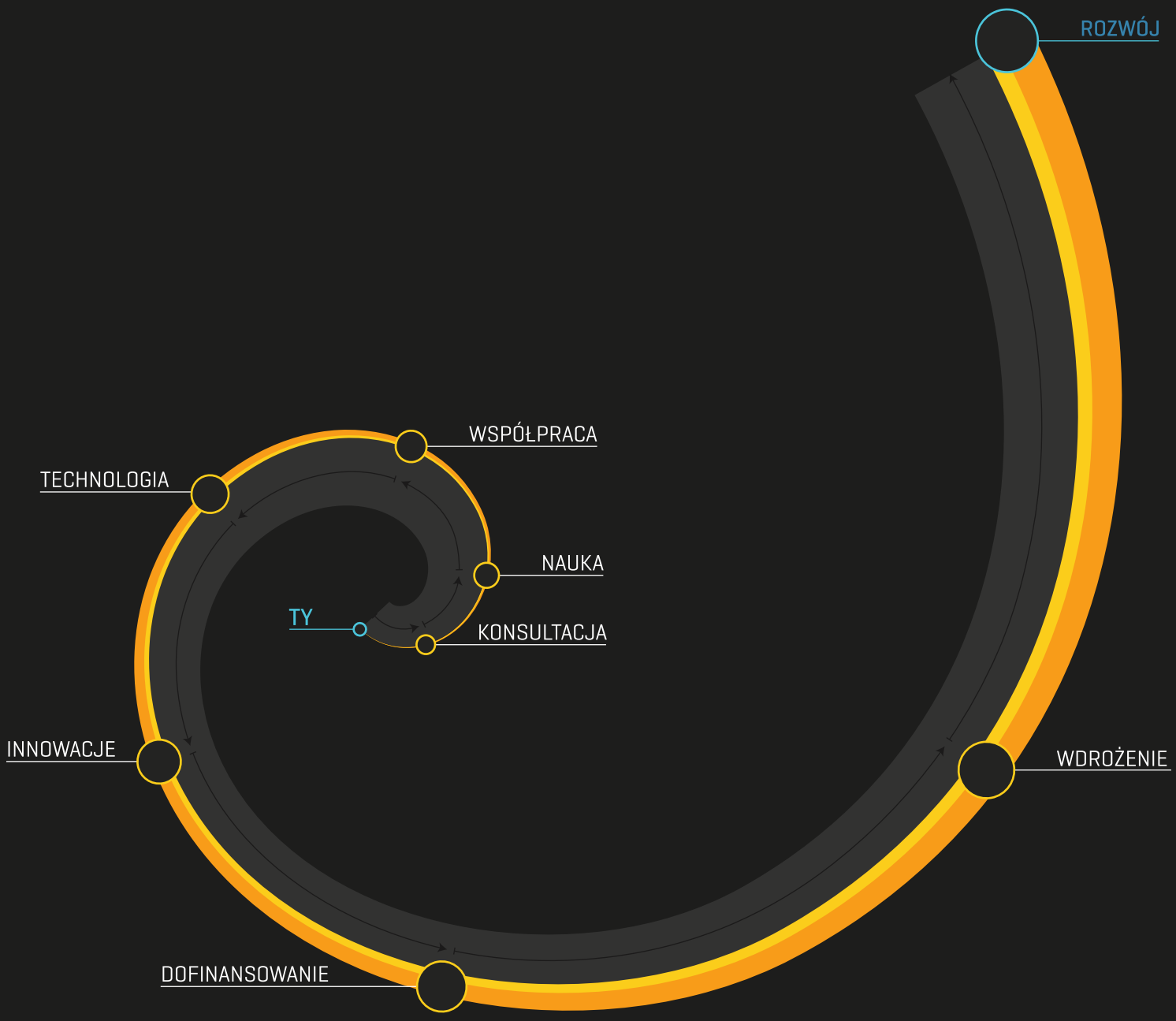
GLIWICE TECHNO PARK

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 Justyna Kurek

(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

Poglądy i tezy przedstawione w publikacji nie muszą odzwierciedlać stanowiska Parku Naukowo-Technologicznym TECHNOPARK GLIWICE Sp. z o.o., a jedynie stanowisko Autora.

Spis treści

1. Uwagi wprowadzające 3

2. Obowiązujące regulacje prawne w obszarze danych osobowych 4

3. Pojęcie danych osobowych oraz zasady i warunki przypisywania danym informacjom waloru danych osobowych 5

4. Konsekwencje uznania wskazanych informacji za dane osobowe 9

5. Obowiązki administratora danych osobowych 10

6. Zmiana sposobu wykorzystania danych 15

7. Uwagi końcowe 17

1. Uwagi wprowadzające

Przedmiotem niniejszej opinii są obowiązujące prawne i administracyjne uwarunkowania dotyczące gromadzenia i przetwarzania danych pozyskiwanych z przestrzeni publicznej oraz perspektywy zmian w tym zakresie. Ponadto, zakres analizy obejmuje możliwość dalszego udostępniania danych uzyskanych w przestrzeni publicznej w celu ich wykorzystania w ramach usług informacyjnych, w szczególności publicznych i prywatnych aplikacji mobilnych.

Niniejsza analiza odnosi się do czterech kategorie danych:

1. danych pochodzących z monitoringu miejskiego;
2. danych pochodzących z urządzeń pomiarowych wykorzystywanych w przestrzeni publicznej, takich jak informacje o natężeniu ruchu, informacje pochodzące z transportu drogowego;
3. danych o użytkownikach telefonii komórkowej pochodzących z urządzeń GPS, stacji bazowych, informacji udostępnianych przez samych użytkowników w sieci www);
4. systemów wynikających z koncepcji inteligentnego miasta, między innymi informacji pochodzących z energetycznych urządzeń pomiarowych lub rejestrów publicznych.

Pojęcie przestrzeni publicznej i zakres danych w ten sposób pozyskiwanych

Pojęcie przestrzeni publicznej zostało zdefiniowane w ustawie z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (tekst jednolity z dnia 2 czerwca 2012 r. Dz.U. z 2012 r. poz. 647 ze zm.) Zgodnie z art. 2 pkt 6 tej ustawy pojęcie obszaru przestrzeni publicznej obejmuje 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 obejmuje więc wszelkie miejsca powszechnie dostępne i nieodpłatne. Jest to przestrzeń w której może znaleźć się każda jednostka społeczna. Są to więc drogi, ulice, place miejskie oraz stale dostępne budowle i budynki. Danymi pozyskiwanymi z przestrzeni publicznej będą więc wszelkie informacje pochodzące między innymi z urządzeń pomiarowych badających natężenie ruchu, urządzeń monitoringu a także nagrania z kamer wideo-nadzoru.

Pojęcie inteligentnego miasta

Koncepcja inteligentnego miasta zakłada istnienie wielowarstwowego, terytorialnego system innowacji, który łączy wiedzę o działalności instytucji dla współpracy w zakresie edukacji i innowacji oraz cyfrowe przestrzenie komunikacji i interakcji w celu zmaksymalizowania możliwości rozwiązywania problemów miasta. Cechą charakterystyczną inteligentnego miasta jest wysoka wydajność w dziedzinie innowacji, ponieważ innowacyjność i umiejętność rozwiązywania nowych problemów to główne cechy inteligencji.[1]

W praktyce, koncepcja inteligentnego miasta może przybierać postać systemów inteligentnych sieci energetycznych, czyli współpracujących ze sobą urządzeń i systemów służących optymalizacji zużycia energii elektrycznej. Koncepcja inteligentnego miasta zakłada także powiązanie informacji pochodzących z różnych źródeł w celu optymalnego zarządzenia infrastrukturą oraz procesami. Może ona przybrać postać próby połączenia informacji pochodzących z różnych rejestrów publicznych.

Jednym z bardziej złożonych problemów związanych z koncepcją inteligentnego miasta jest prawna oraz organizacyjna ochrona danych osobowych użytkowników. Przykładowo bowiem, optymalizacja procesów zarządzania zużyciem energii elektrycznej w gospodarstwach domowych wymusza gromadzenie i przetwarzanie danych osobowych końcowych odbiorców energii. Także powiązanie i przetwarzanie w innych celach danych osobowych znajdujących się w rejestrach publicznych zakłada zmianę celu przetwarzania w stosunku do pierwotnego celu gromadzenia danych, co powoduje liczne konsekwencje prawne, w szczególności na gruncie przepisów o ochronie danych osobowych.

2. Obowiązujące regulacje prawne w obszarze danych osobowych

Dla problematyki objętej niniejszym zapytaniem szczególne znaczenie ma reżim ochrony danych osobowych. Wszelkie wskazane bowiem *w petitum* informacje z powiazaniu z innymi

1 Podobnie również definicja stworzona przez zespół Politechniki Poznańskiej http://tsiss.wordpress.com/2011/12/04/inteligentne-miasta/

informacjami, którymi dysponuje podmiot przetwarzający, z dużym prawdopodobieństwem, umożliwiały będą identyfikacje osób fizycznych. Obecnie głównych aktem prawnym regulującym zasady i warunki gromadzenia i przetwarzania danych osobowych jest 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, zwana dalej „uodo"). Przepisy obowiązującej ustawy 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 także uwagę Rzecznik Praw Obywatelskich i Generalny Inspektor Ochrony Danych Osobowych, którzy podkreślają niedopuszczalność braku ustawowej regulacji w tym zakresie. Od kilku miesięcy trwają prace nad założeniami szczególnej ustawy która odnosiła się będzie to tej tematyki. Prace te prowadzone są w resorcie spraw wewnętrznych i administracji.

Należy także wskazać, iż w Unii Europejskiej trwają ponadto prace nad uregulowaniem problematyki ochrony danych osobowych w ramach instrumentu o zasięgu horyzontalnym, obejmującym terytorium całej Unii Europejskiej – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych iswobodnym przepływem takich danych (dokument

COM (2012) 11 final) .

3. Pojęcie danych osobowych oraz zasady i warunki przypisywania danym informacjom waloru danych osobowych

Podstawowe znaczenie dla poruszanej kwestii ma kwalifikacja poszczególnych informacji z przestrzeni publicznej takich jak: obraz z kamer wideo, informacji o natężeniu ruchu, numerów rejestracyjnych, informacji o położeniu pochodzącej z nadajników GPS oraz stacji bazowych telefonii komórkowej, informacji z inteligentnych liczników energii i rejestrów publicznych jako danych osobowych.

Należy na wstępie podkreślić iż zakres informacji, które mogą być kwalifikowane jako dane osobowe jest zmienny w czasie i zależy od środków technologicznych, którymi dysponuje administrator danych a także innych posiadanych przez niego informacji. Często wskazywanym przykładem jest obraz z kamer przemysłowych. W zależności od rozdzielczości oraz dodatkowych środków takich jak książka wejść i wyjść czy funkcjonalność rozpoznawania głosu, nagranie takie będzie poddane pod reżim ochrony danych osobowych lub też takiego przymiotu mieć nie będzie.

Pojęcie danych osobowych zostało zdefiniowane w ustawie o ochronie danych osobowych. Zgodnie z art. 6 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy czym osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Pod pojęciem danych osobowych można również rozumieć poszczególne informacje o osobistych i rzeczowych stosunkach określonej lub możliwej do określenia osoby fizycznej. Z zakresu pojęcia danych osobowych wyłączone są informacje umożliwiające identyfikację innych podmiotów, niż osoby fizyczne. Ochroną tych aktów objęte są jedynie osoby fizyczne.

Dla wykładni pojęcia danych osobowych podstawowe znaczenie mają więc pojęcia „informacja" i „identyfikacja". Pojęcie informacji wyznacza przedmiot i zakres ochrony prawnej danych osobowych.[2] W prawie polskim brak jest legalnej definicji tego pojęcia. Powszechnie przyjmuje się za Grażyną Szpor, iż informacja jest niematerialnym dobrem przenaszalnym, które zmniejsza niepewność.[3] Polski ustawodawca posługuje się w ustawie o ochronie danych osobowych pojęciem „wszelkie informacje". Wskazuje on na szeroki zakres pojęcia danych osobowych. Pojęcie to obejmować będzie nie tylko znaki językowe, ale także inne okoliczności towarzyszące znakom językowym i informacje pozajęzykowe. Mogą być to zarówno informacje na papierze, jak i w pamięci systemu operacyjnego.[4]

Identyfikacja oznacza natomiast możliwość odróżnienia w grupie danej osoby od pozostałych członków grupy. Przy czym identyfikacja nie musi oznaczać wskazania tej osoby z imienia i z nazwiska. Wystarczające jest wskazanie okoliczności pozwalających na określenie tej osoby w sposób niepowtarzalny.[5] Przyjmuje się ponadto, iż dana osoba jest możliwa do zidentyfikowania, jeżeli mimo że nie została jeszcze zidentyfikowana, taka identyfikacja jest możliwa.[6] Nie można więc charakteru osobowego z góry przypisać do żadnej kategorii danych.[7] Nawet taka dana jak nazwisko tylko w pewnych sytuacjach umożliwia bezpośrednią identyfikację osoby. W przypadku popularnych

2 G. Szpor, Pojęcie informacji a zakres ochrony danych osobowych [w:] P. Fajgielski Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia, Wydawnictwo KUL Lublin 2008, str. 15.
3 G. Szpor, Pojęcie informacji..., str. 8.
4 A. Drozd, Pojęcie danych osobowych [w:] Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia, P. Fajgielskired. Wydawnictwo KUL Lublin 2008, str. 23.
5 A. Drozd, Pojęcie danych osobowych …, str. 24.
6 Opinia 4/2007 w sprawie pojęcia danych osobowych przyjęta w dniu 20 czerwca 2007 r. Grupy Roboczej ds. Danych Osobowych powołanej na mocy art. 29, str. 12.
7 Por. A. Mednis, Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej, PiP 1997, z. 6, s. 35; P. Barta, P. Litwiński, Ustawa o Ochronie Danych Osobowych, Komentarz, C.H. Beck 2009, str.88

nazwisk np. „Kowalski“, „Nowakowski“ informacja taka nie będzie wystarczająca do odróżnienia danej osoby w grupie.[8]

Dla zakwalifikowania danej informacji jako danych decydujące znaczenie ma możliwość identyfikacji osoby fizycznej, przy zachowaniu adekwatnych do sytuacji środków technicznych i organizacyjnych. Informacje nie będą uznane za dane osobowe, jeżeli takiej identyfikacji nie umożliwiają, lub jeżeli taka identyfikacja wiązałaby się z nadmiernym wysiłkiem ze strony podmiotu zobowiązanego. Warunek identyfikacji wyraźnie akcentują także projektowane przepisy Rozporządzenia Unii Europejskiej. Twórcy projektu przy kwalifikacji informacji jako danych osobowych posługują się warunkiem iż informacja taka musi umożliwiać pośrednią lub bezpośrednią identyfikację za pomocą wszelkich środków, które z rozsądnym prawdopodobieństwem mogą być użyte (art. 4 pkt. 1 projektu Com (2012) 11 fin). Dla zdefiniowania w projektowanych przepisach europejskich, zakresu obowiązku identyfikacyjnego spoczywającego na administratorze danych, istotne znaczenie ma także dyspozycja art. 10 projektu Rozporządzenia. Zgodnie z tym przepisem, jeśli dane przetwarzane przez administratora nie umożliwiają mu identyfikacji osoby fizycznej, administrator nie ma obowiązku uzyskania dodatkowych informacji w celu identyfikacji podmiotu danych wyłącznie ze względu na konieczność respektowania przepisów niniejszego rozporządzenia.

Zakwalifikowanie danych informacji jako danych osobowych uzależnione jest od czynników zewnętrznych i technologicznych możliwości identyfikacji tej osoby. Nie jest istotne aby osoba, której dane dotyczą była znana podmiotowi przetwarzającemu dane. Przepisy wymagają jedynie aby była ona określona.[9] Już samo stwierdzenie, że informacje w połączeniu z innymi danymi, którymi dysponuje administrator bądź inna osoba, umożliwiają bądź mogą umożliwić w przyszłości identyfikację, jest wystarczające dla przypisania danym waloru umożliwiającego identyfikację, a tym samym uznania ich za daną osobową.[10]

Praktyczne problemy interpretacyjne w określeniu, jakie informacje będą stanowiły dane osobowe, potwierdza praktyka administracyjna. W literaturze przedmiotu podkreśla się ponadto, iż danymi osobowymi są wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby, nie tylko te informacje, które same służą identyfikacji. Sama bowiem pojedyncza informacja w zasadzie prawie nigdy nie pozwala na określenie tożsamości osoby, której dotyczy.[11] W zależności od technicznych i technologicznych możliwości identyfikacyjnych, danymi

8 Podobnie G. Sibiga, Postępowanie w sprawach ochrony danych osobowych, Wydawniczy ABC Warszawa 2003, str. 35.
9W. Däubler, J.P. Hjort, M. Schubert M. Wolmerath, Arbeitsrecht, wydanie 2, C.H. Beck 2010, Komentarz do §
10Podobnie X. Konarski, Serwisyspołecznościowe – nowyparadygmatochronydanychosobowych? [w:] OchronaDanychOsobowych. Skutecznośćregulacji, G. Szpor, red. Municipium 2009, str. 180 i następne.
11 J. Barta, P. Fajgielski, R. Markiewicz, Ochrona Danych Osobowych. Komentarz, Zakamycze 2004, str. 369.

osobowymi mogą być między innymi zdjęcia, filmy, dane biometryczne, cechy twarzy czy linie papilarne.

Warto w tym miejscu wskazać na przykłady przywoływane przez Generalnego Inspektora Ochrony Danych Osobowych. W jednym z wywiadów dr Wojciech Wiewiórowski wskazał, iż numery rejestracyjne samochodu same w sobie nie stanowią danych osobowych. Jeżeli jednak dane o numerach samochodów zbiera pracodawca w związku z organizacją firmowego parkingu samochodowego, zabrane dane o numerach rejestracyjnych wraz z już posiadanymi informacjami, umożliwią mu identyfikację osób fizycznych. Także w przypadku miejskich parkometrów, które dodatkowo wymagają podania numerów rejestracyjnych, zachodzi duże prawdopodobieństwo iż dane te w powiązaniu z informacjami z centralnej ewidencji pojazdów, którymi dysponuje urząd, będą umożliwiały identyfikację osób fizycznych.[12]

W literaturze przedmiotu zwraca się również uwagę na fakt, iż za dane osobowe może zostać uznana każda informacja, niezależnie od sposobu i formy jej wyrażenia, bez względu na to czy jest ona powszechnie zrozumiała. Charakter prawny bowiem każdej takiej informacji powinien być oceniany dla każdego jej dysponenta w sposób indywidulany.[13] Przykładowo, numer telefonu może być uznany za daną osobową w związku z tym, iż umożliwia operatorowi identyfikację abonenta, podobnie numer IP komputera a nawet jego MAC adres, będzie dla dostawcy usług pocztowych wystarczający dla zidentyfikowania użytkownika. O tym, na ile poszczególne czynniki identyfikujące pozwalają na ostateczne ustalenie tożsamości, decydują szczególne okoliczności. Zazwyczaj jest to niepowtarzalna kombinacja czynników. W przypadku gdy dostępne czynniki identyfikacyjne nie pozwalają *prima facie* na wyodrębnienie konkretnej osoby, osoba ta może pomimo to być możliwa do zidentyfikowania, ponieważ informacje te w połączeniu z innymi danymi (którymi dysponuje administrator danych) pozwalają na odróżnienie tej osoby od innych. Na zakres znaczeniowy pojęcia danych osobowych istotny wpływ ma więc rozwój technik i technologii informatycznych. Wpływają one bowiem w bezpośredni sposób na możliwości identyfikacji, które zmieniają się wprost z rozwojem technik teleinformatycznych.[14] W niemieckiej doktrynie prawnej przyjmuje się, iż dla określenia, które informacje pozwalają na identyfikację użytkownika, należy zastosować tzw. kryterium proporcjonalności. Zgodnie z tą teorią, dane przestają mieć charakter osobowy, gdy informacje nie mogą w ogóle lub jedynie przy zastosowaniu nieproporcjonalnie dużej ilości czasu,

12http://giodo.gov.pl/1520001/id_art/5676/j/pl
13 G. Sibiga, Postępowanie w sprawach ochrony...str. 33.
14 Podobnie, I. Spiecker gen. Döhmann, Prywatny pomiar „świata" jako problem prawa ochrony danych. O obchodzeniu się z informacją przestrzenną na przykładzie Google StreetView [w:] Internet Ochrona wolności, własności i bezpieczeństwa, G. Szpor, C.H. Beck, Warszawa, 2011, str. 77

kosztów lub działań zostać przypisane zidentyfikowanej lub możliwej do zidentyfikowania osobie.[15] O nieproporcjonalności nakładu pracy muszą decydować względy obiektywne a nie indywidualny przypadek[16]. W literaturze zwraca się uwagę na warunek braku nadmiernego wysiłku dla określenia tożsamości podmiotu.[17]

Reasumując, odnosząc się do poszczególnych kategorii informacji które wymienione zostały w przedmiotowym zamówieniu (wizerunek pochodzący z zapisu monitoringu, informacje o natężeniu ruchu, inne informacje pochodzące z transportu, dane geolokacyjne o użytkownikach pochodzące z nadajników GPS i stacji bazowych telefonii komórkowej), gromadzenie i przetwarzanie takich informacji będzie podlegało reżimowi ochrony danych osobowych pod warunkiem, iż podmiot zarządzający tymi procesami (administrator danych) będzie w stanie na podstawie tych informacji lub też na podstawie tych informacji w powiązaniu z innymi posiadanymi przez siebie danymi, bez podejmowania nadmiernych wysiłków lub pozyskiwania dodatkowych baz danych, dokonać identyfikacji osób fizycznych.

Nie można więc z góry wykluczyć uznania którejkolwiek z podanych kategorii danych za dane osobowe.

4. Konsekwencje uznania wskazanych informacji za dane osobowe

Konsekwencją uznania, iż wskazane informacje stanowią dane osobowe jest nałożenie na podmiot będący w ich posiadaniu i decydujący o sposobie i zakresie ich przetwarzania obowiązków wynikających z przepisów o ochronie danych osobowych. Obowiązki odnoszą się w szczególności do danych osobowych o charakterze tekstowym.

W praktyce, poważne problemy powstają w związku z wypełnianiem obowiązków wynikających z reżimu ochrony danych osobowych w stosunku do danych obrazowych, w tym danych audiowizualnych. Do czasu uchwalenia stosownych przepisów prawnych odnoszących się do tej

15 Między innymi: P. Gola, R. Schomerus, Bundesdatenschutzgesetz Komentarz, C.H Beck, Wydanie 10, 2010, komentarz do § 3 BDSG pkt. 10,; D. Wolfgang , J. P Hjort, M. Schubert, M. Wolmerath, Arbeitsrecht Komentarz, C.H. Beck, Wydanie 2, 2010 r.komenatarz do § 3BDSG pkt. 2. W polskiej literaturze - M. Jagielski, Prawo do ochrony danych osobowych. Standardy europejskie, WoltersKluwer 2010, str. 46.

16 P. Gola, R. Schomerus, BundesdatenschutzgesetzKommentar, C.H. Beck , 10, komenarz do § 3 BDSG. Wydanie, 2010, pkt. 44.

17 Por. m.in. A. Drozd, Pojęcie danych osobowych…str. 26, P. Fajgielski, Kontrola i audyt przetwarzania danych osobowych, Presscom 2010, str. 26.

kwestii, należy w stosunku do takich danych stosować zasady wynikające z przepisów ustawy o ochronie danych osobowych przy uwzględnieniu odmienności wynikających z charakteru danych audiowizualnych. Definiując zasady postępowania i zabezpieczania danych audiowizualnych należy także uwzględnić doświadczenia wynikające z regulacji prawnych obowiązujących w innych państwach Unii Europejskiej i rekomendacje odnoszące się do polskiej ustawy przygotowane przez Generalnego Inspektora Ochrony Danych Osobowych.[18]

Także w przypadku koncepcji inteligentnego miasta, szczególne regulacje odnoszące się do przetwarzania danych osobowych powinny z uwagi na specyfikę tej problematyki zostać uregulowane w przepisach sektorowych, na przykład w przepisach o efektywności energetycznej oraz w prawie energetycznym.

Należy także podkreślić, iż obowiązki w zakresie gromadzenia, przetwarzania i wypełniania obowiązków informacyjnych zaistnieją jedynie w przypadku, gdy informacje same bądź w powiązaniu z innymi informacjami umożliwią podmiotowi zarządzającemu identyfikację osób fizycznych. Ani przepisy ustawy o ochronie danych osobowych ani projektowane przepisy Unii Europejskiej nie nakładają obowiązków związanych z koniecznością podjęcia szczególnych dodatkowych działań w celu identyfikacji podmiotów danych osobowych. W szczególności obowiązujące regulacje nie nakładają szczególnych obowiązków w postaci konieczności zakupu dodatkowych baz danych lub wejścia w porozumienie z innymi podmiotami w celu powiązania danych znajdujących się w różnych systemach w celu identyfikacji podmiotów danych osobowych.

5. Obowiązki administratora danych osobowych

Obowiązujące regulacje prawne nakładają na administratora danych szereg obowiązków związanych z przetwarzaniem i gromadzeniem danych osobowych. Istotną kwestią będzie odpowiednie zabezpieczenie dostępu do danych przed atakiem z zewnątrz. Drugi, bardzo istotny obowiązek, to określenie kręgu podmiotów uprawnionych do dostępu do tego typu informacji. Ponadto, administrator danych powinien uregulować kwestie potencjalnej anonimizacji danych.

18 Pismo Generalnego Inspektora Danych Osobowych z dnia 24 sierpnia 2011 r. do Ministra Spraw Wewnętrznych i Administracji nr GI-035-12/11/40490 dostępne pod adresem http://www.giodo.gov.pl/1520106/id_art/4278/j/pl/

Należy bowiem określić na ile i do którego momentu konieczne jest przechowywanie danych w systemie, w taki sposób aby dane umożliwiały identyfikację osób fizycznych, a do jakich celów wystarczające jest operowanie na danych zanonimizowanych. Szczegółowy opis wszystkich obowiązków związanych z administrowaniem danymi osobowymi wykracza poza zakres niniejszej opinii. Poniżej przedstawione zostaną informacje związane z pozyskiwaniem danych osobowych z przestrzeni publicznej i koncepcji inteligentnego miasta, w szczególności zasady które powinny odnosić się do przetwarzania i gromadzenia danych audio-wizualnych.

a. Podstawa prawa przetwarzania danych osobowych

W każdym przypadku przetwarzania danych osobowych konieczne jest istnienie wyraźnej podstawy prawnej. Zgodnie z obowiązującymi przepisami (art. 23 uodo) podstawę tą mogą stanowić: (1) zgoda osoby, której dane dotyczą przy czym przepisy prawa uniemożliwiają obecnie wyrażania zgody w sposób dorozumiały (2) przepis prawa (3) przetwarzanie danych osobowych prowadzi do zawarcia umowy, której stroną jest podmiot danych (4) prawnie uregulowane zadanie realizowanych dla dobra publicznego (5) prawnie usprawiedliwiony cel administratora danych.

W przypadku przetwarzania wskazanych w *petitum* opinii danych osobowych w zasadzie wykluczone jest uznanie zgody jako przesłanki przetwarzania danych osobowych. Należy wskazać, iż przepisy prawa wyraźnie wskazują iż zgoda podmiotu danych musi być wyrażona w sposób wyraźny rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Musi ponadto istnieć w każdym czasie możliwość jej odwołania.

W odniesieniu do danych obrazowych pochodzących z monitoringu, w braku odmiennych regulacji, które mogłyby znajdować się między innymi w ustawie o monitoringu, nie można uznać za wystarczające pozostawanie przez podmiot danych w strefie objętej monitoringiem jako zgody utrwalanie i przetwarzanie danych o wizerunku. Także włączenie nadajnika bluetooth czy GPS nie należy uznawać za zgodę na przetwarzanie danych osobowych. W przypadku przetwarzania danych pochodzących ze strefy publicznej, wykluczona jest także trzecia podstawa – obowiązki związane z finalizacją umowy.

Podstawą przetwarzania danych osobowych pochodzących ze strefy publicznej powinien być szczególny przepis prawny. W odniesieniu do danych wizualnych objętych monitoringiem ustawa

powinna określać miejsce i okoliczności w których dopuszczalne powinno być stosowanie monitoringu; prawa i obowiązki podmiotu stosującego monitoring, prawa osób objętych monitoringiem. Zasady odnoszące się do przetwarzania tych danych powinny zapewniać równowagę między uzasadnionymi potrzebami podmiotów stosujących monitoring i prawem do prywatności osób objętych nadzorem.

Do czasu uregulowania tej kwestii podstawową prawną przetwarzania danych pochodzących z przestrzeni publicznej może być w szczególności przepis art. 23 ust. 1 pkt. 4 uodo, który legalizuje przetwarzanie danych osobowych jeżeli jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Zadaniem takim będzie z całą pewnością zapewnienie porządku, kwestie bezpieczeństwa, badanie natężenia ruchu w celu synchronizacji świateł.

b. Zasady przetwarzania danych pochodzących z przestrzeni publicznej do czasu uchwalenia stosownych regulacji prawnych

Przetwarzanie danych osobowych pozyskanych z przestrzeni publicznej powinno odbywać się z poszanowaniem prywatności osób, których dane dotyczą i w przy wykorzystaniu adekwatnych środków organizacyjnych i technologicznych w stosunku do celu, któremu służyć ma pozyskiwanie oraz przetwarzanie danych. W opinii nr 4/2004 Grupy roboczej artykułu 29 – europejskiego niezależnego organu ds. ochrony danych osobowych i prywatności zwrócono uwagę m.in. na konieczność respektowania zasady proporcjonalności (dane muszą być adekwatne i istotne dla celów przetwarzania). Systemy wideo nadzoru powinny być stosowane jedynie w przypadku, gdy nie da się osiągnąć celu przy pomocy innych środków prewencyjnych o charakterze fizycznym i/lub logistycznym nie jest wystarczające.

Na konieczność stosowania środków adekwatnych do zamierzonego celu, zwraca również uwagę Generalny Inspektor Ochrony Danych Osobowych, które zalega daleko idącą ostrożność w odniesieniu do pozyskiwanych danych. Rodzaj stosowanych środków powinny być uzależnione od celu któremu mają służyć. Jeżeli celem ma być kontrola natężenia ruchu i synchronizacji sygnalizacji świetlnej, być może nie jest konieczne stosowanie kamer których rozdzielczość umożliwia identyfikację osób prowadzących pojazdy lub zapis numerów rejestracyjnych.

c. zasady przetwarzania danych z inteligentnych sieci energetycznych, w tym inteligentnych liczników

Jednym z bardziej sensytywnych problemów jest kwestia ochrony danych osobowych w przypadku stosowania inteligentnych liczników energetycznych. Należy bowiem zwrócić uwagę, iż tego typu urządzenia gromadzą i przetwarzają bardzo szczegółowe informacje umożliwiające tworzenie profili zachowań użytkowników końcowych. Na podstawie informacji o zużyciu energii można między innymi określić czas przebywania w domu oraz inne dane na temat preferencji i przyzwyczajeń domowników.

Dlatego też konieczne wydaje się uregulowane kwestii ochrony danych osobowych, dostępu do informacji, zasad gromadzenia i administrowania tymi danymi w przepisach sektorowych. Do czasu stworzenia szczególnych regulacji prawnych które powinny znajdować się w przepisach prawa energetycznego, konieczne jest uwzględnienie zasad proporcjonalności i adekwatności stosowanych środków. Należy także rozważyć, czy cel związany z optymalizacją zarządzania nie będzie mógł zostać osiągnięty przy wykorzystaniu danych zanonimizowanych. Należy także rekomendować uwzględnienie kwestii ochrony danych osobowych i ochrony prywatności na etapie projektowania systemu. Podstawą przetwarzania danych może być także w tym przypadku zgoda podmiotu, o ile stosowane zapisy znalazłyby się w umowach na dostawę energii.

d. przetwarzanie danych z rejestrów publicznych

Koncepcja inteligentnego miasta zakłada także ponowne wykorzystywanie danych pochodzących z publicznych rejestrów. Przetwarzanie przez organy publiczne, prowadzące rejestr przedsiębiorców, danych osobowych ma swoją podstawę w przepisach ustawy o ochronie danych osobowych. Zgodnie z art. 23 ust. 1 pkt. 4, przetwarzanie danych osobowych jest dopuszczalne, jeżeli jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Celem takim jest prowadzenie przez podmioty sektora publicznego rejestrów publicznych na podstawie szczególnych regulacji prawnych na przykład ustawy o Krajowym Rejestrze Sądowym. Ustawowa podstawa prowadzenia rejestru, wyłącza konieczność uzyskania odrębnej zgody na przetwarzanie danych osobowych od podmiotu, którego dane dotyczą.

Przepis art. 23 uodo nie stanowi natomiast podstawy do przetwarzania danych osobowych bez uzyskania zgody osoby, której danych dotyczy przez inne podmioty. W szczególności przez podmioty wykorzystujące dane zawarte w rejestrze publicznym do tworzenia innych aplikacji i własnych baz danych. O ile jednak dane takie będą stanowiły informację publiczną, podstawę przetwarzania danych będzie mogła stanowić ustawa o dostępie do informacji publicznej, w szczególności regulacje odnoszące się do ponownego wykorzystywania takiej informacji.

W przypadku ponownego wykorzystywania informacji pochodzących z rejestrów publicznych, ma miejsce typowy przypadek pozyskania danych od innego podmiotu, niż podmiot, którego dane dotyczą. W takiej sytuacji istnieje konieczność pozyskania zgody, o ile nic innego nie wynika z przepisów szczególnych, bądź wykazania innej przesłanki legalizującej przetwarzanie danych osobowych. Powstaje także konieczność wypełnienia obowiązków informacyjnych względem podmiotów danych. Na gruncie obowiązujących obecnie brak jest podstaw prawnych do zwolnienia administratora danych z obowiązku wypełnienia obowiązków informacyjnych względem podmiotów danych osobowych. Przesłanką taką nie są ani koszty, ani trudności organizacyjne.

Potwierdza to również wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 2 czerwca 2011 r. w sprawie II SA/Wa 720/11. W orzeczeniu tym sąd odnosił się do problemu trudności związanych z wykonaniem obowiązku informacyjnego w stosunku do podmiotów danych znajdujących się w bazie Krajowego Rejestru Sądowego. W swoim wyroku w sprawie II SA/Wa 720/11 WSA na zarzut o niewykonalności uzyskania przez podmiot przetwarzający dane osobowe pochodzące z rejestru przedsiębiorców zgody osób fizycznych których dane widnieją w rejestrze odpowiedział, iż trudności organizacyjne nie mogą stanowić podstawy do niewypełniania przez podmiot decyzji GIODO. Sąd zaznaczył iż, „*wbrew zarzutom skargi należy uznać, że zaskarżona decyzja jest wykonalna. Skarżący budując własną bazę danych osobowych posiada dane, które zezwalają mu na wykonanie obowiązku informacyjnego wobec osób, które się w tej bazie znajdują są tam bowiem imiona i nazwiska osób oraz numery PESEL osób fizycznych, a także siedziba podmiotów gospodarczych, w których pełnią one funkcje. Nadto skarżąca może skorzystać z usług Centralnego Biura Adresowego. Fakt, że jest to duże przedsięwzięcie organizacyjne i dotyczy znacznej liczby osób nie oznacza, że jest ono niewykonalne. Skarżący budując dużą bazę danych musiał się liczyć, że w stosunku do takiej liczby osób będzie miał określone przepisami ustawy o ochronie danych osobowych obowiązki”.*

Reasumując, na gruncie obowiązujących przepisów brak jest podstaw do zwolnienia administratora danych z obowiązku informacyjnego wynikającego z przepisów ustawy o ochronie danych osobowych, co stanowi istotne utrudnienie w tworzeniu usług opartych

na informacji sektora publicznego pochodzących z rejestrów publicznych. Zmianę w tym zakresie mogą wprowadzić przepisy Rozporządzenia Unii Europejskiej. Zgodnie z art. 10 projektu jeśli dane przetwarzane przez administratora nie umożliwiają mu identyfikacji osoby fizycznej, administrator nie ma obowiązku uzyskania dodatkowych informacji w celu identyfikacji podmiotu danych wyłącznie ze względu na konieczność respektowania przepisu niniejszego rozporządzenia. Nie będzie miał on więc obowiązku pozyskiwania dodatkowych informacji w celu wypełnienia obowiązków informacyjnych.

6. Zmiana sposobu wykorzystania danych

Odrębnym zagadnieniem jest natomiast możliwość wykorzystania danych w innym celu niż ich pierwotny cel pozyskania. Innym celem może być bowiem tworzenie właśnie wskazanych w *petitum* opinii aplikacji mobilnych. Należy wskazać, iż odmiennie sytuacji wygląda w przypadku organów publicznych a innej w przypadku podmiotów prywatnych.

Zakres działania organów publicznych wyznacza zasada legalizmu wynikająca z art. 7 Konstytucji. *Zgodnie z tym przepisem organy władzy publicznej działają na podstawie i w granicach prawa. Norma ta zawiera domniemywanie kompetencji takiego organu i tym samym nakazuje, by wszelkie działania organu władzy publicznej były oparte na wyraźnie określonej normie kompetencyjnej*. Oznacza to, iż organy państwa nie mogą podejmować działań, które wyraźnie nie wynikałyby z przepisów prawa.

Odmiennie sytuacja wygląda w przypadku podmiotów prywatnych. W przypadku mogą one podejmować każdą aktywność, która nie jest prawnie zakazana. W przypadku podmiotów sektora prywatnego możliwe jest tworzenie nowych aplikacji przy wykorzystaniu posiadanych danych i dokonanie zmiany celu przetwarzania danych. Prawną podstawą tworzenia takich aplikacji może być prawo ponownego wykorzystywania informacji sektora publicznego. Zdefiniowane w art. 23a ustawy o dostępie do informacji publicznej nowe prawo do ponownego wykorzystania informacji publicznej stanowi szczególne uprawnienie wynikające z prawa dostępu do informacji publicznej. Odnosi się ono do wykorzystywania informacji publicznej w innym celu niż jej pierwotny cel wytworzenia. Prawo to

przysługuje każdemu, z zastrzeżeniem wyjątków odnoszących się do ochrony informacji niejawnej i ustawowo chronionych tajemnic, takich jak: interes państwa, prywatność osób fizycznych lub tajemnica przedsiębiorstwa.

W założeniu, ani dyrektywa reuse ani polskie przepisy nie nakładają na organy publiczne będące w posiadaniu informacji, która nadaje się do ponownego wykorzystania żadnych szczególnych obowiązków w zakresie przekształcania, przetworzenia i przygotowania informacji celem ułatwienia procesów jej ponownego wykorzystania. Informacja powinna być udostępniania w formie, w której jest w posiadaniu organów publicznych. Tylko w wyjątkowych sytuacjach powinna być ona poddana procesom przetwarzania. W dyrektywie wyraźnie wskazane jest, iż organy sektora publicznego powinny przychylać się wnioskom o dostarczenie wyciągów z istniejących dokumentów wtedy, kiedy udzielenie takiej zgody wymaga jedynie prostej czynności. Organy sektora publicznego nie powinny być jednakże zobowiązane do dostarczenia wyciągu z dokumentu, jeśli wymaga to nieproporcjonalnie dużego wysiłku.[19] Te same zasady powinny odnosić się do podmiotów krajowych działających na podstawie przepisów ustawy o dostępie do informacji publicznej.

Przepisy o ponownym wykorzystaniu informacji publicznej uprawniają także podmioty wytwarzające i udostępniające informację publiczną do określenia trybu i zasad udostępniania informacji publicznej. W przypadku udostępniania przez zobowiązane pomioty informacji publicznej w celu jest ponownego wykorzystania zasadą jest brak ograniczeń, co do warunków wykorzystywania i bezpłatność. Zgodnie z art. 23b udip podmioty udostępniające są natomiast uprawnione do określenia warunków ponownego wykorzystywania informacji publicznej, w szczególności dotyczących: 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.

Reasumując, na gruncie obowiązujących przepisów podstawą pozyskiwania danych z przestrzeni publicznej mogą być przepisy o dostępie do informacji publicznej, o ile dane te znajdują się w dyspozycji podmiotów sektora publicznego i informacje te nie stanowią tajemnicy prawnie chronionej, na podstawie odrębnych przepisów prawnych. O ile jednak dane nie zostaną zanonimizowane, powstanie obowiązek informacyjnych względem podmiotów danych.

19Tiret 13 zd. 2 dyrektywy reuse

7. Uwagi końcowe

W przypadku większości danych pochodzących z przestrzeni publicznej istnieje duże prawdopodobieństwo uznania tych danych za dane osobowe. Definitywne przesądzenie jakie dane będą stanowiły dane osobowe wymaga szczegółowej analizy wszystkich informacji będących w posiadaniu podmiotu zarządzającego daną informacją. W związku z powyższym przy pozyskiwaniu i gromadzeniu danych należy uwzględnić reżim ochrony danych osobowych.

Podstawą udostępniania i przetwarzania danych w celach innych niż pierwotny cel ich pozyskiwania mogą być przepisy o ponownym wykorzystywaniu informacji sektora publicznego znajdujące się w ustawie o dostępie do informacji publicznej.

TECHNO PARK GLIWICE

SO RIS Sieć Obserwatoriów ICT

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

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI

Śląskie. Pozytywna energia

Regionalna Strategia Innowacji

Raport współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społeczne