechowywanymi przez osoby trzecie, lub posługiwania się, w danym przypadku, szczególnymi technikami lub specjalnymi urządzeniami.

A więc jednym z pierwszych działań, jakie administrator danych musi przedsięwziąć jest sprawdzenie, czy video-nadzór zakłada czy też nie przetwarzanie danych osobowych, o ile dotyczy on osób dających się zidentyfikować. W takim przypadku dyrektywa ma zastosowanie, nawet jeżeli specjalne rozporządzenie na poziomie krajowym przewiduje późniejszą zgodę dla celów bezpieczeństwa publicznego.

Tak jest na przykład w przypadku instalacji przy wejściu lub wewnątrz banku urządzeń, które pozwalają na identyfikację klientów; natomiast, pod pewnymi warunkami, dyrektywa mogłaby nie mieć zastosowania w przypadku filmowania z lotu ptaka, jeżeli obrazu nie można powiększyć w sposób przydatny, lub gdy obrazy nie zawierają danych dotyczących osób, jak na przykład, filmowanie z lotu ptaka terenu w celu lokalizacji źródeł wody lub odpadów, lub dla celów panoramicznej kontroli ruchu na autostradzie.

7. OBOWIĄZKI I ODPOWIEDNIE ZABEZPIECZENIA ZE STRONY ADMINISTRATORA ZBIORÓW

A) Legalność przetwarzania

Administrator musi wcześniej sprawdzić, również w związku z wymogiem, o którym mowa w art. 6 lit. a) dyrektywy dotyczącym legalności przetwarzania, czy działalność nadzorowania jest zgodna z postanowieniami ogólnymi i specjalnymi, mającymi zastosowanie w tej kwestii (ustawy, rozporządzenia, wiążące prawnie kodeksy postępowania). Te postanowienia mogą być również przewidziane dla celów bezpieczeństwa publicznego lub dla celów innych niż ochrona danych osobowych (na przykład konieczność przyznania specjalnego zezwolenia przez szczególne organy administracyjne i przestrzegania wynikających z tego zasad).

Konieczne jest podjęcie wszelkich stosownych środków w celu zagwarantowania, że nadzór z użyciem kamer video będzie zgodny z zasadami ochrony danych, oraz w celu uniknięcia jakiegokolwiek niestosownego wnikania w życie prywatne¹⁵.

Należy również w tym względzie wziąć pod uwagę ewentualne postanowienia dotyczące dobrej praktyki przewidziane w zaleceniach organów nadzoru, jak również inne instrumenty samo-regulacyjne.

¹⁵ Całkiem niedawno pewien bank i lokalna jednostka policji odmówiły spełnienia prośby złożonej przez okradzionego klienta, który wnioskował o wydanie zdjęć zarejestrowanych przez kamerę filmującą, między innymi, bankomat, dotyczących złodzieja, który, po skradzeniu jego karty bankowej nielegalnie posłużył się nią w tym bankomacie, wymawiając się „ochroną życia prywatnego”.

Należy również przejrzeć postanowienia normatywne zawarte w obowiązującym ustawodawstwie krajowym (normy konstytucyjne, postanowienia kodeksu cywilnego i karnego), szczególnie w odniesieniu do „prawa do ochrony wizerunku”¹⁶ lub do ochrony miru domowego, uwzględniając orzecznictwo, które, w pewnych przypadkach, mogło uznać, że niektóre lokale, inne niż prywatne mieszkanie, mogą być traktowane jako pomieszczenia prywatne (na przykład pokoje hotelowe, biura, łazienki, szatnie, wewnętrzne stanowiska telefoniczne itp.).

Jeżeli urządzenia zostały zainstalowane przez osobę prywatną lub przez administrację publiczną, zwłaszcza na poziomie lokalnym, dla celów bezpieczeństwa, wykrywania, zapobiegania i ścigania wykroczeń, należy zastosować szczególną ostrożność, przy określeniu i powiadomieniu o tych celach, w odniesieniu do zadań, które administrator danych może wykonywać zgodnie z prawem. Trzeba będzie wziąć pod uwagę funkcje publiczne, które mogą być wykonywane, zgodnie z prawem, wyłącznie przez odpowiednie organa nieadministracyjne takie jak, w szczególności, organa policji i/lub władze sądownicze.

Szczególny problem dotyczy niektórych organów lokalnych, które nie mają żadnej właściwości bezpośredniej w sprawie bezpieczeństwa i porządku publicznego, a które jednak prowadzą działalność pomocniczą w celu nadzoru. Podobnie niektóre działania nadzorcze prowadzone często pod pretekstem zapobiegania przestępczości, w rzeczywistości służą dostarczaniu dowodów w przypadku popełnienia czynu przestępczego.

B) Specyfika, definicja i legalność celów

Administrator danych musi dbać, aby poszukiwany cel nie był niepewny ani niejasny, również po to, aby posiadać dokładne kryterium oceny zgodności przetwarzania z celem, dla którego jest prowadzone (art. 6 punkt b) dyrektywy).

Ta jasność jest również konieczna, aby móc jasno wyrazić cele nie tylko w informacjach przeznaczonych dla osób, których dane dotyczą, lecz również w stosownym zgłoszeniu, jak również dla celów ewentualnej kontroli wstępnej przetwarzania, prowadzonej zgodnie z art. 20 dyrektywy.

¹⁶ Prawo to przewiduje we Francji i w Belgii „wcześniejszą zgodę”.

Wszelkie dalsze posługiwanie się zgromadzonymi obrazami powinno być wykluczone, ze szczególnym naciskiem na techniczną możliwość reprodukcji (na przykład wyraźny zakaz sporządzania kopii).

Cele te powinny być zaznaczone w dokumencie, który powinien podsumowywać inne ważne aspekty *polityki prywatności*, odnosząc się również do niektórych ważnych aspektów, takich jak wskazanie momentu wymazania obrazów czy wnioski o dostęp i/lub ewentualny wgląd do danych składane przez osoby, których dane dotyczą.

C) Kryteria legalności przetwarzania

Administrator musi upewnić się, czy video-nadzór jest zgodny nie tylko ze szczególnymi postanowieniami, o których mowa w punkcie A), lecz również, w odniesieniu do ochrony danych osobowych, czy spełnia przynajmniej jeden z warunków, czyniących przetwarzanie legalnym, zgodnie z art. 7 dyrektywy.

Z wyłączeniem mniej częstych przypadków wymagających spełnienia wymogów prawa (na przykład niektóre kasyna) lub gdy przetwarzanie jest konieczne dla ochrony wyższych interesów (zdalny nadzór chorych na oddziale intensywnej opieki), administrator często spotyka się z koniecznością spełnienia misji interesu publicznego lub połączonej z wykonywaniem władzy publicznej, która ewentualnie może być regulowana odrębnymi przepisami (na przykład: wykrywanie wykroczeń przeciwko kodeksowi drogowemu, wykrywanie przemocy w środkach komunikacji zbiorowej na terenach o wysokim zagrożeniu przestępczością: art. 7 lit. e); i odwrotnie, administrator może być zmuszony do zapewnienia legalnego interesu, nad którym nie przeważają ani interesy ani prawa i podstawowe wolności osoby, której dane dotyczą (art. 7 lit. f).

W obu tych przypadkach, a szczególnie w drugim, sensytywny charakter przetwarzania wymaga dokładnej analizy zakresu zadań, uprawnień i legalnych interesów administratora danych. Podczas przeprowadzania tej analizy trzeba absolutnie unikać traktowania powierzchownego lub opartego na interpretacjach rozszerzających w sposób arbitralny zakres kompetencji i uprawnień.

W przypadku równowagi między zaangażowanymi interesami, trzeba będzie szczególnie uważnie przeanalizować, wysłuchując wcześniej zainteresowanych stron, możliwość sytuacji, w której interes osób, których dane dotyczą, zasługujący na ochronę znajdzie się w sprzeczności z instalacją systemu lub ze szczególnym sposobem postępowania w odniesieniu do przechowywania lub do innych operacji przetwarzania¹⁷.

Wreszcie zgoda osoby, której dane dotyczą, o ile jest wymagana, musi być wyrażona w sposób jednoznaczny i na podstawie jasnych informacji. Szczególna zgoda musi być wyrażona odrębnie na czynności nadzorowania w miejscach, gdzie odbywa się prywatne życie osoby, której dane dotyczą¹⁸.

Ocena legalności przetwarzania musi również być przeprowadzona z uwzględnieniem postanowień dyrektywy przewidujących szczególne gwarancje dla danych dotyczących wykroczeń (art. 8 ust. 5 dyrektywy)¹⁹.

Dodatkowe środki i ustalenia mogą być wynikiem wstępnej oceny przetwarzania zgodnie z mechanizmem kontroli wstępnej, gdy video-nadzór może stwarzać określone zagrożenia dla praw i wolności osób fizycznych (art. 20 dyrektywy 95/46/WE).

Przetwarzanie prowadzone z użyciem kamer video powinno w każdym razie być przewidziane wyraźnie w postanowieniach ustawodawczych, gdy prowadzone jest przez organ publiczny.

D) Proporcjonalność przy posługiwaniu się video-nadzorem

¹⁷ Art. 6b nowej niemieckiej ustawy federalnej, która weszła w życie 23 maja 2001 r., przewiduje możliwość prowadzenia nadzoru w niektórych miejscach dostępnych publicznie za pomocą urządzeń optycznych lub elektronicznych, pod warunkiem, między innymi, że nie ma powodów sądzić, że zasługujące na ochronę interesy osób, których dane dotyczą, są nadrzędne w stosunku do nadzoru.

¹⁸ Należy zwrócić szczególną uwagę na realną możliwość wyrażenia zgody ważnej w myśl art. 2 punkt h) dyrektywy 95/46/WE („konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie jej danych osobowych”) w przypadku zainstalowania systemu video-nadzoru we współwłasności (wspólnota mieszkaniowa itd.).

¹⁹ Przykładem są zasady zawarte w art. 8 portugalskiej ustawy dotyczącej danych osób podejrzanych o udział w działaniach niezgodnych z prawem lub przestępczych.

Zasada, według której dane muszą być adekwatne i istotne dla celów przetwarzania oznacza, przede wszystkim, że systemy telewizji przemysłowej i inne podobne urządzenia video-nadzoru mogą być stosowane wyłącznie jako środki pomocnicze, to znaczy:

gdy istnieje cel rzeczywiście uzasadniający użycie wyżej wymienionych systemów.

Zasada proporcjonalności oznacza, że systemy te mogą być zastosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, nie wymagające pozyskiwania obrazu (np. wykorzystywanie drzwi antywłamaniowym służące zapobieganiu aktom wandalizmu, instalacja automatycznych bramek i urządzeń kontroli dostępu, wspólnych systemów alarmowych, ulepszone i wzmocnione oświetlenie ulic w nocy, etc.) okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami.

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.

Należy na przykład unikać możliwości instalowania tych systemów przez administrację publiczną dla drobniejszych wykroczeń, na przykład dla wzmocnienia zakazu palenia w szkołach lub w innych miejscach publicznych, lub wyrzucania niedopałków czy śmieci w miejscach publicznych.

Innymi słowy, trzeba stosować w każdym przypadku zasadę, według której dane muszą być adekwatne do wyznaczonego celu, z czego wynika pewnego rodzaju „obowiązek minimalizacji danych” ze strony administratora.

Stąd też instalowanie proporcjonalnego systemu video-nadzoru połączonego z alarmem może być uznane za uprawnione w sytuacji powtarzających się przypadków stosowania przemocy na obszarach nieopodal stadionu, lub w przypadku powtarzających się napadów na terenach podmiejskich w pobliżu przystanków autobusowych. Natomiast inna jest sytuacja w przypadku systemów mających wykrywać (jak to było zgłoszone do pewnego organu ochrony danych) osoby odpowiedzialne za obrażanie kierowcy lub za gryzmolenie na karoserii autobusu (co zresztą nie zostałyby zarejestrowane przez kamerę umieszczoną wewnątrz

pojazdu), lub identyfikować obywateli odpowiedzialnych za drobne wykroczenia administracyjne, na przykład wyrzucanie śmieci na ulicy lub w miejscach, gdzie jest to zabronione, czy też wykrywać osoby odpowiedzialne za okazjonalne kradzieże na basenach.

Ocena proporcjonalności musi być jeszcze bardziej rygorystyczna w przypadku miejsc niedostępnych publicznie.

Wymiana informacji i doświadczeń między właściwymi organami różnych Państw Członkowskich mogłaby okazać się bardzo przydatna²⁰.

Te uwagi odnoszą się zwłaszcza do coraz częstszych przypadków video-nadzoru instalowanego dla celów samoobrony i ochrony mienia, zwłaszcza w pobliżu budynków i urzędów publicznych, wraz z terenami je otaczającymi. W związku z tym narzuca się konieczność bardziej ogólnej oceny pośrednich skutków masowego uciekania się do video-nadzoru (rzeczywista skuteczność odstraszania wynikającego z instalowania licznych systemów, przenoszenie na inne tereny działań wandalów lub innych czynności niezgodnych z prawem, itd.).

E) Proporcjonalność w prowadzeniu nadzorowania z użyciem kamer video

Zasada, zgodnie z którą dane muszą być odpowiednie, istotne i niezbyt obszerne zawiera, po pozytywnej ocenie zgodności z prawem przetwarzania danych prowadzonego z pomocą kamer video, pogłębioną ocenę *proporcjonalności procedur* wyżej wymienionego przetwarzania.

Procedury pozyskiwania obrazu muszą być analizowane ze szczególnym uwzględnieniem następujących aspektów:

- a) kąt filmowania w stosunku do celów przetwarzania²¹ (na przykład, w przypadku nadzoru w miejscach publicznych, kąt nie może pozwalać na uwidocznianie

²⁰ Mogłoby to pomóc w zharmonizowaniu podejścia normatywnego i decyzji administracyjnych, które będą musiały być podejmowane, a które, w pewnych przypadkach, były w przeszłości bardzo rozbieżne (na przykład sale do gry w bingo).

²¹ Przykłady przyjętych ograniczeń w odniesieniu do kąta filmowania znajdujemy w dwóch decyzjach włoskiego organu ochrony danych osobowych. Zakład leczniczy, który chciał zainstalować system pozwalający członkom rodzin/bliskim pacjentów na stałą obserwację chorych znajdujących się w śpiączce, w izolacie lub na oddziale intensywnej opieki, podkreślił konieczność zastosowania odpowiednich urządzeń, uniemożliwiających

szczegółów lub rysów somatycznych niemających znaczenia dla celów przetwarzania, albo na obszarach wewnątrz miejsc prywatnych znajdujących się w pobliżu, zwłaszcza w przypadku używania funkcji zoom);

- b) rodzaj używanych urządzeń pozyskiwania obrazu (stałe lub ruchome);
- c) ich instalacja (położenie kamery, używanie kamer stałych lub ruchomych);
- d) możliwość powiększania obrazu lub używania funkcji zoom już w czasie pobierania obrazu lub *a posteriori*, np. w odniesieniu do przechowywanych obrazów, oraz możliwość zamazania i usuwania poszczególnych obrazów;
- e) funkcja zatrzymania obrazu;
- f) połączenie z „centrum” w celu przekazania sygnału alarmu dźwiękowego lub wizualnego;
- g) kroki podjęte na podstawie video-nadzoru (zamknięcie dróg dostępu, interwencja personelu ochrony itd.).

Po drugie, konieczne jest rozważenie *decyzji, jakie muszą być podjęte w kwestii ewentualnego przechowywania obrazów i okresu ich przechowywania*, okres ten musi być bardzo krótki i określony zgodnie z charakterystyką danego przypadku.

O ile w niektórych przypadkach system polegający na jednorazowym pobieraniu obrazu w obwodzie zamkniętym, bez jego zapisywania (kasa w supermarkecie, na przykład) może być wystarczający, w innych natomiast (przy ochronie prywatnych budynków), mogłoby być uzasadnione nagrywanie obrazów przez kilka godzin i wymazywanie ich automatycznie najpóźniej na koniec dnia i co najmniej na koniec tygodnia. Może być przewidziany jeden wyjątek od tej zasady o ile istnieje racjonalny powód dla oczekiwania, przez określony czas, na ewentualną decyzję władz sądowniczych lub policyjnych jeżeli, na przykład, alarm został wysłany lub została złożona skarga warta rozpatrzenia.

Znowu tytułem przykładu, system, mający na celu kontrolowanie wyłącznie nieuprawnionego wjazdu pojazdów do centrum miasta lub do stref o ograniczonym ruchu powinien rejestrować obraz tylko w przypadku popełnienia wykroczenia.

jednoczesną obserwację innych chorych. W innym przypadku, organ podkreślił administracyjnym organom policji konieczność zastosowania systemu wykrywania naruszeń prędkości, który rejestrowałby tylko tablice rejestracyjne a nie wnętrza pojazdów przekraczających dozwoloną prędkość.

Problem proporcjonalności musi być rozważany w sposób skrupulatny również wtedy, gdy istnieje wymóg przechowywania obrazów przez okres dłuższy, lecz nie przekraczający maksymalnie tygodnia²² (na przykład nadzór kamer video w pobliżu banków w celu identyfikacji osób bywających w banku w dniach poprzedzających dokonanie kradzieży).

Po trzecie należy uważnie rozważyć przypadek, gdzie istnieje możliwość zidentyfikowania osoby dzięki połączeniu obrazu twarzy osoby z innymi informacjami dotyczącymi zarejestrowanych działań lub zachowań (tak jest w przypadku połączenia obrazów z operacjami wykonywanymi przez klientów banku w łatwym do zidentyfikowania momencie).

W tym względzie należy przeanalizować niezaprzeczalną różnicę istniejącą między, z jednej strony, okresowym przechowywaniem obrazów pozyskanych z systemu video-nadzoru zainstalowanego przy wejściu do banku i, z drugiej strony, stworzeniem bazy danych banku, składającej się ze zdjęć i odcisków palców klientów banku, którzy wyrazili na to zgodę, co stanowi znacznie większą ingerencję w życie prywatne.

Na koniec szczególną uwagę należy poświęcić wyborom, jakie mogą zostać dokonane w kwestii *możliwego udostępnienia danych osobom trzecim* (w zasadzie to udostępnianie nie powinno obejmować tych osób, które nie są objęte czynnościami nadzoru), lub całkowitego bądź częściowego rozpowszechniania za granicą lub online tych danych (z uwzględnieniem również postanowień o odpowiedniej ochronie: art. 25 dyrektywy i następne).

Oczywiste jest, że zasada, według której pozyskane obrazy muszą być istotne i niezbyt obszerne, ma zastosowanie również do ewentualnego łączenia informacji przechowywanych przez kilku administratorów systemów video-nadzoru.

Gwarancje te wprowadzają, również na planie operacyjnym, to, co niektóre przepisy wewnętrzne traktują jako *zasadę umiarkowania w posługiwaniu się danymi osobowymi*, która ma na celu jak największe zmniejszenie przetwarzania tych danych.

Ta zasada powinna być stosowana we wszystkich sektorach, z uwzględnieniem faktu, że wiele celów, na pierwszy rzut oka, wymaga posługiwania się danymi osobowymi, a w

²² Duńskie i szwedzkie organy ochrony danych wydały opinię, że zapisy video mogą być przechowywane przez krótki okres nieprzekraczający 30 dni.

rzeczywistości mogą one być osiągnięte bez uciekania się do tych danych, lub z użyciem danych faktycznie zanonimizowanych.

Te rozważania mają zastosowanie również wtedy, gdy istnieje uzasadniona konieczność zrationalizowania zasobów firmy²³ lub ulepszenia usług świadczonych użytkownikom²⁴.

F) Informowanie osób, których dane dotyczą

Przejrzyste i odpowiednie posługiwanie się urządzeniami video-nadzoru oznacza, że informacje mają być udzielane osobom, których dane dotyczą, zgodnie z postanowieniami zawartymi w art. 10 i 11 dyrektywy.

Osoby te muszą być poinformowane, w rozumieniu art. 10 i 11 dyrektywy. Muszą być świadome faktu, że prowadzone są czynności video-nadzoru, również wtedy, gdy są one wykonywane przy okazji spektakli lub imprez publicznych, lub w czasie akcji reklamowych (web-cam – kamery internetowe); muszą być również informowane dokładnie o miejscach będących pod nadzorem.

Nie ma konieczności dokładnego podawania miejsca, w którym zainstalowane są urządzenia, jednakże należy określić w sposób jednoznaczny miejsca nadzorowane.

Tablice informacyjne muszą być umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc (w przeciwieństwie do niektórych przypadków, w których zaakceptowano już odległość 500 m); urządzenia muszą być umieszczone w sposób racjonalny w zależności od sposobu filmowania.

Tablice informacyjne muszą być widoczne i syntetyczne, pod warunkiem, że będą skuteczne, mogą również zawierać symbole używane już w związku z video-nadzorem i z tablicami zakazującymi palenia (mogą różnić się, w zależności od tego, czy obrazy są zapisywane czy nie), które to symbole okazały się użyteczne. Muszą wskazywać cele działań nadzoru jak

²³ Tak jest na przykład w przypadku, gdy trzeba ustalić, ile kas powinno pracować w tym samym czasie w supermarkecie w zależności od przyływu klientów lub gdy trzeba stworzyć optymalną „trasę zakupów” dla konsumentów.

również administratora przetwarzania. Wymiary tablic muszą być proporcjonalne do miejsca, gdzie są umieszczone.²⁵

Szczególne i uzasadnione ograniczenia dotyczące obowiązku informacyjnego mogą być przewidziane tylko w ramach ograniczeń, o których mowa w art. 10, 11 i 13 dyrektywy (na przykład, czasowe ograniczenie może być przewidziane w przypadku gromadzenia danych dla legalnych celów związanych z obronnością, lub, zgodnie z prawem, dla celów realizowania prawa do obrony, tylko w okresie, w którym stanowiłoby to zagrożenie realizacji założonych celów.

Wreszcie szczególną uwagę należy poświęcić odpowiednim środkom przekazywania informacji osobom niewidzącym.

G) Dodatkowe wymogi

W odniesieniu do innych warunków, środków zapobiegawczych i gwarancji, przewidzianych w postanowieniach o ochronie danych osobowych i podsumowanych w punkcie 3 (z odniesieniem również do konieczności informowania i poddawania kontroli niezależnego organu ochrony danych przetwarzania danych osobowych, zgodnie z art. 18, 19 i 28 dyrektywy), Grupa Robocza zwraca szczególnie uwagę na następujące kwestie.

- a) Należy wskazać osoby fizyczne, w ograniczonej liczbie, które mogą przeglądać lub mieć dostęp do ewentualnie zarejestrowanych obrazów, wyłącznie dla celów, dla których prowadzony jest video-nadzór, lub dla koniecznego utrzymywania urządzeń, w celu sprawdzenia ich prawidłowego działania, lub wreszcie na złożony wniosek, zgodnie z prawem, przez osobę zainteresowaną lub przez organy policyjne lub sądownicze w celu wykrycia wykroczenia.

Jeżeli celem video-nadzoru jest wyłącznie wykrywanie, zapobieganie i ściganie wykroczeń, rozwiązanie z podwójnym kluczem dostępu do

²⁴ Aby usprawnić wejście do pracy lub na pokład szczególnego środka transportu, gdy istnieje konieczność kontroli tożsamości, wystarczy posłużyć się dokumentem tożsamości ze zdjęciem danej osoby, ewentualnie na nośniku informatycznym, unikając instalowania systemu rozpoznawania twarzy.

²⁵ Można to określić jako podejście „warstwowe”.

zarejestrowanych obrazów (jeden przechowywany przez administratora a drugi przez policję) może w wielu przypadkach okazać się przydatne dla zagwarantowania, że obrazy te będą oglądane tylko przez policję, a nie przez nieuprawniony personel, bez szkody dla realizacji prawa dostępu ze strony osoby, której dane dotyczą, na wniosek złożony w czasie krótkiego okresu przechowywania obrazów.

- b) Stosowne środki bezpieczeństwa muszą zostać podjęte w celu uniknięcia wystąpienia jednej z okoliczności, o których mowa w art. 17 dyrektywy, włącznie z rozprzestrzenianiem informacji, które mogą być użyteczne przy ochronie prawa osoby zainteresowanej, osób trzecich lub administratora danych. Środki te muszą między innymi zapobiegać wszelkim fałszowaniu, zniekształcaniu lub niszczeniu danych lub powiązanych dowodów.
- c) Zasadniczą sprawą jest, aby zarejestrowane obrazy były dobrej jakości, zwłaszcza jeżeli te same nośniki są często ponownie używane, co powoduje ryzyko, że wcześniejsze obrazy mogą nie zostać usunięte w odpowiedni sposób.
- d) Na koniec szczególną uwagę należy zwrócić na nieustającą działalność szkoleniową i uczulającą operatorów, którzy zajmują się tymi operacjami, zwłaszcza w odniesieniu do pełnego przestrzegania właściwych wymogów. Szkolenia administratorów i operatorów, również związane zagrożeń określonymi zagrożeniami, oraz metody właściwej identyfikacji nagranych osób można także uznać za przydatne.

H) Prawa osób, których dane dotyczą

Szczególny charakter gromadzonych danych osobowych nie wyklucza wykonywania przez osoby, których dane dotyczą, praw, o których mowa w art. 13 i 14 dyrektywy, zwłaszcza prawa do wyrażenia sprzeciwu wobec przetwarzania. Dyrektywa 95/46 daje rzeczywiste prawo osobie, której dane dotyczą, wyrażenia w każdej chwili sprzeciwu wobec przetwarzania jej danych osobowych²⁶ z ważnych i legalnych powodów związanych z jej szczególną sytuacją.

Prawo osób, których dane dotyczą, do zapomnienia i na ogół ograniczone przechowywanie obrazów ogranicza zakres stosowania prawa dostępu osób do danych osobowych, które czynią je co najmniej identyfikowalnymi. To prawo musi jednak być zapewnione, zwłaszcza w przypadku konkretnego wniosku, np. pozwalającego na łatwe wyszukanie obrazu, z uwzględnieniem również konieczności czasowego zagwarantowania praw osób trzecich.

Wszelkie ewentualne ograniczenia mające zastosowanie w przypadku, gdy wysiłki, jakie należy poczynić w celu wyszukania obrazów okażą się wyraźnie nieproporcjonalne z uwagi na badania, koszty i zasoby, ze względu na krótki okres przechowywania tych obrazów, powinny być przewidziane wyłącznie przepisami prawnymi (art. 13 ust. 1 dyrektywy). Będzie brane pod uwagę prawo do obrony podmiotu danych wobec specyficznych wydarzeń, które miały miejsce w branym pod uwagę okresie.

I) Dodatkowe gwarancje dotyczące szczególnych przetwarzań

Video-nadzór prowadzony *wyłącznie* z powodów związanych z pochodzeniem rasowym, przekonaniem religijnym, politycznym lub związkowym lub z określonymi zachowaniami seksualnymi osób musi być zabroniony (art. 8 dyrektywy).

Grupa nie ma tutaj zamiaru opracowywać wyczerpującej listy różnych zastosowań video-nadzoru, pragnie jednak podkreślić konieczność zwrócenia większej uwagi na – generalnie,

²⁶ Chyba, że ustawodawstwo krajowe mówi inaczej

tam, gdzie jest to możliwe, w ramach kontroli wstępnej przetwarzania zbiorów prowadzonej zgodnie z art. 20 dyrektywy - na niektóre konteksty, w których obrazy dotyczące zidentyfikowanych lub identyfikowalnych osób zostały zgromadzone, ponieważ te konteksty wymagają szczególnej analizy każdego przypadku.

Dotyczy to zwłaszcza następujących sytuacji wynikających z doświadczeń i stosowanych już praktyk:

- a) stałe połączenie systemów video-nadzoru zarządzanych przez różnych administratorów;
- b) ewentualne łączenie obrazów z danymi biometrycznymi, takimi jak odciski linii papilarnych (na przykład w wejściach do banków);
- c) używanie systemów identyfikujących głos;
- d) przyjmowanie, zgodnie z zasadą proporcjonalności i na podstawie szczególnych przepisów, systemów indeksacji zarejestrowanych obrazów i/lub systemów do zautomatyzowanego wyszukiwania wyżej wymienionych obrazów, zwłaszcza za pomocą danych identyfikujących;
- e) używanie systemów rozpoznawania twarzy, które nie ograniczają się po prostu do rozpoznania kamuflażu osób (fałszywa broda czy peruka), lecz opierających się na technikach umożliwiających wskazanie osób podejrzanych. Chodzi o możliwość automatycznego rozpoznawania osób na podstawie szablonów i/lub wzorców identyfikacyjnych opartych na specyficznych cechach zewnętrznych (kolor skóry, kolor oczu, rysy twarzy itd.) lub na określonych zachowaniach „anormalnych” (gwałtowne ruchy, przechodzenie osoby podejrzanej w określonych odstępach czasu, sposób parkowania samochodu). Z tego względu interwencja operatora jest wskazana, również w świetle możliwych błędów, jakie mogłyby się zdarzyć w przypadkach, o których mowa w punkcie f);
- f) możliwość automatycznego śledzenia trasy przemieszczania się i/lub rekonstrukcji lub przewidzenia zachowań jakiejś osoby;
- g) podejmowanie zautomatyzowanej decyzji w oparciu o profil osoby lub o inteligentne systemy analizy i interwencji nie wynikające z normalnych sytuacji alarmowych (wejście bez identyfikacji, alarm pożarowy itd.).

8. Video-nadzór w miejscu pracy

W opinii Nr 8/2001 w sprawie przetwarzania danych osobowych w miejscu pracy przyjętej 13 września 2001, jak również w *dokumentcie roboczym dotyczącym nadzoru nad komunikacją elektroniczną w miejscu pracy*, przyjętym 29 maja 2002²⁷, grupa zwróciła już uwagę na pewną liczbę zasad mających zastosowanie do ochrony praw, wolności i godności zainteresowanych osób w miejscu pracy.

Poza uwagami poczynionymi w tych dokumentach i konkretnymi zastosowaniami video-nadzoru, konieczne jest, aby systemy video-nadzoru, których bezpośrednim celem jest zdalna kontrola jakości pracy i wydajności, a które zawierają przetwarzanie danych osobowych w tym kontekście, były z założenia zabronione.

Sprawa wygląda inaczej w przypadku systemów video-nadzoru, które są stosowane, gdy istnieją odpowiednie zabezpieczenia, w celu spełnienia wymogów związanych z produkcją lub z bezpieczeństwem w pracy, chociaż ich pośrednim skutkiem byłby zdalny nadzór²⁸.

Doświadczenie dotyczące stosowania nadzoru wskazuje także, że konieczne jest pozostawienie poza nadzorem miejsc zarezerwowanych dla pracowników do prywatnego użytku a nie mających związku z wykonywaną pracą (toalety, prysznice, szatnie, szafki i miejsca wypoczynku); że obrazy zarejestrowane wyłącznie w celu ochrony mienia oraz wykrywania, zapobiegania i ścigania ciężkich wykroczeń nie były wykorzystywane do zarzucania pracownikowi drobniejszych uchybień dyscyplinarnych, oraz że prawo pracowników do sprzeciwu wobec używania zarejestrowanych obrazów powinno być zagwarantowane.

Informacje muszą być przekazywane pracownikom i wszystkim innym osobom pracującym w tych miejscach. Te informacje muszą zawierać dane administratora i cel nadzoru jak również

²⁷ Oba te dokumenty są dostępne pod następującym adresem:

http://www.europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/index.htm

²⁸ W takich przypadkach, poza uwagami zawartymi w niniejszym dokumencie, byłoby również konieczne szczególne uwzględnienie konieczności przestrzegania praw zawartych w układach zbiorowych. Układy te opierają się czasem na kolektywnym informowaniu pracowników lub ich organizacji związkowych (niezależnie od przewidzianych przez przepisy o ochronie danych osobowych informacji indywidualnych); w innych przypadkach wymagana jest wcześniejsza umowa wypracowana w porozumieniu z przedstawicielami pracowników lub z ich organizacjami związkowymi, w celu określenia procedur instalowania systemu,

inne informacje konieczne dla zagwarantowania odpowiedniego przetwarzania dotyczące osób, których dane są gromadzone, na przykład: w jakich przypadkach nagrania będą analizowane przez dyrekcję, czas rejestrowania i termin, w jakim zapis zostanie przedstawiony przedstawicielom prawa. Przekazanie tych informacji za pomocą na przykład symboli, nie może być uznane za wystarczające w kontekście miejsca pracy.

9. PODSUMOWANIE

Grupa robocza opracowała niniejszy dokument aby przyczynić się do jednolitego stosowania przepisów krajowych przyjętych zgodnie z dyrektywą 95/46/WE w dziedzinie video-nadzoru. W tym kontekście, zasadniczą sprawą jest, aby Państwa Członkowskie ukierunkowywały działania producentów, sprzedawców i dostawców usług, jak również jednostek badawczych tak, aby rozwój technologii, oprogramowania i urządzeń technicznych był zgodny z zasadami zawartymi w tym dokumencie.

* * *

Sporządzono w Brukseli, 25 listopada 2002

Za grupę roboczą

Przewodniczący

Stefano RODOTA

zwłaszcza okresu nadzoru i innych szczegółów dotyczących filmowania. W niektórych krajach przewidziana jest interwencja Państwa jeżeli strony nie mogą dojść do porozumienia.