



GIODO

Generalny Inspektor
Ochrony Danych Osobowych

INFORMACJA

Generalnego Inspektora Ochrony Danych
Osobowych o przetwarzaniu i dostępie do
danych geolokalizacyjnych

Lipiec 2017



20-LECIE PRAWA DO OCHRONY
DANYCH OSOBOWYCH **W POLSCE**

1. Definicja lokalizacji

Geolokalizacja polega na ustaleniu informacji o położeniu geograficznym, w którym znajduje się dane urządzenie. Wykorzystuje się w tym celu różne infrastruktury techniczne i informacje zawarte w bazach danych różnych podmiotów prywatnych i publicznych. W Dyrektywie 2002/58/WE o prywatności i łączności elektronicznej „dane lokalizacyjne” zdefiniowano jako wszelkie dane przetwarzane w sieci łączności elektronicznej wskazujące położenie geograficzne urządzenia końcowego wykorzystywanego przez użytkownika publicznie dostępnych usług łączności elektronicznej (smartfon, tablet, laptop itp.).

1.1. Pierwotne źródła danych geolokalizacyjnych

Na przestrzeni wieków dane geolokalizacyjne określano posługując się znanymi punktami odniesienia, dziennikiem podróży, gdzie zapisywano szybkość i kierunek poruszania się, kompasem, położeniem kątowym ciał niebieskich nad horyzontem oraz mapami. Na początku XX wieku zaczęto wykorzystywać fale radiowe, budując radiolatarnie, które służyły do określania położenia okrętów i samolotów. Obecnie geolokalizacja utożsamiana jest głównie z ogólnosiwiatowym systemem GPS (alternatywę stanowią inne systemy nawigacji satelitarnej: europejski GALILEO, rosyjski GLONASS czy chiński BEIDOU), jak również lokalnie rozmieszczonymi stacjami bazowymi telefonii komórkowej czy punktami bezprzewodowego dostępu do Internetu (Wi-Fi). Ponadto na obszarach zamkniętych do lokalizacji mogą być wykorzystywane inne narzędzia takie jak nadajniki sygnałów Bluetooth, kamery monitoringu i różnego rodzaju czujniki.

1.2. Wtórne źródła danych geolokalizacyjnych

Źródłem danych geolokalizacyjnych mogą być ponadto informacje zapisane w różnego rodzaju rejestrach, np. publiczne rejestry IP komputerów czy plikach, np. pliki zdjęć wykonanych urządzeniem z wbudowaną lokalizacją GPS. Dane geolokalizacyjne mogą być także odczytywane z map udostępnianych przez różnego rodzaju geoportale, jak np. geoportal.gov.pl czy mapy.google.pl.

Połączenie i przetwarzanie tych dwóch źródeł danych (pierwotnych i wtórnych) następuje w urządzeniach mobilnych, takich jak smartfony czy tablety, które wyposażone zostały jednocześnie w odbiorniki sygnałów GPS, telefonii komórkowej GPRS, Wi-Fi, Bluetooth oraz aplikacje typu Google Maps, Facebook i inne. Aplikacje te mogą nie tylko dostarczać

informacje o położeniu geolokalizacyjnym określonego urządzenia w danej chwili, ale również odczytywać informacje o lokalizacji innych osób z którymi się kontaktujemy za pośrednictwem telefonu i zainstalowanych w nim różnych aplikacji.

2. Metody ustalania lokalizacji

W ciągu ostatnich lat nastąpił znaczny rozwój technologii lokalizacji bezprzewodowej. Stawia się przed nią również coraz większe wymagania w zakresie wiarygodności, dokładności i szybkości dostarczania. Stąd w wielu aspektach życia codziennego, m.in. w takich jak: transport, ratownictwo, zarządzanie dostawami oraz wielu innych, technologia lokalizacji odgrywa coraz bardziej znaczącą rolę.

Do ustalania lokalizacji dowolnego urządzenia końcowego w przestrzeni otwartej w skali makro wykorzystywane są sygnały radiowe generowane przez różnego rodzaju nadajniki infrastruktury geolokalizacyjnej o ustalonym położeniu, takie jak satelity systemów nawigacji satelitarnej, stacje bazowe telefonii komórkowej czy punkty dostępowe sieci Wi-Fi, tzw. hotspoty oraz zainstalowane w lokalizowanych urządzeniach końcowych aplikacje.

W przypadku usług lokalizacyjnych w skali mikro, odnoszących się do lokalizacji danego urządzenia końcowego wewnątrz budynku, z uwagi na trudności odbioru sygnału z satelitów GPS, rozwijane są inne technologie lokalizujące. Zaliczyć do nich można bezprzewodowe urządzenia dostępowe do sieci typu Wi-Fi czy różnego rodzaju inne nadajniki sygnałów radiowych, które są instalowane w danym budynku, takie jak nadajniki Bluetooth emitujące informacje o najbliższym jego otoczeniu (Beacon-y) czy czytniki i transpondery RFID, omówione szerzej w rozdziale 2.2.

Cała ta infrastruktura pozwala ustalić mniej bądź bardziej precyzyjnie lokalizację geograficzną urządzenia końcowego – a w konsekwencji osoby fizycznej, której to urządzenie towarzyszy lub obiektów, np. samochodów, w których są takie urządzenia zainstalowane. Wyjątkiem są tu telefony stacjonarne, których dokładny adres lokalizacyjny ustala się na podstawie danych, które posiada operator usługi telekomunikacyjnej, do którego sieci telefon ten jest podłączony.

2.1. Technologie lokalizacji zewnętrznej

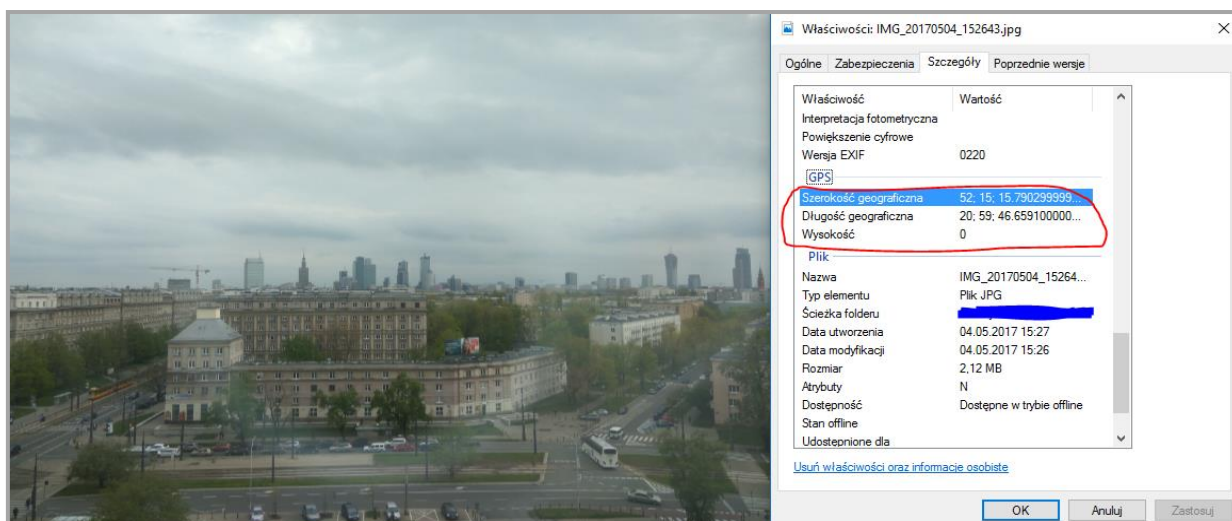
W przestrzeni otwartej, gdzie nie ma naturalnych przeszkód w postaci ukształtowania terenu (góry) czy wysokich zabudowań dla emisji sygnałów radiowych pochodzących z satelitów GPS czy stacji bazowych telefonii komórkowej, wykorzystuje się właśnie sygnały emitowane przez

te urządzenia. Ponadto w niektórych obszarach dodatkowo mogą być używane stacje dostępowe sieci Wi-Fi, których emitowane sygnały, pomimo barier jakimi są ściany pomieszczeń, wydostają się na zewnątrz i mogą mieć zasięg nawet do 400 m.

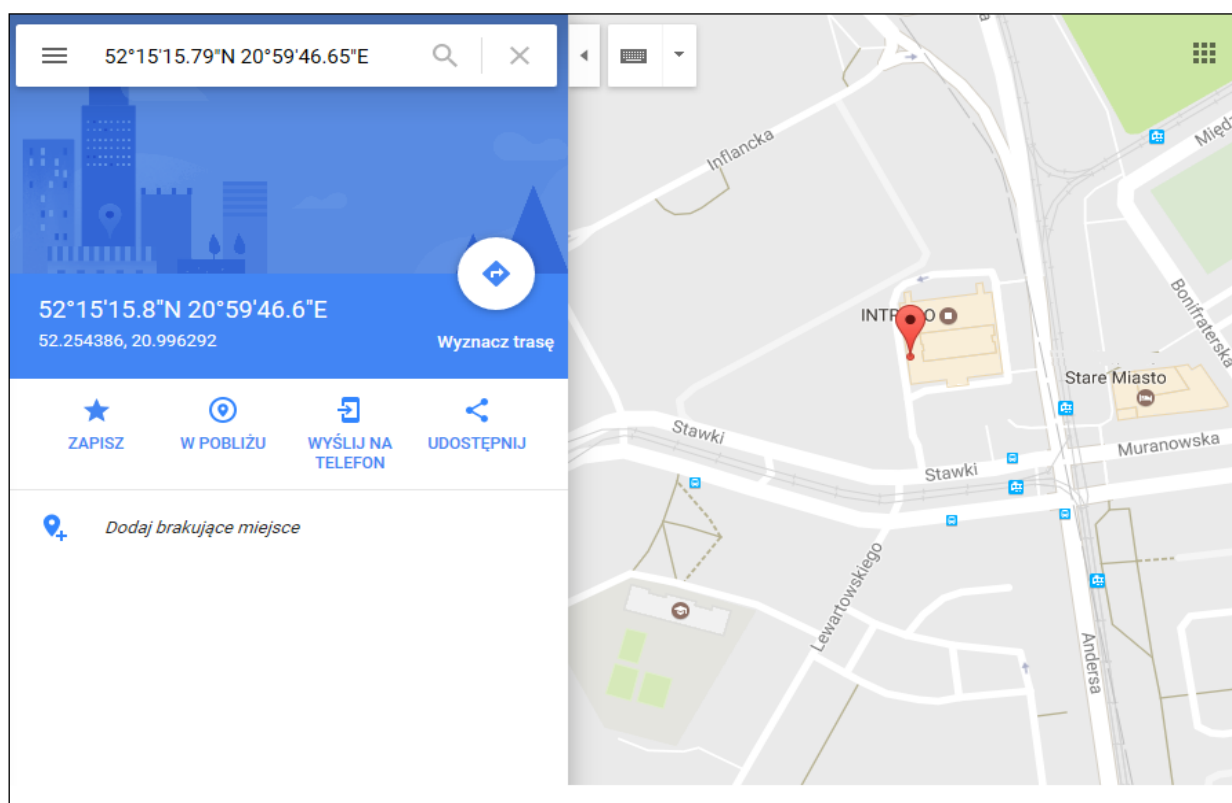
- **Satelite GPS.** Technologia nawigacji satelitarnej GPS do wyznaczenia pozycji geograficznej i czasu wykorzystuje jednocześnie sygnały z co najmniej 4 z 31 satelitów tego systemu dzięki czemu dokładność ustalenia pozycji waha się od 4 do 15 metrów. Informacje o sygnale GPS przekazywane są tylko w jedną stronę, a podmioty zarządzające satelitami nie mają możliwości śledzenia urządzeń, które odebrały sygnał z satelity.

Technologia ta jest w praktyce wykorzystywana do nawigacji lotniczej, samochodowej oraz przez wiele aplikacji mobilnych, które zainstalowane w smartfonach ułatwiają poruszanie się w przestrzeni, a także umożliwiają optymalizację działań, przykładowo znalezienie najkrótszej lub najszybszej drogi do określonego celu (np. aplikacja „Jak dojadę”, korzystająca z danych publicznych). Ponadto technologia nawigacji GPS wykorzystywana jest w wielu urządzeniach typu IoT¹ (Internet Rzeczy), takich jak opaski fitness, inteligentne zegarki, itp. Nawigacja GPS wykorzystywana jest również w cyfrowych aparatach fotograficznych, które do zapisywanego zdjęcia dodają informację o lokalizacji geograficznej aparatu. Dzięki temu, niektóre usługi społecznościowe (np. Facebook, Instagram, Flickr, Twitter) przy wgrywaniu fotografii automatycznie zapisują ich dane lokalizacyjne. Przykładową fotografię z danymi geolokalizacyjnymi pokazano na rys. 1. Na rys. 2 przedstawiono miejsce na mapie, z którego ją wykonano.

¹ Pojęcie IoT (ang. Internet of Things) odnosi się do urządzeń, które poprzez sieć może komunikować się z innymi urządzeniami, w podjęcia określonych działań.



Rys. 1: Zdjęcie i jego metadane wykonane smartfonem z włączoną lokalizacją.



Rys. 2: Wizualizacja na mapie miejsca, z którego wykonano zdjęcie pokazane na rys. 1.

- **System GSM.** Technologia ta wykorzystuje stacje bazowe telefonii komórkowej GSM, które obsługują dany wycinek obszaru geograficznego, by uzyskać łączność głosową bądź internetową. Bazuje ona na pomiarze siły sygnałów odbieranych ze stacji bazowych przez lokalizowane urządzenie, np. telefon, tablet czy laptop. Żeby lokalizacja była w miarę

dokładna, lokalizowane urządzenie musi znajdować się w zasięgu przynajmniej 3 stacji bazowych, co pozwoli na zastosowanie metody triangulacji do wyznaczenia dokładnego położenia urządzenia. Każda stacja bazowa posiada swój unikalny numer identyfikacyjny i określoną lokalizację dzięki czemu możliwe jest wyznaczenie lokalizacji urządzeń znajdujących się w ich zasięgu. Dokładność tak dokonywanej lokalizacji można dodatkowo zwiększyć, wykorzystując takie informacje jak wskaźnik mocy odbieranego sygnału (RSSI), różnicę czasu przyjścia sygnałów (TDOA) oraz kąt odbioru sygnału (AOA).

Należy podkreślić, że operator telekomunikacyjny, zapewniający dostęp do sieci GSM i do przenośnego Internetu, posiada rejestr abonentów zawierający imię i nazwisko, numer PESEL, albo nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego UE numer paszportu lub karty pobytu. Dane te pobierane są od abonenta przy zawieraniu umowy w formie pisemnej lub elektronicznej². Ponadto operator gromadzi informacje na temat urządzenia, w którym karta SIM abonenta jest zamontowana. Są to niepowtarzalne numery takie jak IMEI (numer seryjny urządzenia) i IMSI (numer karty SIM).

- **Technologia Wi-Fi.** Bezprzewodowe punkty dostępowe sieci Wi-Fi działają podobnie jak stacje bazowe telefonii komórkowej. W sieci Wi-Fi do lokalizacji wykorzystywany jest niepowtarzalny dla każdego punktu dostępowego numer identyfikacyjny (adres MAC karty sieciowej) oraz siła emitowanego sygnału. Lokalizacja urządzenia wyliczana jest na podstawie danych lokalizacyjnych wykrytych punktów dostępowych oraz poziomu mocy odbieranych sygnałów. Technologię tę wykorzystuje między innymi firma Google, która podczas tworzenia usługi Street View zbierała również informacje o wykrytych w danym terenie punktach dostępowych sieci Wi-Fi.

Punkty dostępowe Wi-Fi można wykorzystać jako źródło informacji geolokalizacyjnych, ponieważ bez przerwy informują one o swoim istnieniu. Każdy punkt dostępowy Wi-Fi bez przerwy przekazuje swoją nazwę sieciową (SSID) i swój adres MAC, nawet jeżeli nikt nie korzysta z połączenia i nawet jeżeli treści połączenia bezprzewodowego są zaszyfrowane. Większość punktów dostępowych do Internetu szerokopasmowego domyślnie posiada również antenę Wi-Fi. W domyślnym ustawieniu większości powszechnie wykorzystywanych punktów dostępowych w Europie emisja sygnałów Wi-Fi pozostaje włączona również

² Art. 43 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych. Zgodnie z nowymi regulacjami od 2 lutego 2017 roku wszelkie aktywne karty sim są zarejestrowane u operatorów telekomunikacyjnych.

w przypadku, gdy użytkownik podłączył swój komputer (komputery) do punktu dostępowego jedynie za pomocą przewodów kablowych.

2.2. Technologie lokalizacji wewnętrznej

W środowisku zewnętrznym systemy satelitarne oraz stacje bazowe telefonii komórkowej są szeroko rozpowszechnione i odgrywają dominującą rolę. Potencjału tego nie da się jednak wykorzystać do lokalizacji wewnątrz pomieszczeń z uwagi na problemy z zakłóceniami sygnału bezpośredniego, których źródłem jest np. interferencja, szumy i inne zakłócenia związane z przeszkodami mającymi wpływ na propagację fal elektromagnetycznych. Przykładem może być wykorzystanie urządzeń mobilnych w obszarach zamkniętych, takich jak sklepy wielkopowierzchniowe, magazyny, muzea itp.

Do najczęściej stosowanych technologii wykorzystywanych w celach lokalizacyjnych w obszarach zamkniętych należą:

- **Technologia Wi-Fi** - technologia opisane w rozdziale 2.1.
- **Technologia RFID** - technologia ta wykorzystuje czytnik zawierający nadajnik wysyłający sygnał oraz odbiornik, który nasłuchuje odpowiedzi z aktywnych bądź pasywnych znaczników (transponderów). Dzięki technologii RFID dane mogą być przesyłane ze znacznika do czytnika za pośrednictwem fal radiowych. Zazwyczaj znacznik składa się z niepowtarzalnego identyfikatora. Dokładność lokalizacji bazującej na RFID jest uzależniona od gęstości rozmieszczenia czytników sygnału RFID. Pozycjonowanie znacznika RFID opiera się na obserwacjach znaczników przez rozmieszczone w danym obszarze czytniki, które mogą odczytać informację ze znaczników z odległości od 1 do kilku metrów.
- **Dedykowane urządzenia lokalizacyjne** - to urządzenia emitujące fale elektromagnetyczne, zawierające określone informacje lokalizacyjne lub informujące o przedmiotach znajdujących się w najbliższym jego otoczeniu oraz różnego rodzaju sensory (czujniki). Należą do nich między innymi:
 - **Beacony** – małe nadajniki emitujące sygnały Bluetooth Low Energy (BLE), zawierające określone informacje. Beacony wykorzystywane w zamkniętych pomieszczeniach, pozwalają doprecyzować położenie, np. wewnątrz sklepu, bądź wskazać lokalizację określonego produktu. Skuteczność tej technologii poszerza wprowadzony ostatnio nowy standard Bluetooth 5, który w stosunku do swojego poprzednika oferuje do czterech razy większy zasięg (obecnie wersja 4.2 teoretycznie oferuje zasięg do 100 metrów) oraz do

dwóch razy większą szybkość, nie pobierając przy tym więcej energii niż poprzedni standard. Dodatkowo oferuje on do ośmiu razy większą pojemność kanałów rozgłoszeniowych, poprawiając skuteczność wykorzystania dostępnego dla tej technologii pasma promieniowania elektromagnetycznego.

- Obrazowanie naturalnego promieniowania podczerwonego – to odpowiednie czujniki, które są w stanie wychwycić źródło ciepła i temperaturę oraz wykorzystać te informacje dla celów lokalizacyjnych.
- Obrazowanie sztucznego promieniowania podczerwonego – to technologia pozwalająca na interakcję z urządzeniem bez konieczności użycia dodatkowych elementów typu myszka czy joystick umożliwiające śledzenie ruchów osoby do odległości 3,5 m i z dokładnością ok. 1 cm. Technologia ta znajduje również zastosowanie w kontroli wykonywanych ruchów i gestów obserwowanej osoby.
- **Kamery cyfrowe** - systemy optyczne i dedykowane oprogramowanie pozwalają określić położenie obiektu/osoby zarówno na zewnątrz jak i wewnątrz budynku. Skuteczność metod optycznych wynika z ulepszenia i miniaturyzacji nie tylko kamer, ale i czujników z nimi współpracujących (czujniki ruchu, światła). Obecnie obserwuje się intensywny rozwój algorytmów przetwarzających obraz pozwalających uzyskać szczegółowe informacje o położeniu osoby/obektu w przestrzeni nadzorowanej przez kamery. Algorytmy stosowane w takich systemach pozwalają precyzyjnie rozróżnić osoby w kadrze, nawet w mało sprzyjających warunkach.
- **Precyzyjne systemy pomiarowe** - technologia mająca zastosowanie w przemyśle i geodezji gdyż zapewnia dokładność od 0,1 mm do 0,01 mm w zależności od odległości. Technologie te nie są stosowane na masową skalę z uwagi na wysoki koszt.

3. Przykłady wykorzystania geolokalizacji i usług geolokalizacyjnych

Dane dotyczące lokalizacji urządzeń noszonych przez osoby fizyczne lub zainstalowanych w publicznych i prywatnych środkach komunikacji mogą być źródłem bardzo ważnych informacji, np. dla służb ratunkowych. Informacje te mogą być wykorzystywane w różnych celach, w tym do optymalizacji i zwiększenia skuteczności działań.

Z uwagi na charakter tych danych, zwłaszcza w przypadku powiązania z danymi identyfikującymi osoby fizyczne, bardzo ważnym elementem ich przetwarzania jest odpowiednie zabezpieczenie i ścisłe przestrzeganie określonych zasad ich udostępniania. Poniżej przedstawiono kilka przykładów ich wykorzystywania.

3.1. Ułatwienie poruszania się w przestrzeni miejskiej

Rozwiązania mobilne wykorzystujące geolokalizację umożliwiają o wiele sprawniejsze poruszanie się w przestrzeni miejskiej, zarówno z perspektywy pasażera, jak i np. operatora taksówki. Dzięki technologii GPS i GSM, wykorzystując aplikacje mobilne mamy możliwość wygodnego wyznaczenia trasy przejazdu, a dzięki publicznie dostępnym rozkładom jazdy komunikacji miejskiej możemy w łatwy i wygodny sposób sprawnie zaplanować podróż. W miastach operatorzy bądź sami klienci taksówek mają możliwość wyboru kierowcy w oparciu o geolokalizację i natężenie ruchu. Informacja o położeniu taksówki pozwala zaoszczędzić klientowi czas, który musiałby upłynąć, gdyby taksówka musiała przyjechać z odległego miejsca. Zastosowanie takich rozwiązań pozwala kierowcom efektywniej poruszać się po mieście. A to z kolei przekłada się na oszczędności na paliwie, zmniejszenie korków, mniejsze spalanie i ograniczenie zanieczyszczeń emitowanych do środowiska.

3.2. Szybsze udzielenie pomocy przez służby ratunkowe

3.2.1. System pomocy ratunkowej 112

Ustawa Prawo telekomunikacyjne, zgodnie z art. 171 ust. 8, zapewnia służbom ustawowo powołanym do niesienia pomocy dostęp do identyfikacji linii wywołującej oraz danych dotyczących lokalizacji abonentów wywołujących połączenia z numerami alarmowymi bez uprzedniej zgody zainteresowanych abonentów lub użytkowników, jeżeli jest to konieczne do umożliwienia tym służbom wykonywania ich zadań w możliwie najbardziej efektywny sposób.

3.2.2. System eCall

System eCall to ogólnoeuropejski system szybkiego powiadamiania o wypadkach drogowych, który państwa członkowskie mają wdrożyć na swoim terytorium do 1 października 2017 r. zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2015/758 z dnia 29 kwietnia 2015 r. w sprawie wymagań dotyczących wdrożenia systemu pokładowego eCall opartego na numerze alarmowym 112 oraz zmiany dyrektywy 2007/46/WE.

Według założeń, wdrożenie systemu może uratować życie 2,5 tys. osób rocznie. Zgodnie z wytycznymi System eCall ma pozostawać w stanie bezczynności i bez podłączenia do sieci telefonii komórkowej w czasie użytkowania pojazdu. Jego aktywacja ma następować dopiero w wyniku zdarzenia drogowego. Rejestracja i przesyłanie danych / komunikacja głosowa odbywa się tylko w razie wypadku bądź ręcznej aktywacji i żadna strona trzecia (w tym operator telekomunikacyjny, z którego infrastruktury korzysta uruchomiony system) nie ma dostępu do przesyłanych informacji.

Dane osobowe nie są przechowywane dłużej niż to konieczne do celów obsługi sytuacji nadzwyczajnych i są usuwane gdy nie są już niezbędne do tego celu.

W polskim porządku prawnym system eCall zgodnie z przepisami musi zacząć funkcjonować do 1 października 2017 roku. Zgodnie z raportem MSWiA³ w sprawie funkcjonowania systemu powiadamiania ratunkowego w 2016 r. w ministerstwie nadal trwają prace mające na celu finalizację wdrażania systemu eCall w Polsce.

3.3. Optymalizacja kosztów w biznesie i transporcie

Geolokalizacja oraz względne pozycjonowanie pojazdu w stosunku do innych użytkowników dróg a także stałych elementów infrastruktury drogowej może być wykorzystywana do ostrzegania kierowcy przed niebezpieczeństwem. W skrajnych przypadkach systemy takie będą mogły automatycznie podejmować różne akcje, jak np. włączać hamowanie pojazdu. Problematyką tą zainteresowała się Międzynarodowa grupa ds. ochrony danych osobowych i telekomunikacji (International Working Group on Data Protection in Telecommunications), która przygotowuje dokument zatytułowany „Issue Paper on Privacy Issues with *Connected Cars*”. Dokument zakłada, że wspomniane urządzenia mogą gromadzić, przechowywać i przysyłać informacje na temat zachowań i nawyków kierowcy, jak również stanu pojazdu, którym się porusza. Dane te mogą być przechowywane lokalnie, przekazywane innemu pojazdowi bądź gromadzone np. w chmurze. Podłączenie do usług zewnętrznych pozwala w bardzo sprawny sposób zgłosić awarię czy połączyć się z punktem informacyjnym. Należy jednak pamiętać, że poza istotnymi zaletami i korzyściami płynącymi z elektronicznej wymiany danych między urządzeniami zainstalowanymi w samochodach, występują również zagrożenia związane z możliwością ich nieautoryzowanego przejęcia i wywołania niepożądanych skutków jak np. kolizji drogowej. Osobnym zagadnieniem jest kwestia ustalenia administratora danych osobowych i czy gromadzenie danych przez pojazdy nie narusza przepisów o ochronie danych osobowych⁴.

3.4. Optymalizacja kosztów ubezpieczenia (telematyka)

Niektóre firmy ubezpieczeniowe próbują wykorzystać dane o zachowaniu się kierowcy na drodze oraz intensywności korzystania z samochodu (np. liczba przejeżdżanych w ciągu roku kilometrów) do szacowania prawdopodobieństwa spowodowania wypadku czy kolizji

³ <https://mswia.gov.pl/download/1/29673/RAPORT.pdf>

⁴ <https://www.weforum.org/agenda/2015/09/who-owns-connected-car-data/>

i wykorzystać je do zaproponowania odpowiednich zniżek ubezpieczenia. Zbieranie takich informacji wymaga niewątpliwie zgody kierowcy na ich gromadzenie i wykorzystywanie. W wielu przypadkach firmy ubezpieczeniowe oferują zniżki w przypadku zgody na takie monitorowanie jazdy, uzasadniając to tym, że już sama świadomość kierowcy o monitorowaniu stylu jego jazdy przyczynia się do zwiększenia jego bezpieczeństwa na drodze. Niektórzy wskazują również na aspekt ekonomiczny, podkreślając, że dzięki płynności poruszania się i przestrzegania przepisów ruchu drogowego kierowca może zaoszczędzić na paliwie i innych materiałach eksploatacyjnych.

Istotnym problemem w tego typu ofertach jest to, czy zgodę kierowcy na takie monitorowanie można uznać za zgodę dobrowolną i czy w świetle obowiązujących przepisów może ona stanowić podstawę prawną firm ubezpieczeniowych do zbierania w tym celu tak szerokiego zakresu danych celem oceny ryzyka ubezpieczeniowego (ewentualnie profilowania klienta w innych celach).

3.5. Zwiększenie dostępności infrastruktury budynku

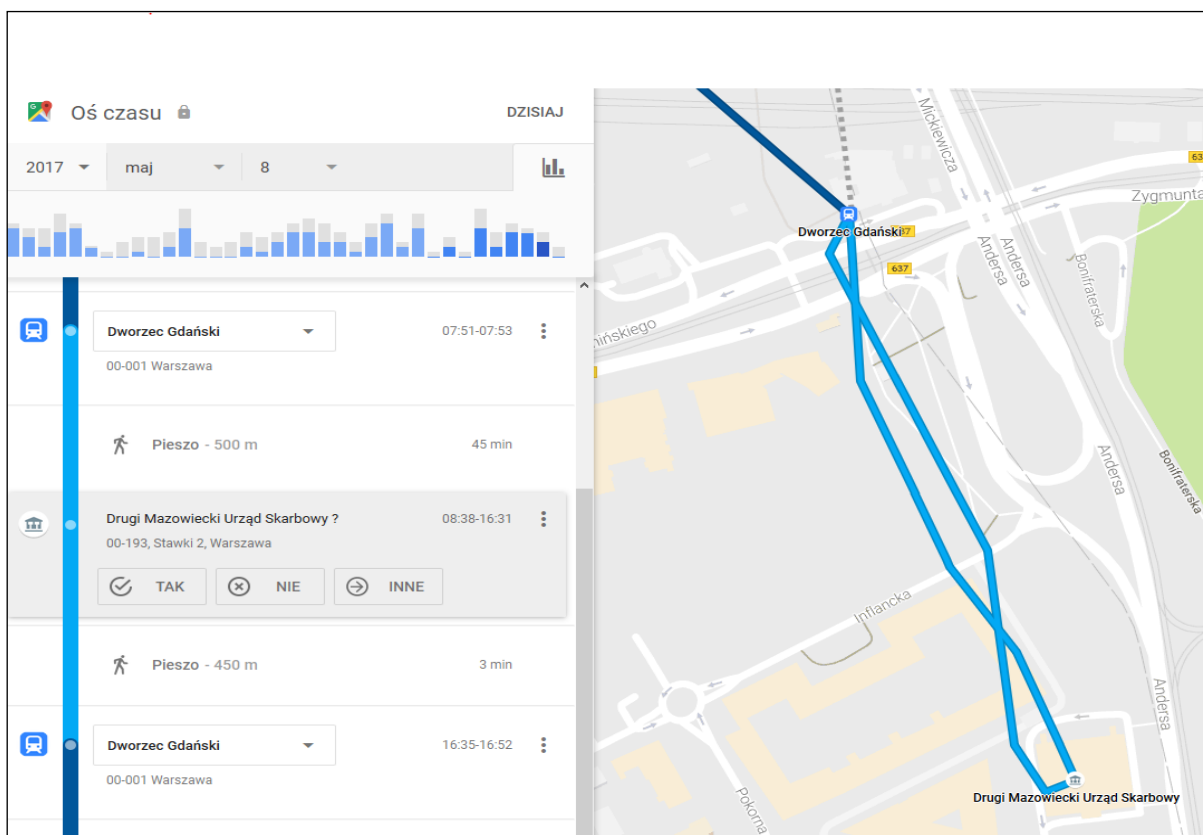
Obecnie szacuje się, że ok. 30-50% osób wchodzących do galerii handlowych ma włączone Wi-Fi. Wykorzystując dedykowaną aplikację mogą wyznaczyć trasę do najbliższej toalety, interesującego sklepu czy parkingu. Niejednokrotnie aplikacje tego typu zachęcają do zakładania konta powiązanego z sieciami społecznościowymi. Dzięki powiązaniu aplikacji np. z Facebookiem, dane lokalizacyjne wewnątrz budynku są poszerzane o inne dane osobowe, które z kolei umożliwiają dotarcie do klienta z określoną ofertą.

Zastosowanie technologii lokalizacyjnych, z wykorzystaniem aplikacji mobilnych, wewnątrz budynków, np. muzeów, pozwala w atrakcyjnej i przystępnej formie dotrzeć do odbiorców z informacją np. o położeniu eksponatów na terenie budynku. Technologia Bluetooth (beacon) pozwala zwiedzającemu łatwiej odnaleźć się w przestrzeni muzeum co może być pewną zachętą do odwiedzania tego typu placówek.

Technologia oparta o beacons pozwala również rozwiązać problem poruszania się osób niepełnosprawnych, zwłaszcza niewidomych. Rozwiązanie może być pomocne nie tylko w znalezieniu właściwego pokoju, ale również pojedynczego przedmiotu. Mikronawigacja jest bardzo precyzyjna i dzięki dedykowanej aplikacji mobilnej osoba niewidoma uzyskuje dostęp do przewodnika po budynku, np. urzędu i sprawach, które można w nim załatwić.

3.6. Inne przykłady użycia

Zastosowanie technologii lokalizacyjnych umożliwia również dostarczenie usług umożliwiających prowadzenie historii lokalizacji oraz otrzymywanie spersonalizowanych wyników w wyszukiwarkach internetowych. Przykładową usługą gromadzącą tego typu dane są usługi geolokalizacyjne firmy Google, zaprezentowane na rys. 3. Z wyświetlanych tam informacji można odczytać o której godzinie dana osoba była w określonym miejscu i jak długo tam przebywała. Podobne informacje o przebytych trasach gromadzą aplikacje mobilne do dedykowanych zastosowań, np. aktywności fizycznej (Endomondo, Runtastic).



Rys. 3. Historia lokalizacji w usługach Google (droga przebyta we wskazanym dniu do miejsca pracy i z powrotem przez użytkownika telefonu z włączoną usługą lokalizacji).

4. Zagrożenia związane z wykorzystaniem danych lokalizacyjnych

4.1. Duża ilość danych osobowych w jednym miejscu

Inteligentne urządzenie przenośne jest bardzo ściśle powiązane z konkretną osobą. Większość osób zazwyczaj trzyma je blisko siebie. Rzadko też zdarza się żeby dana osoba

udostępniała takie urządzenie komuś innemu. W związku z tym większość osób zdaje sobie sprawę, że ich urządzenia przenośne zawierają wiele bardzo prywatnych informacji, zgromadzonych w szczególnych, indywidualnych kontekstach, dotyczących także powiązań z innymi osobami czy podmiotami. Dostawcom usług geolokalizacyjnych umożliwia to zdobycie danych dotyczących nawyków i schematów postępowania właściciela takiego urządzenia oraz tworzenie obszernych, ale i bogatych w informację profili. Przykładowo, schemat braku aktywności w nocy może jednoznacznie informować o miejscu, w którym dana osoba śpi, a regularny schemat podróżowania w ciągu dnia może sugerować lokalizację pracodawcy.

W niektórych aplikacjach dane lokalizacyjne łączy się dodatkowo z danymi gromadzonymi przez czujniki, takie jak: żyroskop, kamery, mikrofony czy czujnik bliskości, uzyskując w ten sposób nowe wartości dodane.

Często zarówno twórcy aplikacji, jak i ich użytkownicy nie są świadomi wymogów i obowiązujących zasad w zakresie ochrony danych osobowych, przez co ich aplikacje mogą wносить istotne zagrożenie dla ochrony życia prywatnego oraz reputacji osób, które z nich będą korzystać, ale także obowiązków informacyjnych leżących po stronie administratora czy praw podmiotów do kontroli procesu przetwarzania danych.

Kluczowe zagrożenia w zakresie ochrony danych osobowych dla użytkownika końcowego stanowi połączenie braku przejrzystości w zakresie kategorii i sposobu przetwarzania danych oraz świadomości w zakresie zagrożeń związanych z ich udostępnienia innym osobom lub podmiotom.

Analizując dane jakie co roku publikuje Urząd Komunikacji Elektronicznej można zauważyć tendencję do stałego szybkiego wzrostu liczby danych przesyłanych w sieciach mobilnych. W roku 2015 użytkownicy Internetu w sieciach mobilnych przesłali o 114% więcej danych niż rok wcześniej. Zwiększył się również ponad dwukrotnie średni wolumen transmisji danych na jednego użytkownika (z ok. 7 GB/rok do ok. 14 GB/rok). Ponadto operatorzy sukcesywnie powiększają zasięg swoich sieci w technologii 4G/LTE (jak wskazuje UKE jeden z polskich operatorów jest w stanie dotrzeć ze swoimi rozwiązaniami do 99,8% ludności kraju). W związku z powyższym raporty UKE dostarczają też ciekawej informacji, jaką jest zauważalna tendencja do zmniejszającej się z roku na rok liczby wysyłanych SMS-ów, czego przyczynę należy upatrywać we wzroście popularności smartfonów (komunikatorów) oraz powszechnym, coraz tańszym dostępie do Internetu mobilnego.

Kiedy rozważa się dostępne środki potrzebne do identyfikowania, należy uwzględnić sytuację, w której użytkownicy zamieszczają w Internecie coraz większą ilość danych osobowych, w tym dotyczących ich lokalizacji, na przykład poprzez publikowanie lokalizacji swojego domu lub miejsca pracy w połączeniu z innymi danymi identyfikującymi. Do publikacji takich danych dochodzi często bez ich wiedzy. Dotyczy to np. portali społecznościowych, na których publikowane zdjęcie może być opatrzone automatycznie informacją o miejscu jego wykonania.

Objętość transmisji danych oraz dynamika ich zmian determinują liczbę danych osobowych udostępnianych aplikacjom oraz usługodawcom, w tym przede wszystkim danych geolokalizacyjnych.

W związku z powyższym, zarówno producenci jak i użytkownicy urządzeń i aplikacji mobilnych z włączonymi usługami geolokalizacji powinni być świadomi potencjalnych zagrożeń jakie wiążą się z przetwarzaniem danych lokalizacyjnych.

4.2. Udostępnianie informacji w aplikacjach mobilnych

Coraz więcej aplikacji w czasie instalacji wymaga od użytkownika zgody na udostępnienie wielu informacji, w tym danych lokalizacyjnych. W przypadku aplikacji dostępnych dla systemu Android, dostęp do informacji o lokalizacji może obejmować:

- informacje o przybliżonej lokalizacji (na podstawie sieci),
- dokładną lokalizację (na podstawie GPS-u i sieci),
- dostęp do informacji lokalizacyjnej z innych źródeł.

Należy pamiętać, że zgadzając się na kilka uprawnień jednocześnie, udostępniamy danej aplikacji cały pakiet danych osobowych. Zdarza się, że są to dane wrażliwe związane chociażby ze stanem zdrowia. W tym kontekście problemem jest stałe rozszerzanie przez producentów możliwości takich aplikacji, ich uatrakcyjnianie, które wiąże się wszakże z ryzykiem poszerzania katalogu o dane nieadekwatne do realizowanego celu.

Należy mieć również na uwadze zakres odbiorców, którym dane udostępniane są na portalach społecznościowych. Zalecanym rozwiązaniem jest zgodnie z zasadą domyślnej prywatności, zastosowanie ustawień początkowych, które wstępnie nie pozwalają na udostępnienie żadnych danych, ale jednocześnie dostarczenie funkcji, które pozwalają użytkownikowi wskazać dane i odbiorców, którym chce je udostępnić. Użytkownik powinien móc wskazać, którzy z jego znajomych mogą widzieć informacje dotyczące jego aktualnej lokalizacji.

Dodatkowy wpływ na identyfikację osoby ma stałe połączenie urządzenia z różnego rodzaju usługami (bankowymi, pocztą elektroniczną, czy portalami społecznościowymi). Włączone na urządzeniu usługi zbierają informacje o naszej aktywności, dzięki czemu administrator tych danych może uzyskać informacje o naszych nawykach czy przekonaniach religijnych. Wykorzystując odpowiednie algorytmy wnioskuje związane z technologią Big Data, możliwe jest na podstawie zgromadzonych danych określenie profili poszczególnych osób, które mogą zostać wykorzystane we wszystkich dziedzinach i branżach. Przykładowo, mogą to być tzw. systemy scoringowe stosowane przez banki posiadające przegląd całej aktywności finansowej klienta, w tym w zakresie miejsca dokonywanych transakcji, np. związanych z wykonywanym przez niego zawodem, czy prywatnymi zainteresowaniami.

Nawet jeżeli osoby fizyczne celowo udostępniają swoje dane geolokalizacyjne w Internecie za pomocą usług dotyczących miejsca pobytu i geotagowania, nieograniczony i pełny dostęp stwarza nowe zagrożenia, które mogą obejmować kradzież danych i włamania, a nawet fizyczną napaść i nękanie.

W przypadku banków warto wspomnieć o Rekomendacji Komisji Nadzoru Finansowego z listopada 2015 roku dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe. Wskazano w niej, że dostawcy usług płatniczych powinni stosować systemy wykrywania i zapobiegania oszustwom w celu identyfikacji podejrzanych transakcji przed wykonaniem przez dostawcę usług płatności internetowej. Systemy te powinny funkcjonować w oparciu o sparametryzowane reguły oraz monitorować nietypowe wzorce zachowań klientów lub ich urządzeń dostępowych (takie jak zmiana adresu lub zakresu adresów IP) podczas sesji usług płatności internetowych, czasem identyfikowane przez sprawdzenie geolokalizacji adresu IP.

4.3. Brak odpowiednich zabezpieczeń

W przeciwieństwie do technologii GPS stosowanej przez jednostki wojskowe, obecny stopień zabezpieczeń technologii cywilnego GPS może budzić obawy i rodzi ryzyko, że liczba aktów spoofingu (podmiana sygnału) może szybko rosnąć. GPS jest pozbawiony mechanizmów uwierzytelniających, przez co wzrasta prawdopodobieństwo zakłócenia lokalizacji innymi sygnałami. Ma to duże znaczenie w odniesieniu np. do takich obiektów jak bezzałogowe statki powietrzne, czyli drony, których zakłócenie lokalizacji może stać się poważnym zagrożeniem dla bezpieczeństwa ruchu lotniczego jak i osób poruszających się na ziemi. Należy więc

oczekiwać, że tworzone rozwiązania prawne na szczeblu unijnym i krajowym zapobiegną takim ryzykom i zapewnią spójną politykę w tym zakresie.

5. Aspekty prawne

Przetwarzanie danych geolokalizacyjnych, tak jak każdego innych danych osobowych musi odbywać się zgodnie z przyjętymi zasadami w przepisach prawa, krajowego i unijnego. Ustawa o ochronie danych osobowych (UODO) jest implementacją unijnej dyrektywy 95/46/WE i zawiera szereg praw i obowiązków stron uczestniczących w procesie przetwarzania danych osobowych. Ustawa, nakłada obowiązek dochowania szczególnej staranności w procesie przetwarzania danych osobowych. Ustanawia ona między innymi podstawowe zasady przetwarzania danych (art. 26 ust. 1), takie jak legalność, celowość, adekwatność oraz ograniczenie okresu czasu przez jaki dane mogą być przetwarzane. Zasady te znalazły swoje odzwierciedlenie również w RODO⁵, które weszło w życie z dniem 25 maja 2016 r. i wchodzi do stosowania z dniem 25 maja 2018 r. Bardziej szczegółowe informacje dotyczące legalności przetwarzania danych lokalizacyjnych oraz zakresu i sposobu ich wykorzystywania zawarto w opiniach nr 02/2013⁶, 13/2011⁷ i 5/2005⁸ Grupy Roboczej Art. 29 Dyrektywy 95/46/WE⁹.

5.1. Zasady przetwarzania danych osobowych

Do najważniejszych zasad dotyczących przetwarzania danych osobowych wskazywanych w przepisach Dyrektywy 95/46, UODO, a także RODO należą:

Zasada legalności (art. 23 ust 1 pkt. 1 UODO, art. 6 ust 1 RODO)

Zasada ta stanowi, że przetwarzanie danych osobowych przez administratora powinno odbywać się z zachowaniem jednej z przesłanek legalności przetwarzania określonych w art.

⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

⁶ Opinia Grupy Roboczej Art. 29 w sprawie aplikacji na urządzenia inteligentne z 27 lutego 2013 r.
http://www.giodo.gov.pl/plik/id_p/4328/j/pl/

⁷ Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych (WP185).
http://www.giodo.gov.pl/plik/id_p/2357/j/pl/

⁸ Opinia 5/2005 grupy roboczej art. 29 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną - http://giodo.gov.pl/plik/id_p/2314/j/pl/

⁹ Grupa Robocza Art. 29 ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwana dalej Grupą Roboczą Art. 29, powołana została na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

23 ust. 1 UODO lub odpowiednio art. 6 ust. 1 RODO. W kontekście danych geolokalizacyjnych, oprócz zgody oraz przepisu prawa, przesłanką legalności może być konieczność realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną lub gdy przetwarzanie jest niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. Możliwą przesłanką jest także wypełnianie prawnie usprawiedliwionego celu realizowanego przez administratora danych czy odbiorcy danych o ile przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Zasada celowości (art. 26 ust. 1 pkt 2 UODO, art. 5 ust. 1 pkt b RODO)

Zasada celowości stanowi, że dane osobowe powinny być przetwarzane wyłącznie w zakresie, w jakim jest to niezbędne do osiągnięcia celu przetwarzania. Ponadto zbieranie danych osobowych, w tym geolokalizacyjnych, powinno być dokonywane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Przetwarzanie danych w celu innym niż ten, dla którego zostały pierwotnie zebrane może następować tylko pod ściśle określonymi warunkami i jeśli nie narusza praw i wolności podmiotu danych (art. 26 ust. 2 UODO).

Zasada adekwatności (art. 26 ust. 1 pkt 3 UODO, art. 5 ust. 1 pkt c RODO)

Ustawa określa również zasadę adekwatności wskazującą na konieczność przetwarzania tylko takiego rodzaju danych i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych.

Zasada merytorycznej poprawności (art. 26 ust. 1 pkt 3 UODO, art. 5 ust. 1 pkt d RODO)

Administrator danych jest obowiązany zapewnić merytoryczną poprawność danych osobowych. Chodzi o to, aby były one zgodne ze stanem rzeczywistym (prawdziwe, pełne, kompletne i aktualne). W tym celu konieczne jest, aby w procesie przetwarzania danych administrator każdorazowo oceniał m.in. wiarygodność źródła pozyskania danych, ale i aktualność danych, na których wykonuje jakiegokolwiek operacje.

Zasada ograniczenia czasowego (art. 26 ust. 1 pkt 4 UODO, art. 5 ust. 1 pkt e RODO)

Na administratora przepisy ustawy nakładają również obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania. Po osiągnięciu celu (np. wskazaniu najbliższych punktów gastronomicznych na mapie) dane powinny zostać usunięte bądź zanonimizowane. Chyba, że użytkownik wyraził oddzielną wyraźną zgodę na dalsze wykonywanie operacji na tych danych.

Zasada integralności i poufności (art. 36 UODO, art. 5 ust. 1 pkt f RODO)

Dane osobowe, w tym geolokalizacyjne, powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Dane geolokalizacyjne w kontekście nowych przepisów

Należy podkreślić, że nowe przepisy o ochronie danych osobowych, które będą miały zastosowanie od 25 maja 2018 roku, nie znoszą wyżej wymienionych zasad i obowiązków, w tym informacyjnych. Pozycja osoby, której dane osobowe są przetwarzane będzie wzmocniona poprzez szereg nowych obowiązków i zasad, takich jak prawo do przenoszenia danych czy obowiązek uwzględniania przez administratora danych zasad domyślnej prywatności (privacy by default) i uwzględnienia prywatności w fazie projektowania (privacy by design).

5.2. Kto i kiedy jest administratorem danych?

Podobnie jak operatorzy telekomunikacyjni, którzy przetwarzają lokalizację konkretnego urządzenia za pomocą swoich stacji bazowych, właściciele baz danych z mapowanymi punktami dostępowymi Wi-Fi przetwarzają dane osobowe, kiedy obliczają lokalizację konkretnego inteligentnego urządzenia przenośnego. Określając zarówno cele, jak i środki takiego przetwarzania, podmioty te stają się administratorami danych w rozumieniu art. 7 pkt 4 UODO czy art. 4 pkt 7 RODO.

Adres MAC punktu dostępowego Wi-Fi należącego do osoby fizycznej w połączeniu z jego obliczoną lokalizacją należy traktować jako dane osobowe. Bez względu na sposób, w jaki gromadzone są te dane (jednorazowo lub systematycznie), właściciel takiej bazy danych (będącej zbiorem danych osobowych) powinien wypełniać obowiązki zawarte w przepisach o ochronie danych osobowych.

Aplikacje mobilne umożliwiają przetwarzanie danych geolokalizacyjnych niezależnie od twórcy systemu operacyjnego, jak również administratorów infrastruktury systemu geolokalizacji. Jednakże w sytuacji, gdy aplikacja geolokalizacyjna przetwarza dane użytkownika nie tylko przy użyciu urządzenia, na którym została zainstalowana, ale również przy użyciu zasobów producenta lub dystrybutora tej aplikacji, wówczas producenta tego lub dostawcę należy traktować jako administratora tych danych.

Również twórca systemu operacyjnego inteligentnego urządzenia przenośnego może być administratorem danych w zakresie przetwarzania danych geolokalizacyjnych, jeżeli proponuje on użytkownikowi gromadzenie jego danych (np. żądając wstępnej rejestracji lub gromadząc informacje dotyczące lokalizacji w celu poprawy jakości usług). Często przytaczanym przykładem funkcji jest automatyczne dostarczanie aktualizacji strefy czasowej w oparciu o lokalizację. Twórca systemu operacyjnego jest również administratorem danych, jeżeli oferuje platformę reklamową lub środowisko przypominające sklep internetowy z aplikacjami i jest w stanie przetwarzać dane osobowe wynikające z (instalacji i stosowania) aplikacji wyposażonych w funkcję geolokalizacji niezależnie od dostawców aplikacji.

5.3. Uzasadnione podstawy przetwarzania

Dane geolokalizacyjne przetwarzane są nie tylko za pomocą systemu operacyjnego czy aplikacji zainstalowanej na inteligentnym urządzeniu przenośnym. Wiele usług dostępnych przez przeglądarkę internetową umożliwia przetwarzania danych dotyczących lokalizacji, jak np. wspomniane już geotagowanie zdjęć.

Należy pamiętać, że zgodnie z art. 23 ust. 1 pkt 1 UODO oraz art. 6 ust 1 pkt a) RODO, najczęstszą podstawą do przetwarzania danych osobowych, w tym danych geolokalizacyjnych, jest zgoda użytkownika. Zgodą (art. 7 pkt 5 ustawy) jest oświadczenie woli pochodzące od osoby, której dane dotyczą, którego treścią jest zgoda na przetwarzanie danych tego, kto składa to oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie. Z definicji tej nie wynikają szczegółowe zasady formułowania klauzuli zgody, ale warto podkreślić, że z treści zgody na przetwarzanie danych osobowych powinno wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego na co się godzi. W związku z tym sama techniczna możliwość urządzenia do przekazywania danych osobie trzeciej, w przypadku jeśli osoba, której dane są przekazywane nie ma o tym wiedzy, nie stanowi o legalnym przetwarzaniu danych. Podobnie w przypadku, jeżeli domyślne ustawienia systemu operacyjnego pozwalają na przekazywanie danych dotyczących lokalizacji (przy braku interwencji ze strony jego użytkowników), sytuacji takiej nie można traktować jako dobrowolnego wyrażenia zgody.

Niezależnie od europejskich dyrektyw o ochronie danych konsorcjum World Wide Web (W3C) opracowało wstępną specyfikację API geolokalizacji, w której podkreślono konieczność

uzyskania uprzedniej, wyraźnej i świadomej zgody¹⁰. Konsorcjum W3C wyjaśnia w szczególności konieczność poszanowania wycofania zgody, doradzając podmiotom wdrażającym specyfikację, aby uznawały, że „treści dostępne pod danym adresem URL zmieniają się w taki sposób, że wcześniej udzielone zezwolenia na lokalizację nie mają już zastosowania w przypadku danego użytkownika; lub że użytkownicy mogą po prostu zmienić zdanie”.

Przykładowo, aplikacja udziela informacji na temat pobliskich restauracji. Aby możliwa była jej instalacja, podmiot opracowujący aplikację musi uzyskać zgodę. Aby uzyskać dostęp do danych geolokalizacyjnych podmiot opracowujący aplikację musi osobno poprosić o zgodę, np. podczas instalacji lub przed uzyskaniem dostępu do geolokalizacji. Konkretna zgoda oznacza, że zgoda musi być ograniczona do konkretnego celu polegającego na poinformowaniu użytkownika o pobliskich restauracjach. Dostęp do danych dotyczących lokalizacji z urządzenia można w związku z tym uzyskać jedynie, gdy użytkownik wykorzystuje daną aplikację w tym celu. Zgoda użytkownika na przetwarzanie danych geolokalizacyjnych nie stanowi pozwolenia dla aplikacji na ciągłe gromadzenie danych dotyczących lokalizacji z urządzenia. Dalsze przetwarzanie tego rodzaju wymaga dodatkowych informacji i osobnej zgody.

Przetwarzanie danych na podstawie zgody jest problematyczne w odniesieniu do pracowników i dzieci.

Wiele ograniczeń w zakresie pozyskiwania przez pracodawcę danych osobowych pracowników kreują przepisy prawa pracy. Pracodawcy mogą stosować tę technologię wyłącznie po wykazaniu, iż jest to niezbędne do osiągnięcia wyraźnie określonego celu, przy czym nie dla wszystkich celów pozyskiwanie takich danych jest konieczne. Przed uzyskaniem zgody pracodawca powinien zastanowić się, czy rzeczywiście istnieje konieczność i uzasadniony powód kontrolowania dokładnej lokalizacji pracowników, w świetle ich podstawowych praw i wolności, przy zachowaniu pełnej transparentności tego procesu (obowiązek informacyjny).

Problematyczna wydaje się także kwestia zgody, jako podstawy prawnej do wykorzystywania przez pracodawcę danych geolokalizacyjnych pracownika, w zakładanych celach (np. kontrola czasu pracy, ocena jakości pracy, czy kontrola bezpieczeństwa w miejscu pracy),

¹⁰ <http://www.w3.org/TR/geolocation-API/>

o ile nie jest wyrażana w warunkach pełnej dobrowolności. Dodatkowo, przy wykorzystaniu tej przesłanki pamiętać należy o możliwości jej odwołania w każdym czasie, co może być wręcz sprzeczne z interesem pracodawcy.

W przypadku dzieci rodzice muszą ocenić, czy zastosowanie takiej aplikacji jest uzasadnione w szczególnych okolicznościach, uwzględniając nie tylko takie kryterium jak bezpieczeństwo dziecka, ale także poszanowanie jego godności. Należy podkreślić, że w opinii nr 2/2009¹¹ na temat ochrony danych osobowych dzieci Grupa Robocza Art. 29 napisała: „*nigdy nie powinna mieć miejsca sytuacja, w której ze względów bezpieczeństwa dzieci stają się przedmiotem nadmiernego nadzoru ograniczającego ich niezależność. W związku z tym należy znaleźć równowagę między ochroną intymności i prywatności dzieci a ich bezpieczeństwem*”. Zgodnie z obecnie obowiązującym prawem rodzice są odpowiedzialni za zapewnienie swoim dzieciom prawa do prywatności. W nowej perspektywie jaką niesie ze sobą RODO krajowe przepisy o ochronie danych osobowych będą określały granicę wieku dziecka korzystającego z usług społeczeństwa informacyjnego wyrażającego zgodę na przetwarzanie swoich danych osobowych, w tym danych geolokalizacyjnych.

5.4. Obowiązek informacyjny

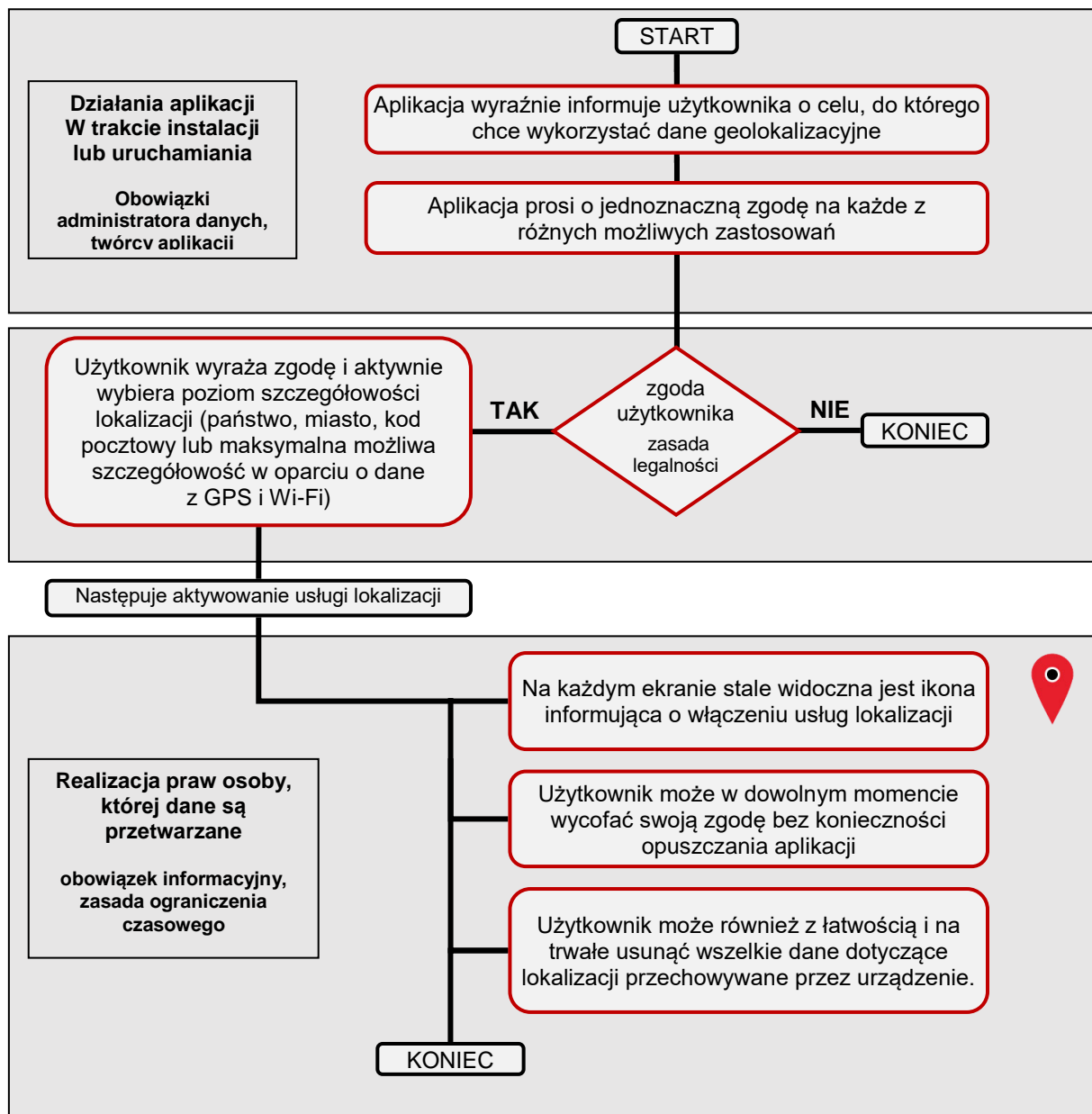
Każdy administrator danych musi należycie informować osoby, których dane są przetwarzane o kluczowych elementach przetwarzania danych zgodnie z art. 24 UODO oraz art. 12, 13 i 14 RODO, a przede wszystkim o celu zbierania danych, prawie dostępu do treści swoich danych oraz ich poprawiania a także o możliwości cofnięcia zgody.

W odniesieniu do tożsamości administratora danych, użytkownicy potrzebują wiedzy na temat tego, kto jest prawnie odpowiedzialny za przetwarzanie ich danych osobowych oraz jak uzyskać kontakt z administratorem. W innym przypadku nie mogą oni wykonywać swoich praw, takich jak prawo dostępu do danych (zdalnie) przechowywanych na ich temat. W związku z tym administrator danych obowiązany jest przekazać tej osobie informacje o adresie siedziby i pełnej nazwie a w przypadku, gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku. Obowiązek ten powinien zostać spełniony przed rozpoczęciem gromadzenia danych.

Grupa Art 29 w opinii 13/2011 w odniesieniu do sposobu wykonywania obowiązku informacyjnego w przypadku usług geolokalizacji zaleca ponadto (rys. 4), aby użytkownik

¹¹ WP160, Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół).

urządzenia lub aplikacji, które mają włączoną funkcję lokalizacji był o tym fakcie informowany w sposób ciągły poprzez wyświetlanie stosownej ikony.



Rys. 4. Schemat prawidłowej praktyki wypełniania obowiązku informacyjnego dla dostawców aplikacji mobilnych wyposażonych w funkcję geolokalizacji zalecany przez Grupę Art. 29.

Jeżeli dostawcy aplikacji wyposażonych w funkcję geolokalizacji zamierzają wyznaczać lokalizację urządzenia więcej niż raz, muszą informować o tym swoich klientów tak długo, jak długo czynność ta jest wykonywana. Muszą również umożliwić swoim klientom podtrzymanie lub wycofanie wyrażonej zgody w możliwie prosty sposób.

5.5. Prawa osób, których dane dotyczą

Osoby, których dotyczą dane, mają prawo dostępu do danych dotyczących lokalizacji pobranych przez różnych administratorów danych ze swoich inteligentnych urządzeń przenośnych, jak również do informacji na temat celów przetwarzania i odbiorców lub kategorii odbiorców, którym dane są ujawniane. Informacje muszą być przekazane w formie czytelnej dla człowieka, tj. w postaci położenia geograficznego, a nie abstrakcyjnych numerów na przykład stacji bazowych.

Osoby, których dotyczą dane, w ramach procesu kontroli procesu przetwarzania własnych danych, mają również prawo wglądu do potencjalnych profili opartych na takich danych dotyczących lokalizacji. Jeżeli informacje dotyczące lokalizacji są przechowywane, użytkownicy powinni mieć możliwość aktualizowania, poprawiania lub usuwania takich informacji.

Zaleca się, aby administratorzy danych poszukiwali bezpiecznych sposobów zapewniania bezpośredniego dostępu on-line do danych dotyczących lokalizacji i potencjalnych profili. Jeżeli użytkownik wykonuje swoje prawo dostępu, administrator musi zapewnić użytkownikowi informacje dotyczące przetwarzanych danych i źródła tych danych. Jeżeli administrator podejmuje zautomatyzowane decyzje w oparciu o połączone dane, musi on także poinformować użytkownika o zasadach podejmowania tych decyzji przed uzyskaniem zgody na profilowanie. Może mieć to miejsce w przypadkach, w których ocenia się wyniki lub postępowanie użytkownika w oparciu o dane geolokalizacyjne oraz sposób jego przemieszczania się.

5.6. Okres przechowywania

Dostawcy usług geolokalizacyjnych i aplikacyjnych powinni określić okres przechowywania danych dotyczących lokalizacji nie dłuższy, niż jest to konieczne do celów, dla których dane były pobierane lub dla których są dalej przetwarzane. Muszą zapewnić usunięcie danych geolokalizacyjnych lub profili uzyskanych na podstawie takich danych po ustaniu celu uzasadniającego przetwarzanie w zakładanym okresie.

W przypadku, w którym konieczne jest gromadzenie anonimowych danych dotyczących historii lokalizacji przez twórcę systemu operacyjnego lub aplikacji w celu aktualizowania lub udoskonalania świadczonych usług, należy dołożyć wszelkich starań, aby uniemożliwić, nawet w sposób pośredni identyfikację podmiotów danych.

6. Doświadczenia GODO w kontekście przetwarzania danych geolokalizacyjnych

Technologia GPS

Od 2012 roku do Biura GODO wpłynęło ok. 20 zgłoszeń zbiorów, w których przetwarzane są dane osobowe w oparciu o dane geolokalizacyjne. W tym ok. 6 zgłoszeń pochodzi od administratorów danych osobowych oferujących usługi z zakresu: monitorowania pojazdów GPS, oprogramowania pozwalającego na wygodne zarządzanie flotą pojazdów (kontrola czasu pracy pojazdów i pracowników, kontrola paliwa, zarządzanie ruchem pojazdów w terenie, alerty wysyłane na mail lub sms pozwalają na natychmiastową reakcję na różne zdarzenia dotyczące pojazdów w terenie).

Oferty takie są kierowane zarówno do klientów prowadzących działalność gospodarczą w celu tworzenia Ewidencji Przebiegu Pojazdów¹², jak i do klientów indywidualnych w celach poprawy bezpieczeństwa¹³.

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1 Ustawy o ochronie danych osobowych, tzn. zgodę osoby, której dane dotyczą, a także art. 23 ust. 1 pkt 3 – jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. Zakres przetwarzanych danych o osobach ogranicza się wyłącznie do danych zwykłych.

W 2014 roku zgłoszony został zbiór przez administratora obsługującego serwis społecznościowy oferujący narzędzia i usługi on-line umożliwiające tworzenie i pobieranie tras GPS z wykorzystaniem aplikacji mobilnych oraz używania technologii mobilnych i rozwiązań internetowych do komunikowania się z innymi uczestnikami społeczności (trasy turystyczne, rowerowe i inne). Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1 Ustawy o ochronie danych osobowych, tzn. zgodę osoby, której dane dotyczą. W zbiorze przetwarzane są wyłącznie dane zwykłe.

¹² Tworzenie takiej ewidencji wymaga ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2016 r. poz. 710

¹³ Poprzez precyzyjną lokalizację pozycji pojazdu w przypadku kradzieży, sprawdzenie stanu pojazdu oraz miejsca ostatniej zarejestrowanej lokalizacji, unieruchomienie za pomocą komunikatów SMS, powiadomienia o zdarzeniach, alarmach

W 2016 roku wpłynęło zgłoszenie od administratora danych oferującego usługę aplikacji mobilnej służącej do zamawiania taksówek. Po uruchomieniu aplikacji w telefonie GPS lokalizuje ona na mapie telefon użytkownika i pokazuje wszystkie dostępne taksówki w okolicy.

Również w 2016 roku wpłynęło ok. 10 zgłoszeń od administratorów danych oferujących aplikacje mobilne działające na podobnej zasadzie jak podany wyżej przykład. Były to:

- Aplikacja informująca o wydarzeniach i aktywnościach (kulturalne, sportowe, towarzyskie, hobby i in.) w najbliższej okolicy, która wykrywa lokalizację i wyświetla na mapie.
- Aplikacja mobilna na smartfonie z urządzeniem lub urządzeniami beacon, która pozwala na całodobowe kontrolowanie miejsc bądź rzeczy, poprzez system nadajników tworzących strefę, obsługiwaną za pomocą smartfona. Informuje o lokalizacji (np. w przypadku kradzieży).
- Aplikacja pozwalająca dzięki specjalnej opasce kontrolowanie zdrowia innej osoby, również jej lokalizacji w razie wypadku. W przypadku tego zgłoszenia zakres danych wykracza poza dane zwykłe, w odróżnieniu od innych wskazanych przypadków zgłoszeń. Specyfika i cel aplikacji warunkuje przetwarzanie danych związanych ze zdrowiem osoby. Jako podstawę prawną przetwarzania danych osobowych administrator wskazał art. 23 ust. 1 pkt 1 Ustawy o ochronie danych osobowych, tzn. zgodę osoby, której dane dotyczą, a także art. 23 ust. 1 pkt 3 – jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. Natomiast jako podstawę prawną przetwarzania danych osobowych szczególnie chronionych (stan zdrowia) administrator wskazał art. 27 ust. 2 pkt 1 ustawy tj. zgodę na piśmie.
- Aplikacja pozwalająca na ustalenie lokalizacji osoby potrzebującej pomocy w górach;
- Aplikacja pozwalająca ustalić miejsca przyjazne zwierzętom;
- Aplikacja, która pomoże załatwić formalności po śmierci bliskiej osoby;
- Aplikacja pozwalająca zlokalizować zgubiony bądź skradziony telefon;
- Aplikacja pozwalająca odnaleźć restauracje, kawiarnie w okolicy, uzyskać informacje o zniżkach, nabyć zniżki, kupony, rabaty;
- Aplikacja pozwalająca ustalić dojazd do dowolnego miejsca komunikacją miejską;
- Aplikacja skierowana do rowerzystów, zawiera trasy, możliwość rywalizacji użytkowników aplikacji, porównywanie wyników itp.

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1 Ustawy o ochronie danych osobowych, tzn. zgodę osoby, której dane dotyczą. W zbiorach danych tworzonych przez ww. aplikacje przetwarzane są wyłącznie dane zwykłe.

Geolokalizacja oparta na punktach dostępowych Wi-Fi

Od 2008 roku zgłaszane były zbiory, w których wykorzystywana jest technologia Wi-Fi. Wśród ok. 20 zgłoszonych zbiorów Administratorzy danych osobowych oferują usługi HOTSPOT jako narzędzia pozwalające na udostępnianie łącza internetowego użytkownikom. Statystyki udostępniane właścicielom HotSpotów pozwalają śledzić ruch w sieci, m. in. informują o użytkownikach (adresy MAC, IP, czas logowania, czas sesji, obciążenie łącza, aktywni użytkownicy, zakończone usługi). Punkty dostępowe Wi-Fi można wykorzystać jako źródło informacji geolokalizacyjnych, ponieważ bez przerwy zgłaszają one swoje istnienie.

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1 Ustawy o ochronie danych osobowych, tzn. zgodę osoby, której dane dotyczą, a także art. 23 ust. 1 pkt 3 – jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. Jako dodatkową podstawę poza powyższymi wskazywano art. 23 ust. 1 pkt 5 – prawnie usprawiedliwione cele realizowane przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Administratorami danych osobowych zgłaszającymi tego typu zbiory były również podmioty publiczne, tj. Gminy dla kategorii osób - użytkowników sieci Wi-Fi. W tych przypadkach jako podstawę prawną wskazywano ustawę z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2016 r. poz. 446), Ustawę z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489).

W zbiorach tych zakres przetwarzanych danych ogranicza się wyłącznie do danych zwykłych.

System monitorowania i zarządzania klientami operatorów GSM

W 2015 roku zgłoszono ok. 12 zbiorów administratorów danych oferujących usługę systemu monitorowania i zarządzania klientami operatorów GSM, w tym automatyczne powiadamianie o wygasających umowach.

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1 Ustawy o ochronie danych osobowych, tzn. zgodę osoby, której dane dotyczą, a także

art. 23 ust. 1 pkt 3 – jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, a także art. 23 ust. 1 pkt 5 – prawnie usprawiedliwione cele realizowane przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

7. Wnioski

Usługi geolokalizacyjne bez wątpienia na dobre zadomowiły się w naszym codziennym życiu. Pozwalają zaoszczędzić czas i ponoszone koszty zarówno w sferze prywatnej, biznesowej jak i publicznej. Wachlarz dostępnych usług pozwala dostosować nasze potrzeby do otaczającego nas świata. Jednak jak każda technologia, geolokalizacja wymaga poszanowania życia prywatnego każdej osoby fizycznej. Kluczowe zagrożenia dla użytkownika końcowego odnośnie ochrony danych osobowych stanowi połączenie braku przejrzystości oraz świadomości odnośnie przetwarzanych danych przez administratorów, którzy dzięki danym geolokalizacyjnym mają możliwość śledzenia osób z użyciem inteligentnych urządzeń przenośnych w różnych celach, począwszy od reklamy behawioralnej po monitorowanie dzieci. Nieodłączność urządzeń przenośnych i ich użytkowników, pozwala uzyskać dokładny wgląd w życie prywatne użytkowników. Jednym z największych zagrożeń jest brak świadomości użytkowników tych urządzeń o tym do kogo mogą trafić informacje o ich lokalizacji i w jakim celu mogą być wykorzystywane. O ile większość użytkowników zdaje sobie sprawę z tego, że informacje geolokalizacyjne dotyczące jego urządzenia przetwarzane są przez operatorów usług telekomunikacyjnych, tak nie wszyscy mają świadomość, że informacje te mogą trafiać również do administratorów aplikacji mobilnych z których korzystamy, czy osób z którymi się komunikujemy. Przykładem tej ostatniej sytuacji może być zdjęcie z danymi lokalizacyjnymi wysłane do osoby, z którą się komunikujemy, co pokazano na rys. 1.

Innym szczególnym zagrożeniem jest nie w pełni świadome wyrażenie przez użytkownika zgody na przetwarzanie jego danych geolokalizacyjnych. Pomijając fakt, że zgoda wyrażona przez użytkownika może być nieważna z uwagi na niezrozumiałość i nieaktualność informacji na temat kluczowych elementów przetwarzania danych geolokalizacyjnych przedstawionych użytkownikowi, zgoda wyrażona w określonych okolicznościach na potrzeby określonej usługi pozostawia włączoną funkcję geolokalizacji również po zakończeniu korzystania z niej.

W związku z wymienionymi wyżej wymaganiami, GR Art. 29 w swojej opinii dotyczącej przetwarzania danych geolokalizacyjnych zwróciła uwagę na zadania i obowiązki w zakresie ochrony danych geolokalizacyjnych adresowane do różnych stron. Za najważniejsze w tym zakresie strony uznano twórców systemów operacyjnych, dostawców aplikacji i osoby trzecie, takie jak administratorzy portali społecznościowych.

Ponieważ dane dotyczące lokalizacji, pochodzące z inteligentnych urządzeń przenośnych, ujawniają szczegółowe informacje osobiste na temat życia prywatnego właścicieli takich urządzeń, główną uzasadnioną podstawą do przetwarzania takich danych jest uprzednia świadoma zgoda, która nie może być utożsamiana z akceptacją warunków ogólnych korzystania z usługi. Musi dotyczyć konkretnie i odrębnie każdego celu, dla którego przetwarza się dane, w tym na przykład profilowania lub reklamy behawioralnej stosowanych przez administratora danych. Jeżeli nastąpi istotna zmiana celów przetwarzania danych, administrator danych musi ponownie uzyskać stosowną zgodę. Istotną koncepcją jakiej powinni trzymać się twórcy aplikacji jest idea domyślnej ochrony danych. Zgodnie z tą ideą usługi lokalizacji muszą być domyślnie wyłączone, a ewentualny mechanizm ich wyłączenia nie jest tożsamy z uzyskaniem świadomej zgody użytkownika.

W odniesieniu do mapowania punktów dostępowych Wi-Fi przedsiębiorstwa mogą mieć uzasadniony interes w obowiązkowym gromadzeniu i przetwarzaniu adresów MAC oraz obliczaniu lokalizacji punktów dostępowych Wi-Fi w celu świadczenia usług geolokalizacyjnych. Aby zachować równowagę między prawami administratora danych a prawami osoby, której dotyczą dane, administrator danych musi umożliwić łatwe i trwałe wycofanie się z bazy danych bez konieczności podawania dodatkowych danych osobowych.

Administrator danych powinien spełniać ustawowy obowiązek informacyjny w sposób jasny, wyczerpujący, zrozumiały dla szerokiego grona odbiorców, które nie ma wiedzy technicznej. Informacja ponadto ma być stale i łatwo dostępna, gdyż ważność zgody jest nierozzerwalnie związana z jakością informacji na temat usługi geolokalizacyjnej. Wyrażenie zgody na przetwarzanie danych geolokalizacyjnych ma szczególne znaczenie z punktu widzenia danych osobowych dziecka. Nierzetelne podejście do obowiązku informacyjnego przez administratora danych jak i w odniesieniu do dzieci przez rodzica, może rodzić pytanie czy ze społecznego punktu widzenia rozwój tego rodzaju usług, nie spowoduje, że jednostki od najmłodszych lat przyzwyczajane będą do niemal stałego monitorowania co może skutkować tym, że przestaną je postrzegać jako niepożądaną ingerencję w ich życie.

Administratorzy informacji geolokalizacyjnych z urządzeń przenośnych powinni umożliwiać swoim klientom dostęp do ich danych dotyczących lokalizacji w formacie czytelny dla człowieka oraz pozwalać na poprawianie i usuwanie niepotrzebnych danych osobowych.

Dostawcy aplikacji wykorzystujących funkcję geolokalizacji lub usług geolokalizacyjnych powinni wdrażać politykę przechowywania, która zapewnia usuwanie danych geolokalizacyjnych lub profili otrzymanych na podstawie takich danych po uzasadnionym okresie. Jeżeli twórca systemu operacyjnego lub administrator infrastruktury geolokalizacji przetwarza niepowtarzalny numer, taki jak adres MAC lub identyfikator UDID w odniesieniu do danych dotyczących lokalizacji, niepowtarzalny numer identyfikacyjny może być przechowywany wyłącznie do celów operacyjnych przez maksymalnie 24 godziny.

Reasumując, geolokalizacja ułatwia funkcjonowanie we współczesnym świecie, umożliwiając optymalizację czasu i ponoszonych kosztów. Dane geolokalizacyjne stanowią szczególny typ danych osobowych, albowiem umożliwiają poznanie nie tylko położenia osoby fizycznej, ale ich analiza pozwala wyodrębnić wiele innych danych osobowych, szczególnie chronionych przez prawo, takich jak informacje o życiu seksualnym, poglądy polityczne, filozoficzne, stan zdrowia, wyznanie czy informacje o nałogach. Dlatego też należy pamiętać o obowiązkach stron, podstawie przetwarzania danych, obowiązku informacyjnym, prawie osób, których dane dotyczą czy okresie przechowywania danych geolokalizacyjnych.

Z tych względów, w perspektywie przepisów RODO, konieczne jest dokonanie przeglądu obowiązującego ustawodawstwa pod kątem zapewnienia procesowi przetwarzania danych geolokalizacyjnych najwyższych standardów ochrony.