Stanisław Piątek*
Paweł Piątek**

Anonimizacja danych objętych tajemnicą telekomunikacyjną

Spis treści

Streszczenie

Celem artykułu jest ocena warunków wykorzystania zasobów danych towarzyszących telekomunikacji, przetwarzanych przez przedsiębiorców telekomunikacyjnych, do realizacji innych celów niż wykonywanie usług telekomunikacyjnych, w sposób, który nie narusza praw i interesów podmiotów tych danych. Artykuł zmierza do wykazania, że prawo polskie implementuje przepisy Unii Europejskiej dotyczące ochrony danych przetwarzanych w sektorze telekomunikacyjnym w sposób nieprawidłowy, ograniczając lub nawet eliminując dopuszczalność anonimizacji danych. W artykule dokonano analizy dopuszczalności anonimizacji danych dotyczących użytkowników, danych transmisyjnych, w tym danych lokalizacyjnych oraz danych o lokalizacji, służących do świadczenia usług o wartości wzbogaconej.

Słowa kluczowe: anonimizacja; prawo telekomunikacyjne; dane osobowe; dane transmisyjne; dane o lokalizacji.

I. Wprowadzenie

Informacje i dane są powszechnie traktowane jako odrębna kategoria zasobów, które mogą być wykorzystane w działalności gospodarczej oraz w różnych przedsięwzięciach publicznych podnoszących dobrobyt społeczny. Przedsiębiorcy telekomunikacyjni generują w związku z prowadzoną działalnością ogromne zasoby danych, które są produktem ubocznym obsługi procesów transmisji informacji pomiędzy użytkownikami usług. W celu obsłużenia procesu komunikacji, szczególnie pomiędzy użytkownikami znajdującymi się w ruchu, konieczne jest pozyskanie i przetworzenie

* Profesor, Kierownik Katedry Prawnych Problemów Administracji i Zarządzania Wydziału Zarządzania Uniwersytetu Warszawskiego; e-mail: piatek@supermedia.pl.

** Prawnik, współpracownik Cyfrowego Polsatu S.A.; e-mail: pawel-piatek@wp.pl.

wielu informacji, które można wykorzystać nie tylko w celu wykonania zasadniczej usługi telekomunikacyjnej, lecz także do innych celów społecznie użytecznych. Ponieważ dane towarzyszące komunikowaniu są bezpośrednio związane z prywatnością i autonomią informacyjną człowieka, podlegają ścisłej ochronie prawnej. Ochrona ta wynika z licznych aktów prawa międzynarodowego dotyczących podstawowych praw człowieka, z aktów prawnych Unii Europejskiej oraz z przepisów krajowych. Instytucją prawną służącą na poziomie prawa krajowego ochronie tych danych w sektorze telekomunikacyjnym jest instytucja tajemnicy telekomunikacyjnej. W takim zakresie, w jakim dane towarzyszące telekomunikacji są uznawane za dane osobowe, mogą być one chronione również przepisami o ochronie danych osobowych.

Celem artykułu jest ocena warunków wykorzystania zasobów danych towarzyszących telekomunikacji, przetwarzanych przez przedsiębiorców telekomunikacyjnych, do realizacji innych celów niż wykonywanie usług telekomunikacyjnych, w sposób, który nie narusza praw i interesów podmiotów tych danych. Zakres rozważań nie obejmuje tych przypadków, w których prawodawca legalizuje inny cel przetwarzania niż wykonanie usługi telekomunikacyjnej za względu na określony interes publiczny (np. retencja danych) lub interes podmiotu danych (np. przetwarzanie danych o lokalizacji w przypadku połączeń alarmowych). Artykuł dotyczy warunków takiego przetwarzania danych generowanych w działalności telekomunikacyjnej, które polega na ich anonimizacji, czyli pozbawieniu cech identyfikujących konkretnych użytkowników usług oraz wykorzystaniu tych danych do celu innego niż świadczenie usług telekomunikacyjnych[1].

Artykuł zmierza do wykazania, że prawo polskie implementuje przepisy Unii Europejskiej dotyczące ochrony danych przetwarzanych w sektorze telekomunikacyjnym w sposób nieprawidłowy, nadmiernie restrykcyjny, ograniczając lub nawet eliminując dopuszczalność anonimizacji danych. Nie przyczynia się to do podniesienia poziomu ochrony prywatności i autonomii informacyjnej użytkowników usług, a jednocześnie pogarsza pozycję konkurencyjną krajowych przedsiębiorców, utrudnia ich udział w przedsięwzięciach ogólnoeuropejskich dotyczących wykorzystania danych pochodzących z działalności telekomunikacyjnej, a ostatecznie ogranicza możliwość wykorzystania zanonimizowanych danych w celu podniesienia dobrobytu społecznego.

Realizacja powyższego zamiaru wymaga rozważań dwojakiego rodzaju. Po pierwsze, konieczna jest analiza podstaw i warunków prawnych anonimizacji tych danych na gruncie prawa Unii Europejskiej oraz w prawie krajowym, zidentyfikowanie rozbieżności i określenie niezbędnych dostosowań prawa krajowego. Elementem tych rozważań jest także ocena skutków anonimizacji dla możliwości wykorzystywania tych danych. Na tych zagadnieniach skoncentrowana jest analiza zawarta w niniejszym opracowaniu. Po drugie, konieczna jest analiza skutecznych sposobów dokonywania anonimizacji danych telekomunikacyjnych, co jest zagadnieniem z zakresu nauk technicznych oraz technik informacyjnych i wykracza poza zakres tego artykułu.

Anonimizacja danych jest zabiegiem, który przeprowadzony w sposób skuteczny i nieodwracalny pozwala na wykorzystanie ogromnych zasobów danych generowanych przy świadczeniu usług w sieciach telekomunikacyjnych przy jednoczesnym zachowaniu prywatności osób korzystających z tych usług oraz zapewnieniu im autonomii informacyjnej dotyczącej ich danych osobowych. Dane zanonimizowane mogą służyć realizacji zadań publicznych (np. projektowaniu przestrzeni publicznej z wykorzystaniem danych o przemieszczaniu się ludzi), a także mogą

[1] Por. cele anonimizacji danych osobowych w świetle „Opinion 05/2014 on Anonymisation Techniques", 10 kwietnia 2014, WP 126, s. 5.

być wykorzystane w celu świadczenia usług zaspokajających określone potrzeby społeczne (np. ostrzegania o zatorach drogowych) i stanowić źródło dodatkowego dochodu przedsiębiorcy telekomunikacyjnego. Anonimizacja może obejmować wszystkie rodzaje danych chronionych, przetwarzanych przez przedsiębiorców telekomunikacyjnych – dane transmisyjne, w tym dane lokalizacyjne; dane o lokalizacji i dane dotyczące użytkownika, które w pewnym zakresie są danymi osobowymi.

Dane zanonimizowane albo tracą charakter danych chronionych ustawą (dane osobowe), albo pozostają danymi określonego rodzaju, ale już zanonimizowanymi, co umożliwia ich przetwarzanie bez konieczności spełniania określonych warunków (np. bez zgody podmiotu danych) albo przetwarzanie ich do innych celów niż przed anonimizacją. Z reguły po anonimizacji ograniczenia w zakresie przetwarzania ulegają co najmniej znacznemu ograniczeniu, w niektórych obszarach ochrona zostaje całkowicie wyłączona. Środowisko elektroniczne, charakterystyczne dla sektora telekomunikacyjnego, szczególnie sprzyja anonimizacji, w odróżnieniu od środowisk usługowych lub urzędowych, w których dane są przetwarzane w postaci papierowej.

II. Dane chronione tajemnicą telekomunikacyjną

Punktem wyjścia do oceny dopuszczalności zastosowania anonimizacji, jako środka umożliwiającego przetwarzanie danych gromadzonych w sektorze telekomunikacyjnym do innych celów niż świadczenie usług telekomunikacyjnych, jest pojęcie tajemnicy telekomunikacyjnej. Tajemnica telekomunikacyjna jest bowiem główną instytucją służącą ochronie danych przetwarzanych przez przedsiębiorców telekomunikacyjnych. Analiza ochronnego oddziaływania tej instytucji jest szczególnie istotna z tego względu, iż tego rodzaju instytucja nie występuje w prawie Unii Europejskiej, które w sprawach ochrony danych osobowych i prywatności wyznacza minimalne wymagania dla prawa krajowego.

Zgodnie z art. 159 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2014 r., poz. 243, dalej: Pt) tajemnica telekomunikacyjna obejmuje dane dotyczące użytkownika; treść indywidualnych komunikatów; dane transmisyjne, w tym dane lokalizacyjne; dane o lokalizacji oraz dane o próbach uzyskania połączenia między zakończeniami sieci. Objęte ochroną dane dotyczące użytkowników obejmują zarówno użytkowników będących osobami fizycznymi, jak i użytkowników instytucjonalnych. W przypadku osób fizycznych dane dotyczące użytkowników są w większości danymi osobowymi, które przedsiębiorca pozyskuje przy zawieraniu i wykonywaniu umowy o świadczenie usług telekomunikacyjnych. Instytucja tajemnicy telekomunikacyjnej zapewnia tym danym dodatkową ochronę, gdyż jako dane osobowe podlegają one, co do zasady, ochronie przysługującej danym osobowym. Pozostałe rodzaje danych typowo telekomunikacyjnych podlegają ochronie wynikającej z tajemnicy telekomunikacyjnej, choć część z tych danych można również uznawać za dane osobowe, w świetle przepisów o ochronie danych osobowych.

Rozgraniczenie ochronnego oddziaływania przepisów dotyczących danych osobowych oraz przepisów sektorowych dotyczących telekomunikacji zostało ukształtowane w prawie krajowym w sposób istotnie odbiegający od ram wyznaczonych prawem unijnym. Na gruncie prawa UE, analizy pod tym kątem wymagają przepisy ogólne o ochronie danych, czyli dyrektywa 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 (Dz.U. L 281

z 23.11.1995, s. 31 ze zm.) (dalej: dyrektywa 95/46/WE). Sektorowa ochrona danych przetwarzanych w telekomunikacji wynika z dyrektywy 2002/58/WE o prywatności i łączności elektronicznej[2] (dalej: dyrektywa 2002/58/WE). Relacje między ochroną wynikającą z unijnych przepisów ogólnych i sektorowych wyjaśnia motyw 10 dyrektywy 2002/58/WE, który postanawia, że w „sektorze łączności elektronicznej dyrektywę 95/46/WE stosuje się w szczególności do wszystkich spraw dotyczących ochrony podstawowych praw i wolności, które nie są szczegółowo objęte przepisami niniejszej dyrektywy, włączając zobowiązania nałożone na kontrolera oraz prawa jednostek". Dyrektywę sektorową należy zatem stosować do ochrony praw i wolności objętych przepisami dyrektywy sektorowej, natomiast przepisy dyrektywy 95/46/WE o ochronie danych należy stosować w sprawach pozostałych.

Prawo krajowe zawiera rozstrzygnięcie idące w innym kierunku. Przepis art. 159 ust. 1 pkt 1 Pt poddaje ochronie wynikającej z tajemnicy telekomunikacyjnej wszystkie dane o użytkowniku przetwarzane przez przedsiębiorcę telekomunikacyjnego. Objęcie tych danych tajemnicą telekomunikacyjną powoduje, że można je przetwarzać jedynie w przypadkach określonych w art. 159 ust. 2 Pt, a zatem, gdy przetwarzanie jest przedmiotem usługi lub jest niezbędne do jej wykonania, gdy następuje za zgodą nadawcy lub odbiorcy, których te dane dotyczą, służy zapewnieniu dowodów transakcji handlowej lub celów łączności w działalności handlowej lub gdy jest konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi. Taka konstrukcja tajemnicy telekomunikacyjnej w odniesieniu do danych o użytkowniku, uniemożliwia lub co najmniej utrudnia wykorzystanie ogólnych tytułów do przetwarzania danych osobowych wynikających z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014, poz. 1182; dalej: uodo). Dotyczy to w szczególności takiego tytułu, jak wypełnienie prawnie usprawiedliwionego celu realizowanego przez administratora danych, gdy przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Wzmocnienie ochrony sektorowej danych osobowych na gruncie przepisów krajowych następuje na skutek stosowania reguły wynikającej z art. 5 uodo, zgodnie z którą, jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw. Ochrona wynikająca z Pt, na skutek stosowania przepisów o tajemnicy telekomunikacyjnej, które zakazują przetwarzania innego niż wyraźnie przewidziane w Pt, ma silniejszy skutek ochronny niż wynika z przepisów uodo. Nawet zawarte w art. 159 ust. 2 pkt 4 Pt odesłanie do innych przepisów ustawowych i odrębnych nie będzie skuteczne w odniesieniu do uodo, ze względu na treść art. 5 uodo.

Niepewność po stronie praktyki co do zakresu zastosowania przepisów Pt i uodo pogłębiają rozbieżne oceny przedstawiane w literaturze. J. Barta, P. Fajgielski i R. Markiewicz reprezentują pogląd, że niektóre przepisy ustawy – Prawo telekomunikacyjne przewidują dalej idącą ochronę niż przepisy uodo, co powoduje wyłączenie stosowania części przepisów uodo. Jednocześnie przyznają, że w niektórych kwestiach szczegółowych ocena w tym zakresie jest niezwykle trudna i z pewnością można stwierdzić jedynie, że ochrona ta jest inaczej ukształtowana[3]. Na trudności w ocenie sformułowania „dalej idąca ochrona" wskazują również P. Barta i P. Litwiński, którzy jednocześnie stwierdzają, że normy regulacji sektorowych zawierają, co do zasady, przepisy

[2] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37 ze zm.).

[3] J. Barta, P. Fajgielski, R. Markiewcz, *Ochrona danych osobowych. Komentarz*, Wolters Kluwer Polska – LEX, Warszawa 2011, s. 263.

przewidujące dalej idącą ochronę[4]. Uznają oni, że jeżeli przepis o charakterze szczególnym uzupełnia lub rozszerza obowiązki przewidziane w uodo, wówczas przepisy tej ustawy powinny być stosowane. Natomiast odnośnie do aspektów przetwarzania danych osobowych, których ustawa sektorowa nie reguluje, należy stosować przepisy uodo. Odnosząc się do kwestii przetwarzania danych o abonentach będących osobami fizycznymi określonych w art. 161 Pt, wypowiadają się przeciwko możliwości oparcia tego przetwarzania na przepisach uodo, gdyż prowadziłoby to do obniżenia standardów w zakresie ochrony danych[5]. P. Fajgielski, rozpatrując relację między ochronnym oddziaływaniem przepisów uodo i Pt, uznaje, że z art. 5 uodo wynika zasada prymatu przepisów przewidujących większy poziom ochrony, niezależnie od tego czy właściwe przepisy znajdują się w ustawie ogólnej (uodo), czy w regulacjach szczegółowych (Pt). Wyprowadza z tej zasady obowiązek stosowania przez administratorów danych w poszczególnych sektorach przepisów uodo, gdy przepisy sektorowe nie zawierają odpowiednich regulacji. Natomiast tam, gdzie trzeba ustalać czy przepisy sektorowe przewidują ocenę „dalej idącą" jest to zadanie niezwykle trudne[6].

Na skutek włączenia danych dotyczących użytkowników w obręb tajemnicy telekomunikacyjnej i ustanowienia wyraźnych zakazów naruszania tej tajemnicy, poza przypadkami wyraźnie przewidzianymi w Pt, przetwarzanie przez przedsiębiorców telekomunikacyjnych danych użytkowników bezpośrednio na podstawie uodo wiąże się z poważnym ryzykiem. Wydaje się, że ryzyko to można wyeliminować w obecnym stanie prawnym tylko działaniami legislacyjnymi.

Ochrona danych transmisyjnych, danych lokalizacyjnych i danych o lokalizacji za pomocą przepisów o tajemnicy telekomunikacyjnej nie budzi zastrzeżeń i pokrywa się z zakresem ochronnego zastosowania przepisów dyrektywy 2002/58/WE. Rozbieżności pomiędzy prawem unijnym i prawem krajowym występują natomiast w sprawach dopuszczalności anonimizacji tych danych.

III. Podstawy prawne anonimizacji danych w prawie unijnym i krajowym

Anonimizacja jest jedną z operacji na danych podlegających ochronie, które są przewidziane przepisami unijnymi dotyczącymi tej ochrony.

Na gruncie unijnego prawa ochrony danych osobowych motyw 26 dyrektywy 95/46/WE stwierdza, że „zasady ochrony danych nie mają zastosowania do danych, którym nadano anonimowy charakter w taki sposób, że podmiot danych nie będzie mógł być zidentyfikowany; zasady postępowania w rozumieniu art. 27 mogą być przydatnym instrumentem w udzielaniu wskazówek co do sposobów nadawania danym charakteru anonimowego oraz zachowania w formie, w której identyfikacja osoby, której dane dotyczą, nie jest dłużej możliwa".

Dyrektywa 2002/58/WE w motywie 26 stwierdza, że „dane dotyczące ruchu wykorzystywane w marketingu usług komunikacyjnych lub dostarczenia usług tworzących wartość dodaną powinny również zostać usunięte lub uczynione anonimowymi po dostarczeniu usług". Przepis art. 6 ust. 1 tej dyrektywy stanowi, że „dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności

[4] P. Barta, J. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, C.H. Beck, Warszawa 2013, s. 56.

[5] P. Barta, J. Litwiński, Ustawa…,. s. 60.

[6] P. Fajgielski, *Ochrona danych osobowych w telekomunikacji – aspekty prawne*, Lubelskie Towarzystwo Naukowe, Lublin 2002, s. 222.

elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu (…)". Przepis ten jest bardzo istotny, gdyż potwierdza możliwość anonimizacji nie tylko danych dotyczących lokalizacji, którym poświęcony jest art. 9 tej dyrektywy, lecz także wszelkich danych transmisyjnych, czyli danych o ruchu, zgodnie z terminologią unijną. Wskazuje on na konieczność usunięcia lub anonimizacji danych, których przetwarzanie nie korzysta już z podstaw przewidzianych dyrektywą. Można z tego sformułowania wnioskować, że ochronny efekt usunięcia i anonimizacji danych o ruchu powinien być porównywalny, choć poszczególne przepisy dotyczące anonimizacji mogą prowadzić do odmiennego wniosku. Zasadność i dopuszczalność anonimizacji danych transmisyjnych, jak najszybciej po wytworzeniu i zgromadzeniu tych danych, potwierdza opinia Grupy Roboczej ds. Artykułu 29 w związku z doświadczeniami duńskiego organu ochrony danych osobowych analizującego praktyki przetwarzania danych transmisyjnych czterech operatów sieci komórkowych[7].

Szczególny przepis dyrektywa 2002/58/WE poświęca anonimizacji danych dotyczących lokalizacji. Przepis art. 9 ust. 1 dyrektywy 2002/58/WE dotyczący usług o wartości wzbogaconej stanowi, że „[w] przypadku gdy dane dotyczące lokalizacji inne niż dane o ruchu, odnoszące się do użytkowników lub abonentów publicznych sieci łączności lub publicznie dostępnych usług łączności elektronicznej, mogą być przetwarzane, przetwarzanie może mieć miejsce tylko wówczas, gdy dane te są anonimowe lub za zgodą użytkowników, lub abonentów, w zakresie i przez okres niezbędny do świadczenia usługi tworzącej wartość dodaną".

W prawie krajowym przepisy ustawowe przewidują w pewnym zakresie anonimizację danych przetwarzanych w sektorze telekomunikacyjnym. Ustawa Pt przewiduje w art. 166 ust. 1 pkt 2 anonimizację danych o lokalizacji jako środek legalizujący wykorzystywanie tych danych bez konieczności uzyskiwania zgody podmiotu danych. Jest to jednak jedyny przepis w Pt dotyczący w sposób wyraźny anonimizacji danych o typowo telekomunikacyjnym charakterze. Anonimizację przewiduje również art. 2 ust. 3 uodo, w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji. Do takich danych mają zastosowanie jedynie przepisy rozdziału 5 uodo, czyli przepisy o zabezpieczeniu danych osobowych.

Porównanie przepisów o anonimizacji w prawie unijnym i krajowym dotyczącym sektora telekomunikacyjnego wskazuje, że prawo krajowe odbiega w pewnym zakresie od unijnego wzorca. Podstawowa różnica dotyczy braku w prawie krajowym przepisu przewidującego możliwość anonimizacji danych transmisyjnych, a w konsekwencji także danych lokalizacyjnych wskazujących położenie geograficzne urządzenia końcowego użytkownika usług publicznych przetwarzanych dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne. Dyrektywa 2002/58/WE traktuje anonimizację tych danych za operację równoważną ich usunięciu, tworzy podstawę do ich przetwarzania i w pełni legalizuje taką operację na głównym zasobie danych przetwarzanych przez przedsiębiorców telekomunikacyjnych. Natomiast ustawa krajowa w ogóle nie przewiduje takiej możliwości. Ze względu na zasadę dopuszczającą w art. 159 ust. 2 Pt tylko operacje przetwarzania danych wyraźnie dopuszczone

[7] Opinion 05/2014 on Anonymisation Techniques, WP 216, s. 8.

przepisami, w praktyce eliminuje to możliwość anonimizacji danych transmisyjnych, w tym danych lokalizacyjnych w celu dalszego ich przetwarzania.

W odniesieniu do danych osobowych przetwarzanych w sektorze telekomunikacyjnym różnica pomiędzy prawem krajowym i unijnym wynika z poddania przetwarzania tych danych przepisom o tajemnicy telekomunikacyjnej, a nie przepisom o ochronie danych osobowych. Z dyrektywy 95/46/WE wynika, że anonimizacja wyłącza dane poddane uprzednio ochronie przysługującej danym osobowym z zakresu tej ochrony. Na gruncie prawa krajowego wniosek taki można wyprowadzić z definicji danych osobowych w art. 6 ust. 1 uodo, z której wynika, że za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zastosowanie tego wniosku do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego zderza się z przepisami o tajemnicy telekomunikacyjnej wzmocnionych przepisem art. 5 uodo, wyłączającym zastosowanie ogólnych przepisów o ochronie danych osobowych ze względu na zastosowanie szczególnej ochrony wynikającej z przepisów Pt.

Największą zgodność można stwierdzić w odniesieniu do „danych o lokalizacji" w rozumieniu art. 159 ust. 1 pkt 4 Pt oraz „danych dotyczących lokalizacji innych niż dane o ruchu" w rozumieniu art. 9 ust. 1 dyrektywy2002/58/WE. Obydwa przepisy przewidują możliwość anonimizacji danych, która jest alternatywną w stosunku do zgody abonenta podstawą przetwarzania tych danych. Kwestią wymagającą dalszych rozważań jest natomiast zakres dopuszczalnego przetwarzania zanonimizowanych danych o lokalizacji, gdyż zarówno w prawie unijnym, jak i krajowym, przetwarzanie takich zanonimizowanych danych poddane jest istotnym ograniczeniom.

Nie ulega wątpliwości, że anonimizacja jest jedną z operacji przetwarzania danych chronionych, a zatem konieczne jest wykazanie podstawy prawnej dla jej przeprowadzenia. Niekiedy jest ona zrównywana z operacją usunięcia danych, ale skutek anonimizacji nie jest tak radykalny. Anonimizacja danych osobowych jest jedną z form „dalszego przetwarzania danych" w rozumieniu uodo (*further processing*), a zatem podstawy anonimizacji można się doszukiwać we wszystkich legalnych celach przetwarzania danych przewidzianych ustawą. Taki wniosek formułuje na gruncie dyrektywy 95/46/WE Grupa Robocza ds. Artykułu 29 w odniesieniu do celów wymienionych w art. 7 tej dyrektywy, pod warunkiem zachowania wszystkich wymagań dotyczących ograniczenia celu przetwarzania[8]. W swojej opinii Grupa Robocza formułuje również wniosek dalej idący, iż z zasady ograniczenia czasowego przetwarzania danych dla celów, dla których je zebrano, wynika konieczność co najmniej anonimizacji, o ile nie usunięcia danych po upływie uzasadnionego okresu ich przetwarzania. Na gruncie Pt anonimizacja danych chronionych tajemnicą telekomunikacyjną musi być wyraźnie przewidziana, gdyż operacje nieprzewidziane w ustawie są jednoznacznie zakazane. Brak wyraźnego przepisu o anonimizacji danych transmisyjnych w Pt stanowi zatem poważną przeszkodę ze względu na konstrukcję tajemnicy telekomunikacyjnej.

IV. Charakter prawny anonimizacji danych chronionych

Ani przepisy unijne, ani przepisy krajowe w zakresie telekomunikacji i ochrony danych osobowych nie definiują anonimizacji, nie wskazują też technik anonimizacyjnych. Prawidłowe ustalenie czym jest anonimizacja wymaga ustalenia co podlega ochronie, gdyż anonimizacja polega głównie na pozbawieniu informacji tych elementów, ze względu na które zapewniono im

[8] Opinion 05/2014…, s. 7.

ochronę. Jest to widoczne szczególnie wyraźnie w przypadku danych osobowych, gdyż co do zasady, anonimizacja prowadzi do pozbawienia informacji cech charakteryzujących dane osobowe. Identyfikowalność osoby fizycznej i anonimizacja to przeciwstawne stany faktyczne powiązane w taki sposób, że możliwość identyfikacji wyklucza anonimowość. Dlatego punktem wyjścia do ustalenia czym jest anonimizacja jest dyskusja nad tym, jakie cechy posiadają dane chronione (osobowe, transmisyjne, lokalizacyjne, dane o lokalizacji), których wyeliminowanie prowadzi do wyłączenia lub co najmniej ograniczenia ochrony. Podstawą do takich ustaleń są każdorazowo definicje danych osobowych (art. 6 uodo), danych transmisyjnych, w tym danych lokalizacyjnych (art. 159 ust. 1 pkt 3 Pt) oraz danych o lokalizacji (art. 159 ust. 1 pkt 4 Pt).

Przepisy uodo i Pt, nawet jeżeli przewidują anonimizację, to jej nie definiują. Okrojoną definicję anonimizacji, dostosowaną do specyfiki świadczenia usług drogą elektroniczną, zawiera art. 19 ust. 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz.1422; dalej: uśude). Zgodnie z tym przepisem anonimizacja danych polega na usunięciu wszelkich oznaczeń identyfikujących usługobiorcę lub zakończenie sieci telekomunikacyjnej albo system teleinformatyczny, z którego korzystał usługobiorca. Szczegółowe reguły anonimizacji orzeczeń sądowych określa załącznik nr 5 do zarządzenia Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej (Dz. Urz. MS 2003, Nr 5, poz. 22 ze zm.). Zarządzenie określa w sposób szczegółowy sposób anonimizacji poszczególnych rodzajów danych (imion i nazwisk osób fizycznych, nazw osób prawnych i instytucji, znaków i numerów identyfikujących, ulic i miejscowości).

Definicję anonimizacji zawiera norma ISO 29100:2011, która uznaje, że jest to proces, w wyniku którego informacja identyfikująca personalnie zostaje nieodwracalnie zmieniona w taki sposób, że podmiot informacji identyfikującej personalnie nie może być już zidentyfikowany pośrednio lub bezpośrednio ani samodzielnie przez administratora informacji personalnej, ani we współpracy z jakimkolwiek innym podmiotem[9]. W opinii Grupy Roboczej ds. Artykułu 29 stwierdzono, że „dane anonimowe" w rozumieniu dyrektywy można zdefiniować jako wszelkie informacje dotyczące osoby fizycznej, która jest niemożliwa do zidentyfikowania przez administratora danych lub inną osobę, „biorąc pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania tej osoby". Dane, którym nadano anonimowy charakter „są danymi anonimowymi, które wcześniej dotyczyły osoby możliwej do zidentyfikowania, lecz której zidentyfikowanie nie jest już możliwe"[10]. W opinii z roku 2014 Grupa Robocza ds. Artykułu 29 wyprowadziła definicję anonimizacji z motywu 26 dyrektywy 95/46/WE, zgodnie z którym wszelkie dane zanonimizowane muszą być pozbawione elementów wystarczających do identyfikacji podmiotu danych. W szczególności, dane te muszą być przetwarzane w taki sposób, że nie można już na ich podstawie zidentyfikować osoby fizycznej poprzez użycie wszelkich rozsądnych środków możliwych do wykorzystania zarówno przez administratora danych, jak i przez osobę trzecią[11]. W opinii tej stwierdzono, że podstawową cechą anonimizacji z perspektywy celu ochrony danych osobowych jest osiągnięcie stanu tak trwałego, jak w wyniku usunięcia danych[12].

[9] *Anonymization – process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party*. IS ISO/IEC29100, 2011-12-15, Information technology – Security techniques – Privacy framework.

[10] Opinia 4/2007 w sprawie pojęcia danych osobowych, WP 136, s. 21.

[11] Opinion 05/2014…, s. 5.

[12] Ibidem, s. 6.

W literaturze uznaje się, że anonimizacja danych osobowych polega na dokonaniu takich operacji, które powodują pozbawienie informacji cech osobowych. Zdaniem P. Barty i P. Litwińskiego anonimizacja w praktyce odpowiada dokonaniu takich operacji, które polegają na usunięciu części informacji o charakterze osobowym, umożliwiających połączenie pozostałych informacji z konkretną osobą fizyczną. Zdaniem tych autorów anonimizacja (w odróżnieniu od usunięcia danych) skutkuje możliwością dalszego dokonywania operacji na części informacji, które samodzielnie i łącznie nie umożliwiają zidentyfikowania tożsamości konkretnej osoby fizycznej[13]. A. Drozd uznaje, że anonimizacja oznacza taką operację na danych osobowych, która powoduje, że określenie tożsamości osoby, której dane dotyczą, wymagałoby nadmiernych kosztów, czasu lub działań[14]. D. Korff określa dane „anonimowe" jako dane, które nie mogą być powiązane z konkretną osobą fizyczną. Dane „zanonimizowane" to dane, które wcześniej były powiązane z taką osobą, ale obecnie nie mogą być wiązane z tą osobą[15]. Sposób podejścia do anonimizacji w państwach członkowskich UE, głównie od strony możliwych sposobów rozumienia danych pozwalających na identyfikację (*identifiable information*), referują według stanu z końca lat 90. J.R. Reidenberg i P.M. Schwartz[16]. Urząd Komisarza ds. Informacji w Wielkiej Brytanii uznaje za dane zanonimizowane takie dane, które same nie pozwalają na zidentyfikowanie jakiejkolwiek osoby fizycznej, a także nieprawdopodobne jest, aby umożliwiały identyfikację osoby fizycznej poprzez zestawienie ich z innymi danymi[17]. W dyskusjach praktyków wskazuje się, że anonimizacja wymaga dokonania takich operacji na identyfikatorach osób fizycznych, które polegają na ich usunięciu, ukryciu, zagregowaniu lub zmianie[18].

W sumie z przytoczonych wyżej stanowisk można wyprowadzić wniosek, że anonimizacja polega na pozbawieniu chronionej informacji takiej zawartości, która pozwala na powiązanie tej informacji z konkretną osobą za pomocą możliwych i uzasadnionych środków.

Dyskusja nad istotą anonimizacji powinna uwzględniać okoliczności przetwarzania danych, gdyż dane anonimowe dla jednego podmiotu, mogą stracić cechę anonimowości w zestawieniu z danymi, jakie posiada inny podmiot. Dlatego koniecznym etapem procesu anonimizowania danych chronionych jest ocena dostępności innych danych oraz środków, które mogą być wykorzystane przez inne osoby lub organizacje, w szczególności użytkowników Internetu do reidentyfikacji podmiotów, których dane są chronione. Dotyczy to reidentyfikacji na podstawie danych posiadanych przez inne podmioty oraz danych dostępnych publicznie, np. publicznie dostępnych rejestrów. To może być trudne do prawidłowej oceny w środowisku danych cyfrowych, dostępnych w Internecie, do których dostęp ma nieograniczona liczba osób. Szczególnie trudno jest ocenić prawdopodobieństwo pojawienia się w przyszłości nowych danych pozwalających na reidentyfikację. Dlatego kwestia „względności" (relatywności) anonimizacji w perspektywy dysponenta danych i podmiotów, które uzyskują dostęp do danych zanonimizowanych, jest stale obecna w dyskusjach.

13 P. Barta, P. Litwiński, Ustawa…, s. 99.

14 A. Drozd, *Zasada ograniczenia czasowego przetwarzania danych osobowych w świetle ustawy o ochronie danych osobowych*, [w:] G. Sibiga, X. Konarski (red.), Ochrona danych osobowych. Aktualne problemy i nowe wyzwania, Wolters Kluwer Polska S.A., Warszawa 2007, s. 146.

15 D. Korff, Working Paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, LRDP KANTOR Ltd, 2010, s. 48.

16 J.R. Reidenberg, P.M. Schwartz, Data Protection Law and On-line Services: Regulatory Responses. Raport przygotowany dla Komisji Europejskiej, s. 134–135.

17 Anonymisation: managing data protection risk, Code of practice. Information Commisioner's Office, s. 6. Pobrano z: http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

18 About Anonymisation: for data about people. Pobrano z: http://www.ukanon.net/

W literaturze dotyczącej przetwarzania danych osobowych wskazuje się, że uzasadnione jest odmienne kwalifikowanie informacji dotyczącej osoby fizycznej w zależności od tego, kto daną informację przetwarza. Informacja może mieć charakter osobowy dla jednego podmiotu, będącego administratorem danych osobowych, ale nie będzie miała tego charakteru dla odbiorcy danych. Przytaczany jest w związku z tym przykład przekazywania danych o numerze telefonu do celów marketingowych przez przedsiębiorcę telekomunikacyjnego, dla którego jest to informacja o charakterze osobowym, natomiast nie ma ona takiego charakteru dla odbiorców tej informacji[19].

Precyzyjnie określenie okoliczności, których wystąpienie powoduje, że identyfikacja podmiotu danych nie jest już możliwa, jest bardzo trudne i zawsze wymaga uwzględniania specyfiki środowiska informacyjnego, w którym dane są przetwarzane. Ryzyko reidentyfikacji musi być rozpatrywane nie tylko z uwzględnieniem dostępu innych podmiotów do danych zanonimizowanych, lecz także z uwzględnieniem czynnika czasu. Podkreśla się, że szybki postęp technologii przetwarzania danych może spowodować dezaktualizację ustaleń dotyczących skuteczności anonimizacji danych. Motyw 26 dyrektywy 95/46/WE wskazuje, że „w celu ustalenia czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby". Sformułowanie to jest więc otwarte na wszelkie dostępne techniki przetwarzania, zestawiania i porównywania danych, samodzielnie przez dysponenta danych, jak i we współpracy z innymi podmiotami. Ze względu na występujące ryzyko reidentyfikacji podmiotu danych Grupa Robocza ds. Artykułu 29 podkreśla, że anonimizacja powinna być nieodwracalna[20].

Mimo istniejących trudności opinia 5/2014 Grupy Roboczej wskazuje jednak okoliczności, które należy uwzględniać przy ocenie kwestii nieodwracalności anonimizacji. Dokonując anonimizacji, podmiot dysponujący danymi powinien zwrócić uwagę na możliwe techniki reidentyfikacji podmiotów danych, ocenić wykonalność i prawdopodobieństwo zastosowania takich technik, ocenić zagrożenia ze strony różnych podmiotów zainteresowanych przełamaniem bariery anonimizacyjnej w dostępie do danych. Oceniając możliwość reidentyfikacji, należy uwzględnić wykonalne operacje zestawiania różnych danych w przetworzonym zbiorze albo zestawiania danych z różnych przetworzonych zbiorów. Jeżeli dostępny jest zbiór danych, który zestawiony z danymi zanonimizowanymi pozwala na reidentyfikację osób fizycznych, to takie dane nie mogą być uznane za dane zanonimizowane. Nie jest przy tym istotna intencja podmiotu przetwarzającego, ale obiektywna możliwość identyfikacji podmiotu danych na podstawie zbioru danych. Specjalnej uwagi wymagają przypadki przekazywania danych zanonimizowanych do wykorzystania innym podmiotom, szczególnie gdy warunki ich wykorzystywania umożliwiają zestawianie tych danych z innymi informacjami[21]. Możliwość reidentyfikacji ocenia się w taki sam sposób dla podmiotu dysponującego danymi, jak dla podmiotów trzecich, które otrzymują dane poddane anonimizacji.

Ocena skuteczności anonimizacji powinna być dokonywana zarówno z perspektywy administratora danych, jak i innych podmiotów posługujących się danymi zanonimizowanymi. Wymóg

[19] P. Litwiński, *Udostępnianie danych osobowych w ustawie o ochronie danych osobowych*, [w:] G. Sibiga, X. Konarski (red.), Ochrona danych osobowych…, s. 125.

[20] Opinion 05/2014…, s. 5.

[21] A. Cavoukian, *Looking Forward: De-identification Developments – New Tools*, New Challenges, Information & Privacy Commissioner, Ontario, Canada, May 2013.

braku identyfikowalności osoby fizycznej na podstawie zanonimizowaych danych odnosi się tak do administratora danych, jak i do osób trzecich, które posługują się danymi zanonimizowanymi.

W przypadku, gdy podmiot przetwarzający nie usuwa elementów identyfikujących już w fazie zdarzenia generującego dane (np. zdarzeń sieciowych) i zachowuje część danych identyfikujących, ogranicza się do maskowania danych identyfikujących, pozostawia do swojej dyspozycji dane pierwotne, to zestawu danych otrzymany w wyniku takich zabiegów nie można uznać za zestaw danych zanonimizowanych. W przypadku, gdy podmiot przetwarzający dokona takiej nieodwracalnej agregacji danych, że na poziomie danych zagregowanych identyfikacja poszczególnych podmiotów jest rzeczywiście niemożliwa, wówczas można uznać, iż identyfikacja została dokonana prawidłowo[22].

Dyskusje prowadzone w literaturze, a także w środowiskach praktyków, wskazują że anonimizacja pełna jest niewątpliwie możliwa, choć jej następstwem może się okazać nieprzydatność danych do przetwarzania w zamierzonym celu. W przypadku anonimizacji bardzo często wystąpi konieczność wyważenia stopnia anonimizacji, tak aby zanonimizowane dane były przydatne do realizacji celu (gospodarczego, badawczego), co wymaga odpowiedniej zawartości informacyjnej, a jednocześnie aby zostały pozbawione cech, które są przesłanką ochrony (danych osobowych, transmisyjnych, lokalizacyjnych).

V. Warunki i skutki anonimizacji danych chronionych

Na gruncie przepisów uodo skutki anonimizacji określono wyraźnie jedynie w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, które po ich wykorzystaniu zostaną poddane anonimizacji (art. 2 ust. 3 uodo). W świetle dyrektywy 95/46/WE do danych zanonimizowanych, które uprzednio stanowiły dane osobowe, nie stosuje się przepisów o ochronie danych osobowych. Niektóre oceny dotyczące skutków anonimizacji idą bardzo daleko w kierunku dopuszczenia różnych sposobów korzystania z takich danych. W opinii brytyjskiego organu do spraw ochrony danych publikacja takich zanonimizowanych danych przez administratora nie podlega ograniczeniom wynikającym z ustawodawstwa o ochronie danych osobowych, nawet wówczas, gdy administrator dysponuje informacjami pozwalającymi na reidentyfikację osób fizycznych objętych danymi zanonimizwoanymi[23]. W literaturze podejmowane są jednak również rozważania czy anonimizacja całkowicie wyłącza zanonimizowane dane z reżimu ochrony danych osobowych, czy też jedynie ogranicza zastosowanie przepisów dotyczących wykonywania obowiązku zapewniania dostępu do danych, prawa do ich korygowania oraz obowiązków informacyjnych w stosunku do podmiotu danych[24].

W sektorze telekomunikacyjnym zastosowanie anonimizacji do danych użytkowników będących osobami fizycznymi napotyka przeszkodę wynikającą z włączenia danych o użytkownikach do zakresu danych chronionych tajemnicą telekomunikacyjną. Przepisy chroniące tajemnicę telekomunikacyjną przewidują anonimizację jedynie w odniesieniu do danych o lokalizacji. Dopiero oparcie operacji przetwarzania danych o użytkownikach na przepisach uodo otwierałoby drogę

[22] Opinion 05/2014…, s. 9.

[23] Anonymisation: managing data protection risk…, s. 13.

[24] J.A. Reidenberg, P. M. Schwartz, Data Protection…, s. 27.

do anonimizacji tych danych, które następnie mogłyby zostać wykorzystane do innych celów niż zostały pierwotnie zgromadzone. Wydaje się, że obecnie anonimizacja danych osobowych abonentów i użytkowników końcowych usług telekomunikacyjnych, przetwarzanych przez przedsiębiorcę telekomunikacyjnego, w celu wykorzystania ich do innych celów niż pierwotnie zostały zgromadzonej nie jest dopuszczalna. Przedsiębiorcy telekomunikacyjni mogą jedynie usuwać te dane po zakończeniu okresów, w których mogą przetwarzać te dane.

W sposób wyraźny anonimizację danych o lokalizacji przewiduje art. 166 ust. 1 Pt, który w celu wykorzystania danych o lokalizacji wymaga od dostawcy albo uzyskania zgody podmiotu danych, albo dokonania anonimizacji tych danych. W przypadku anonimizacji danych o lokalizacji na podstawie art. 166 ust. 1 pkt 2 Pt, dane nie tracą charakteru danych o lokalizacji w rozumieniu Pt, a jedynie zmienia się podstawa prawna do ich przetwarzania. Po anonimizacji można przetwarzać dane o lokalizacji bezpośrednio na podstawie ustawy, natomiast przed anonimizacją potrzebna jest zgoda abonenta lub użytkownika końcowego na przetwarzanie. Anonimizacja danych o lokalizacji może być osiągnięta przez zwiększenie obszaru, co zwiększy liczbę podmiotów i obiektów generujących dane, ograniczenie częstotliwości publikacji, co prowadzi do zwiększenia liczby zdarzeń, ograniczenie danych (np. obcięcie adresów IP), unikanie informacji lokalizacyjnej na poziomie terminala abonenta lub innych lokalizowanych urządzeń itp.[25].

Na kolejnym etapie mamy jednak do czynienia z zanonimizowanymi danymi o lokalizacji użytkownika sieci lub usług telekomunikacyjnych. Z art. 166 ust. 1 Pt wynika, że takie zanonimizowane dane, pozostają danymi o lokalizacji, z tym że na ich podstawie nie można zidentyfikować podmiotu danych, ale można ustalić jego położenie geograficzne z mniejszą lub większą precyzją albo położenie większych grup tych podmiotów. To powoduje, że ma do nich zastosowanie przepis art. 166 ust. 4 Pt, zgodnie z którym dane o lokalizacji mogą być przetwarzane wyłącznie dla celów niezbędnych do świadczenia usług o wartości wzbogaconej. Taki wynik wykładni językowej art. 166 Pt został potwierdzany w literaturze przez P. Koralewskiego[26]. Wydaje się, że analogiczny wniosek można sformułować na gruncie wykładni językowej cytowanego wyżej art. 9 dyrektywy 2002/58/WE. Zatem również po anonimizacji dane o lokalizacji mogą być wykorzystywane tylko do świadczenia usługi tworzącej wartość dodaną. Na świadczenie tych usług konieczna jest zgoda usługobiorcy, będącego użytkownikiem lokalizowanego urządzenia (np. telefonu) lub dysponentem takiego urządzenia (np. właściciel lokalizowanego środka transportu). Anonimizacja danych o lokalizacji, zwalniająca z konieczności uzyskiwania zgody na przetwarzanie danych o lokalizacji, jest w praktyce zastępowana zamówieniem na świadczenie usługi o wartości wzbogaconej z wykorzystaniem zanonimizowanych danych o lokalizacji. Zatem sama anonimizacja danych o lokalizacji nie zwalnia przedsiębiorcy telekomunikacyjnego z obowiązku uzyskania zgody na wykorzystanie tych danych do świadczenia usług o wartości wzbogaconej dla podmiotu danych.

Inne wnioski można wyprowadzić z analizy opinii Grupy Roboczej ds. Artykułu 29. W opiniach Grupy Roboczej wskazuje się na wykorzystanie danych o lokalizacji dla różnych celów, które nie są związane ze świadczeniem usługi dla podmiotu danych o lokalizacji. Przykładowo, opinia w sprawie usług geolokalizacji za pomocą urządzeń przenośnych typu smart wskazuje, że dane ze stacji bazowych GSM mogą być wykorzystywane w sposób innowacyjny do wykrywania

[25] Anonymisation: managing…, s. 32.

[26] P. Koralewski, *Usługi oparte na przetwarzaniu danych geograficznych*, iKAR 2012, nr 6(1), s. 70.

zatorów drogowych, na podstawie analizy przenoszenia terminali do kolejnych stacji bazowych w świetle przewidywanej szybkości przemieszczania się na drodze w poszczególnych porach dnia[27]. Ponieważ do wytworzenia takiej informacji muszą być przetwarzane dane o lokalizacji dużej liczby terminali, a nie tylko o lokalizacji osób korzystających z usługi informacji o zatorach drogowych, oznacza to, że przetwarzanie zanonimizowanych danych o lokalizacji nie ogranicza się do danych lokalizacyjnych użytkowników usługi. Z opinii wynika zatem możliwość zerwania zależności pomiędzy wykorzystaniem zanonimizowanych danych o położeniu podmiotu i świadczeniem usług wyłącznie na rzecz tego podmiotu.

Jednak w obecnym stanie prawnym ostrożna interpretacja art. 166 ust. 4 Pt i art. 9 ust. 1 dyrektywy 2002/58/WE przemawia za tym, aby zanonimizowane dane o lokalizacji podmiotów, które nie wyraziły zgody na przetwarzanie ich danych, były wykorzystane do świadczenia usług o wartości wzbogaconej tylko tym podmiotom. Wyraźne potwierdzenie, iż zanonimizowane dane o lokalizacji mogą być wykorzystane do świadczenia usług o wartości dodatkowej na rzecz innych podmiotów byłoby ważnym uzupełnieniem istniejącego stanu prawnego.

Anonimizacji mogą być poddane jedynie dane, które były przetwarzane legalnie przez przedsiębiorcę, w szczególności zostały uzyskane w sposób zgodny z prawem. Na gruncie prawa ochrony danych osobowych anonimizacja mieści się w pojęciu „dalszego przetwarzania", które z reguły wiąże się ze zmianą celu przetwarzania. Zatem „dalsze przetwarzanie" powinno być poprzedzone przetwarzaniem danych osobowych na podstawie jakiegokolwiek tytułu ustawowego lub na podstawie zgody podmiotu danych. Na gruncie przepisów dyrektywy 2002/58/WE uzasadniony jest podobny wniosek w odniesieniu do danych transmisyjnych (danych o ruchu) oraz danych dotyczących lokalizacji. Jakiekolwiek przetwarzanie danych transmisyjnych lub danych o lokalizacji może na kolejnym etapie przejść w fazę anonimizacji przetwarzanych danych, co będzie się łączyło ze zmianą podstawy prawnej przetwarzania i możliwością zmiany celu przetwarzania. Zgodnie z art. 6 ust. 1 dyrektywy 95/46/WE oraz art. 6 ust. 1 i art. 9 ust. 1 dyrektywy 2002/58/WE anonimizacja (albo usunięcie danych) są jednocześnie koniecznym etapem po wykonaniu czynności, do których dane niezanonimizowane były potrzebne, o ile nie występuje inny tytuł do przetwarzania, a w szczególności do przechowywania danych. Zatem w świetle prawa unijnego usunięcie lub anonimizacja są naturalnym etapem postępowania z danymi podlegającymi ochronie, które już zostały wykorzystane do celów realizowanych przez dysponenta danych. Ponieważ na usunięcie danych nie jest konieczne uzyskiwanie zgody podmiotu danych (art. 23 ust. 1 pkt 1 uodo), takie samo podejście należałoby zastosować do anonimizacji danych. Ustawa o ochronie danych osobowych zapewnia ochronę m.in. poprzez żądanie uzyskania zgody w tych przypadkach, gdy przetwarzanie danych może prowadzić do negatywnych następstw dla podmiotu danych. Usunięcie lub anonimizacja takich zagrożeń nie powoduje. Anonimizacja danych osobowych musi jednak być zgodna z zasadami przetwarzania danych osobowych. Pożądane jest także zapewnienie transparentności polityki przedsiębiorcy w sprawie anonimizacji danych podlegających ochronie. Nie musi to polegać na powiadamianiu podmiotów danych o anonimizacji danych. Może natomiast wyrażać się publikacją polityki wykorzystywania danych zanonimizowanych, ich udostępniania (ograniczony czy publiczny), występowania ryzyka reidentyfikacji i ich charakteru, objaśnieniem sposobu anonimizacji itp.

[27] Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, s. 4.

Zakres anonimizacji nie zawsze musi obejmować całość danych, szczególnie wówczas, gdy administrator przetwarza dane tej samej osoby w różnych celach. Osiągnięcie jednego z tych celów prowadzi do usunięcia lub anonimizacji danych przetwarzanych w tym właśnie celu, a nie wszystkich danych dotyczących danej osoby[28]. W przypadku przedsiębiorcy telekomunikacyjnego, który przetwarza różne dane objęte tajemnicą telekomunikacyjną usunięciu lub anonimizacji podlegają tylko dane zbędne do realizacji uprawnionego celu.

Przy ocenie skuteczności anonimizacji należy uwzględniać sposób wykorzystania zanonimizowanych danych. Wykorzystanie tych danych w ramach przedsiębiorcy telekomunikacyjnego niesie ze sobą mniejsze ryzyko niż przekazanie zanonimizowanych danych podmiotowi trzeciemu lub pełne upublicznienie zanonimizowanych danych. Istotne są również potencjalne następstwa ewentualnej reidentyfikacji. Większa ostrożność jest wymagana, jeżeli reidentyfikacja mogłaby zagrażać powstaniem szkody majątkowej, naruszeniem dóbr osobistych itp. Szczególną ostrożność należy również zachować, jeżeli dane zanonimizowane mogą być zestawiane z publicznie dostępnymi bazami danych (np. książki telefoniczne) lub mogą być reidentyfikowane na podstawie wyszukiwania w Internecie.

VI. Anonimizacja a pseudonimizacja danych

W dyskusji nad możliwościami wykorzystania zanonimizowanych danych do innych celów niż pierwotnie zostały zgromadzone należy odróżnić techniki anonimizacji od technik pseudonimizacji, choć często o tych technikach mowa jest łącznie w związku z zasadą minimalizacji przetwarzania danych. Należy odnotować, iż dyrektywa 2002/58/WE zaleca w motywie 9, aby państwa członkowskie, dostawcy usług i zainteresowani użytkownicy rozwijali odpowiednie technologie służące zastosowaniu gwarancji przewidzianych w dyrektywie, ze szczególnym uwzględnieniem celu zminimalizowania przetwarzania danych osobowych oraz wykorzystywania, gdzie możliwe, danych anonimowych lub pseudonimowych. Pseudonimizacja jest zatem uprawnioną techniką minimalizacji przetwarzania danych chronionych i ograniczania ryzyka związanego z ich przetwarzaniem.

Pseudonimizacja polega na zastąpieniu unikalnej cechy podmiotu danych inną informacją, która zmniejsza prawdopodobieństwo bezpośredniej identyfikacji podmiotu danych, ale jej nie wyklucza. W przypadku pseudonimizacji identyfikacja może być dokonywana w sposób pośredni[29]. Brytyjski organ do spraw ochrony danych definiuje pseudonimizację jako proces oznaczania osób fizycznych w zbiorze danych za pomocą unikalnego identyfikatora, który nie identyfikuje podmiotu danych w świecie realnym[30]. D. Korff uznaje za dane pseudonimizowane takie dane, które mogą być powiązane z osobą w razie posiadania klucza dekodującego danych[31]. Pseudonimizacja danych chronionych w telekomunikacji (np. w postaci zastąpienia numeru IMSI numerem tymczasowym, haszowanie, kodowanie, tokenizację) podnosi bezpieczeństwo przetwarzania, szczególnie na wypadek nieuprawnionego dostępu do danych, ale nie prowadzi do anonimizacji[32]. Istotną cechą pseudonimizacji jest odwracalność tej procedury dla dysponenta danych. W opracowaniu

[28] A. Drozd, Zasada ograniczenia czasowego…, s. 147.

[29] P. Lee, *Anonymisation is great, but don't undervalue pseudonymisation*. Pobrano z: http://privacylawblog.ffw.com/2014/anonymisation-is-great-but-dont-undervalue-pseudonymisation

[30] Anonymisation: managing data…, s. 49.

[31] D. Korff, Working Paper, No. 2…, s. 48

[32] Opinion 5/2014…, s. 20.

brytyjskiego organu ds. ochrony danych osobowych rozróżnienie pomiędzy anonimizacją a pseudonimizacją jest dokonywane w taki sposób, że dane zanonimizowane są podstawą do wytworzenia zagregowanej informacji, natomiast pseudonimizacja prowadzi do wytworzenia informacji zanonimizowanej na poziomie jednostki, co z natury łączy się z nieco większym ryzykiem[33].

Pseudonimizacja niezależnie od jakości zastosowanych zabezpieczeń nie spełnia wymagań, jakie wiąże się z anonimizacją danych chronionych tajemnicą telekomunikacyjną, w tych przypadkach, gdy taka operacja jest dozwolona.

VII. Podsumowanie

Anonimizacja danych chronionych w sektorze telekomunikacyjnym może być rozwiązaniem umożliwiającym wykorzystanie ogromnych zasobów danych, którymi dysponują przedsiębiorcy telekomunikacyjni, do osiągnięcia celów społecznie użytecznych, ale bez naruszania prywatności i autonomii informacyjnej użytkowników usług telekomunikacyjnych. Obecnie możliwości stosowania anonimizacji danych chronionych są ograniczone na skutek rozbieżności pomiędzy przepisami prawa Unii Europejskiej a przepisami krajowymi dotyczącymi ochrony tych danych. Minimalny program poprawy sytuacji w analizowanej sprawie polega na usunięciu tych rozbieżności.

Pierwsza z tych rozbieżności polega na włączeniu danych dotyczących użytkowników będących osobami fizycznymi w obręb tajemnicy telekomunikacyjnej, co powoduje, że operacje nieprzewidziane prawem telekomunikacyjnym na tych danych są prawnie wątpliwe. W szczególności dotyczy to anonimizacji i przetwarzania tych danych dla wypełnienia prawnie usprawiedliwionego celu administratora danych, pod warunkiem zachowania praw i wolności osoby, której dane dotyczą. Niezbędna zmiana polega na wyraźnym poddaniu przetwarzania typowych danych osobowych przez przedsiębiorcę telekomunikacyjnego przepisom ustawy o ochronie danych osobowych. Reżim ochronny tajemnicy telekomunikacyjnej powinien być ograniczony do typowych danych telekomunikacyjnych (transmisyjnych, w tym lokalizacyjnych oraz danych o lokalizacji).

Druga zmiana powinna polegać na wyraźnym dopuszczeniu anonimizacji danych transmisyjnych, w tym danych lokalizacyjnych, jako ekwiwalentu ich usuwania. Pozwoli to usunąć ewidentną rozbieżność pomiędzy dyrektywą 2002/58/WE a polską ustawą. Rozbieżność ta uniemożliwia obecnie legalną anonimizację danych transmisyjnych, w tym danych lokalizacyjnych.

Trzecia zmiana mogłaby się ograniczyć do odmiennej interpretacji przepisów dotyczących wykorzystania zanonimizowanych danych o lokalizacji, w takim kierunku, aby możliwe było ich wykorzystanie nie tylko do świadczenia usług o wartości dodatkowej podmiotom tych danych, lecz także innym osobom.

[33] Anonymisation: managing data…, s. 7.