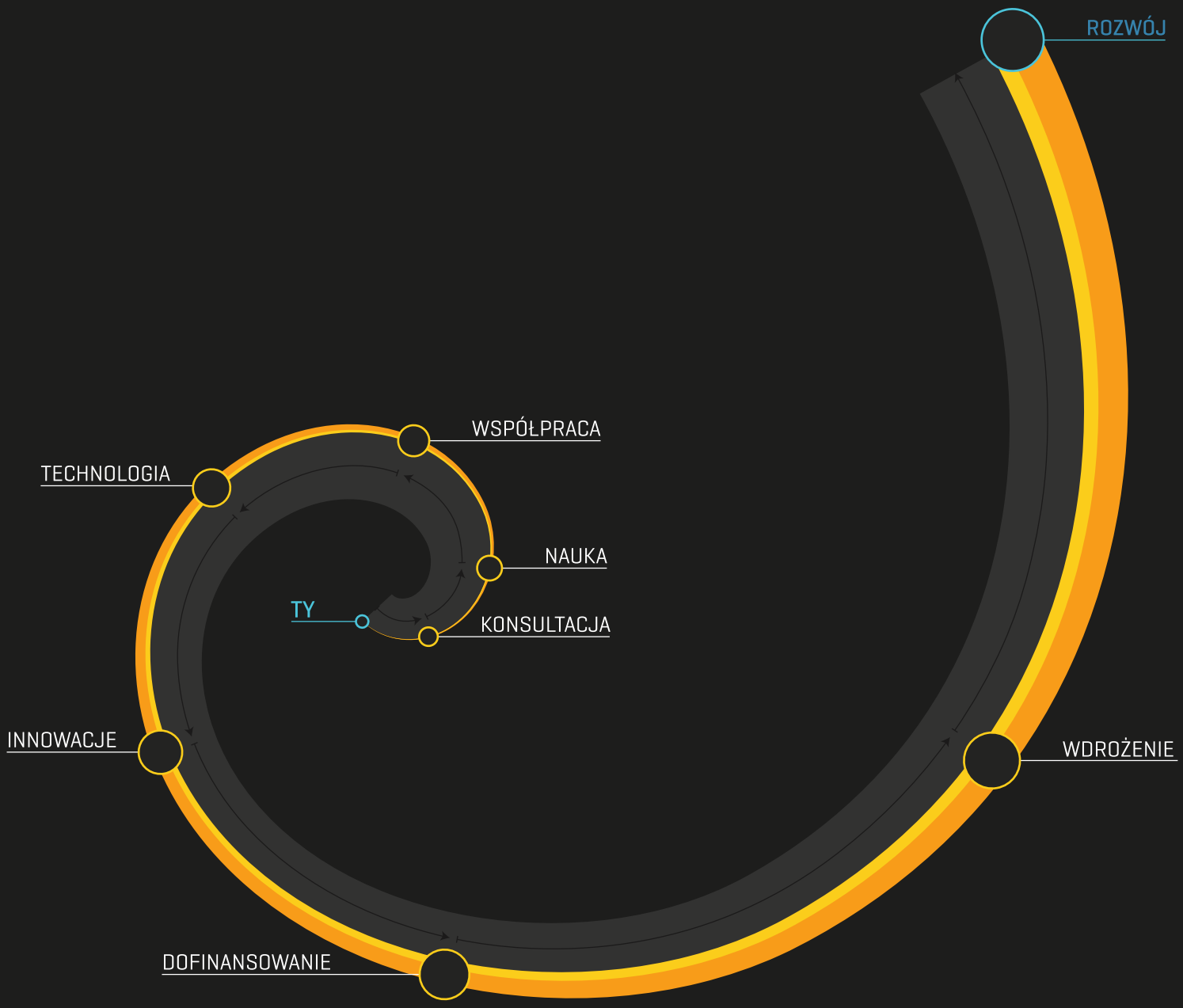
GLIWICE TECHNO PARK

SO RIS Sieć Obserwatoriów ICT

Obserwatorium ICT

www.obserwatoriumict.pl

Raport Obserwatorium ICT



WWW.RIS.SLASKIE.PL

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Śląskie.
Pozytywna energia

Regionalna Strategia Innowacji

Raport współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Autor raportu

dr hab. Grażyna Szpor

(Uniwersytet Ekonomiczny w Katowicach)

Publikacja współfinansowana przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach projektu systemowego „Zarządzanie, wdrażanie i monitorowanie Regionalnej Strategii Innowacji Województwa Śląskiego (3edycja)" (Program Operacyjny Kapitał Ludzki, Poddziałanie 8.2.2)

Publikacja Bezpłatna

Spis treści

1. Przedmiot, kontekst i cel opinii

Przedmiotem opinii jest **stan prawny oraz perspektywy jego zmian w Polsce w zakresie ochrony tożsamości i dóbr osobistych w przestrzeni publicznej w aspekcie monitoringu miejskiego i systemów "inteligentnego miasta" a także możliwość zbierania, przetwarzania oraz dalszego udostępniania takich danych w celu ich wykorzystania w ramach usług informacyjnych w szczególności publicznych i prywatnych aplikacji mobilnych**

Opinia powstała w związku z zapytaniem Nr 28/8.2.2/2012w sprawie przygotowania raportu dla obserwatorium w ramach projektu systemowego „Zarządzanie, wdrażanie i monitorowanie Regionalnej Strategii Innowacji Województwa Śląskiego" realizowanego w ramach poddziałania 8.2.2 PO KL.

Celem niniejszej opinii jest przedstawienie podstawowych - aktualnych i projektowanych - zasad prawnej ochrony dóbr osobistych i tożsamości, przy przetwarzaniu danych w ramach monitoringu miejskiego i systemów inteligentnego miasta oraz możliwości ponownego wykorzystania tych danych dla innych celów w ramach usług informacyjnych.

Poza zakresem opinii pozostaje analiza treści ponad stu obowiązujących w Polsce aktów ustawowych o charakterze dziedzinowym odnoszących się do monitoringu, przesądzających o tym, jakie działania powinny podjąć poszczególne podmioty prowadzące monitoring. Poza zakresem opinii pozostaje także analiza kilkuset aktów regulujących funkcjonowanie ponad dwustu istniejących w Polsce rejestrów publicznych i determinujących możliwość integracji zawartych tam danych rejestrowych w ramach koncepcji inteligentnego miasta. Uwagi z tego zakresu, przedstawione zostały dla sygnalizacji problemów prawnych, których rozwiązanie wymagałoby jednak sporządzenia odrębnej opinii. Wobec toczących się procesów legislacyjnych opinia nie przesądza też ostatecznie kwestii, które wymagają uprzednich rozstrzygnięć prawodawcy.

2. Stanowisko

2.1. Monitoring miejski i systemy inteligentnego miasta mają służyć przede wszystkim dobru publicznemu. Mogą przy tym wspierać ochronę dóbr osobistych [np. zdrowia] ale i naruszać te dobra [np. wolność, prywatność], zwłaszcza w zakresie, w którym umożliwiają określenie tożsamości osób fizycznych [dane osobowe].

2.2. Do zasobów informacji publicznej powstających w ramach monitoringu i systemów inteligentnego miasta zapewnia się dostęp i możliwość ponownego wykorzystania dla celów komercyjnych i niekomercyjnych, o ile przepisy prawne nie ustanawiają ograniczeń jawności ze względu na ochronę prywatności i danych osobowych oraz liczne tajemnice prawnie chronione.

2.3. Standardy ochrony dóbr osobistych i danych osobowych wyznaczają akty prawa międzynarodowego, europejskiego i krajowego, które odnoszą się do monitoringu i koncepcji inteligentnego miasta, ale nie wyodrębniają związanych z nimi problemów i tylko sporadycznie operują tymi pojęciami.

2.4. Zbieranie danych w przestrzeni publicznej, ich przetwarzanie oraz dalsze udostępnianie, regulują w Polsce liczne akty odnoszące się do infrastruktury informacyjnej, w tym do monitoringu oraz systemów informacyjnych uwzględnianych w koncepcji inteligentnego miasta, zawierające także przepisy nakładające na niektóre kategorie podmiotów przetwarzających dane [np. policję, straż miejską], obowiązki związane z ochroną dóbr osobistych i danych osobowych.

2.5. Regulacja ochrony prywatności i danych osobowych, elektronicznych usług publicznych, dostępu do informacji i jej ponownego wykorzystania dla celów komercyjnych i niekomercyjnych jest oceniana krytycznie i przygotowywane są projekty jej zmian. Planowane są nowe akty: rozporządzenie i dyrektywa Parlamentu Europejskiego i Rady w sprawie przepływu i ochrony danych osobowych, nowa polska ustawa o monitoringu [wizyjnym] a także nowelizacje aktów obowiązujących, m.in.: dyrektywy o informacji sektora publicznego, ustawy o dostępie do informacji publicznej oraz ustawy o informatyzacji podmiotów realizujących zadania publiczne.

2.6. Ochrona dóbr osobistych i danych osobowych w ramach monitoringu ma być gwarantowana poprzez wprowadzenie nowych przepisów, określających m.in. miejsca i okoliczności, w jakich stosowanie monitoringu jest dopuszczalne, prawa i obowiązki podmiotu prowadzącego monitoring, prawa osób objętych monitoringiem, oraz zasady dotyczące wykorzystywania danych zebranych w procesie monitoringu.

2.7. Przetwarzanie danych, w tym ich integracja i ponowne wykorzystanie w celach innych niż zostały zebrane w ramach systemów „inteligentnego miasta", w szczególności w związku z rozpowszechnieniem inteligentnych systemów pomiarowych, będzie przedmiotem nowej regulacji, obejmującej nowe instrumenty ochrony danych osobowych, w tym obowiązkowy wymóg, aby administratorzy danych przeprowadzali ocenę skutków w zakresie ochrony danych, a także obowiązek zgłaszania naruszeń danych osobowych.

3. Uzasadnienie

3.1. PODSTAWOWE POJĘCIA

3.1.1. Dobra osobiste to bezspornie zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość. Zgodnie z ustaleniami doktryny i utrwalonej linii orzecznictwa do dóbr osobistych zaliczamy także prywatność. Prywatność charakteryzuje się w doktrynie jako możliwość decydowania o własnym życiu bez ingerencji innych osób, układanie sobie życia według własnej woli, ograniczoną dostępność dla innych. Prywatność sensu stricto nazywana jest intymnością i obejmuje stany cechy i procesy znane tylko jednostce. Prawo do prywatności według klasycznej definicji to „prawo do bycia pozostawionym w spokoju." Subiektywne poczucie zagrożenia i naruszenia dóbr osobistych jest zróżnicowane w zależności od cech osobowych i sytuacji życiowej jednostki oraz jej otoczenia.

3.1.2. Tożsamość to słownikowo m.in. „fakty, cechy, dane personalne pozwalające zidentyfikować jakąś osobę". W prawie publicznym informacje umożliwiające - bez nadmiernych kosztów, czasu i działań - określenie tożsamości osoby fizycznej, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, kulturowe lub społeczne to dane osobowe.

3.1.3. Przestrzeń publiczna obejmuje według definicji legalnej „obszar o szczególnym znaczeniu dla zaspokojenia potrzeb mieszkańców, poprawy jakości ich życia i sprzyjający nawiązywaniu kontaktów społecznych ze względu na jego położenie oraz cechy funkcjonalno-przestrzenne, określony
w studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy." Przestrzeń publiczna sensu largo to obszar „nieprywatny", „miejsca ogólnie dostępne".

3.1.4. Monitoring pojmowany jest jako stała obserwacja i kontrola procesów lub zjawisk albo stały nadzór nad obiektem chronionym. Monitoring wizyjny odnosi się do technologii, która służy rejestracji obrazu i stanowi szczególny rodzaj wideoutrwalania. Obraz z kamery monitoringowej może być przekazywany na duże odległości i odtwarzany na monitorach (np. w celu promocji miejsc turystycznych) i/lub zapisywany na elektronicznych nośnikach danych. Szczególnym rodzajem wideoutrwalania jest wideonadzór, w którego ramach obraz rejestrowany przez kamery przekazywany do centrum obserwacyjnego jest tylko oglądany (np. dla poszerzenie pola widzenia osoby, sprawującej nadzór nad powierzonym obszarem) oglądany i zapisywany na elektronicznych nośnikach informacji (np. dla analizy szczegółów lub celów dowodowych), albo tylko zapisywany (np. w celu zniechęcenia do przestępstw oraz dowodowym przez zapewnienie możliwości odtworzenia w przyszłości).

3.1.5. Inteligentne miasto (smart city) to pojęcie pozaprawne. Koncepcja smart city zakłada, że największe korzyści można osiągnąć dzięki zintegrowanemu rozwojowi, dochodzeniu do zrównoważonego modelu życia, pracy, mobilności i przestrzeni publicznej z pomocą nowoczesnych technologii, ale także przez zmianę zachowań mieszkańców i promocję partnerstwa licznych podmiotów. KE wskazuje jako dobre praktyki: technologie satelitarne ułatwiające kierowanie ruchem drogowym, energooszczędne domy, nowe źródła energii, mniejszy hałas i zanieczyszczenie powietrza. Z wdrażaniem tej koncepcji wiążą się takie rozwiązania, jak np. inteligentne sieci energetyczne, sieci zarządzające synchronizacją świateł czy integracja danych z rejestrów publicznych.

3.2. INFORMACJA PUBLICZNA – DOSTĘP I PONOWNE WYKORZYSTANIE

3.2.1. W prawie Unii Europejskiej standardy informacyjne wyznaczają art. 255 Traktatu Amsterdamskiego z 1997 r. oraz akty soft law, m.in.: Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (PSI) (Dz.U. L 345/90 z dnia 31 grudnia 2003 r. Nr 345, s. 90.) i Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE), (Dz.Urz. UE L z dnia 25 kwietnia 2007 r., Nr 108, s. 1). Standardy jawności uwarunkowane ekologicznie ustanowiła już wcześniej Konwencja o dostępie do informacji, udziale społeczeństwa w podejmowaniu decyzji oraz dostępie do sprawiedliwości w sprawach dotyczących środowiska, sporządzona w Aarhus dnia 25 czerwca 1998 r., która została ratyfikowana przez Polskę (Dz. U. z dnia 9 maja 2003 r). Kompleksowe ujęcie prezentuje Konwencja Rady Europy o dostępie do dokumentów publicznych uchwalona w Tromso 18 czerwca 2009 r., która dotąd nie została podpisana przez Polskę. W aktach tych uwzględnia się, że konsekwencją dostępu do publicznych zasobów informacyjnych jest ich ponowne wykorzystywanie, także w celach innych niż zostały zebrane.

3.2.2. W Polsce istotę prawa do informacji jako obywatelskiego prawa politycznego określa art. 61 Konstytucji stanowiący, że obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Ponadto na mocy art. 74 Konstytucji, usytuowanego w katalogu wolności i praw ekonomicznych, socjalnych i kulturalnych, „każdy ma prawo do informacji o stanie i ochronie środowiska". W polskiej Konstytucji wśród wolności i praw osobistych „każdemu zapewnia się

wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji (art. 54 ust. 1). Wszelkie ograniczenia wolności informacyjnej muszą być przewidziane przez prawo. Za konieczną w społeczeństwie demokratycznym ze względu na bezpieczeństwo, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności uważa się m.in. prawną ochronę tajemnic.

3.2.3. W urzeczywistnianiu prawa do informacji podstawowe znaczenie ma w Polsce ustawa z 6 września 2001 r. o dostępie do informacji publicznej, ale można wskazać kilkadziesiąt innych ustaw, gdzie zagadnienia te pojawiają się w odniesieniu do konkretnych stosunków prawnych. W ponad 140 ustawach i rozporządzeniach znajdują się normy odsyłające do ustawy o dostępie do informacji publicznej. Prawo do informacji to prawo uzyskania dostępu do informacji, któremu odpowiadają obowiązki ich udostępniania po stronie władz publicznych i innych wskazanych ustawowo podmiotów. Podmioty udostępniające informację publiczną to: organy władzy publicznej, organy samorządów gospodarczych i zawodowych, podmioty reprezentujące zgodnie z odrębnymi przepisami Skarb Państwa, podmioty reprezentujące państwowe osoby prawne albo osoby prawne samorządu terytorialnego, podmioty reprezentujące inne państwowe jednostki organizacyjne albo jednostki organizacyjne samorządu terytorialnego, podmioty reprezentujące inne osoby lub jednostki organizacyjne, które wykonują zadania publiczne lub dysponują majątkiem publicznym, osoby prawne, w których Skarb Państwa, jednostki samorządu terytorialnego lub samorządu gospodarczego albo zawodowego mają pozycję dominującą w rozumieniu przepisów o ochronie konkurencji i konsumentów, związki zawodowe i ich organizacje oraz partie polityczne. Prawo dostępu do informacji o sprawach publicznych, zwane „prawem do informacji publicznej", przysługuje każdemu i nie wolno żądać wykazania interesu prawnego lub faktycznego od osoby wykonującej to prawo (art. 2). Obejmuje ono uprawnienie do niezwłocznego uzyskania informacji publicznej zawierającej aktualną wiedzę o sprawach publicznych, do uzyskania informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego, wglądu do dokumentów urzędowych i dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów. Udostępnianie informacji publicznej może — jak stanowi ustawa o dostępie do informacji publicznej — przybierać formy ustną i pisemną, a następować w drodze: ogłoszenia, wyłożenia, wywieszenia, zainstalowania, wstępu na posiedzenia organów oraz poprzez materiały, w tym audiowizualne i teleinformatyczne dokumentujące te posiedzenia. W celu powszechnego udostępniania informacji publicznej utworzono urzędowy publikator teleinformatyczny — Biuletyn Informacji Publicznej [BIP]. Do udostępniania informacji publicznej w BIP obowiązane są będące w posiadaniu takich informacji władze publiczne oraz inne podmioty wykonujące zadania publiczne. Informacja publiczna, która nie została udostępniona w BIP, jest udostępniana na wniosek. Ogólnie zastrzega się, że przepisy ustawy o dostępie do informacji publicznej nie naruszają przepisów

innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi.

3.2.4. Elementem europejskich standardów prawa do informacji jest dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (PSI). W Polsce ponowne wykorzystanie uwzględniono najpierw w ustawie z 4 marca 2010 r. o infrastrukturze informacji przestrzennej, która określa zasady tworzenia oraz użytkowania tej infrastruktury a w szczególności zadania i kompetencje organów administracji prowadzących takie rejestry publiczne, które zawierają zbiory danych przestrzennych. W ustawie o infrastrukturze zamiast o jednolitym „dostępie do informacji", stanowi się o dostępie do 5 typów „usług danych przestrzennych" (wyszukiwania, przeglądania, pobierania, przekształcania, umożliwiania uruchamiania), zobowiązując organy administracji prowadzące rejestry publiczne, do tworzenia i obsługiwania, w zakresie swojej właściwości, sieci usług dotyczących zbiorów i usług danych przestrzennych. Powszechne prawo do nieodpłatnego uzyskania informacji od władz publicznych ogranicza się w ustawie o infrastrukturze do wyszukiwania i przeglądania informacji przestrzennych, natomiast pozostałe operacje na danych traktuje się nie jako elementy dostępu a jako ponowne wykorzystanie udostępnionych danych.

3.2.5. W ustawie z 16 września 2011 r. o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw, przyjęto, że każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu i ponownemu wykorzystywaniu na zasadach i w trybie określonych w niniejszej ustawie (art. 1 ust. 1) i każdemu przysługuje, z zastrzeżeniem art. 5, prawo do ponownego wykorzystywania informacji publicznej. W rozdziale 2 a stanowi się, że wykorzystywanie przez osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej informacji publicznej lub każdej jej części, będącej w posiadaniu podmiotów zobowiązanych, niezależnie od sposobu jej utrwalenia (w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej), w celach komercyjnych lub niekomercyjnych, innych niż jej pierwotny publiczny cel wykorzystywania, dla którego informacja została wytworzona, stanowi ponowne wykorzystywanie informacji publicznej i odbywa się na zasadach określonych w tym rozdziale (art. 23a. 1.) Obowiązani do udostępniania informacji publicznej w celu ponownego wykorzystywania na zasadach i w trybie określonych w ustawie są: Prezes Rady Ministrów, jednostki sektora finansów publicznych, inne państwowe jednostki organizacyjne nieposiadające osobowości prawnej, inne osoby prawne, utworzone w celu zaspokajania potrzeb o charakterze powszechnym, niemających charakteru przemysłowego ani handlowego (jeżeli bezpośrednio albo pośrednio: a) finansują je w ponad 50% lub b) posiadają ponad połowę udziałów albo akcji, lub c) sprawują nadzór nad organem zarządzającym, lub d) mają prawo do powoływania ponad połowy składu organu nadzorczego lub zarządzającego), a także związki wymienionych podmiotów. Przepisów nowego

rozdziału nie stosuje się do: 1) informacji publicznych, których udostępnienie zostało uzależnione od wykazania interesu indywidualnego na podstawie odrębnych przepisów, 2) przekazywania informacji publicznych między podmiotami wykonującymi zadania publiczne, w celu realizacji zadań określonych prawem. Przepisy nowego rozdziału „nie naruszają przepisów innych ustaw określających odmienne zasady wykorzystywania informacji publicznej, pod warunkiem, że stwarzają gwarancje zachowania zasad wynikających z niniejszej ustawy". Informacje publiczne są udostępniane w celu ich ponownego wykorzystywania w zasadzie bez ograniczeń warunkami i bezpłatnie [z zastrzeżeniem ust. 2 i 3 oraz art. 23c]. Jednak podmiot zobowiązany może określić warunki ponownego wykorzystywania informacji publicznej dotyczące: 1) obowiązku poinformowania o źródle, czasie wytworzenia i pozyskania informacji publicznej od podmiotu zobowiązanego, 2) obowiązku dalszego udostępniania innym użytkownikom informacji w pierwotnie pozyskanej formie, 3) obowiązku informowania o przetworzeniu informacji ponownie wykorzystywanej, 4) zakresu odpowiedzialności podmiotu zobowiązanego za przekazywane informacje (art. 23b. 1.). Podmiot zobowiązany określa sposób korzystania z informacji publicznych spełniających cechy utworu w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych lub stanowiących bazę danych w rozumieniu ustawy z dnia 27 lipca 2001 r. o ochronie baz danych, zapewniający możliwość dowolnego wykorzystywania utworu lub bazy danych, do celów komercyjnych i niekomercyjnych, tworzenia i rozpowszechniania kopii utworu lub bazy danych, w całości lub we fragmentach, oraz wprowadzania zmian i rozpowszechniania utworów zależnych. Podmiot zobowiązany może nałożyć opłatę za udostępnienie informacji publicznej w celu ponownego wykorzystywania na wniosek, jeżeli przygotowanie informacji w sposób wskazany we wniosku wymaga poniesienia dodatkowych kosztów. Nakładając opłatę, uwzględnia się koszty przygotowania i przekazania informacji publicznej w określony sposób i w określonej formie oraz inne czynniki, jakie będą brane pod uwagę przy nietypowych wnioskach o ponowne wykorzystywanie informacji publicznej, które mogą mieć wpływ w szczególności na koszt lub czas przygotowania i przekazania informacji. Łączna wysokość opłaty nie może przekroczyć sumy kosztów poniesionych bezpośrednio w celu przygotowania i przekazania informacji publicznej w celu ponownego wykorzystywania w określony sposób i w określonej formie. (art. 23 c), co różni polską regulację od Dyrektywy, w której dopuszcza się rozsądny zysk z inwestycji1. [por. M. Jaśkowska. Dostęp do informacji publicznej a informatyzacja administracji publicznej. W: Prawne problemy informatyzacji administracji Red. G. Szpor. Municipium. Warszawa 2008]

[1]; G. Szpor. Restrukturyzacja regulacji infrastruktury informacyjnej. [w:] Internet. Ochrona wolności, własności i bezpieczeństwa. Red. G. Szpor. CH Beck. Warszawa 2011, s. 211-224

3.3. OCHRONA DÓBR OSOBISTYCH I DANYCH OSOBOWYCH

3.3.1. Prawna ochrona dóbr osobistych ma podstawy m.in. w Europejskiej Konwencji Praw Człowieka, Konstytucji RP oraz przepisach Kodeksu cywilnego. Podstawowym przedmiotem art. 8 Konwencji jest ochrona jednostki przed arbitralną ingerencją ze strony organów władzy publicznej. Każda ingerencja na podstawie ustępu pierwszego art. 8 musi być uzasadniona w świetle drugiego ustępu tego artykułu, mianowicie jako ingerencja "przewidziana przez ustawę" i "konieczna w demokratycznym społeczeństwie" ze względu na jeden z uzasadnionych prawnie celów w nim wymienionych. Zgodnie z ustaloną linią orzeczniczą Trybunału pojęcie konieczności oznacza, iż ingerencja odpowiada pilnej potrzebie społecznej oraz, w szczególności, iż jest proporcjonalna do jednego z uzasadnionych prawnie celów realizowanych przez organy władzy. Artykuł ten może także obejmować ponadto obowiązki pozytywne wpisane w skuteczne "poszanowanie" życia prywatnego. Obowiązki te mogą uwzględniać przyjmowanie środków mających na celu zabezpieczenie poszanowania dla życia prywatnego, nawet w sferze stosunków pomiędzy osobami, obejmujących zarówno ustanowienie ram regulacyjnych dla aparatu sądowniczego i wykonawczego chroniących prawa indywidualne, jak i wprowadzanie, gdy to stosowne, konkretnych środków. Na Państwach spoczywa pozytywny obowiązek zapewnienia prawa swych obywateli do skutecznego poszanowania ich fizycznej i psychicznej integralności. Obowiązki te mogą pociągać za sobą przyjmowanie środków, włącznie z zapewnieniem skutecznej i dostępnej ochrony prawa do poszanowania życia prywatnego.

W art. 23 Kc wymienia się przykładowo dobra osobiste człowieka którymi są w szczególności: zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska. Według utrwalonej linii orzecznictwa do dóbr osobistych zalicza się także prywatność. Art. 24 stanowi, że, ten czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba, że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny (§ 1.). Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych (§ 2). Uprawnienia te nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim i w prawie wynalazczym (§ 3). Generalnie, dobra osobiste pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Ochrona ta uwarunkowana jest wystąpieniem

zagrożenia lub naruszenia określonego dobra. W świetle orzecznictwa „Każde dobro osobiste skupia w sobie dwa elementy - chronioną wartość (np. dobre imię, cześć, wizerunek) oraz prawo żądania od innych jej poszanowania. Wystarczające dla stwierdzenia naruszenia dobra osobistego może być ustalenie, że określona wypowiedź mogła potencjalnie wywołać negatywną ocenę osoby domagającej się ochrony swoich dóbr". Subiektywne poczucie zagrożenia i naruszenia dóbr osobistych, w tym prywatności, jest zróżnicowane w zależności od cech osobowych i sytuacji życiowej jednostki oraz jej otoczenia. Mimo bogatego orzecznictwa - w tym interpretującego art. 47 Konstytucji RP z 2 kwietnia 1997 r., który stanowi, że każdy ma prawo do ochrony prawnej życia prywatnego - nie da się wytyczyć precyzyjnych granic ochrony. Np. monitoring w celu ochrony będącego dobrem osobistym zdrowia, może kolidować z prawem do ochrony innego dobra osobistego: prywatności. Równocześnie nie ulega wątpliwości, że dopuszczalność monitoringu jest uzależniona od respektowania prawa do prywatności. Także Generalny Inspektor Ochrony Danych Osobowych w wystąpieniu z 11 października 2012 r. rozpatrywał ją w kontekście Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przywołując raport dotyczący zasad, jakie w celu ochrony prywatności powinny być stosowane przy pozyskiwaniu i przetwarzaniu danych za pomocą środków monitoringu wizyjnego opracowany przez Grupę Projektową w zakresie Ochrony Danych Osobowych (CJ-PD) przyjęty przez Europejski Komitet ds. Współpracy Prawnej (CDCJ) na 78 spotkaniu w dniach 20-23 maja 2003 r. oraz raport Komisji Weneckiej Rady Europy: „Wideonadzór Miejsc Publicznych".

3.3.2. Ochrona danych osobowych ma umocowanie w Konwencji nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych, Dyrektywie 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), zmienionej dyrektywą 2009/136/WE. Ponadto w art. 8 Karty Praw Podstawowych UE, ustanowiono - niezależne od prawa do prywatności - prawo do ochrony danych osobowych. W Polsce ramy prawne wyznacza Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (art. 51) oraz ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. z dnia 6 lipca 2002 r. Dz.U. Nr 101 poz. 926).

Zasadą obowiązującą na gruncie przepisów ustawy o ochronie danych osobowych jest przypisanie odpowiedzialności z tytułu przestrzegania jej przepisów administratorowi danych. W odniesieniu do zarejestrowanych zbiorów administrator danych osobowych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem.

Zasada legalności odnosi się nie tylko do uodo, ale i do innych aktów regulujących przetwarzanie danych osobowych. Obowiązkiem administratora jest też zapewnienie, aby dane były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, (z zastrzeżeniem ust. 2 i 3), merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (art. 26 ust. 1). Nie budzi także wątpliwości, że naruszeniem tajemnicy osoby upoważnionej do przetwarzania danych osobowych będzie nie tylko przekazanie informacji osobie nieuprawnionej, ale także samo stworzenie możliwości dostępu takiej osoby do informacji (G. Sibiga. Tajemnica osoby upoważnionej do przetwarzania danych osobowych. W: Ochrona danych osobowych. Skuteczność regulacji. Wyd. Municipium. Red. G. Szpor Warszawa 2009, s. 234- 235).
Coraz wyraźniej, zwłaszcza na poziomie europejskim, zauważa się sprzężenie zwrotne między ochroną danych a rozwojem gospodarczym, czego wyrazem było już odrębne ujęcie w Karcie praw podstawowych Unii Europejskiej prawa do prywatności i prawa do ochrony danych osobowych stanowiącego m.in., że dane osobowe „muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą" (Karta Praw Podstawowych Unii Europejskiej. OJ C 364 z 18.12.2000). Przepisy obowiązującej ustawy o ochronie danych osobowych nie zawierają szczególnych regulacji odnoszących się do problematyki przetwarzania danych audiowizualnych, w szczególności pochodzących z monitoringu i innych kamer. Na konieczność uregulowania tej kwestii w ramach dedykowanego aktu prawnego, zwracają uwagę Rzecznik Praw Obywatelskich i Generalny Inspektor Ochrony Danych Osobowych, którzy podkreślają potrzebę ustawowej regulacji monitoringu.

3.4. REGULACJA MONITORINGU W PRZESTRZENI PUBLICZNEJ

3.4.1. Monitoring regulowany jest obecnie w Polsce w około 250 ustaw i rozporządzeń, z czego ponad 60 reguluje „systemy monitoringu." Poszczególne akty dotyczą różnych zagadnień, m.in. ochrony bezpieczeństwa i porządku publicznego, ochrony zdrowia, ochrony środowiska, jakości żywności, wydatkowania środków publicznych. Zakres, dostępność i możliwość łączenia danych z tego monitoringu nie została dotąd kompleksowo zbadania. Monitoring wizyjny miejsc publicznych regulowany jest m.in. w ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz.U.2011.287.1687 j.t.), ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779, z późn. zm.) i rozporządzeniu RM z dnia 16 grudnia 2009 r. w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską)

(Dz.U.2009.220.1720). Przykładem aktualnej kompleksowej regulacji odrębnej monitoringu jest rozporządzenie MSWiA z dnia 10 stycznia 2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej, wydane na podstawie art. 11 ust. 9 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 oraz z 2010 r. Nr 127, poz. 857 i Nr 152, poz. 1021).

3.5. UWAGI DE LEGE LATA I PROJEKTY ZMIAN REGULACJI

3.5.1. W opinii organów właściwych w sprawach ochrony prywatności i danych osobowych: Rzecznika Praw Obywatelskich i Generalnego Inspektora Ochrony Danych Osobowych regulacja w zakresie monitoringu wizyjnego i e-usług publicznych jest niespójna, rozproszona i fragmentaryczna. Przeprowadzone z pomocą tych organów badania ankietowe, wykazały, że w 2011 roku blisko 90% badanych miast wojewódzkich i powiatowych wykorzystywało monitoring wizyjny finansowany z lokalnego budżetu, a 75% miało kamery zintegrowane w ramach miejskiego systemu monitoringu (Fundacja Panoptykon. „Monitoring w polskich miastach i w oczach społeczeństwa" 2011). nie zapewniając należytej ochrony prywatności i danych osobowych, a koncepcja inteligentnego miasta zwiększa zagrożenia w tym zakresie.

W Unii Europejskiej trwają prace nad uregulowaniem problematyki ochrony danych osobowych w ramach instrumentu o zasięgu horyzontalnym, obejmującym terytorium całej Unii Europejskiej – Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (COM (2012) 11 final). Projektowana jest ponadto odrębna dyrektywa w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych [COM/2012/010 final - 2012/0010 (COD)]. 2 Planowana jest także zmiana dyrektywy o informacji sektora publicznego, regulującej ponowne wykorzystanie do celów komercyjnych i niekomercyjnych.

W projekcie unijnego rozporządzenia artykuł 33, który dotyczy oceny skutków w zakresie ochrony danych stanowi, że jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych. Do operacji przetwarzania stwarzających szczególne ryzyko zalicza się tam m.in. : (a) systematyczną i kompleksową ocenę aspektów osobowych osoby fizycznej bądź operacje przetwarzania mające na celu analizę lub przewidzenie w szczególności sytuacji ekonomicznej, miejsca pobytu, stanu zdrowia, preferencji

[2]http://eurlex.europa.eu/Notice.do?val=646249:cs&lang=pl&list=646970:cs,647000:cs,646969:cs,645944:cs,645963:cs,646245:cs,646249:cs,646083:cs,645670:cs,645674:cs,&pos=7&page=15&nbl=1056&pgs=10&hwords=przetwarzaniem%20danych%20osobowych~&checktexte=checkbox&visu=#texte

osobistych, wiarygodności lub zachowania osoby fizycznej, która opiera się na automatycznym przetwarzaniu, i na której opierają się środki, które wywołują skutki prawne dotyczące danej osoby lub mają na nią istotny wpływ oraz (c) monitorowanie publicznie dostępnych miejsc, zwłaszcza przy wykorzystaniu urządzeń optyczno-elektronicznych (wideonadzór) na szeroką skalę. Ocena obejmować ma przynajmniej ogólny opis przewidywanych operacji przetwarzania, ocenę ryzyk dla praw i wolności podmiotów danych, środki przewidywane w celu sprostania ryzykom, gwarancje, środki i mechanizmy bezpieczeństwa mające zagwarantować ochronę danych osobowych oraz wykazać zgodność z rozporządzeniem, uwzględniając prawa i słuszne interesy podmiotów danych i innych zainteresowanych osób. Jeśli administrator jest organem lub podmiotem publicznym i jeśli przetwarzanie wynika z obowiązku prawnego na mocy art. 6 ust. 1 lit. c) przewidującego zasady i procedury operacji przetwarzania przewidziane przez prawo Unii, ust. 1-4 nie stosuje się, chyba, że państwa członkowskie uznają przeprowadzenie takiej oceny przed przetwarzaniem za niezbędne.
W organach unijnych rozpatrywany jest też wniosek dotyczący dyrektywy zmieniającej dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (ISP) oraz w sprawie otwartych danych
Od kilku miesięcy trwają prace nad założeniami odrębnej ustawy, która odnosiła się ma do monitoringu wizyjnego. Prace te prowadzone są w resorcie spraw wewnętrznych.

3.6 ZASADY MONITORINGU

Zasady monitoringu wizyjnego mają zostać sprecyzowane w odrębnej ustawie. Zapewne uwzględniać będą w znacznym stopniu rekomendacje Rzecznika Praw Obywatelskich i Generalnego Inspektora Ochrony Danych Osobowych a także doświadczenia wynikające z porządków prawnych innych państw.
Zgodnie z postulatami Generalnego Inspektora Ochrony Danych Osobowych, regulacje dotyczące monitoringu powinny w szczególności określić (1) miejsca i okoliczności, w jakich stosowanie monitoringu jest dopuszczalne, (2) prawa i obowiązki podmiotu prowadzącego monitoring, (3) prawa osób objętych monitoringiem, oraz (4) zasady dotyczące wykorzystywania danych zebranych w procesie monitoringu. Określone w tych regulacjach warunki prawne stosowania monitoringu powinny zapewnić równowagę między uzasadnionymi potrzebami podmiotów stosujących monitoring i prawem do prywatności osób, które zostały objęte monitoringiem. [Rekomendacje GIODO dostępne są pod adresem http://www.giodo.gov.pl/plik/id_p/2363/j/pl/]

Rzecznik Praw Obywatelskich w rekomendacjach odnośnie do prawodawstwa odnoszącego się do kwestii monitoringu zwraca uwagę na to, że w wielu miejscach, monitoring instalowany jest bez ustawowej podstawy prawnej oraz na konieczność poszukiwania równowagi między bezpieczeństwem obywateli a ochroną ich prywatności, co jest jednym z największych wyzwań wobec instrumentarium, jakie zapewnia rozwój nowych technologii.3 Podkreśla się, iż stosując środki ograniczające należy zwrócić uwagę w szczególności na zasadę proporcjonalności ograniczeń. Zgodnie z poglądem wyrażonym w wyroku Trybunału Konstytucyjnego (Sygn. akt K 23/98), zasada ta: „z jednej stawia przed prawodawcą każdorazowo wymóg stwierdzenia rzeczywistej potrzeby ingerencji w danym stanie faktycznym w zakres prawa bądź wolności jednostki. Z drugiej strony winna ona być rozumiana jako wymóg stosowania takich środków prawnych, które będą skuteczne, a więc rzeczywiście służące realizacji zamierzonych przez prawodawcę celów. Zawsze chodzi o środki niezbędne, w tym sensie, że chronić będą określone wartości w sposób i w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków.”4

Decydując o stosowanym systemie monitoringu należy przede wszystkim zastanowić się nad tym czy stosowane środki są adekwatne do celu, któremu mają służyć. Jeżeli na przykład system monitoringu ma służyć wskazaniu wolnych miejsc parkingowych, nie ma potrzeby, aby zbierane były numery rejestracyjne samochodów, czy utrwalane wizerunki twarzy osób fizycznych.

Rzecznik Praw Obywatelskich zwraca także uwagę na obowiązki informacyjne: konieczność zapewnienia przejrzystości procesu powstawania systemu monitoringu. System monitoringu powinien być stosowany przy zachowaniu zasad jawności oraz transparentności jego funkcjonowania. Badania wykazują, że w ok. 40% przypadków badanego monitoringu miejskiego, obywatele w ogóle nie byli o fakcie jego istnienia informowani. Tymczasem informacja taka powinna być umieszczona każdorazowo w miejscu instalacji kamer oraz zawierać dane podmiotu prowadzącego monitoring.

Także Generalny Inspektor Ochrony Danych Osobowych zwraca uwagę na konieczność szerokiego uwzględnienia kwestii ochrony prywatności w projektowanych przepisach o monitoringu. Powołuje się na opinię nr 4/2004 Grupy roboczej artykułu 29, w której akcentowana jest konieczność respektowania zasady proporcjonalności w przypadku posługiwania się monitoringiem.5 Grupa art. 29 rekomenduje, aby urządzenia służące do takiego monitoringu były stosowane wyłącznie jako środki

[3]Rekomendacje Rzecznika Praw Obywatelskich w sprawie ustawy o monitoringu dostępne są pod adresem http://www.rpo.gov.pl/pliki/13499650170.pdf.

[4]Rekomendacje RPO http://www.rpo.gov.pl/pliki/13499650170.pdf

[5]Opinia 4/2004 "Processing of Personal Data by Means of Video Surveillance", WP 89, 11 lutego 2004 r. Deklaracja grupy roboczej art. 29 dotycząca egzekwowania prawa, WP 101, 25 listopada 2004 r. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm.

pomocnicze, jeśli istnieje cel rzeczywiście uzasadniający ich użycie i tylko w sytuacji, gdy inne środki fizycznej i logistycznej ochrony będą ewidentnie niewystarczające. 6

Generalny Inspektor Ochrony Danych Osobowych zwraca także uwagę na konieczność poddania pod kontrolę organu nadzorczego stosowanych schematów monitoringu, w tym kontroli wstępnej. GIODO proponuje kilka alternatywnych metod spełnienia tego obowiązku. Nadzór może być wypełniany w formie (1) zgody (2) zgłoszenia do podmiotu sprawującego nadzór , bądź też (3) poprzez spełnienie określonych warunków. Każdy z tych warunków będzie zgodny z dyrektywą o ochronie danych osobowych.

Proponuje się alternatywnie: (1) Wprowadzenie obowiązku zgłaszania projektów systemu monitoringu do akceptacji przez organu ochrony danych osobowych lub innego urzędu, w przypadku, gdy w systemie stosowane jest automatyczne przetwarzanie obrazu mające na celu rozpoznanie osób, identyfikację określonego typu zachowań, lub inne mechanizmy wprowadzające indeksację zarejestrowanych obrazów z danymi osobowymi. Jak podkreśla GIODO, celem takiego zgłoszenia byłaby weryfikacja przez organ zastosowanych przez administrator środków ochrony danych osobowych. Obowiązek zgłoszenia mógłby zastąpić obowiązek rejestracji powstałego w ten sposób zbioru danych osobowych. Drugim rozwiązaniem jest wprowadzenie obowiązku zgłaszania zbiorów danych osobowych tworzonych w wyniku stosowania monitoringu. Według GIODO należałoby wówczas dokładnie określić warunki zaklasyfikowania powstałego w wyniku monitoringu nagrania do danych osobowych. 7

W przypadku stosowania mechanizmów wideonadzoru istotne jest także wprowadzenie obowiązków informacyjnych względem podmiotów stosujących tą metodę kontroli. GIODO, podobnie jak RPO zwraca uwagę, iż podmiot stosujący monitoring powinien poinformować osoby, które mogłyby znaleźć się w jego obszarze o istnieniu monitoring, a także obszarze jego stosowania.

Generalny Inspektor Ochrony Danych Osobowych zwraca także uwagę na konieczność respektowania obowiązków informacyjnych względem podmiotów objętych wideonadzorem. Z uwagi na pewne odmienności związane z właściwościami wideonadzoru, obowiązki informacyjne uregulowane w ustawy o ochronie danych osobowych, muszą być stosowane z uwzględnieniem tych odmienności. Organ ochrony danych osobowych zwraca uwagę, iż osoba, której wizerunek został zarejestrowany w systemie monitoringu, powinna mieć prawo do uzyskania informacji dotyczących operacji przetwarzania danych jej dotyczących. Szczególne przepisy prawne powinny jednak regulować

[6]Rekomendacje Generalnego Inspektora Ochrony Danych Osobowych dotyczące ustawy o monitoringu dostępne są pod adresem http://www.giodo.gov.pl/plik/id_p/2363/j/pl/.

[7]Rekomendacje Generalnego Inspektora Ochrony Danych Osobowych dotyczące ustawy o monitoringu dostępne są pod adresem http://www.giodo.gov.pl/plik/id_p/2363/j/pl/.

kwestię, jak w szczegółach wypełnić ten obowiązek aby nie doprowadzić do naruszenia praw osób trzecich, które również znajdują się na nagraniu.

Kwestią istotną jest także proponowany sposób wykonania przez podmiot danych osobowych, prawa żądania korekty lub usunięcia danych zarejestrowanych w systemie monitoringu. W odniesieniu do zakresu i sposobu realizacji tego uprawnienia Generalny Inspektor Ochrony Danych Osobowych proponuje wprowadzenie na żądanie podmiotu danych procedury „zakrywania" wizerunku skarżącej się osoby a także ograniczenie prawa do ingerencji w nagranie, w przypadku, gdy zarejestrowany obraz jest przechowywany tylko przez określony okres, np. 2–4 tygodni, i z uwagi na brak incydentów, w czasie, jaki obejmowało nagranie.

Reasumując, podmioty stosujące środki wideonadzoru, powinny w sposób rozważny definiować zakres informacji, które będą zbierane, biorąc pod uwagę warunek adekwatności planowanych środków oraz cel i zastosowania. Środki tak inwazyjne, jak monitoring powinny być stosowane jedynie w przypadku, gdy na pomocą innych środków nie będzie możliwe osiągnięcie zakładanego celu.

4. Zasady wykorzystania informacji w inteligentnym mieście

Zasady wykorzystania informacji publicznej w celach innych niż zostały zebrane, mają być bardziej zróżnicowane w ramach usług informacyjnych podmiotów publicznych i niepublicznych, co dotyczy także aplikacji mobilnych.

Wynika to nie tylko z projektu europejskiego rozporządzenia w sprawie przepływu i ochrony danych osobowych, bo można wskazać jeszcze inne koncepcje zmierzające w tym kierunku odnoszące się do koncepcji inteligentnego miasta.

W odniesieniu do projektu zmian dyrektywy o informacji sektora publicznego (którego konkretyzacją są w Polsce m.in. przepisy o ponownym wykorzystaniu w ustawie o dostępie do informacji publicznej) Europejski Inspektor Ochrony Danych proponuje określić w bardziej jednoznaczny sposób zakres zastosowania dyrektywy ISP do danych osobowych, wprowadzić wymóg dokonywania oceny przez dany organ sektora publicznego przed udostępnieniem do ponownego wykorzystania jakichkolwiek ISP zawierających dane osobowe, w stosownych przypadkach wprowadzić wymóg pełnej lub częściowej anonimizacji danych oraz wymóg zamieszczenia w warunkach licencji wyraźnego zakazu ponownej identyfikacji osób fizycznych oraz ponownego wykorzystania danych osobowych, co mogłoby mieć wpływ na osoby, których te dane dotyczą, zamieścić wymóg, aby warunki licencji na ponowne wykorzystanie ISP zawierały klauzulę o ochronie danych w każdym przypadku wiążącym się z przetwarzaniem danych osobowych, w stosownych przypadkach ze względu na ryzyko związane z ochroną danych osobowych, zamieścić wymóg nakazujący

wnioskodawcom wykazanie (poprzez ocenę skutków dotyczącą ochrony danych lub w inny sposób), że podjęto odpowiednie działania w celu uniknięcia wszelkiego ryzyka w kwestii ochrony danych osobowych, a wnioskodawca będzie je przetwarzać zgodnie z mającymi zastosowanie przepisami dotyczącymi ich ochrony, wyraźnie stwierdzić, że ponowne wykorzystanie danych osobowych można uzależnić od jego celu, czyniąc tym samym odstępstwo od ogólnej zasady zezwalającej na ponowne wykorzystanie do wszelkich celów komercyjnych i niekomercyjnych. Ponadto EIOD zaleca, aby rozważyć umożliwienie obciążenia licencjobiorców kosztami wstępnego przetworzenia (np. digitalizacji), anonimizacji i agregacji w stosownych przypadkach oraz - aby Komisja opracowała dalsze wytyczne skupiające się na anonimizacji i licencjonowaniu

Komisja przyjęła 9 marca 2012 r. zalecenie w sprawie przygotowań do rozpowszechnienia inteligentnych systemów pomiarowych [C(2012) 1342 wersja ostateczna]. Według opinii Europejskiego Inspektora Ochrony Danych dotyczącej zalecenia Komisji w sprawie przygotowań do rozpowszechnienia inteligentnych systemów pomiarowych (http://www.edps.europa.eu) powinien być wprowadzony obowiązkowy wymóg, aby administratorzy danych przeprowadzali ocenę skutków w zakresie ochrony danych, a także obowiązek zgłaszania naruszeń danych osobowych

Obserwatorium ICT

www.obserwatoriumict.pl

Data publikacji: wrzesień 2013

Park Naukowo-Technologiczny "Technopark Gliwice" ul. Konarskiego 18C, 44-100 Gliwice
info@technopark.gliwice.pl | www.technopark.gliwice.pl

Raport współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społeczne