

VI FORUM INFORMACJI

i Ochrony Danych Osobowych

23-25.10 HOTEL COPERNICUS

TORUŃ LUB UDZIAŁ ONLINE

Przegląd pytań prejudycjalnych i orzecznictwa TSUE w sprawach dotyczących danych osobowych

r. pr. Magdalena Czaplińska



Zagadnienia wstępne

Na przestrzeni kilku ostatnich lat stosowania rodo ujawnił się szereg wątpliwości i rozbieżności co do kwalifikowania określonych informacji jako danych osobowych. Choć ideą rodo było zapewnienie jednolitości w stosowaniu przepisów o ochronie danych osobowych, to zróżnicowany katalog czynników spowodował, że w praktycznym wymiarze widoczny jest niejednolity sposób podchodzenia do kwalifikowania poszczególnych informacji jako danych osobowych (Opinia Grupy Roboczej art. 29 nr 4/2007).

Regułą w kwalifikowaniu informacji jako danych osobowych jest to, że w pewnych okolicznościach pewne dane będą danymi osobowymi, a w innych nie.



Zagadnienia wstępne

Nie budzi wątpliwości, że danymi osobowymi będą takie informacje, jak: imię, nazwisko, PESEL czy numer dokumentu identyfikującego daną osobę, np. dowód tożsamości czy paszport, lub zazwyczaj adres. Problematiczną kwestią natomiast są takie informacje, jak adres IP komputera i adres poczty elektronicznej. Nie ulega wątpliwości, że ocena, czy dana informacja stanowi dane osobowe, musi być dokonywana w konkretnych przypadkach, z uwzględnieniem ich specyfiki.



Sprawa C 101/01

Na tle przepisów dyrektywy 95/46/WE TSUE uznał, że danymi osobowymi są m.in. nazwisko osoby w połączeniu z jej numerem telefonu lub informacjami dotyczącymi jej warunków pracy czy sposobu spędzania wolnego czasu oraz informacja, że osoba na skutek doznanego urazu stopy korzystała ze zwolnienia lekarskiego (sprawa C-101/01).

Czy operacja polegająca na zamieszczeniu na stronie internetowej danych różnych osób pozwalających je zidentyfikować za pomocą nazwiska albo innych środków, np. numeru telefonu lub informacji dotyczących ich warunków pracy i sposobów spędzania wolnego czasu, stanowi „przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany” w rozumieniu art. 3 ust. 1 dyrektywy 95/46. Na tak postawione zagadnienie TSUE odpowiedział twierdząco, uznając że danymi osobowymi są informacje, takie jak te, które były umieszczane przez B. Lindqvist.



Połączone sprawy C-465/00, C-138/01 i C-139/01, sprawa C-73/07

W innym orzeczeniu TSUE uznał za dane osobowe nazwiska osób i ich roczne dochody. Wyrok w tej sprawie został wydany na skutek pytania prawnego dotyczącego tego, czy przepisy o ochronie danych osobowych należy interpretować w ten sposób, że stoją na przeszkodzie regulacji krajowej nakładającej na organy państwowe obowiązek gromadzenia i komunikowania danych na temat dochodów do celów publikacji nazwisk i dochodów pracowników (połączone sprawy C-465/00, C-138/01 i C-139/01).



Połączone sprawy C-465/00, C-138/01 i C-139/01, sprawa C-73/07

W sprawie sporu pomiędzy Tietosuojaaltuutettu (inspektorem ochrony danych osobowych) a Tietosuojaalakunta (komisją ds. ochrony danych) w przedmiocie działań związanych z przetwarzaniem danych osobowych dokonywanych przez spółki Satakunnan Markkinapörssi Oy i Satamedia Oy TSUE uznał za dane osobowe dane dotyczące dochodów z działalności zarobkowej i kapitału, a także majątku osoby fizycznej (sprawa C-73/07).



Sprawa C-524/06

Zbiory władz publicznych obejmujące dane osobowe, które zawierają jedynie materiał informacyjny już upowszechniony przez media, należą do zakresu zastosowania dyrektywy, dlatego imię i nazwisko zostało uznane za dane osobowe obok daty i miejsca urodzenia, płci, narodowości, stanu cywilnego, historii wjazdów i opuszczania terytorium danego państwa, statusu pobytu, szczegółów dotyczących kolejnych paszportów, meldunków, oznaczenia urzędów i służb przekazujących dane (wyrok wydany w sprawie C-524/06).



Case IP

- Adres IP (ang. Internet Protocol Address) to liczba nadawana interfejsowi, grupie interfejsów (broadcast, multicast), bądź całej sieci komputerowej opartej na protokole IP, służąca do identyfikacji elementów warstwy trzeciej modelu OSI – w obrębie sieci oraz poza nią (tzw. adres publiczny).
- Adres IP nie jest numerem rejestracyjnym komputera – nie identyfikuje jednoznacznie fizycznego urządzenia – może się dowolnie zmieniać (np. przy każdym wejściu do internetu), kilka urządzeń również może dzielić jeden publiczny adres IP.



Opinia 4/2007 z 2007 r.

- W opinii tej Grupa Robocza art. 29 uznała adresy IP za dane dotyczące osoby możliwej do zidentyfikowania. Grupa Robocza art. 29 stwierdziła, że:

„dostawcy dostępu do internetu i administratorzy sieci lokalnych mogą, używając sposobów, jakimi można się posłużyć, zidentyfikować użytkowników internetu, którym przydzielili adresy IP, ponieważ systematycznie «rejestrują» oni w pliku datę, godzinę, czas trwania i dynamiczne adresy IP przydzielone użytkownikom internetu. To samo można powiedzieć o dostawcach usług internetowych prowadzących rejestr na serwerze http. W takich przypadkach można niewątpliwie mówić o danych osobowych. (...)



Opinia 4/2007 z 2007 r.

(...) Zwłaszcza w przypadkach, gdy przetwarzanie adresów IP ma na celu zidentyfikowanie użytkowników komputera (na przykład przez posiadaczy praw autorskich w celu ścigania użytkowników za pogwałcenie praw autorskich), administrator przewiduje, że «sposoby, jakimi można się posłużyć» w celu zidentyfikowania osoby mogą się stać dostępne, na przykład w drodze sądowej (w przeciwnym razie gromadzenie danych nie miałyby sensu), i że w związku z tym informacje te należy uważać za dane osobowe”.



Opinia 4/2007 z 2007 r.

- Szczególny przypadek stanowią niektóre rodzaje adresów IP, które w pewnych okolicznościach nie pozwalają na zidentyfikowanie użytkownika z różnych względów technicznych i organizacyjnych.
- Przykładem mogą być adresy IP przypisane do komputera w kawiarni internetowej, gdzie identyfikacja użytkownika nie jest wymagana. Można by twierdzić, że dane dotyczące użycia komputera X w pewnym przedziale czasowym nie pozwalają na zidentyfikowanie osoby „przy użyciu sposobów, jakimi można się posłużyć”, i że w związku z tym nie stanowią one danych osobowych.



Opinia 4/2007 z 2007 r.

- Jednakże należy odnotować, że dostawcy usług internetowych nie wiedzą najczęściej, czy dany adres IP pozwala na zidentyfikowanie, i że w związku z tym przetwarzają oni dane związane z takim adresem IP w taki sam sposób, jak informacje związane z adresami IP użytkowników zarejestrowanych i możliwych do zidentyfikowania. Dlatego też poza przypadkiem, gdy dostawca usług internetowych może stwierdzić z całkowitą pewnością, że dane dotyczą użytkowników niemożliwych do zidentyfikowania, musi on ze względów bezpieczeństwa traktować wszystkie informacje związane z adresem IP jako dane osobowe.



Wyrok wydany 19 października 2016 r. w sprawie C-582/14

- Trybunał Sprawiedliwości Unii Europejskiej orzekł, że adresy IP mogą być danymi osobowymi. W stanie faktycznym rozpoznawanym w tej sprawie rząd niemiecki postulował przyjęcie teorii subiektywnej i podnosił, że adresy IP zbierane („logowane”) przez strony rządowe nie są danymi osobowymi, ponieważ na ich podstawie administrator strony internetowej nie może samodzielnie ustalić nazwiska czy też adresu właściciela określonego adresu IP. Takie dane są zwykle w wyłącznym posiadaniu dostawcy usługi dostępu do internetu (ISP), a administrator strony internetowej nie ma do nich dostępu.



Wyrok wydany 19 października 2016 r. w sprawie C-582/14

- Trybunał przychylił się pośrednio do teorii subiektywnej, stwierdził jednak, że prawo niemieckie prawdopodobnie umożliwia administratorowi strony internetowej – w szczególności w przypadku ataku hakerskiego – zwrócenie się do odpowiednich organów, które mogą nakazać dostawcy dostępu do internetu ujawnienie tożsamości właściciela danego adresu IP. Jednocześnie, zgodnie z motywem 26 dyrektywy 95/46/WE przy ustalaniu, czy istnieje „możliwość identyfikacji” należy brać pod uwagę „wszystkie środki, których podjęcie przez administratora lub jakąkolwiek osobę trzecią jest – racjonalnie rzecz biorąc – prawdopodobne”. Jeśli istnieją środki, których zastosowanie przez administratora w celu identyfikacji osoby kryjącej się za danym adresem IP jest racjonalnie prawdopodobne, adresy IP należy – zdaniem Trybunału – uznać za dane osobowe.



Decyzja Prezesa UODO z 2021 r.

- Informacją dotyczącą osoby jest zarówno informacja odnosząca się do niej wprost, jak i taka, która odnosi się bezpośrednio do przedmiotów czy urządzeń, ale poprzez możliwość powiązania tych przedmiotów bądź urządzeń z określoną osobą pośrednio stanowi informację także o niej samej. Adres IP jest unikatowym numerem przyporządkowanym urządzeniom sieci komputerowych. Jest zatem informacją dotyczącą komputera, a nie konkretnej osoby fizycznej, zwłaszcza wtedy gdy możliwe jest współużyczenie jednego adresu IP przez wielu użytkowników w ramach sieci lokalnej.



Decyzja Prezesa UODO z 2021 r.

- Tam, gdzie adres IP jest na dłuższy okres lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej. W związku z powyższym w ocenie Prezesa UODO zarówno adres IP, jak i ID plików cookies z uwagi na uzasadnione prawdopodobieństwo zidentyfikowania w powiązaniu z tymi danymi stanowią dane osobowe.



Wyrok WSA w Warszawie z 11 lipca 2022 r., II SA/Wa 3993/21 – orzeczenie nieprawomocne

- W uzasadnieniu zaskarżonej decyzji brak jednak ustaleń zarówno do przyjętego w niej przez Prezesa UODO kryterium kwalifikacji adresu IP jako danej osobowej (tj. przypisania go na dłuższy czas lub na stałe do konkretnego urządzenia), jak i do określonych w art. 4 pkt 1, w powiązaniu z motywami 26 i 30 rodo, warunków uznania tego identyfikatora za daną osobową. Także z akt sprawy nie wynika, by w tym zakresie prowadzono postępowanie wyjaśniające. Na ich podstawie można stwierdzić, że już w pierwszym piśmie (z 7 lipca 2021 r.) wystosowanym do skarżącej w trybie art. 58 ust. 1 lit. a i lit. e rodo z żądaniem udzielania informacji i złożenia wyjaśnień, organ nadzorczy niejako „z góry” założył, że zarówno adres IP, jak i sztucznie nadany ID z cookies stanowią dane osobowe J. O.



Wyrok WSA w Warszawie z 11 lipca 2022 r., II SA/Wa 3993/21

- Spółka w odpowiedzi z 13 sierpnia 2021 r. wyraziła stanowisko, że numer IP/ID użytkownika nie daje jej możliwości zidentyfikowania osoby odwiedzającej jej stronę internetową, a co za tym idzie, że nie przetwarzała danych osobowych uczestnika postępowania w tym zakresie, bowiem informacje te nie stanowią dla niej danych osobowych. Złożyła także do akt sprawy dokumenty mające jej zdaniem potwierdzać brak możliwości identyfikacji użytkownika strony. Mimo to, Prezes UODO nie prowadził w toku postępowania jakichkolwiek czynności w celu ustalenia, czy informacje objęte rozstrzygnięciem zaskarżonej decyzji, tj. adres IP oraz sztucznie nadany ID z cookies w istocie są informacjami o możliwej do zidentyfikowania osobie fizycznej, tj. takiej, którą można bezpośrednio lub pośrednio zidentyfikować (art. 4 pkt 1 rodo).



Wyrok WSA w Warszawie z 11 lipca 2022 r., II SA/Wa 3993/21

- W uzasadnieniu zaskarżonej decyzji odwołał się natomiast do wywiedzionych w wyroku Naczelnego Sądu Administracyjnego z 19 maja 2011 r. (I OSK 1079/10) warunków kwalifikacji adresu IP jako danej osobowej, jednak nie wyjaśnił, czy w realiach przedmiotowej sprawy są one spełnione. Z akt sprawy nie wynika, czy adres IP przypisany do interfejsu sieciowego urządzenia, za pomocą którego J. O. nawiązał połączenie w celu odwiedzenia strony internetowej skarżącej był adresem stałym czy zmiennym.



Wyrok Trybunału w sprawie C-597/19

Systematyczne rejestrowanie adresów IP użytkowników oraz udostępnianie ich nazw i adresów pocztowych podmiotowi praw własności intelektualnej lub osobie trzeciej w celu umożliwienia wytoczenia powództwa o odszkodowanie jest, pod określonymi warunkami, dopuszczalne.

Inicjatywy i żądania kierowane w tym zakresie powinny być uzasadnione, proporcjonalne i nie mieć znamion nadużycia, a ponadto powinny one być ustanowione w krajowym środку ustawodawczym ograniczającym zakres praw i obowiązków wynikających z przepisów prawa Unii.



Opinia rzecznik generalnej w sprawie C-115/22 | NADA

Rzecznik generalna Tamara Ćapeta uważa, że krajowy organ antydopingowy, który publikuje w internecie dane osobowe sportowca zawodowego na dopingu nie narusza rodo.

- Rodo zezwala na przetwarzanie danych osobowych w z góry określonym kontekście bez konieczności przeprowadzania jakiegokolwiek zindywidualizowanej oceny proporcjonalności. Decyzja ustawodawcy austriackiego o ustanowieniu wymogu ujawnienia społeczeństwu danych osobowych sportowców zawodowych naruszających przepisy antydopingowe nie podlega zatem dodatkowej ocenie proporcjonalności w każdym indywidualnym przypadku.



Opinia rzecznik generalnej w sprawie C-115/22 | NADA

Ingerencja w prawa sportowców zawodowych wynikająca z publicznego ujawnienia informacji może być uzasadniona prewencyjnym celem polegającym na odstraszeniu młodych sportowców przed popełnianiem naruszeń antydopingowych i informowaniu zainteresowanych stron.

- Rzecznik generalna Tamara Čápetá wyjaśniła również, że w nowoczesnych społeczeństwach jedynym sposobem spełnienia ogólnego obowiązku ujawnienia informacji, takiego jak nałożony przez ustawodawcę austriackiego w niniejszej sprawie, jest publikacja w internecie.



Wyrok Trybunału w sprawie C-205/21

Systematyczne gromadzenie danych biometrycznych i genetycznych każdej osoby, której przedstawiono zarzuty, dla celów ich rejestracji policyjnej jest niezgodne z wymogiem zapewnienia wzmocnionej ochrony w odniesieniu do przetwarzania wrażliwych danych osobowych.

W wydanym wyroku Trybunał uściślił przede wszystkim warunki, na jakich przetwarzanie danych biometrycznych i genetycznych przez organy policji może być uznane za dozwolone prawem krajowym w rozumieniu dyrektywy 2016/680. Orzekł on następnie w przedmiocie stosowania wskazanego w tej dyrektywie wymogu dotyczącego danych kategorii osób, w odniesieniu do których istnieją poważne podstawy do stwierdzenia, że uczestniczyły one w popełnieniu przestępstwa, a także w przedmiocie poszanowania prawa do skutecznej ochrony sądowej oraz zasady domniemania niewinności w wypadku, gdy ustawodawstwo krajowe umożliwia właściwemu sądowi krajowemu udzielenie zezwolenia na przymusowe zbieranie danych uznanych za „wrażliwe” przez prawodawcę Unii.



Wyrok Trybunału w sprawach połączonych C-793/19

- Trybunał Sprawiedliwości potwierdził, że unijne prawo sprzeciwia się uogólnionemu i niezróżnicowanemu zatrzymywaniu danych o ruchu i danych dotyczących lokalizacji, z wyjątkiem przypadków poważnego zagrożenia dla bezpieczeństwa narodowego.

Sprzeczne z prawem Unii są krajowe środki ustawodawcze przewidujące, do celów zwalczania poważnej przestępczości i zapobiegania poważnym zagrożeniom dla bezpieczeństwa **publicznego**, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych dotyczących lokalizacji.



Wyrok Trybunału w sprawach połączonych C-793/19

- Prawo unijne nie sprzeciwia się natomiast przepisom krajowym – umożliwiającym, w celu ochrony bezpieczeństwa **narodowego**, nakazanie dostawcom usług łączności elektronicznej uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych dotyczących lokalizacji, w sytuacjach, gdy dane państwo członkowskie napotyka poważne zagrożenie dla bezpieczeństwa **narodowego**, które okazuje się rzeczywiste i aktualne lub możliwe do przewidzenia. Taki nakaz może podlegać kontroli sądu lub niezależnego organu administracyjnego i może zostać wydany jedynie na określony czas, ograniczony do tego, co ściśle niezbędne, jednak z możliwością przedłużenia w przypadku utrzymywania się tego zagrożenia.



Opinia rzecznika generalnego w sprawie C-340/21

- Niezgodny z prawem dostęp osób trzecich do danych osobowych pociąga za sobą odpowiedzialność administratora za domniemaną winę i może prowadzić do powstania podlegającej naprawieniu szkody niemajątkowej.
- Aby administrator mógł zostać zwolniony z odpowiedzialności, musi udowodnić, że w żaden sposób nie odpowiada za zdarzenie, które doprowadziło do powstania szkody. Obawa przed nieuczciwym wykorzystaniem danych osobowych w przyszłości może stanowić szkodę niemajątkową uprawniającą do odszkodowania jedynie pod warunkiem, że chodzi o rzeczywistą i pewną szkodę emocjonalną, a nie o zwykłą trudność lub niedogodność



Wyrok Trybunału w sprawie C-487/21

- Prawo do uzyskania „kopii” danych osobowych oznacza przekazanie osobie, której dane dotyczą, wiernej i zrozumiałej kopii wszystkich tych danych.
- Prawo to obejmuje prawo do uzyskania kopii fragmentów dokumentów, całych dokumentów lub wyciągów z baz danych, które zawierają te dane, jeżeli jest to niezbędne, aby umożliwić osobie, której dane dotyczą, skuteczne wykonywanie praw przyznanych jej przez rodo.



Wyrok Trybunału w sprawie C-460/20

- Prawo do usunięcia danych („prawo do bycia zapomnianym”): operator wyszukiwarki powinien usunąć linki do informacji zawartych w treści, do której odsyłają te linki w sytuacji, gdy osoba żądająca ich usunięcia udowodni, że informacje te są w oczywisty sposób nieprawdziwe.



Wyroki TSUE w sprawach C-579/21 i C-154/21

- Każdy ma prawo wiedzieć, kiedy i dlaczego były przeglądane jego dane osobowe.
- Każdy ma prawo wiedzieć, komu zostały przekazane dotyczące go dane osobowe.



Wyrok Trybunału w sprawie C-597/19

- Dostęp w celach karnych do zbioru danych pochodzących z łączności elektronicznej i dotyczących ruchu lub lokalizacji, które pozwalają na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego, jest dozwolony jedynie w celu zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom bezpieczeństwa publicznego.



Opinia rzecznika generalnego w sprawie C-252/21 | Meta Platforms i in. (Ogólne warunki korzystania z sieci społecznościowej)

- Organ ochrony konkurencji może, w ramach wykonywania przysługujących mu uprawnień, wziąć pod uwagę to, czy dana praktyka handlowa jest zgodna z ogólnym rozporządzeniem o ochronie danych (rodo).
- Wyrok Trybunału w sprawie C-34/21
- Transmitowanie na żywo w formie wideokonferencji publicznego nauczania szkolnego podlega rodo.



Wyrok Trybunału w sprawie C-132/21 | Nemzeti Adatvédelmi és Információszabadság Hatóság

Środki administracyjne i środki ochrony prawnej przed sądem cywilnym przewidziane przez ogólne rozporządzenie o ochronie danych mogą być wykonywane równocześnie i niezależnie od siebie.

- Rodo przewiduje różne środki ochrony prawnej osobom powołującym się na naruszenie tych przepisów, przy czym każdy z tych środków powinien być wykonywany „bez uszczerbku” dla pozostałych. Zatem nie przewiduje ono pierwszeństwa lub wyłączności ani żadnej zasady nadrzędności oceny dokonanej przez organ kontroli lub sąd w odniesieniu do istnienia naruszenia danych praw. W konsekwencji Trybunał zauważył, że środki administracyjne i środki ochrony prawnej przed sądem cywilnym przewidziane przez rodo mogą być wykonywane równocześnie i niezależnie od siebie.



Wyrok Trybunału w sprawie C-300/21 | Österreichische Post (szkoda niemajątkowa związana z przetwarzaniem danych osobowych)

- Samo naruszenie rodo nie daje prawa do odszkodowania.
- Prawo do odszkodowania przewidziane w rodo jest podporządkowane, w jednoznaczny sposób, trzem kumulatywnym przesłankom: naruszenie rodo, szkoda majątkowa lub niemajątkowa wynikająca z tego naruszenia i związek przyczynowy między szkodą a naruszeniem. Stąd każde naruszenie rodo, samo w sobie, nie rodzi prawa do odszkodowania.
- Prawo do odszkodowania nie jest zastrzeżone dla szkód majątkowych osiągających określoną wagę. Rodo nie wspomina o takim wymogu i takie ograniczenie zaprzeczałoby szerokiej koncepcji pojęcia „szkody” przyjętej przez prawodawcę Unii.



Dziękuję za uwagę

VI FORUM INFORMACJI
i Ochrony Danych Osobowych

