

Monitoring wizyjny – część I

Geneza i czasy współczesne



podinsp. Jacek Wróbel
nadkom. w st. spocz. Piotr Podsiedlik
Zakład Prewencji i Ruchu Drogowego

Monitoring wizyjny – cz. I

Geneza i czasy współczesne



Katowice 2016

Redakcja:
mł. insp. Dariusz Walczak

Redakcja techniczna i korekta:
Paweł Mięsiak

© Szkoła Policji w Katowicach, Katowice 2016. Pewne prawa zastrzeżone.

Niniejsza publikacja w całości stanowi materiał dydaktyczny Szkoły Policji w Katowicach.
Publikacja dostępna jest na licencji:
Creative Commons – Uznanie autorstwa – Użycie niekomercyjne – Bez utworów zależnych
3.0 Polska (CC-BY-NC-ND) 3.0. Polska.

Postanowienia licencji są dostępne pod adresem:
<http://creativecommons.org/licenses/by-nc-nd/3.0/pl/legalcode>

Spis treści

Wstęp	4
1. Monitoring wizyjny – definicja pojęcia	5
2. Geneza monitoringu wizyjnego	7
3. Rodzaje systemów monitoringu wizyjnego – kierunki ich rozwoju	17
4. Monitoring wizyjny w Polsce	29
Literatura	34

Przypadło nam żyć i pracować w czasach ogromnego i bardzo szybkiego rozwoju techniki i informatyki, które we wszystkich dziedzinach życia służą człowiekowi. Dynamiczny rozwój cyfryzacji świata niesie za sobą jednak wiele zagrożeń, związanych z wykorzystaniem dobrodziejstw współczesności do celów własnych i niekiedy niezgodnych z prawem. W związku z tym szeroko pojęte instytucje i organizacje powołane do walki z przestępczością nie mogą pozostawać w tyle w tym swoistym wyścigu cyfrowych zbrojeń.

Powyższa publikacja dotyczy tylko maleńkiego fragmentu jednej z dziedzin walki z przestępczością za pomocą techniki informatycznej, a mianowicie wykorzystania **monitoringu wizyjnego**.

W tej 3-częściowej pracy przybliżone zostały podstawowe aspekty wykorzystania przez organy ścigania bardzo skutecznego środka do walki z przestępczością jakim jest właśnie monitoring wizyjny. Każda z części publikacji odnosi się do innej problematyki, jednakże są ze sobą powiązane tematyką wykorzystania monitoringu wizyjnego w pracy współczesnej Policji. Pierwsza z części opisuje genezę i krótki rys historyczny monitoringu, część druga odnosi się do aspektu prawnego wykorzystania monitoringu w procesie karnym, natomiast trzecia traktuje o praktycznym wykorzystaniu monitoringu w pracy organów ścigania, odnosząc się zarówno do czynności prewencyjnych, interwencyjnych, jak i wykrywczych.

Publikacja w swoim zamyśle nie ma stanowić kompendium wiedzy na temat tej dynamicznie rozwijającej się problematyki. Lektura skryptu daje jednak solidny fundament do przyswojenia wiedzy w zakresie praktycznego wykorzystania monitoringu wizyjnego w codziennej służbie Policji, ale i innych służb. Skrypt powinien być szeroko wykorzystywany zarówno w procesie dydaktycznym szkoleń podstawowych, jak i kursów specjalistycznych.

Rozdział 1.

Monitoring wizyjny – definicja pojęcia

Monitoring wizyjny – system przekazywania informacji polegający na planowym (ciągłym, prowadzonym w ściśle określony sposób za pomocą wytycznych funkcjonalnych i procedury) obserwowaniu (często również rejestracji) za pomocą środków technicznych zdarzeń, które zachodzą w określonym miejscu, mający na celu zapobieganie przestępstwom, wykroczeniom, wypadkom oraz przypisanie winy, odpowiedzialności za popełnione czyny¹.

Monitoring wizyjny, zwany też telewizją dozorowaną lub przemysłową, a w języku angielskim CCTV (*Closed Circuit TeleVision* – telewizja w układzie zamkniętym) – to system przekazywania oraz rejestracji obrazu z określonych miejsc w zamkniętym systemie odbiorczym, mający na celu nadzór nad obszarem, w którym zainstalowane zostały kamery tego systemu². Jest to zatem system, który pozwala na śledzenie z odległości zdarzeń rejestrowanych przez od jednej do niekiedy nawet kilkuset kamer jednocześnie.

Monitoringiem wizyjnym najczęściej objęte są wszelkiego rodzaju instytucje, firmy, a także określone obszary otwarte, co ewidentnie świadczy o tym, iż przedmiotem monitorowania są osoby znajdujące się w jego zasięgu.

W skład systemu monitoringu wizyjnego wchodzi kamery, z których obraz jest transmitowany do centrum odbiorczego, którego personel na monitorach może obserwować rejestrowane zdarzenia. System monitoringu wizyjnego tym różni się od zwykłej telewizji, że obraz z kamer w jego wypadku jest przekazywany (drogą radiową, kablową) i odbierany tylko w centrum odbiorczym, a nie w nieograniczonej liczbie odbiorników.

¹ M. Ordysińska, *Aspekty prawne funkcjonowania systemów monitoringu wizyjnego w Polsce. Cz. I.*, [w:] „Systemy Alarmowe” nr 4/2006, s. 38.

² Por. Kister Ł. – *Prawne aspekty dopuszczalności monitoringu wizyjnego – ochrona wizerunku osoby*, „Ochrona Mienia i Informacji” nr 6/2010.

Warto również przytoczyć w tym miejscu definicję monitoringu zaproponowaną przez Generalnego Inspektora Ochrony Danych Osobowych w *Wymaganiach w zakresie regulacji monitoringu*, zgodnie z którą: **monitoring (wideonadzór)** – to zdalny odbiór obrazu lub obrazu i dźwięku z przestrzeni znajdującej się w polu widzenia kamer zainstalowanych w określonych punktach w pobliżu monitorowanego obszaru. Natomiast **system monitoringu** – to zespół kamer, urządzeń przesyłowych, elektronicznych nośników danych, urządzeń rejestracji danych, urządzeń odtwarzających zarejestrowane dane oraz oprogramowania wykorzystywanego w celu osiągnięcia określonej funkcjonalności w zakresie monitoringu.

Rozdział 2.

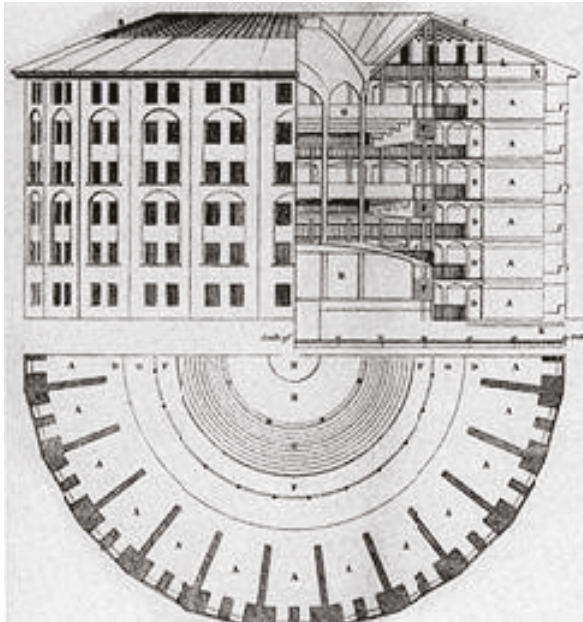
Geneza monitoringu wizyjnego³

Historia monitoringu wizyjnego w postaci zbliżonej do obecnie znanej sięga czasów II wojny światowej. Jednakże pomysły monitorowania obywateli pochodzą z czasów znacznie odleglejszych. Można powiedzieć, iż załączkiem obecnego monitoringu wizyjnego było oświetlanie ulic średniowiecznych miast. Po zapadnięciu zmroku nie tylko zamykano ze względów bezpieczeństwa bramy miejskie, ale także w wielu miastach wprowadzony został zakaz wychodzenia na ulicę bez pochodni lub latarni. Pod koniec XVII w. król Francji Ludwik XIV powołał do życia policję i wprowadził państwowy monopol na oświetlanie miast. Od tej chwili każdy miał stać się widzialny dla funkcjonariuszy.

Model kontroli idealnej zaproponowany został przez Jeremy'ego Benthama, był to tzw. *Panopticon*. Zgodnie z zamysłem autora byłyby to budynek w kształcie pierścienia z umieszczoną pośrodku wieżą, której szerokie okna miały wychodzić na wewnętrzną fasadę pierścienia. Okrągły budynek podzielony byłby na cele, z których każda zajmowałaby całą jego grubość. Cele miałyby dwa okna, jedno skierowane do wewnątrz, na okna wieży, a drugie na zewnątrz pierścienia, pozwalając w ten sposób przechodzić światłu przez celę na wylot. W wieży należało umieścić nadzorcę, a w każdej z cel zamknąć szaleńca, chorego, skazańca, robotnika albo ucznia. Głównym efektem miało być wzbudzenie w uwięzionym świadomego i trwałego przeświadczenia o widzialności, które daje gwarancję automatycznego funkcjonowania władzy.

³ W oparciu o historię monitoringu przedstawioną przez P. Waszkiewicz, *Wielki Brat. Rok 2010...*, s. 30-43.

⁴ Tamże.



Rys. 1. Panopticon Jeremy'ego Benthama z 1791 r.
Źródło: <http://en.wikipedia.org/wiki/Panopticon>. (28.11.2011)

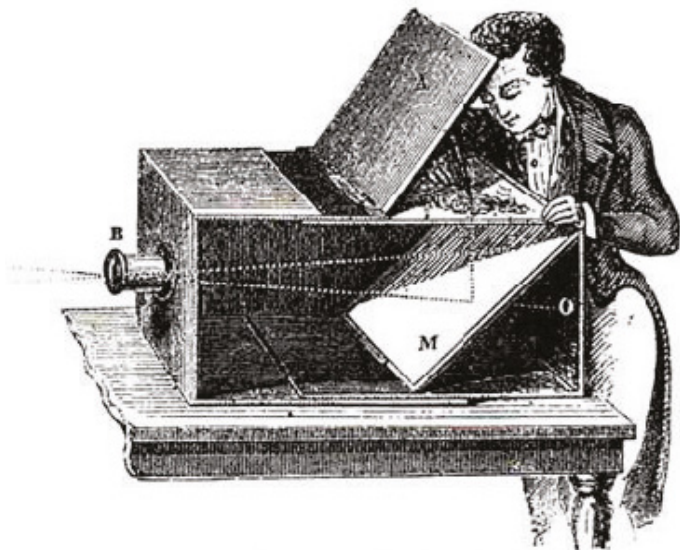
Nadzór, nawet faktycznie nieciągły w działaniu, byłby nieprzerwanie skuteczny. Wystarczyć miała sama świadomość jego istnienia u osób umieszczonych w celach. Osadzeni nie widzieliby kiedy są obserwowani, a kiedy nie. Władza jest niewidzialna i nieweryfikowalna. Ujarmia ona i zmusza do dobrego zachowania: szaleńca do spokoju, robotnika do pracy, ucznia do pilności, chorego do przestrzegania zaleceń lekarza⁵. Taki idealny *Panopticon*, pozwalający na kontrolowanie zachowania uczestników, przypominać może studio „Wielkiego Brata”.

⁵ Zob. Foucault M., *Nadzorować i karać*, Warszawa 1993, s. 195-197.



Rys. 2. Budynek więzienia Presidio Modelo, Isla De la Juventud na Kubie
Źródło: <http://en.wikipedia.org/wiki/File:Presidio-modelo2.JPG>. (28.11.2011)

Grupami podlegającymi szczególnemu zainteresowaniu i nadzorowi ze strony stróżów prawa od początku byli włóczędzy, przestępcy i prostytutki. Od 1857 roku każda jednostka brytyjskiej policji była zobowiązana przekazywać dokładną liczbę znanych złodziei, rabusiów, paserów, prostytutek, osób podejrzanych, bezdomnych oraz włóczęgów do *Home Office* (ministerstwa spraw wewnętrznych). Ideę kontroli obywateli dzięki wykorzystaniu nowinek technicznych realizowano już w XIX wieku. Miały one zastępować funkcjonariuszy w inwigilacji i zbieraniu materiału dowodowego. W latach 20. XIX w. *camera obscura* pozwalała w Glasgow gromadzić dowody przeciwko złodziejom kieszonkowym.



Rys. 3. Camera obscura

Poszukiwanie naukowych metod wspomagających walkę z przestępczością odbywało się niezależnie w różnych państwach. Wykorzystywano do tego kolejno pojawiające się wynalazki – *camera obscura*, fotografia (fotografia kryminalistyczna).

W 1935 roku komendant policji w Chesterfield – Thomas Wells w celu zebrania materiału dowodowego nagrywał z ukrycia kamerą 16 mm przyjmowanie nielegalnych zakładów na rynku miasta. Pozwoliło to na zatrzymanie 39 mężczyzn. Nagranie to, wykorzystane w trakcie postępowania sądowego jako dowód, pozwoliło na skazanie 14 mężczyzn (w konsekwencji skazani zostali tylko ci, którzy się przyznali do winy).

Historia współczesnego systemu monitoringu wizyjnego liczy około 70 lat. Za pierwszy uważany jest system zainstalowany przez firmę Siemens w Peenemünde na wyspie Uznam, gdzie od 1942 roku odbywały się testy rakiet V2. System miał za zadanie przekazywać obraz z miejsca startu rakiet, w którym ze względów bezpieczeństwa nie mogli przebywać ich twórcy, do bezpiecznego bunkra.

Początkowo przez długi okres system monitoringu wizyjnego określany był mianem „telewizji przemysłowej”, co spowodowane było pierwszym i przez pewien czas głównym sposobem wykorzystania tego urządzenia, czyli kontrolą linii produkcyjnych w fabrykach, nadzorowaniem pracowników, a także obserwowaniem procesów, które mają miejsce w nieprzyjaznym dla człowieka środowisku, np. w zbiornikach z trującymi chemikaliami, piecach hutniczych. Szerokie zastosowanie znalazł monitoring wizyjny również w nauce, pozwalając m.in. na śledzenie zachowania zwierząt w ich naturalnym środowisku. Również na niektórych kierunkach studiów wykorzystuje się możliwość przekazywania obrazu na odległość, np. skomplikowane operacje medyczne.

Pierwszą próbę wykorzystania kamer telewizyjnych w celu ułatwienia pracy policji odnotowano w listopadzie 1947 roku w trakcie uroczystości towarzyszących ślubowi przyszłej królowej Anglii Elżbiety II. Policja londyńska sprawdzała wtedy możliwość użycia kamer telewizji BBC do nadzorowania przebiegu wydarzenia, jednak koszty okazały się zbyt wysokie⁶.

Systemy telewizji przemysłowej stosowane są do zarządzania ruchem drogowym w dużych miastach. Początek takiego wykorzystania kamer przypada na lata 50. XX w. Podobny system monitoringu wizyjnego został stworzony w Warszawie w latach 2005-2008.

Wykorzystanie monitoringu wizyjnego w celu poprawy bezpieczeństwa publicznego miało miejsce w roku 1960 w Londynie. Wtedy to policja brytyjska wykorzystwała do ochrony tajskiej rodziny królewskiej, podczas wizyty w Londynie, specjalnie w tym celu zainstalowane na Trafalgar Square dwie kamery, których zadaniem było obserwowanie zgromadzonego tłumu. Kamery ponownie wykorzystano w listopadzie 1960 roku podczas obchodów święta Guy’a Fawkesa.

Rok 1960 był zresztą przełomowy dla techniki filmowej, a co za tym idzie systemu monitoringu wizyjnego, albowiem wtedy wynaleziono technologię kasyety wideo

⁶ Williams C., *Police filming English streets in 1935: the limits of mediated identification*, „Surveillance & Society” 2009, No. 6 (1).

i magnetowidu. Kasety wideo umożliwiła wielokrotne nagrywanie i odtwarzanie taśm bez potrzeby kosztownego procesu wywoływania chemicznego.

W latach 70. XX w. rozpoczęto poszerzanie obszaru objętego zasięgiem systemu nadzoru wizyjnego o banki, kasyna i lotniska, tj. o miejsca o szczególnym charakterze, gdzie również pojawiły się systemy kamer. Za pierwszy komercyjny system uznawany jest oferowany podmiotom prywatnym od 1967 roku przez firmę Photoscan na rynku brytyjskim. Jego zadaniem było przeciwdziałanie kradzieżom sklepowym.

Powstawały też systemy obejmujące swoim działaniem przestrzeń publiczną, mające za zadanie poprawę bezpieczeństwa. Pionierami w tym przypadku wykorzystania monitoringu wizyjnego byli Brytyjczycy. W październiku 1984 r. w czasie konferencji Partii Konserwatywnej w nadmorskim Brighton terroryści z Irlandzkiej Armii Republikańskiej dokonali nieudanego ataku na ówczesną premier Margaret Thatcher, detonując w hotelu bombę i zabijając pięć osób. Kiedy w następnym roku konserwatyści spotkali się w Bournemouth, nad ich bezpieczeństwem czuwał nowy elektroniczny policjant w postaci kamer telewizyjnych tworzących system nadzoru wizyjnego. System składał się z 18 kamer. Po konferencji został rozmontowany, ale już w 1986 r. w niewielkim angielskim miasteczku King's Lynn zainstalowano na stałe trzy kamery, które obserwowały najbardziej niespokojne miejsca. Przystępność tam znacznie spadła⁷.

Wizyjne systemy bezpieczeństwa zaczęły w Wielkiej Brytanii wyrastać jak grzyby po deszczu po roku 1993, kiedy to z centrum handlowego w Merseyside w pobliżu Liverpoolu 12 lutego 1993 r. uprowadzono, a następnie bestialsko zamordowano dwuletniego Jamiego Bulgera. Kamery monitoringu okazały się pomocne w zidentyfikowaniu, a w konsekwencji w zatrzymaniu i skazaniu sprawców owej zbrodni – dwóch 10-latków. Zdarzenie to rozpoczęło prawdziwy boom w dziedzinie monitoringu wizyjnego.

⁷ Zob. Szyborski K., *Wszyscy jesteśmy w ukrytej kamerze. Kamera nabiera rozumu*, „Polityka” nr 29/2007.

W roku 2003 w Wielkiej Brytanii (stolicy monitoringu) zainstalowanych było ponad 4 mln kamer monitoringu wizyjnego – jedna kamera przypada na 14 osób. Przeciętny londyńczyk mógł się spodziewać, że po wyjściu z domu, w ciągu jednego dnia może zostać zarejestrowany około 300 razy. W samym londyńskim metrze działa 6 tys. kamer.

Nie bez znaczenia dla rozwoju systemów monitoringu wizyjnego jest fakt, iż pochodzące z niego nagrania są wymarzoną celem dla mediów – tych opiniotwórczych, jak i tabloidów.

Spośród nagłośnionych w mediach spraw, w kontekście których pojawiły się nagrania z kamer monitoringu wizyjnego, należy wspomnieć wydarzenia z 20 kwietnia 1999 r., kiedy to w szkole średniej w amerykańskiej miejscowości Columbine z rąk dwóch uczniów – Erica Harrisa i Dylana Klebolda zginęło 12 uczniów i jeden nauczyciel, a na koniec obaj popełnili samobójstwo. Kamery zainstalowane w szkole nie zapobiegły wprawdzie tragedii, ale utrwaliły m.in. ostatnie chwile życia obu sprawców, co następnie było przekazywane w mediach.

Innym przykładem wykorzystania w mediach nagrań z kamer systemu CCTV przedstawiających sprawców głośnego zdarzenia są zamachy terrorystyczne dokonane w Londynie w dniu 7 lipca 2005 r., w efekcie których zginęły 52 osoby, a 700 zostało rannych. Kamery zarejestrowały czterech sprawców wchodzących na stację Luton, a także przed rozdzieleniem się w londyńskim metrze. Sprawców wytypowano wprawdzie podczas śledztwa powybuchowego m.in. na podstawie ujawnionych przy ich zwłokach biletów oraz informacji od rodziny, jednak nagrania pozwoliły na odtworzenie ich *modus operandi*, a jako nośne medialnie utrwaliły publiczny wizerunek monitoringu wizyjnego jako skutecznego środka walki z przestępczością, także tą o charakterze terrorystycznym. W toku śledztwa ujawniono również nagrania z 28 czerwca 2005 r., kiedy to późniejsi sprawcy przeprowadzili próbę „na sucho”, pokonując całą trasę planowanego zamachu.

Dwa tygodnie później – 21 lipca 2005 r. odbyła się w londyńskim metrze nieudana próba dokonania podobnych zamachów. Nagrania z systemu monitoringu wizyjnego

przedstawiające niedoszłych zamachowców umożliwiły ich identyfikację, późniejsze aresztowanie i stanowiły materiał dowodowy w procesie, w którym cała czwórka została uznana za winnych zarzucanych im czynów⁸. Następnego dnia po nieudanych zamachach z 21 lipca 2005 r. doszło do tragicznej pomyłki i Jean Charles de Menezes, brazylijski elektryk, został omyłkowo zastrzelony przez policję na stacji metra Stoczkwell. Pomyłono go z poszukiwanym zamachowcem. Początkowo policja informowała, że brak jest jakichkolwiek nagrań z systemu CCTV, co w obliczu wszechobecności kamer w Londynie budziło poważne wątpliwości mediów i opinii publicznej⁹. Zapis zainstalowanych w metrze kamer pozwolił odtworzyć faktyczny przebieg całego wypadku i zdemaskować nieprawdziwą wersję zdarzeń przedstawioną przez policję.

Inny przykład głośnej próby zamachu terrorystycznego ilustrowanej w mediach nagraniami z monitoringu wizyjnego miał miejsce w Niemczech 31 lipca 2006 r. Ładunki wybuchowe o potencjalnym rażeniu porównywalnym z ładunkami użytymi rok wcześniej w Londynie, pozostawione w dwóch pociągach ruszających z dworca w Kolonii z powodu wady konstrukcyjnej nie eksplodowały. Zarejestrowano natomiast niedoszłych zamachowców, kiedy pakowali swoje „bagażę” do pociągu. Na podstawie nagrań z dworcowych kamer sprawcy zostali zidentyfikowani. Nie powstrzymało to ich przed wyjazdem tego samego dnia poza granice Europy, ale dzięki współpracy z libańską służbą bezpieczeństwa zostali zatrzymani¹⁰.

12 kwietnia 2006 r. na Dworcu Centralnym w Brukseli, 17-letni Joe Van Holsbeek zginął od siedmiu ciosów nożem, kiedy nie chciał oddać napastnikom swojego odtwarzacza MP3. Śmierci Joe kamery monitoringu wizyjnego na dworcu w Brukseli przyglądały się bacznie. Dzięki nim schwytanie obu sprawców zajęło zaledwie kilka dni. Sprawcami okazali się dwaj nastolatki (wówczas w wieku 16 i 17 lat) narodowości polskiej – Mariusz O. i Adam G.

⁸ *Four guilty over 21/7 bomb plot*. BBC News 24, <http://news.bbc.co.uk/1/hi/uk/6284350.stm> (06.12.2011).

⁹ Wright S. – *No CCTV to reveal why police shot Brazilian*. „Daily Mail” 13.08.2005 r.

¹⁰ Latsch G., Kleinhubbert G., Meyer C., Stark H., Ulrich P. – *Alptraum der Fahnder*. „Der Spiegel” 35/2006 z 28.08.2006.

Zdarzają się jednak przypadki, w których pomimo znacznej liczby kamer systemu CCTV brak jest nagrania dokumentującego interwencję funkcjonariuszy, mogącego stawiać ich w niekorzystnym świetle. Głównym przypadkiem jest historia, która miała miejsce 14 października 2007 r. na lotnisku w Vancouver. 40-letni Robert Dziekański, który przyleciał z Polski do swojej matki, po 10 godzinach czekania na hali bagażowej zaczął zachowywać się agresywnie, na co policja zareagowała użyciem paralizatora, wskutek czego Polak zmarł. W celu ujawnienia faktycznego przebiegu zdarzeń, sprzecznego z wyjaśnieniami uczestniczących w nim funkcjonariuszy wykorzystano nagranie wideo wykonane przez przypadkowego pasażera – Paula Pritcharda¹¹.

W nocy z 22 na 23 lipca 2006 r. w miejscowości Exeter w Wielkiej Brytanii miał miejsce gwałt i brutalne pobicie 48-letniej kobiety. Oskarżony, a następnie skazany na karę podwójnego dożywocia został 25-letni Jakub Tomczak. Głównymi dowodami w tej sprawie była analiza DNA nasienia zabezpieczonego na miejscu zdarzenia i nagrania z kamer monitoringu wizyjnego¹².

Przedstawione przypadki stanowią jedynie najbardziej medialne zdarzenia śledzone przez opinię publiczną ze szczególnym zainteresowaniem z powodu wagi zarejestrowanych wydarzeń, ich nietypowości czy naruszenia uprawnień przez funkcjonariuszy mających stać na straży prawa i porządku.

Opisując historię monitoringu wizyjnego i zjawiska zwiększania liczby systemów CCTV należy wspomnieć o jego polityczno-ekonomicznym tle. Gwałtowny rozwój systemów CCTV, którego początek przypada na lata 90. XX w. bywa niekiedy łączony z zakończeniem okresu zimnej wojny. Wydatki na zbrojenia ponoszone przez państwa po obu stronach żelaznej kurtyny doprowadziły do powstania przemysłu militarnego zatrudniającego dziesiątki tysięcy pracowników i kumulującego pokaźny zysk dla akcjonariuszy. Kiedy upadł przeciwnik, który uzasadniał gigantyczne zbrojenia, z dnia na dzień podważony został sens ponoszenia związanych z tym wydatków. Zaczęto

¹¹ *Zarzuty dla kanadyjskich policjantów za śmierć Polaka?* <http://serwisy.gazeta.pl/swiat/1,34223,4695331.html>.

¹² Szostak V., *Dożywocie – jest wyrok ws. Jakuba T.*, „Gazeta Wyborcza” z 28.01.2008 r., s. 2.

mówić o tzw. dywidendzie pokojowej, czyli oszczędnościach, które można przeznaczyć na polepszenie edukacji i opieki zdrowotnej. Dywidenda ta dla przemysłu zbrojeniowego oznaczała jednak bardziej zagrożenie niż możliwość, zgodnie z tezą, że trudno w ciągu jednego dnia przestawić profil produkcji z pocisków na lekarstwa. Dylemat ten został rozwiązany poprzez reorientację – wykorzystanie technologii militarnych, ale w sektorze bezpieczeństwa wewnętrznego. Dwa międzynarodowe koncerny produkujące broń już w 1989 roku zawarły kontrakty z *Home Office* na dostarczanie technologii nigdy wcześniej nie stosowanych w sektorze cywilnym.

Wzrostowi liczby kamer towarzyszy wysoka ocena ich przydatności ze strony opinii publicznej oraz domaganie się rozszerzenia systemu na jeszcze nie objęte nim obszary. Mało kto zwraca uwagę na wszechobecność kamer, która jeszcze kilka lat temu mogła wydawać się wizją rodem z „Roku 1984” Georga Orwella.

Rozdział 3.

Rodzaje systemów monitoringu wizyjnego – kierunki ich rozwoju

Podstawowym kryterium podziału systemów monitoringu wizyjnego stanowi sposób postępowania z obrazem, który przekazywany jest przez kamery do centrum odbiorczego. Możemy wyróżnić trzy najczęstsze rozwiązania¹³:

- 1) w centrum odbiorczym znajdują się operatorzy śledzący (w sposób nieprzerwany lub tylko w określonych godzinach) na monitorach trafiające z kamer obrazy, które mogą być rejestrowane w celu późniejszego ich wykorzystania,
- 2) brak operatorów – obraz jednak jest rejestrowany,
- 3) obraz nie jest rejestrowany ani nie ma operatorów w miejscu, do którego jest on transmitowany.

Każde z przedstawionych rozwiązań może składać się z różnych podtypów, np. w miejsce operatorów, których głównym zadaniem jest obserwowanie obrazu z kamer, mogą to robić pracownicy, którym wyznaczono inne zadania, a tylko okazjonalnie zerkają na monitory. Ma to miejsce w części systemów policyjnych, kiedy oficer dyżurny wykonując swoje podstawowe czynności ma możliwość nieprzerwanego podglądu na nadzorowany przez kamery teren lub w sklepach, w których obraz z kamer umieszczonych w różnych punktach jest widoczny dla osoby obsługujących klientów zza lady. Natomiast trzecie zaprezentowane rozwiązanie może pojawiać się w osiedlowych systemach monitoringu wizyjnego, z których obraz jest transmitowany przez kanał lokalnej telewizji, a mieszkańcy dzięki temu mogą mieć wgląd w to, co aktualnie dzieje się w ich sąsiedztwie, a w wypadku zaobserwowania zagrożenia mogą poinformować odpowiednie służby¹⁴.

¹³ Waszkiewicz P., *Wielki Brat...*, *op. cit.*, s. 43.

¹⁴ Tamże.

Systemy monitoringu wizyjnego możemy podzielić również na **stacjonarne** i **mobilne**. Systemy stacjonarne tworzą kamery zamontowane na stałe, z kolei systemy mobilne złożone są z kamer, które można zainstalować w dowolnym miejscu, a obraz z nich może trafić zarówno do centrum odbiorczego zlokalizowanego na stałe w jednym miejscu, jak i mobilnego umiejscowionego w przedziale ładunkowym specjalnie przystosowanego samochodu dostawczego. Systemy mobilne bardzo często wykorzystywane są podczas zabezpieczania imprez masowych: meczów piłkarskich, manifestacji, koncertów itp.



Rys. 4. Policyjny radiowóz wyposażony w kamery

Systemy monitoringu wizyjnego mogą również składać się z kamer, które są **widoczne** dla każdego lub dodatkowo oznaczone specjalnymi znakami (w niektórych krajach jest to prawnie wymagane), a niekiedy administratorom zależy na uzyskaniu materiału w drodze działań **utajonych**. W tym miejscu można przywołać kamery monitoringu umieszczane przez pracowników Lasów Państwowych w miejscach, w których ludzie urządzili sobie wysypisko śmieci. Zadaniem takich kamer jest rejestracja prawnie zabronionego działania, wraz z wizerunkiem jego sprawcy.



Rys. 5. Kamera umieszczona w lesie w okolicy Olsztyna

Często ukryte kamery są montowane przez pracodawców w celu nadzorowania pracy ich pracowników. Takie kamery służą kontrolowaniu tego, co robią oni w trakcie pracy bez świadomości bezpośredniego nadzoru ze strony przełożonych, czy wypełniają oni swoje obowiązki, a w przypadku zadań związanych z obrotem gotówką, czy nie działają na niekorzyść swojego pracodawcy lub jego klientów.

Wykorzystywane w chwili obecnej systemy monitoringu wizyjnego bardzo często pozwalają na aktywne sterowanie kamerami i dokonywanie dokładnych zbliżeń. Możliwa jest praca kamer nie tylko w ciągu dnia, ale również w trybie nocnym przy wykorzystaniu chociażby podczerwieni. Niektóre systemy wyręczają obsługę, poprzez obserwowanie terenu według zaplanowanego schematu, co nie wyklucza przejścia kontroli nad ruchem wybranej kamery przez operatora lub samoczynne włączenie się przy wykryciu ruchu lub zmiany temperatury.

Kilkadziesiąt tysięcy widzów obecnych w styczniu 2001 r. na dorocznym meczu futbolowym Super Bowl we florydzkim mieście Tampa nie zdawało sobie sprawy, że są uważnie śledzeni. Miejskowa policja wykorzystła to wydarzenie, aby po raz pierwszy na tak wielką skalę przetestować nowy inteligentny system bezpieczeństwa

FaceTrac, potrafiący automatycznie rozpoznawać rysy twarzy przestępców znanych z policyjnych kartotek. Kamery rejestrowały wszystkich wchodzących na stadion kibiców i ich wizerunki przekazywały do komputera, który identyfikował 128 specyficznych parametrów – takich jak rozstaw oczu, grubość warg, owal twarzy – i porównywał je z zawartością kryminalnego banku danych. Choć zdania na temat oceny tego przedsięwzięcia były podzielone, policyjne komputery rozpoznały w tłumie 19 przestępców. Na razie system *FaceTrac* regularnie stosują kasyna gry w Las Vegas, by wykryć wśród graczy znanych oszustów. Rozpoznawanie twarzy jest tylko jednym z wielu problemów, nad jakimi pracuje dziś armia programistów.

Możliwe jest połączenie kamer z mikrofonami, które pozwoliłyby dodać do przekazywanego obrazu fonię. Umożliwia to lepszą ocenę charakteru obserwowanych zdarzeń oraz uzyskanie bardziej wartościowego materiału dowodowego. obrońcy swobód obywatelskich wskazują jednak na zagrożenie jeszcze szerszą ingerencją w sferę prywatną obywateli¹⁵.

Przykładem zaawansowanego systemu wykorzystującego sprzęgnięcie wizji z fonią jest **SENTRI** (*Smart Sensor Enabled Neural Threat Recognition and Identification – inteligentny czujnik umożliwiający neurologiczne rozpoznanie i identyfikację zagrożenia*) opracowany przez firmę Safety Dynamics. Jest to zintegrowany z kamerą zestaw trzech mikrofonów, które wyławiają z otoczenia zapisane w systemie dźwięki, lokalizują ich źródło, a następnie przekierowują na nie kamerę i alarmują obsługę centrum odbiorczego. Dźwiękami podnoszącymi alarm mogą być strzały z broni palnej, eksplozja materiałów wybuchowych, a także hałas spowodowany piłą łańcuchową czy nawet silnikiem samochodowym¹⁶.

¹⁵ Reichgot M. – *Law enforcement takes surveillance to audio level*. http://www.usatoday.com/travel/2005-07-05-electroniccrime_x.htm?csp=34.

¹⁶ Zob. <http://www.safetymatics.net/>.



Rys. 6. SENTRI w Los Angeles¹⁷

Komputerowa analiza dźwięków rejestrowanych przez mikrofony sprzężone z kamerami została wykorzystana w holenderskim mieście Groningen. Tamtejszy system miejskiego monitoringu wizyjnego został w listopadzie 2006 roku uzupełniony o monitorowanie dźwiękowe. System nazwano **Sound Intelligence** (wywiad dźwiękowy). Jego zadaniem jest wychwytywanie agresji w głosie przechodniów i alarmowanie operatorów kamer o takich wydarzeniach. Umożliwia to fakt, że agresywnym zachowaniom towarzyszy wzrost napięcia krtani, zniekształcający w specyficzny sposób dźwięki wytwarzane przez struny głosowe¹⁸.

Inny sposób przekazywania dźwięku na odległość wykorzystany został przez system monitoringu wizyjnego w Ipswich i Londynie, gdzie głos przekazywany jest w przeciwnym kierunku – przez mikrofon zainstalowany na stanowisku operatora do głośnika zainstalowanego przy kamerze. Umożliwia to zwracanie uwagi osobie naruszającej porządek, uświadomienie jej, że jest obserwowana. Uwaga operatorów kamer skupia się zatem na zakłóceniach porządku, takich jak: spożywanie alkoholu

¹⁷ Źródło: tamże.

¹⁸ *Big brother is listening to you*, New Scientist z 21.11.2006, s. 27.

w nieprzeznaczonych do tego miejscach czy śmiecenie w miejscu publicznym, czyli czynach niebędących przestępstwami, co najwyżej wykroczeniami¹⁹.

Około 2005 roku na stacji metra w Barcelonie zainstalowano system o nazwie **VSIP** (*Video Surveillance Intelligent Platform*), który daje wyobrażenie o możliwości elektronicznych metod inwigilacji. System ten może identyfikować poruszające się w polu widzenia kamery obiekty – ludzi, psy, samochody – i każdy z nich śledzić indywidualnie, nawet jeśli jest to osoba otoczona tłumem innych ludzi. Pozwala to monitorować trasę obserwowanego obiektu oraz sposób jego poruszania się. Dla przykładu, jeśli na peronie metra wybuchnie bójka, kamera dostrzeże osobników wykonujących charakterystyczne gwałtowne ruchy, nietypowe dla zachowań ludzi w spieszącym się do pociągu tłumie. Może też dostrzec, że któryś z uczestników zajścia zmienił nagle pozycję z pionowej na poziomą, a zatem upadł ugodzony ciosem. Jeśli wyspecjalizowany program wykrywa bójkę, automatycznie uruchamia system alarmowy i dalsze działania przejmują już obserwujący ekrany policjanci. Inny algorytm służy do wykrywania gapowiczów przeskakujących bramki przy wejściu.

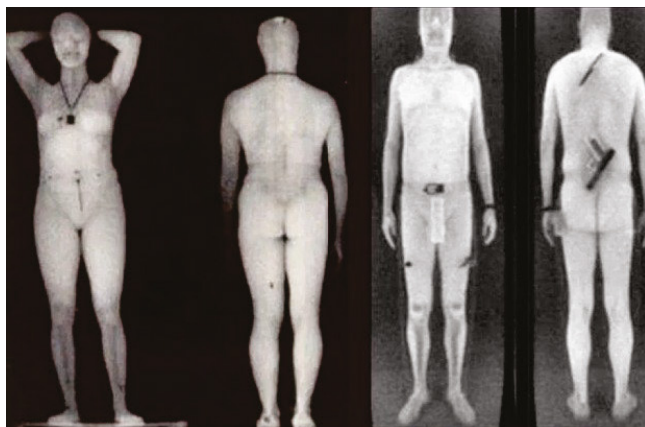
Kamery mogą być też łączone z urządzeniami wykorzystującymi promieniowanie rentgenowskie, tworząc w ten sposób tzw. skanery. Umożliwia to nie tylko zapoznanie się z zawartością bagażu podróżnych na lotniskach (wykorzystywane to jest od wielu lat na całym świecie), ale także z przenoszonymi przez nich przedmiotami, takimi jak broń czy materiały wybuchowe. Promieniowanie o odpowiedniej długości fal skanuje osobę, co pozwala obejrzeć na ekranie zdjęcie bez ubrania i dzięki temu sprawdzić, co znajduje się pod nim. W chwili obecnej są one wykorzystywane na niewielką skalę na lotniskach i testowane również na dworcach kolejowych i stacjach metra. System ten nazwany został *electronic wand* (elektroniczna magiczna różdżka), wzbudzając sporo kontrowersji i wątpliwości dotyczących granic ingerencji w prywatność nieświadomych niczego obywateli, jak i samej efektywności. Przede wszystkim dlatego, że wymaga pozostawienia w ciągłej gotowości funkcjonariuszy interweniujących

¹⁹ *Talking CCTV heading to Ipswich*. http://www.bbc.co.uk/suffolk/content/articles/2007/04/04/rob_dunger_cctv_feature.shtml (30.11.2011)).

bezpośrednio po zidentyfikowaniu przedmiotu podobnego do broni. Jest to możliwe np. na terenie portów lotniczych, ale wiąże się z dodatkowymi kosztami – przede wszystkim zatrudnienia personelu – w przypadku innych miejsc, gdzie miałyby być wykorzystywane, np. stacja metra, dworzec kolejowy czy na otwartej przestrzeni²⁰.



Rys. 7. Przykład wykorzystania promieni rentgenowskich do sprawdzania tego, co osoba ukrywa pod ubraniem²¹.



Rys. 8. Przykład tzw. „nagich skanerów”²²

²⁰ *Could X-ray scanners work on the street?* <http://news.bbc.co.uk/1/hi/magazine/6309917.stm>. (30.11.2011).

²¹ Źródło: tamże.

²² http://technologie.gazeta.pl/internet/1,104530,11322719,Powazna_luka_bezpieczenstwa_w_nagich_skanerach_html

Wydawać się może, że szerokie spektrum możliwości może przynieść połączenie systemów monitoringu z programami komputerowymi analizującymi obraz przekazywany do centrum odbiorczego. Za pierwszy system wykorzystujący automatyczną analizę obrazów uznawany jest **system rozpoznawania tablic rejestracyjnych pokazdów** (ang. *Automatic Number Plate Recognition System – ANPRS*) wykorzystywany w londyńskim systemie bezpieczeństwa noszącego nazwę „Stalowy krąg” (ang. *Ring of steel*). System ten powstał po serii zamachów bombowych dokonanych na początku lat 90. XX w. przez Irlandzką Armię Republikańską na terenie Wielkiej Brytanii. Tworzy go kilkadziesiąt kamer zainstalowanych na zwężonych w tym celu ulicach wjazdowych do City. Na każdym wjeździe są zainstalowane przynajmniej dwie kamery – jedna rejestrująca tablice rejestracyjne, natomiast druga kierowcę i pasażera. Są one połączone z systemem komputerowym identyfikującym je automatycznie. Kiedy poszukiwany samochód jest zidentyfikowany, podnoszony jest alarm. Operatorzy są też poinformowani kiedy zostaje zidentyfikowane podejrzane zachowanie, takie jak próba jazdy niewłaściwą stroną drogi lub pod prąd ulicą jednokierunkową czy też nieopuszczenie monitorowanego obszaru w wyznaczonym czasie²³. Londyński ANPRS w chwili obecnej jest w stanie zanalizować do 5 tys. tablic rejestracyjnych w ciągu minuty. Obecnie ANPRS wykorzystywany jest w wielu krajach, w tym również w Polsce.

Rozpoznanie tablicy rejestracyjnej to tylko namiastka możliwości, jakie stwarza dzisiejsza technologia. Informatycy od lat pracują nad systemem, który pozwoliłby na rozpoznawanie twarzy. Już niedługo kamera sprzężona z odpowiednim oprogramowaniem i bazą zdjęć osób poszukiwanych powinna dopasować jedno do drugiego i wychwycić przestępcę, gdy tylko ten wejdzie w jej pole widzenia.

Połączenie systemu monitoringu wizyjnego z systemem komputerowym rozpoznającym obraz twarzy testował niemiecki Federalny Urząd Kryminalny. Od października 2006 roku do lutego 2007 roku na dworcu kolejowym w Moguncji odbył się szeroko zakrojony eksperyment. Zainstalowano sześć kamer, które miały za zadanie

²³ Stephen G. (red.), *Cities, War and Terrorism: Towards an Urban Geopolitics*, Malden-Oxford-Carlton 2004, s. 281-284.

rozpoznać twarze biorących udział w eksperymencie dwustu uczestników, którzy wyposażeni zostali w specjalny transponder sygnalizujący ich obecność na dworcu. Wyniki przeprowadzonego eksperymentu nie były zadowalające. Podobne wyniki przyniosły badania prowadzone na zlecenie Agencji Zaawansowanych Projektów Obronnych Amerykańskiego Departamentu Obrony. System rozpoznał 35% osób poszukiwanych, przy 10-procentowym współczynniku fałszywych alarmów. Wnioski z innych badań prowadzonych przez niezależne od producentów oprogramowania instytucje są podobne: brakuje, przynajmniej na razie, systemów radzących sobie w zadowalający sposób z automatycznym rozpoznawaniem twarzy ludzkich. Im większa jest baza danych osób poszukiwanych, tym częściej system dokonuje błędnych rozpoznań. Okazuje się, że twarze ludzkie z perspektywy odpowiedniego oprogramowania różnią się od siebie mniej niż byśmy tego oczekiwali.

Na lotnisku w Sydney od 2002 roku testowany jest system firmy Cognitec – FaceVACS, rozpoznający zapisane w banku danych twarze obsługi lotniska i pracowników linii lotniczych. Zadaniem tego systemu jest obsługiwanie tzw. inteligentnych bramek i docelowo zautomatyzowanie kontroli na lotniskach.

Systemy takie, niezależnie od ich faktycznej zdolności identyfikacyjnej, mogą stawać się coraz bardziej popularne ze względu na swoją pozorną „bezinwazyjność”. Identyfikacja za ich pomocą polega na porównaniu wcześniej wprowadzonego zdjęcia osoby z jej wizerunkiem zarejestrowanym przez kamerę. Opiera się więc na podobnej zasadzie jak systemy porównujące wzór linii papilarnych czy inne niepowtarzalne cechy biometryczne. Dzięki systemom automatycznego rozpoznawania twarzy odbywa się to jednak bezkontaktowo.

Rozmaitość takich programów jest niczym nieograniczona i nic nie stoi na przeszkodzie, by sprawdzać na przykład, ilu pasażerów metra lub nieświadomych niczego przechodniów wyciera chusteczką nos bądź kicha. Ta ostatnia informacja może być ważna dla służby zdrowia, spodziewającej się wybuchu epidemii grypy.

W krajach Unii Europejskiej inteligentna inwigilacja przybierze zapewne wkrótce masową skalę, gdyż Komisja Europejska przeznaczyła w 2004 r. ponad 60 mln euro

na wstępne badania, których owocem ma być system zwany **ISCAPS** (*Integrated Surveillance of Crowded Areas for Public Safety* – **zintegrowany system obserwacji miejsc publicznych w celu zapewnienia bezpieczeństwa**). Ma on sięgać po wszystkie nowe narzędzia inteligentnej inwigilacji, m.in. technikę elektronicznego podsłuchu rozmów za pomocą automatycznego czytania z ruchu warg, nad której rozwojem pracują badacze z brytyjskiego Surrey University.

Kolejnym projektem, który ma sprawić, że będziemy żyli bezpieczniej jest INDEC. Jak możemy wyczytać na stronie internetowej projektu²⁴, został on zainicjowany przez Polską Platformę Bezpieczeństwa Narodowego. Propozycja projektu została zgłoszona przez grupę 17 europejskich partnerów pod przewodnictwem Akademii Górniczo-Hutniczej w Krakowie. Głównym koordynatorem projektu jest prof. Andrzej Dziech. W skład konsorcjum projektu wchodzi 11 uczelni wyższych, 4 firmy oraz 2 przyszli użytkownicy systemu (policja z Irlandii Północnej oraz z Polski). Należy podkreślić, iż INDEC jest projektem badawczym umożliwiającym naukową pracę nad innowacyjnymi technikami i algorytmami do walki z terroryzmem oraz inną działalnością przestępczą zagrażającą obywatelom Unii Europejskiej. Obszar badawczy projektu INDEC zostało określony przez 7PR jako „inteligentny system obserwacji środowiska miejskiego”. Pracę nad projektem rozpoczęły się 1 stycznia 2009 roku i będą trwać przez 60 miesięcy. INDEC ma na celu stworzenie narzędzi zwiększających bezpieczeństwo obywateli i poufność zarejestrowanych oraz przechowywanych informacji. Obejmuje to użycie innowacyjnych metod do wykrywania zagrożeń zarówno w sferze rzeczywistej (inteligentne kamery), jak i wirtualnej (sieci komputerowe, Internet).

Głównymi celami projektu UNDEC są:

- stworzenie inteligentnego systemu przetwarzania informacji multimedialnych do automatycznego wykrywania zagrożeń i rozpoznawania działań przestępczych lub przemocy,

²⁴ <http://www.indec-project.eu/front-page> (22.05.2012).

- opracowanie technik dla ochrony danych i prywatności w zakresie przechowywania i transmisji danych opartych na kryptografii kwantowej i nowych metodach cyfrowych znaków wodnych,
- stworzenie prototypu systemu zapewniającego wsparcie dla działań funkcjonariuszy policji w postaci nowych technik i rozwiązań, w tym narzędzi do wykrywania i rozpoznawania zagrożeń w Internecie; wiąże się to z implementacją nowego rodzaju modułu wyszukiwania informacji multimedialnych z użyciem techniki cyfrowych znaków wodnych oraz metadanych.

Metodologia projektu INDECT zakłada w pierwszej kolejności rozpoznanie określonych przestępstw (dziecięca pornografia w Internecie, promowanie zakazanych symboli, handel ludzkimi organami, rozprzestrzenianie niebezpiecznego oprogramowania, jak również akty terroryzmu, bandytyzmu), a następnie wykrywanie źródła zidentyfikowanych przestępstw (na przykład: konkretnych kryminalistów kryjących się za przestępstwami).

Przewidywanymi wybranymi efektami projektu są:

- inteligentna analiza danych wideo i audio w celu wykrywania zagrożeń w obszarze miejskim,
- narzędzia wspomagające wykrywanie treści kryminalnych w zasobach Internetu z ochroną prywatności,
- moduł szybkiej detekcji oraz wyszukiwania zagrożeń w oparciu o technikę cyfrowych znaków wodnych i wykorzystanie kompleksowych badań nad technologią znaków wodnych w celu wyszukiwania semantycznego, nakierowanego na pornografię dziecięcą,
- implementacja rozproszonego systemu komputerowego zdolnego do efektywnego przetwarzania informacji,
- przygotowanie narzędzi i technologii do ochrony prywatności i danych podczas przechowywania i transmisji informacji przy użyciu kryptografii kwantowej i nowych technik znaków wodnych.

Człowiek pozostaje niezbędnym elementem takiego systemu bezpieczeństwa, lecz tylko wtedy, gdy trzeba podjąć decyzję o ewentualnej interwencji. Inteligentne systemy inwigilacji mogą jednak osiągnąć jeszcze wyższy poziom przenikliwości i pomagać nie tylko w wykrywaniu przestępstw, lecz także w ich prewencji. Rama Chellappa z University of Maryland pracuje nad algorytmem, który potrafiłby wykryć podejrzaną zachowanie, zanim dojdzie do zakłócenia bezpieczeństwa publicznego. Jeśli ktoś ukrywa coś pod płaszczem (dajmy na to bombę), porusza się i zachowuje inaczej niż ktoś, kto nie jest obciążony takim brzemieniem. Te zmiany powinny być możliwe do identyfikacji i przetłumaczenia na język komputera. Komputer może także zarejestrować, że ktoś pozostawił w publicznym miejscu niesiony pakunek i oddalił się. Połączenie rozmaitych algorytmów niebawem zwiększa sprawność inteligentnych systemów inwigilacji. W przyszłości kamera, która wykryje osobę niosącą jakiś pakunek – ukryty bądź nie – zidentyfikuje ją na podstawie rysów twarzy i w razie potrzeby zaalarmuje odpowiednie służby.

Rozdział 4.

Monitoring wizyjny w Polsce²⁵

Bardzo trudno jest jednoznacznie wskazać datę pierwszego zastosowania w Polsce kamery do obserwacji otoczenia, jednak historia monitoringu wizyjnego w Polsce liczy sobie zapewne przeszło 30 lat. Monitoring wizyjny był stosowany w ramach telewizji przemysłowej w miejscach pracy, w dużych zakładach przemysłowych, przede wszystkim jako element wspomagający pracę straży przemysłowej. Istnieje duże prawdopodobieństwo, że po raz pierwszy na dużą skalę i z przeznaczeniem prewencyjnym kamery zastosowano na przełomie lat 70. i 80. XX w. na Dworcu Centralnym PKP w Warszawie. Objęto wówczas monitoringiem przede wszystkim perony dworcowe, okolice skrytek bagażowych, a zatem miejsca o natężonym ruchu, gdzie podróżni stawali się łatwym łupem złodziei kieszonkowych i gdzie odbywał się handel środkami odurzającymi.

Jako przykład pierwszego w Polsce wykorzystania systemu CCTV obejmującego przestrzeń publiczną wskazuje się Komorowo, w którym w roku 1997 zainstalowano system składający się z siedmiu kamer²⁶. Pewne jest, że od tego czasu liczba zainstalowanych systemów monitoringu wizyjnego zdecydowanie wzrosła, jak również rozrosły się systemy już istniejące.

W Warszawie, w której pierwsze kamery systemu monitoringu miejskiego zainstalowane zostały w roku 2001²⁷, liczy obecnie 494 kamery. Podobne tendencje wzrostowe zaobserwować możemy również w innych polskich miastach. Poznań

²⁵ Na podstawie P. Waszkiewicz, *Wielki Brat...*, *op. cit.*, s. 55-58.

²⁶ Bielski M., *Miejski system telewizji użytkowej – moda czy konieczność*, „Systemy Alarmowe” nr 3/2000, s. 8.

²⁷ Kalicki A., *Zastosowanie polskiej normy PN-EN 50132-7 na systemy dozorowe CCTV przy projektowaniu monitoringu wizyjnego Warszawy*. Warszawa 2002, s. 9-16.

dysponuje 161 kamerami²⁸, Gdańsk 150²⁹, Wrocław 32³⁰, a Kraków zaledwie 17³¹ (dane dotyczą tylko kamer zakładanych przez władze miasta).

Liczyby te bynajmniej nie szokują, jednak wyraźnie widać tendencję do rozwoju i zwiększania zasięgu monitoringu miejskiego. Obecnie, idąc za przykładem stolicy, dąży się do tworzenia zintegrowanych miejskich centrów monitoringu. Prowadzić ma to do zakończenia swoistego chaosu związanego zarówno z instalacją kamer, jak i ich obsługą. Część kamer w polskich miastach nadal jest instalowana osobno przez Policję, straż miejską czy prywatne firmy działające na zlecenie miasta. Prowadziło i nadal prowadzi to do absurdów, choćby takich jak w Lubartowie. Należące do miasta kamery obsługuje tu Policja, za to ich konserwacją oraz serwisem zajmuje się firma prywatna. Kiedy dochodzi do sytuacji, jak np. „brud na kamerach utrudnia obserwowanie tego, co dzieje się na ulicach”, urzędnicy i policjanci jedynie bezradnie rozkładają ręce, gdyż konieczne jest skontaktowanie się zarówno z firmą serwisową, jak i następnie porozumienie się z miejskimi urzędnikami co do uregulowania płatności. W tym czasie kamery nadal są brudne, a niektóre pozostają uszkodzone³². Inny przykład to wadliwa instalacja kamer w Opolu. Prywatna firma zainstalowała kamery, nie zostawiła jednak rzetelnej dokumentacji, co obecnie po wygaśnięciu gwarancji utrudnia ich naprawę. Miasto musi toczyć spory z prywatnym wykonawcą w sprawie naprawy instalacji i pokrycia jej kosztów³³.

Możemy wyróżnić cztery modele obsługi systemów monitoringu wizyjnego w Polsce:

²⁸ „System Monitoringu Wizyjnego Miasta Poznania”, <http://www.poznan.pl/> (27.09.2010).

²⁹ <http://www.gdansk.pl/> (27.09.2010).

³⁰ <http://www.duw.pl/> (27.09.2010).

³¹ <http://krakow.gazeta.pl/> (27.09.2010).

³² *Policja spogląda brudnym okiem kamery*, <http://www.dziennikwschodni.pl/> (27.09.2010).

³³ *Niechlujny monitoring*, <http://wiadomosci.gazeta.pl/> (27.09.2010).

1. systemy w pełni podlegające Policji – centrala mieści się na terenie budynków Policji, a operatorami są funkcjonariusze lub cywilni pracownicy Policji. Model ten bardzo popularny był w latach 90. XX w.,
2. systemy podlegające nadzorowi Policji, ale obsługiwane przez inny podmiot, najczęściej straż gminną, chociaż może to być inna jednostka samorządu terytorialnego. Obecnie najczęściej występujące rozwiązanie – centrale mieszczą się na terenie budynków Policji, podgląd z kamer trafia również do oficera dyżurnego Policji, ale personelem są strażnicy gminni lub pracownicy samorządu terytorialnego,
3. systemy obsługiwane przez inną niż Policja służbę mundurową – np. Straż Graniczną, Straż Ochrony Kolei,
4. systemy obsługiwane przez podmiot prywatny bez jakiegokolwiek udziału czynnika publicznego czy samorządowego. Ten model jest coraz częstszy i nie dotyczy jedynie przestrzeni w dużych centrach handlowo-usługowych, ale także otwartej przestrzeni. Wykorzystywany jest nie tylko na przestrzeniach otwartych, ale także o ograniczonym dostępie – fabryki, kompleksy biurowe, osiedla zamknięte oraz tam, gdzie dostęp jest otwarty dla każdego.

Spśród najgłośniejszych spraw, w których wykorzystano nagrania z krajowych systemów monitoringu wizyjnego, można wymienić chociażby trzy.

Warszawa 20 października 2005 r. nieznany sprawca, określany jako „bombiarz” sparaliżował na wiele godzin stolicę, rozmieszczając na głównych liniach komunikacyjnych 15 atrap ładunków wybuchowych. W mediach opublikowane zostało zdjęcie domniemanego „bombiarza” pochodzące z kamer w centrum handlowym, z którego wysłał maila do kilku redakcji telewizyjnych serwisów informacyjnych ostrzegając o podłożeniu atrap, jednak do dziś nie pomogło to w jego identyfikacji. Sprawę umorzono.



Rys. 9. Wizerunek „bombiarza” zarejestrowany przez kamerę monitoringu

W nocy z 13 na 14 maja 2006 r. po zdobyciu przez Legię Warszawa mistrzostwa Polski w piłce nożnej, tłum fanów rozpoczął celebrowanie tego faktu na Placu Zamkowym i Rynku Starego Miasta. Świątowanie szybko przemieniło się w całonocne zamieszki uliczne. W wyniku podjętych działań zatrzymanych zostało 231 osób. Pokładano nadzieję w nagraniach kamer monitoringu miejskiego, które utrwały przebieg całego zdarzenia. Jednakże podczas rozpraw sądowych zabezpieczone nagrania nie były wykorzystywane, albowiem stwierdzono, że na większości z nich obraz jest mało czytelny, zdjęcia kręcone w nocy, z dużej odległości, nałożyły się na to również refleksy z pobliskich latarni. W efekcie uniemożliwiło to identyfikację indywidualną sprawców konkretnych czynów.

Najbardziej spektakularne wykorzystanie nagrań z kilku niezależnych systemów monitoringu wizyjnego miało miejsce podczas konferencji prasowej prowadzonej przez prokuratora krajowego Jerzego Engelkinga w dniu 31 sierpnia 2007 r. Podczas konferencji zaprezentowane zostały efekty śledztwa prowadzonego przez Centralne

Biuro Antykorupcyjne w sprawie przecieku informacji na temat przygotowywanej przez CBA akcji w Ministerstwie Rolnictwa i Rozwoju Wsi.

Zauważyć należy, iż pomiędzy Polską a Wielką Brytanią istnieje wciąż spory dystans zarówno w bezwzględnej liczbie zainstalowanych kamer, jak i proporcjonalnej – w przeliczeniu na 1000 mieszkańców. Systemy monitoringu wizyjnego są jednak coraz powszechniejsze nad Wisłą, a przytaczane najgłośniejsze medialnie przypadki przyczyniły się do upowszechnienia wiedzy, a przynajmniej wyrobienia sobie własnego zdania o monitoringu wizyjnym w polskim społeczeństwie. Przykładem na coraz częstsze wkraczanie systemów CCTV w życie codzienne jest też upowszechnienie się systemów monitoringu w szkołach publicznych.

Literatura

- Danilewicz W., *Prawne pojęcie wizerunku*, „Edukacja Prawnicza” nr 6 (117)/2010.
- GIO DO, *Wymagania w zakresie regulacji monitoringu*, http://www.atosochrona.pl/wgrane_pliki/monitoring.pdf.
- Grzybowski S., *Ochrona dóbr osobistych według przepisów ogólnych Kodeksu cywilnego*, Warszawa 1957.
- Kister Ł., *Prawne aspekty dopuszczalności monitoringu wizyjnego – ochrona wizerunku osób*, „Ochrona Mienia i Informacji” nr 6/2010.
- Kosiarski M., *Ostrożnie udostępniamy informacje o sobie. Rozmowa z Michałem Serzyckim* – GIO DO, „Rzeczpospolita” z 10.11.2008.
- Kryszkiewicz M., *Zero prywatności dla niebezpiecznych więźniów*. „Gazeta Prawna” z 26.02.2009 r.
- Makosz A., *Informacje z ulicznych kamer poza kontrolą*, „Dziennik Gazeta Prawna” z 11.06.2010 r.
- Malinowski T., *Aspekty prawne a prawa dziecka w świetle zastosowania systemów monitoringu wizyjnego*, „Zabezpieczenia” nr 4/2011.
- Ordysińska M., *Aspekty prawne funkcjonowania systemów monitoringu wizyjnego w Polsce. Cz. II. Konwencje prawne funkcjonowania systemów monitoringu*, „Systemy Alarmowe” nr 5/2006.
- Ritterman S., *Komentarz do ustawy o prawie autorskim*, Kraków 1937.
- Waszkiewicz P., *Wielki Brat. Rok 2010. Systemy monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne*, Warszawa 2011.
- Sprawozdanie z działalności GIO DO za rok 2000.
- Sprawozdanie z działalności GIO DO za rok 2003.

Zakład Prewencji i Ruchu Drogowego

podinsp. Jacek Wróbel
nadkom. w st. spocz. Piotr Podsiedlik

Szkoła Policji w Katowicach
ul. gen. Jankego 276
40-684 Katowice-Piotrowice
www.katowice.szkolapolicji.gov.pl

