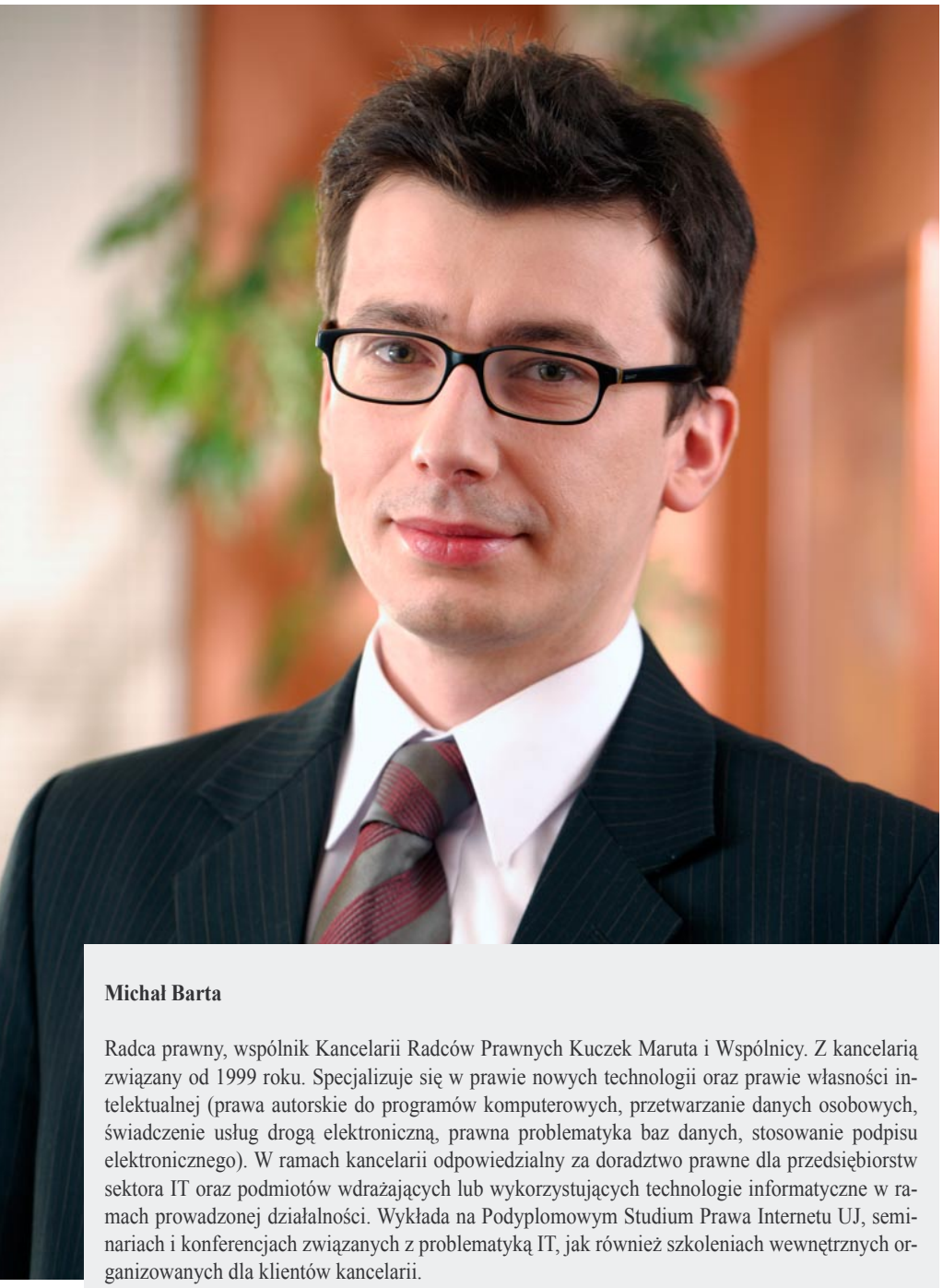
Czy adres IP jest prawnie chroniony jak imię i nazwisko?

– status prawny adresów IP z punktu widzenia zasad ochrony danych osobowych



Michał Barta

Radca prawny, wspólnik Kancelarii Radców Prawnych Kuczek Maruta i Wspólnicy. Z kancelarią związany od 1999 roku. Specjalizuje się w prawie nowych technologii oraz prawie własności intelektualnej (prawa autorskie do programów komputerowych, przetwarzanie danych osobowych, świadczenie usług drogą elektroniczną, prawna problematyka baz danych, stosowanie podpisu elektronicznego). W ramach kancelarii odpowiedzialny za doradztwo prawne dla przedsiębiorstw sektora IT oraz podmiotów wdrażających lub wykorzystujących technologie informatyczne w ramach prowadzonej działalności. Wykłada na Podyplomowym Studium Prawa Internetu UJ, seminariach i konferencjach związanych z problematyką IT, jak również szkoleniach wewnętrznych organizowanych dla klientów kancelarii.

Jeśli firma nie istnieje w Internecie, to w ogóle nie istnieje – głosi powszechnie przywoływany slogan i… trudno się z nim nie zgodzić. Banalne jest wręcz stwierdzenie, że obecnie nie da się prowadzić jakiejkolwiek działalności biznesowej, bez względu na jej charakter, jak i rozmiar, bez dysponowania własnymi stronami WWW, adresem e-mail, a coraz częściej także serwisem WAP.

Sytuacja taka w oczywisty sposób zmusza menedżerów do uwzględnienia w trakcie budowania modeli biznesowych inwestycji w infrastrukturę IT, a także w coraz bardziej wyrafinowane usługi internetowe oraz systemy zarządzania informacją elektroniczną. Naturalna koncentracja na optymalizacji rozwiązania technologicznego pod kątem oczekiwań biznesowych bardzo często idzie w parze z niedocenianiem lub wręcz ignorowaniem aspektu prawnego związanego z funkcjonowaniem systemów służących do zbierania, przetwarzania oraz udostępniania informacji drogą elektroniczną. To duży błąd, który może skutkować niebagatelnymi konsekwencjami w zakresie odpowiedzialności cywilnej, konsekwencjami o charakterze administracyjnym, jak i – w skrajnych przypadkach – nawet odpowiedzialnością karną. Oprócz coraz powszechniej identyfikowanych ograniczeń prawnych stawianych korzystaniu z przedmiotów praw własności intelektualnej do poszczególnych rodzajów informacji, jej zbiorów lub komponentów (autorskie prawa majątkowe, prawa własności przemysłowej, prawa do baz danych) oraz obowiązków związanych ze świadczeniem szeroko definiowanych przez prawo usług elektronicznych – nie mniej istotną rolę odgrywają regulacje prawne określające ramy i warunki legalnego przetwarzania informacji dotyczących osób fizycznych, tj. zasady przetwarzania danych osobowych. Obserwując porównawczo wysiłki legislacyjne w tym obszarze, jak również tendencje interpretacyjne dotyczące istniejących regulacji, bezsprzecznie uznać należy, że region europejski ewidentnie przoduje we wzmacnianiu ochrony prawnej na tym polu, wyznaczając bardzo wysokie standardy ochrony prywatności, w tym danych osobowych. Konsekwencją takiego podejścia musi być oczywiście stawianie rygorystycznych wymagań i limitów dla swobodnego operowania informacją o charakterze indywidualnym. Z uwagi na członkostwo Polski w strukturach Unii Europejskiej rozwiązania takie automatycznie lub w bar-

dzo krótkim czasie po ich przyjęciu stają się obowiązującym w Polsce prawem lub – z uwagi na obowiązek tzw. pro-unijnej wykładni przepisów prawnych – w praktyce obowiązującą jego interpretacją.

Dużą rolę w niedocenianiu problemu ograniczeń w dysponowaniu informacją personalną, zbieraną od użytkowników przy wykorzystaniu sieci informatycznych, odgrywa wciąż niestety pokutujące przekonanie, że do momentu, w którym użytkownik nie zostanie poddany procedurze, w ramach której powinien dobrowolnie podać określone informacje dotyczące jego osoby (np. wypełnić formularz rejestracyjny zawierający jego dane), dane „automatycznie" zbierane od niego w związku z korzystaniem z określonych zasobów informatycznych pozostają w pełni anonimowe, a skoro tak – nie pojawia się w takim przypadku problem ochrony prywatności, czy też bardziej szczegółowo – problem przetwarzania danych osobowych. Przekonanie to oparte jest na założeniu, że skoro powszechna komunikacja internetową (np. publiczny dostęp do stron WWW) polega de facto na komunikacji komputera z komputerem, to w normalnych warunkach tożsamość użytkownika pozostaje „w ukryciu", a administratorzy stron i serwisów WWW nie identyfikują informacji „pozostawianych" w ich zasobach przez użytkowników jako informacji dotyczących konkretnych osób. Przekonanie to jest mitem niebezpiecznym dla obydwu stron komunikacji internetowej. Przy odrobinie wysiłku, wykorzystaniu niekoniecznie bardzo zaawansowanej wiedzy informatycznej oraz znajomości standardów zachowań użytkowników sieci – w wielu przypadkach można na podstawie takich niby-anonimowych danych ustalić nie tylko tożsamość osoby korzystającej z określonych zasobów sieci, lecz również jej zainteresowania, preferencje polityczne etc. Serwisy internetowe, takie jak Google czy Yahoo, gromadzą i przez dłuższy okres przechowują (do niedawna jeszcze przez okres do 2 lat od pozyskania) różnego rodzaju informacje dotyczące zachowań użytkowników sieci (w tym zapytań umieszczanych w wyszukiwarkach, odwiedzanych stron itp.), czyniąc to przede wszystkim w celu optymalizacji i precyzyjnego kierunkowania działań reklamowych, stanowiących przecież zasadnicze źródło ich przychodów.

Pojedyncza informacja jest z tego punktu widzenia pozbawiona większego znaczenia. Wartość ma jedynie większa ich ilość – tym większą, im większy jest zbiór informacji. Ponadto w ramach tych informacji powinny znaleźć się też takie, które pozwolą w przyszłości szybko rozpoznać użytkownika i zdefiniować optymalny kontent, który powinien zobaczyć na swoim ekranie. Zasadniczą informacją wiążącą poszczególne rejestrowane w sieci zachowania oraz umożliwiającą w przyszłości rozpoznanie użytkownika i zdefiniowanie charakterystycznych dla niego cech i zachowań w sieci są obecnie numery identyfikujące urządzenie używane w celu komunikacji internetowej, czyli tzw. adresy IP (ang. Internet Protocol Address), tj. „unikatowe numery, przyporządkowane urządzeniom sieci komputerowych", które są zgodnie z najpowszechniej aktualnie stosowanym formatem zwanym IP wersja 4. Jak wiadomo, adresy IP mogą być stałe (tj. niezmienne w każdym przypadku korzystania przez użytkownika z sieci za pomocą danego urządzenia) lub dynamiczne (tj. w każdym przypadku inne – a przynajmniej potencjalnie). Te ostatnie najczęściej przydzielane są użytkownikom sieci przez dostawców usług internetowych z posiadanej przez nich puli. Możliwe jest również współużywanie jednego adresu IP przez kilku użytkowników w ramach sieci lokalnej. Adres IP (poza przypadkami celowego jego maskowania przez użytkownika) jest praktycznie zawsze „widziany" przez urządzenie, z którym łączy się użytkownik Internetu. Powszechną praktyką na różnego rodzaju forach, listach dyskusyjnych, portalach, serwisach internetowych jest utrwalanie i przechowywanie przez administratorów adresów IP użytkowników łączących się z takimi miejscami w sieci, a w przypadku serwisów umożliwiających użytkownikowi udział w tworzeniu treści (kontentu) strony WWW – bywa, że i udostępnianie ich przez administratorów innym publicznym użytkownikom, najczęściej poprzez wyświetlanie adresu IP przy publikowanej przez użytkownika treści.

Ponieważ za sieciową aktywnością urządzenia w sieci z reguły kryje się działalność konkretnego człowieka, niezaprzeczalnie niemal w każdym przypadku istnieje teoretyczna możliwość powiązania adresu IP z konkretną osobą przejawiającą aktywność w sieci. Oczywiście, w zależności od tego, kto będzie dysponował taką informacją (adresem IP) łatwiej lub trudniej będzie zidentyfikować taką osobę (bez problemu zrobi to np. dostawca dostępu Internetu, który zawarł umowę z użytkownikiem i przydzielił mu dany nr IP) – co ma kluczowe znaczenie z punktu widzenia istnienia lub nie ochrony prawnej takich danych.

I tu właśnie pojawia się zasadnicze pytanie: czy adres IP może być prawnie chronioną daną osobową? Odpowiedź na to pytanie ma fundamentalne znacznie dla oceny zakresu obowiązków, jakie ciążą na menedżerze IT, choć jednocześnie jest to dopiero początek drogi do tego celu.

Co to jest „dana osobowa"?

Ustawa z dnia z dnia 29 sierpnia 1997 roku o ochronie danych osobowych w przepisie art. 6 definiuje pojęcie danych osobowych jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej".

Pojęcie „osoby zidentyfikowanej" nie wymaga raczej interpretacji, problem pojawia się natomiast, kiedy staramy się ustalić, kim jest „osoba możliwa do zidentyfikowania". Ustawodawca na gruncie przepisów ustawy (art. 6 ust. 2) wyjaśnia, jak należy rozumieć to pojęcie, stanowiąc, że jest to „osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne".

Ponieważ jednak tak sformułowana definicja obejmowałaby praktycznie każdą informację dotyczącą jakiejś osoby (bo przecież przy nieograniczonych staraniach i nakładach niemal w każdym przypadku można „bezpośrednio lub pośrednio" określić tożsamość osoby, której informacja dotyczy), ustawodawca stawia jednocześnie definicyjną granicę tego pojęcia. Otóż zgodnie z art. 6 ust. 3 ustawy: „Informacji nie uważa się za umożliwiającą określenie tożsamości osoby (ergo nie uważa się też za daną osobową), jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań".
Podsumowując: „dana osobowa" to:

- Informacja;
- Dotycząca osoby fizycznej;
- Której tożsamość jest znana lub co najmniej możliwa do bezpośredniego lub pośredniego ustalenia bez nadmiernych, kosztów czasu lub działań.

Jak w kontekście tej definicji prezentuje się adres IP?

Łatwo stwierdzić, że numer IP niesie ze sobą pewną wartość informacyjną, a konkretnie mówi nam, jak „nazywa się" w sieci urządzenie, którego użyto, aby przeprowadzić określone działania (umieścić wpis na forum, wpisać zapytanie do przeglądarki, kliknąć na określoną reklamę itp.). Z pewnością adres IP jest więc „informacją", spełnia więc pierwszą przesłankę definicyjną „danych osobowych".

Osoba fizyczna czy urządzenie?

Odpowiedź na drugie pytanie (czy adres IP dotyczy osoby fizycznej?) nastręcza już pewne trudności. Można bowiem twierdzić, że dany numer IP ze swej istoty nie odnosi się do osoby, lecz do urządzenia, z którego mogą przecież korzystać różne osoby (taką wątpliwość zgłaszają J. Barta, P. Fajgielski i R. Markiewicz w: „Ochrona danych osobowych. Komentarz", 2007). Co więcej, w przypadku dynamicznych adresów IP przydzielanych „na bieżąco" przez ISP lub też korzystania z pojedynczego IP przez kilku użytkowników sieci lokalnej – jest to wręcz regułą. Na tej podstawie można byłoby więc argumentować, że adres IP, już ze swej istoty, nigdy nie powinien stanowić danej osobowej. Warto tutaj wskazać, że przedstawione stanowisko przez długi czas było podstawową argumentacją prezentowaną przez prawników Google w sporze z Komisją Europejską, która starała się wymóc na firmie konieczność traktowania adresów IP jako danych osobowych i respektowania związanych z tym ograniczeń prawnych.

Z drugiej jednak strony takie rozumowanie prowadziłoby do wykluczenia z tego zakresu pojęcia np. numerów telefonów komórkowych (także identyfikujących wyłącznie użytą kartę SIM), czyli informacje powszechnie (i chyba słusznie) uznawane jednak za dane osobowe. W efekcie – przyjęcie takiego stanowiska prowadziłoby więc do bardzo daleko idącego i zdecydowanie niezgodnego z celem regulacji ustawowej zawężenia pojęcia „danych osobowych".

Należy ponadto wskazać, że pojawiający się w sieci adres IP – niezależnie od tego, czy jest on dynamiczny, stały, czy współużytkowany – zawsze (pomijając może tylko wciąż stosunkowo rzadkie przypadki w całości zautomatyzowanych działań poszczególnych urządzeń) jest rezultatem działania konkretnej osoby fizycznej, a w konsekwencji – jak wskazywałem wyżej – zawsze istnieje choćby teoretyczna możliwość powiązania IP z kon-

kretną osobą fizyczną. Patrząc w ten sposób, drugą przesłankę definicyjną „danych osobowych" należałoby więc jednak uznać za spełnioną.

Jak więc rozstrzygnąć przedstawioną wyżej kontrowersję?

Pomocna dla rozstrzygnięcia tego dylematu może okazać się treść słynnej już „Opinii 4/2007 w sprawie pojęcia danych osobowych", przyjętej w dniu 20 czerwca 2007 roku przez oficjalny unijny organ doradczy powołany do interpretacji regulacji Dyrektywy: Grupę Roboczą Ds. Ochrony Danych Osobowych Powołanej Na Mocy Art. 29 (dalej zwaną: „Grupą art. 29"). Gremium to zdefiniowało swoisty test, którego wynikiem jest udzielenie odpowiedzi, czy dana informacja dotyczy osoby fizycznej, czy też nie. W treści opinii stwierdzono bowiem, że można przyjąć, że aby dane można było uznać za „dotyczące" osoby fizycznej powinien występować element „treść" LUB element „cel", LUB element „skutek".

Rozwijając to podejście, Grupa art. 29 stwierdziła, że element „treść" występuje, gdy „informacja jest na temat pewnej osoby" (np. wyniki jej analiz medycznych). Z kolei element „cel" wystąpi, gdy „dane są lub mogą być wykorzystywane w celu oceny osoby, jej traktowania w określony sposób lub też wpływania na jej status lub zachowania". Przykładem takich danych, wskazanym przez Grupę art. 29 jest np. billing rozmów telefonicznych prowadzonych ze stacjonarnego telefonu firmowego, przypisanego do firmy (a więc nie osoby fizycznej), ale standardowo znajdującego się w godzinach pracy pod kontrolą danego pracownika. Z ostatnim przypadkiem („skutek"), zdaniem Grupy art. 29, będziemy mieć natomiast do czynienia, gdy co prawda nie wystąpi żaden z dwóch wskazanych wyżej elementów, ale „użycie danych prawdopodobnie będzie miało wpływ na prawa i interesy danej osoby". Przykładem podawanym w tym kontekście przez Grupę art. 29 jest oparty o GPS system alokacji wolnych taksówek do zleceń klientów. Pomimo, że system przetwarza dane samochodów (nie występuje element „treść"), a jego celem nie jest ocena kierowców (nie występuje też element „cel"), to jednak dane przetwarzane przez system potencjalnie mogą posłużyć takim celom, gdyż zawierają informacje, czy samochód przemieszcza się, jaką trasą jedzie, z jaką prędkością etc., a więc łącznikiem jest element „skutek".

Poddając zdefiniowanemu przez Grupę art. 29 testowi adresy IP, należałoby, jak się wydaje, uznać, że mimo, iż adresy IP nie dotyczą co prawda osób fizycznych ze względu na brak elementu „treść" (identyfikują tylko urządzenie), to jednocześnie jednak dotyczą konkretnych osób z uwagi na element „cel" lub element „skutek", w zależności od konkretnych okoliczności faktycznych. Element „cel" wystąpiłby np. w kontekście adresów IP zbieranych w zawiązku z identyfikacją osób korzystających z forów internetowych, list dyskusyjnych, natomiast element „skutek" – w przypadku zbierania takich danych w innych celach, takich jak chociażby statystyki dotyczące „geograficznego" pochodzenia osób odwiedzających stronę WWW, odwiedzanych stron, klikniętych reklam.

Kiedy osoba jest „identyfikowalna"?

Skoro dwie pierwsze przesłanki ustawowe uznania adresów IP za „dane osobowe" mogłyby zostać uznane za spełnione, należałoby się więc w następnej kolejności zająć trzecią z nich, zdecydowanie najtrudniejszą do analizy, tj. oceną, czy osoba, której dotyczy informacja w postaci adresu IP, jest „zidentyfikowana lub możliwa do zidentyfikowania". Jest oczywistym, że w kontekście adresów IP nie można przyjąć, iż osoba jest „zidentyfikowana" już poprzez sam adres IP. Ale czy jest ona „możliwa do zidentyfikowania"? Musimy tutaj pamiętać, że „możliwość identyfikacji" – na gruncie zarówno Dyrektywy 95/46/WE Parlamentu Europejskiego oraz Rady z dnia 24 października 1995 roku, jak i polskich przepisów o ochronie danych osobowych – została w sposób prawnie wiążący zdefiniowana i nie można posługiwać się tutaj potocznym rozumieniem takiego sformułowania.

Zasadniczo podejście Grupy art. 29 wyrażone w treści powoływanej już Opinii, jest następujące: ocena wystąpienia trzeciej przesłanki ściśle zależeć będzie od kontekstu, w jakim konkretne dane będą funkcjonować. Jeżeli kontekst ten umożliwia dysponentowi identyfikację osoby – przesłanka jest spełniona. W trakcie analizy pojęcia „danych osobowych" Grupa art. 29 posłużyła się przykładem dobrze obrazującym względny charakter tej przesłanki, wskazując, że bardzo pospolite nazwisko z pewnością z reguły nie pozwala na ustalenie tożsamości danej osoby i wyodrębnienie jej z ogółu populacji danego kraju, najczęściej będzie jednak zupełnie wystarczające dla identyfikacji w klasie ucznia o takim nazwisku. Ta sama rodzajowo informacja może być więc raz traktowana jako „dana osobowa", kiedy indziej może być pozbawiona tego statusu prawnego, a zależeć to będzie wyłącznie od tego, ile innych informacji i jakiego rodzaju jej towarzyszą oraz jakimi możliwościami zebrania dodatkowych powiązanych z nią informacji dysponuje osoba, która weszła w jej posiadanie. W tym kontekście mówi się w doktrynie o zjawisku „niepowtarzalnej kombinacji" czynników identyfikujących, a także o „subiektywizacji" pojęcia danych osobowych.

Ponieważ ani unijne, ani polskie regulacje nie wyróżniają w jakikolwiek szczególny sposób danych związanych z komunikacją elektroniczną, w tym adresów IP, spośród ogółu informacji stanowiących lub raczej mogących stanowić dane osobowe, ta ogólna zasada powinna więc znaleźć pełne zastosowanie również na gruncie oceny prawnego statusu adresów IP. W kontekście adresów IP, kluczową okolicznością dla oceny, czy będziemy mieć do czynienia z danymi osobowymi, czy też nie, są możliwości dysponenta takich danych (np. osoby prowadzącej serwis internetowy) do dokonywania identyfikacji osób, które takimi adresami się posłużyły, w szczególności dysponowanie innymi informacjami, które można powiązać i przypisać do danego adresu IP (np. adresem e-mail, nazwą organizacji etc.).

Oceniając „identyfikowalność" osoby, która posłużyła się danym adresem IP, należy wziąć pod uwagę wszystkie sposoby, jakimi ich dysponent się posłużyć w celu dokonania takiej identyfikacji. Oczywiście nie wystarcza w tym przypadku czysto hipotetyczna możliwość odróżnienia. Przykładowo, jeżeli ustalenie tożsamości byłoby możliwe lub nastąpiło wyłącznie w rezultacie usterki technicznej lub naruszenia przez inną osobę obowiązku zachowania poufności – nie sposób mówić o istnieniu uprzedniej możliwości identyfikacji osoby. Podobnie należy ocenić sytuację, gdy ustalenie tożsamości byłoby, co prawda, możliwe w „normalny sposób", jednak pociągałoby za sobą bardzo wysokie koszty lub było bardzo czasochłonne.

W praktyce w wielu wypadkach nie będzie konieczne sięganie po nadzwyczajne środki czy koszty. Dla ilustracji dwa przykłady. Dostawca Internetu (ISP), który zawarł umowę z konkretną osobą fizyczną (dysponuje jej nazwiskiem, adresem etc.) przydziela takiej osobie stały adres IP, lub nawet zapewnia możliwość korzystania z adresu dynamicznego, może – wyłącznie na podstawie posiadanych przez siebie informacji – z dużym prawdopodobieństwem ustalić, kto korzystał z takiego adresu w danym czasie. Dla tego podmiotu adres IP będzie więc daną osobową. Analogiczna sytuacja będzie miała miejsce w przypadku adresów IP użytkowników list dyskusyjnych lub innych usług internetowych, w ramach których dla skorzystania z usługi konieczne jest założenie profilu oraz podanie danych identyfikujących (np. serwisy aukcyjne). W takich przypadkach może dojść do ciekawej sytuacji, w której adres IP użytkownika niezalogowanego nie będzie daną osobową, ale wraz z pierwszym zalogowaniem się go do profilu nastąpi jego powiązanie z odpowiednimi danymi identyfikującymi w wyniku czego IP stanie się daną osobową.

Ocena możliwości identyfikacji osoby, a więc w konsekwencji uznania IP za „dane osobowe", powinna być również dynamicznie analizowana w kontekście zmian technologicznych, w wyniku których identyfikacja użytkownika na podstawie adresu IP będzie możliwa lub w znacznym stopniu łatwiejsza (tańsza, mniej czasochłonna) niż wcześniej. Wtedy informacje o adresach IP, które dla danego dysponenta nie były dotąd danymi osobowymi, mogą stać się nimi właśnie z tego powodu, pomimo że zakres informacji, którymi dysponuje danych podmiot, nie ulegnie zmianie.

Przedstawione powyżej podejście było i jest powszechnie prezentowane w ramach oceny innego rodzaju informacji jako potencjalnych danych osobowych. Zaprezentowanie go więc również przez europejska grupę doradczą w kontekście oceny adresów IP nie jest zaskoczeniem. Wnioski Grupy art. 29 odnoszące się do oceny adresów IP jako danych osobowych są jednak jeszcze dalej idące. Zdaniem Grupy art. 29 nie bez znaczenia dla oceny, czy IP jest daną osobową jest bowiem również cel, w jakim adresy IP są zbierane. Jak argumentuje się w treści przywoływanej już Opinii 4/2007, może bowiem zdarzyć się tak, że osoba zbierająca takie dane co prawda nie posiada lub, co do zasady, nie jest w stanie „w normalnym trybie" uzyskać innych informacji pozwalających na identyfikację, jednak zbiera takie informacje właśnie w celu ew. późniejszej identyfikacji. Podawanym przykładem tego rodzaju działań jest monitoring video miejsc publicznych, np. galerii handlowych, przejść podziemnych, dworców. W takim przypadku utrwalane i przechowywane są wizerun-

ki oraz zachowania osób, których tożsamości administrator sytemu praktycznie nie jest w stanie ustalić. Jednak w opinii Grupy art. 29 w takich przypadkach, właśnie z uwagi na cel działań i poniekąd niezależnie od kontekstu informacyjnego (kombinacji czynników identyfikujących), zbierane dane należy jednak uznawać za dane osobowe. Taka interpretacja może oczywiście stanowić potencjalnie spory problem dla administratorów serwisów internetowych (także takich, które nie wymagają imiennego logowania), którzy nie traktują archiwizowanych adresów IP jako danych osobowych z uwagi na nieposiadanie przez nich innych danych lub sposobów umożliwiających identyfikację użytkowników. Celem zbierania przez nich informacji o adresach IP (choćby nawet pobocznym) jest bowiem zachowanie danych umożliwiających identyfikację użytkowników „w razie potrzeby", nawet jeżeli inne posiadane lub dostępne w danej chwili administratorowi informacje w praktyce wykluczają możliwość identyfikacji.

W podobnym duchu, podzielając, jak się wydaje, podejście zaprezentowane przez Grupę art. 29, wypowiadał się początkowo na ten temat również Michał Sarzycki – Generalny Inspektor Ochrony Danych Osobowych (odpowiedzi na pytania czytelników, „Gazeta Prawna" z dnia 23 października br.; „Lepiej nie ujawniać numeru komputera", „Rzeczpospolita" z dnia 12 listopada br.). Zdaniem GIODO, dane o adresach IP traktować należy jako dane osobowe nawet w sytuacji, gdy administrator jedynie „przewiduje, że sposoby, jakimi można się posłużyć w celu zidentyfikowania osoby, mogą się stać dostępne, na przykład w drodze sądowej".

Jedyny wyjątek, jaki zauważa Grupa art. 29, a w ślad za nią GIODO w niedawno opublikowanej (28.07.2008 r.) oficjalnej wypowiedzi na stronach internetowych urzędu (*http://www.giodo.gov.pl*), to „z definicji anonimowe" adresy IP komputerów kafejek internetowych, których, co do zasady, nie powinno się traktować jako danych osobowych. Jednocześnie jednak Grupa art. 29 zaleca traktowanie takich danych przez administratorów systemów IT analogicznie, jak danych osobowych, wskazując, że adresy te dla przeciętnego administratora są praktycznie nie do odróżnienia od pozostałych, zasadniczo stanowiących prawnie chronione dane osobowe.

Stanowisko Grupy art. 29 w kwestii adresów IP jako danych osobowych na pierwszy rzut oka wydaje się być w pewnym stopniu wewnętrznie sprzeczne. Z jednej strony bowiem, na poziomie ogólnym, Grupa 29 twierdzi, iż dla uznania informacji za daną osobową nie wystarczy wyłącznie hipotetyczna możliwość ustalenia tożsamości osoby, to w odniesieniu do adresów IP de facto jednak przyjmuje, że wystarcza.

Trudno znaleźć uzasadnienie dla odmiennego traktowania adresów IP – z jednej strony i innego rodzaju danych osobowych – z drugiej. Wydaje się, że prawidłowe podejście powinno być jednak analogiczne jak w przypadku innych informacji, a ocena, czy adres IP stanowi, czy też nie, daną osobową, nie powinna być uzależniona od wyłącznie potencjalnej możliwości skojarzenia go w przyszłości z konkretną osobą, zwłaszcza w sytuacjach, gdy taka identyfikacja byłaby możliwa wyłącznie w przypadku wystąpienia dodatkowych okoliczności (np. podejrzenia popełnienia przestępstwa). Status adresu IP jako danej osobowej, czyli informacji możliwej do powiązania z konkretną osobą fizyczną, powinien raczej wynikać wyłącznie z aktualnych w danym czasie możliwości, tj. dodatkowych informacji oraz sposobów identyfikacji dostępnych dysponentowi takich danych (administratora). Wydaje się, że przy dokonywaniu takiej oceny przede wszystkim należałoby przeprowadzić test, czy administrator może w danej chwili wyłącznie własnymi staraniami (i to nie „nadmiernymi", jak to stanowi ustawa), bez konieczności zaistnienia jakichkolwiek dodatkowych i niezależnych od niego okoliczności, z dużym prawdopodobieństwem ustalić tożsamość użytkownika posługującego się danym IP. Jeżeli nie – nie należałoby, moim zdaniem, takich informacji traktować jako dane osobowe. Takie stanowisko wydaje się zgodne z zaprezentowaną na wstępie konstrukcją definicji danych osobowych, praktycznie identyczną na gruncie Dyrektywy 95/46/WE oraz polskiej ustawy o ochronie danych osobowych. Fundamentem tej definicji jest bowiem nie potencjalna, lecz realna, istniejąca w danym czasie i w odniesieniu do konkretnego administratora możliwość powiązania informacji z konkretną osobą fizyczną. Oczywiście, jak wskazywałem już nieco wyżej, „dano-osobowy" status informacji jest dynamiczny i powinien podlegać weryfikacji wraz z pozyskiwaniem przez dysponenta dodatkowych informacji lub pojawienia się nowych sposobów identyfikacji użytkownika. Taka zmiana statusu nie powinna być jednak antycypowana.

Biorąc pod uwagę, że w kwestii statusu prawnego adresów IP stanowisko GIODO w jakikolwiek znaczący sposób raczej nie będzie odbiegać od stanowiska europejskich organów doradczych, w konsekwencji należy się chyba oswoić z myślą, że adresy internetowe w praktyce kontroli i decyzji GIODO będą jednak – przynajmniej w najbliższym czasie – w szerokim spektrum przypadków faktycznych traktowane jako dane osobowe.

To nie tylko teoria...

Kształtujące się „europejskie" podejście do ochrony adresów IP (znajdujące odzwierciedlenie chociażby w publicznych i szeroko komentowanych w sieci wypowiedziach Petera Scharra, unijnego komisarza ds. ochrony prywatności, a jednocześnie przewodniczącego Grupy art. 29) staje się już dziś niemałym problemem dla kolosów Internetu, takich jak: Google, Yahoo czy Microsoft, prowadzących swoje interesy na terytorium Unii. Nota bene nie bez znaczenia jest tu również fakt, że amerykański system ochrony danych osobowych jest mniej restrykcyjny i zdecydowanie mniej sformalizowany niż europejski. Amerykański rodowód (siedziba) tych firm nie chroni ich jednak w żaden sposób, gdyż, prowadząc działalność także na terytorium Unii, zobowiązane są podporządkować się obowiązującym na jej terytorium regulacjom prawnym. Tu też ze szczególną wyrazistością, głownie z uwagi na wskazane wyżej rozbieżności pomiędzy systemami prawnymi UE i USA, ujawnia się pewien paradoks prawny polegający na zderzeniu globalnego wymiaru Internetu z lokalnymi (częstokroć bardzo różniącymi się od siebie) regulacjami poszczególnych państw lub ich grup.

Odmienności te z tych, czy innych przyczyn nieuwzględnione na etapie budowania rozwiązań internetowych doprowadziły do w efekcie do tego, że praktyki w zakresie utrwalania i przechowywania adresów IP stosowane przez wszystkie wskazane wyżej korporacje internetowe od mniej więcej roku są przedmiotem szczegółowych badań ze strony Grupy art. 29. Rozgorzała w efekcie bardzo ciekawa dla obserwatorów, acz nierówna, wojna na argumenty. Pierwsze jej wyniki przyniosły ostatnie dni – w dniu 11 września br. Google pod naciskami Unii Europejskiej zgodził się na istotne skrócenie okresu przechowywania informacji numerów IP do z 18 do 9 miesięcy. To już drugie wymuszone przez Unię podejście Google do problemu terminów przechowywania danych, który z początkiem tego roku skrócił standardowo dotychczas przyjmowany dwuletni okres ich przechowywania. Komisarz unijny ds. wymiaru sprawiedliwości Jacques Barrot uznał to za krok w dobrą stronę, lecz zapowiedział, że Unia będzie dążyć do respektowania właściwego, jej zdaniem, jeszcze krótszego, bo maksymalnie 6-cio miesięcznego okresu przechowywania takich danych. To jednak dopiero pierwsze efekty starcia potrzeby biznesowej i, nie ukrywajmy, sporych zysków przeglądarek pozyskiwanych z Internetu (przede wszystkim chodzi o zyski z bardzo „wartościowej", mocno spersonalizowanej reklamy kontekstowej) z pryncypialnym podejściem do ochrony prywatności jednostki. Jako że stawka jest niebagatelna, a gracze bardzo poważni – na ostateczne rozstrzygnięcie tej batalii przyjdzie nam jednak jeszcze trochę poczekać. A czasu na rozstrzygnięcie jest coraz mniej, gdyż, jak stwierdził Marc Rosberg – przewodzący Electronic Privacy Information Center (EPIC): *„Idziemy już w stronę IPv6, gdzie sprawa identyfikacji osób po adresie IP będzie jeszcze bardziej krytyczna"*. ■