Ochrona danych osobowych w telekomunikacji.

Glosa do wyroku Naczelnego Sądu Administracyjnego w Warszawie z dnia 21 lutego 2014 r. (I OSK 2324/12, LEX nr 1427782)

Przepisy prawa telekomunikacyjnego i ustawy o ochronie danych osobowych należy interpretować łącznie, mając na uwadze przepisy Konstytucji. Artykuł 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych dopuszcza ich przetwarzanie, gdy jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów. Takim celem jest między innymi ściganie sprawców przestępstw, również z oskarżenia prywatnego.

I.

Komentarz do powyższej tezy poprzedzony musi zostać przywołaniem kontekstu faktycznego i prawnego sprawy. Przedmiotowy wyrok Naczelnego Sądu Administracyjnego (dalej: NSA) wydany został w następstwie rozpatrzenia skargi kasacyjnej od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie (dalej: WSA w Warszawie) z dnia 18.06.2012 r. (sygn. akt II SA/Wa 842/12) w sprawie ze skargi na decyzję Generalnego Inspektora Ochrony Danych Osobowych (dalej: GIODO) w przedmiocie odmowy udostępnienia danych osobowych. Wyrokiem NSA uchylono zaskarżony wyrok i przekazano sprawę do ponownego rozpoznania sądowi I instancji. Wspomniana powyżej decyzja GIODO, wydana po ponownym rozpatrzeniu sprawy, na podstawie art. 138 § 1 pkt 1 ustawy z 14.06.1960 r. – Kodeks postępowania administracyjnego (t.j. Dz. U. z 2013 r. poz. 267, ze zm.), art. 159 i art. 161 ustawy z 16.07.2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2013 r., poz. 243, ze zm.; dalej: P.t) oraz art. 5, art. 12 pkt 2 i art. 22 ustawy z 29.08.1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.; dalej: u.o.d.o.). Utrzymywała ona w mocy decyzję poprzedzającą, w której odmówiono stronie uwzględnienia wniosku o nakazanie przedsiębiorcy telekomunikacyjnemu udostępnienia danych użytkownika domeny internetowej, posługującego się zidentyfikowanym adresem IP, który dokonał zniesławiającego stronę wpisu. W wyroku WSA w Warszawie uznano, iż *„żądane przez skarżącego dane osobowe dotyczące użytkownika domeny internetowej (…) posługującego się adresem IP (…), który (…) dokonał zniesławiającego go wpisu, podlegają, jak słusznie uznał organ, ochronie przewidzianej z ustawy – Prawo telekomunikacyjne w związku z art. 5 ustawy o ochronie danych osobowych”*. Sąd I instancji podzielił przy tym stanowisko wyrażone w wyroku NSA z 26.01.2009 r. (I OSK 174/08), że *„art. 159 ust. 2 Prawa telekomunikacyjnego jest przepisem przewidującym silniejszą ochronę danych, niż przepis art. 23 ust. 1 ustawy o ochronie danych osobowych i to dlatego to on znajdzie zastosowanie jako podstawa legalizująca przetwarzanie danych objętych tajemnicą telekomunikacyjną”*. Podkreślił przy tym, iż co prawda ustawodawca w przepisie art. 159 ust. 4 P.t. *„przewidział możliwość zwolnienia z zachowania tajemnicy telekomunikacyjnej, ale prawo do tego zostało zastrzeżone wyłącznie dla sądu lub prokuratora”*. Zdaniem WSA w Warszawie GIODO *„zasadnie odmówił skarżącemu pozytywnego rozpatrzenia*

jego wniosku, gdyż jego pozytywne rozpatrzenie doprowadziłoby do nieuprawnionego ujawnienia danych osobowych".

Odnosząc się do przywołanej na wstępie tezy sformułowanej w wyroku NSA z 21.02.2014 r. (I OSK 2324/12), odnieść wypada się do dwóch zagadnień. Po pierwsze, kwestii interpretacji przepisów ustawy Prawo telekomunikacyjne i ustawy o ochronie danych osobowych z uwzględnieniem przepisów Konstytucji Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483, ze zm.; dalej: Konstytucja RP). Po drugie, dopuszczalności przetwarzania danych osobowych w odniesieniu do postępowania w sprawach o przestępstwa prywatnoskargowe.

II.

Pogląd wyrażony przez NSA w odniesieniu do zasad interpretacji ustawy w oparciu o Konstytucję RP nie budzi żadnych wątpliwości. Oczywistym jest, iż interpretacja każdego przepisu rangi ustawowej dokonywana powinna być z uwzględnieniem norm rangi konstytucyjnej, zwłaszcza wówczas, gdy dotyczą one materii praw i wolności jednostki. Sama Konstytucja RP dokonuje klasyfikacji praw i wolności na prawa i wolności osobiste, polityczne, ekonomiczne, socjalne i kulturalne. Jeśli chodzi o te, które odgrywają naczelną rolę w odniesieniu do ochrony danych osobowych i reguł ich przetwarzania, to mowa tutaj przede wszystkim o postanowieniach przepisów art. 47, 49 i 51 Konstytucji RP, w których poręczono – prawo do ochrony prawnej życia prywatnego (art. 47 Konstytucji RP), wolność i ochronę tajemnicy komunikowania się (art. 49 Konstytucji RP), a w konsekwencji uzależniono możliwość zobowiązania jednostki do ujawnienia informacji jej dotyczącej od decyzji ustawodawcy i to ze względu na interes publiczny (art. 51 Konstytucji RP). Należą one do praw i wolności osobistych, których jednakże nie sposób interpretować pomijając wymiar konstytucyjny *„przyrodzonej godności człowieka"*, wymienionej już w Preambule Konstytucji RP, a następnie w przepisie art. 30 Konstytucji RP stanowiącym – *„Przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych."*. Dodać należy, że Sąd Najwyższy w wyroku z 21.03.2007 r. (I CSK 292/06, LEX nr 308851) zdefiniował pojęcie godności osobistej, uznając, iż jest ona *„wewnętrznym przekonaniem człowieka o swoim moralnym i etycznym nieposzlakowaniu oraz czci, jako wyrazu pozytywnego ustosunkowania się innych ludzi do wartości osobistej i społecznej określonej jednostki"*. W świetle takiego jej postrzegania można pokusić się o stwierdzenie, iż cześć człowieka stanowi wartość wyższą aniżeli tajemnica komunikowania się i towarzyszące jej prawo do ochrony danych osobowych, co uzasadnia możliwość udostępnienia tych ostatnich dla dochodzenia prawnej ochrony czci jednostki.

III.

Co do drugiej części tezy, to zwrócić należy uwagę na kilka kwestii. Po pierwsze, na kwestię objęcia adresu IP pojęciem danych osobowych. Po drugie, na treść pojęcia prawnie usprawiedliwionego celu względem zamiaru wszczęcia postępowania w sprawie o przestępstwo prywatnoskargowe. Po trzecie, na istotę samego przestępstwa zniesławienia.

Odnosząc się do charakteru prawnego adresu IP, stwierdzić należy, że w świetle dotychczasowego orzecznictwa NSA, może być on traktowany jako dane osobowe, jeżeli jest na stałe lub przez dłuższy okres czasu przypisany do określonego urządzenia, użytkowanego przez określony

podmiot[1]), ponieważ stanowi wówczas informację pozwalającą zidentyfikować konkretną osobę fizyczną. Dodać należy, iż jakkolwiek tajemnica komunikowania się, o której mowa w przepisie art. 49 Konstytucji RP, jest to dawna tajemnica korespondencji, poszerzona o pewne elementy związane chociażby ze współczesnym rozwojem technologicznym, to zakresem tajemnicy telekomunikacyjnej objęta jest w tym przypadku nie tylko sama treść przekazu, jak miało to miejsce przy wymianie korespondencji za pośrednictwem poczty tradycyjnej, ale również dane dotyczące użytkowników tj. podmiotów, które korzystają z publicznie dostępnej sieci telekomunikacyjnej lub żądają świadczenia takiej usługi (art. 2 pkt 49 P.t.).

W myśl postanowień przepisu art. 23 ust. 1 pkt 5 u.o.d.o., przetwarzanie danych jest dopuszczalne wtedy, gdy *„jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą”*, przy czym za taki „prawnie usprawiedliwiony cel” uważa się w szczególności *„dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej”*, a zatem dochodzenie roszczeń na drodze cywilnoprawnej. Przypomnieć zatem warto w tym kontekście wyrok WSA w Warszawie z 2.12.2013 r. (II SA/Wa 1400/13, LEX nr 1421795), w którym wyraził on opinię, że *„Analiza treści art. 23 u.o.d.o. prowadzi do wniosku, iż adres zamieszkania osoby fizycznej trudno zaliczyć do kategorii prawnie chronionych dóbr osobistych. Ważyć przy tym należy interesy obu stron, tj. wnioskodawcy i osoby, której dotyczą żądane przez niego dane osobowe.”*, zaś *„Odmowa udostępnienia skarżącemu danych osobowych, w sytuacji gdy poszukuje on sądowej ochrony swoich dóbr osobistych, naruszonych jego zdaniem m.in. w wyniku działań pozwanego, prowadziłoby do nieuzasadnionej ochrony osoby, którą pozwał do sądu.”*.

Uzupełniając, przywołać wypada jednak również wyrok z 7.10.2011 r. (II SA/Wa 364/11, LEX nr 950577), gdzie WSA w Warszawie stwierdził, że *„Dane autorów internetowych wpisów ukrywających się pod pseudonimami mogą być ujawnione tylko w razie wniesienia pozwu do sądu. Sam zamiar skierowania sprawy do sądu nie wystarczy.”*. Taka wykładnia sugerowałaby zatem, iż w przypadku postępowania w sprawie o przestępstwo ścigane z oskarżenia prywatnego, dopuszczalne jest udostępnienie danych osobowych dotyczących użytkownika domeny internetowej posługującego się adresem IP, o ile wniósł on do sądu prywatny akt oskarżenia w sprawie o przestępstwo zniesławienia, o którego istocie będzie jeszcze mowa w końcowej części niniejszych rozważań.

Nie sposób nie zwrócić w tym kontekście uwagi także na relację postanowień ustawy Prawo telekomunikacyjne i ustawy o ochronie danych osobowych. Zgodnie z postanowieniami art. 5 u.o.d.o., w sytuacji, gdy przepisy odrębnych ustaw przewidują ochronę danych osobowych dalej idącą, aniżeli przewiduje to ustawa o ochronie danych osobowych, to mają one zastosowanie. Zdaniem doktryny, przepisy ustawy Prawo telekomunikacyjne przewidują, co do zasady, taką dalej idącą ochronę danych osobowych, obejmując pojęciem tajemnicy telekomunikacyjnej szerszy zakres treści i danych osobowych[2]). Wspomnieć trzeba również, że NSA w wyroku z 26.01.2009 r. zajął stanowisko, że *„art. 159 ust. 2 Prawa telekomunikacyjnego jest przepisem przewidującym silniejszą ochronę danych, niż przepis art. 23 ust. 1 ustawy o ochronie danych osobowych i to dlatego to on znajdzie zastosowanie jako podstawa legalizująca przetwarzanie danych objętych*

[1] Zob. wyrok WSA w Warszawie z 3.02.2010 r., II SA/Wa 1598/09, http://orzeczenia.nsa.gov.pl/doc/AD6FF02867; wyrok NSA z 19.05.2011 r., I OSK 1079/10, http://orzeczenia.nsa.gov.pl/doc/42DC7AE3F0

[2] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013, s. 951.

tajemnicą telekomunikacyjną"[3]. Niemniej jednak, czy w przedmiotowej sytuacji kluczowe znaczenie ma zakres ochrony danych osobowych i kwestia nadrzędności ustawy Prawo telekomunikacyjne względem ustawy o ochronie danych osobowych. Podkreślić trzeba, że przepis art. 159 ust. 2 pkt 4 P.t., dopuszcza możliwość zapoznania się z danymi objętymi tajemnicą telekomunikacyjną przez inne osoby niż nadawca i odbiorca komunikatu, gdy *„będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi"*? Czy nie oznacza to, że tym „innym powodem przewidzianym ustawą" jest *„wypełnienie prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych",* o których mowa w przepisie art. 23 ust. 1 pkt 5 u.o.d.o.?

Podzielenie poglądu, iż ustawa Prawo telekomunikacyjne kreuje dalej idącą ochronę aniżeli ustawa o ochronie danych osobowych, nie oznacza bowiem, że wykluczone jest udostępnienie danych chronionych tą pierwszą ustawą z uwagi na „prawnie usprawiedliwiony cel", o którym mowa w art. 23 ust. 1 pkt 5 u.o.d.o. W takim przypadku niezbędna wydaje się jednak każdorazowa redefinicja pojęcia „prawnie usprawiedliwionego celu", wynikająca tak z konkretnych uwarunkowań formalnoprawnych, w szczególności natury konstytucyjnej, jak i z sytuacji faktycznej. W konsekwencji, w świetle okoliczności faktycznych i prawnych stanowiących podstawę wydania glosowanego wyroku, należy postawić sobie nie tylko pytanie, czy prymat przyznać należy ustawie Prawo telekomunikacyjne, czy ustawie o ochronie danych osobowych, ale czy może przysługuje on ustawie karnej poddającej ochronie cześć człowieka jako dobro szczególnie istotne ze społecznego punktu widzenia. Zatem, czy większą wartością jest ochrona tajemnicy telekomunikacyjnej, danych osobowych *in genere*, czy dóbr osobistych, których naruszenie jest prawdopodobne. Tym bardziej, iż rozwój narzędzi związanych ze środkami komunikacji elektronicznej oraz upowszechnienie komunikowania się za ich pomocą (zwłaszcza za pośrednictwem Internetu) sprawia, że wyrażane opinie mają częstokroć charakter anonimowy, zaś osoba, której dobra osobiste naruszono, ma ograniczone możliwości, jeśli ma je w ogóle, identyfikacji sprawcy tegoż naruszenia. Uczestnik wymiany informacji powinien zdawać sobie jednak sprawę, że wyrażając pogląd godzący w czyjeś dobra osobiste (zwłaszcza w sytuacji, gdy może on dotrzeć do nieokreślonej i znaczącej liczby osób) liczyć musi się z możliwością poniesienia odpowiedzialności z tytułu zniesławienia.

Z tego też powodu przypomnieć trzeba inny jeszcze wyrok z 9.11.2012 r. (II SA/Wa 124/12, LEX nr 1249063), gdzie WSA w Warszawie wyraził z kolei pogląd, iż: *„Osoba, która czuje się pokrzywdzona poprzez naruszenie dóbr osobistych ma niewątpliwie prawo dochodzenia przysługujących jej z tego tytułu roszczeń. Takie uprawnienia gwarantuje jej Konstytucja RP (art. 45 ust. 1) oraz przepisy Kodeksu cywilnego. Zatem jeżeli zdecyduje się na podjęcie na drodze sądowej stosownych kroków, to należy rozważyć zasadność udostępnienia jej adresu takiego abonenta, gdyż brak takich danych nie może ograniczać jej prawa do merytorycznego rozpoznania sprawy przez sąd powszechny. Niewskazanie przez powoda miejsca zamieszkania pozwanego wprawdzie nie wyklucza dopuszczalności złożenia pozwu, ale uniemożliwia nadanie mu prawidłowego biegu, a tym samym może skutkować podjęciem przez przewodniczącego czynności przewidzianych w art. 130 § 2 k.p.c. W toku zaś wszczętego procesu przedmiotowy brak może stanowić przesłankę do zawieszenia postępowania na podstawie art. 177 § 1 pkt 6 k.p.c. Dlatego należy przyjąć, że uzasadniona potrzeba posiadania danych adresowych abonenta, który naruszył dobra*

[3] I OSK 174/08, http://orzeczenia.nsa.gov.pl/doc/55EABF3AB6

prawem chronione w znaczeniu przewidzianym w art. 29 ust. 2 ustawy o ochronie danych osobowych, mogła ewentualnie zachodzić, ale dopiero po wszczęciu przez poszkodowanego procesu.". Skoro pokrzywdzony może domagać się zatem dochodzenia swoich praw na gruncie procedury cywilnej, to tym bardziej powinien mieć taką możliwość w procesie karnym, jeśli ustawodawca poddaje określone dobro ochronie nie tylko cywilnoprawnej, ale i prawnokarnej.

Kilka słów poświęcić należy wreszcie istocie przestępstwa zniesławienia ściganego z oskarżenia prywatnego, o którym mowa w przepisie art. 212 ustawy z 6.06.1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.). Nadmienić trzeba już na wstępie, że przedmiotem ochrony jest tutaj cześć, stanowiąca składową godności człowieka, o której mowa w przywołanym na wstępie niniejszych rozważań art. 30 Konstytucji RP, zaś konkretnie cześć zewnętrzna (przedmiotowa), utożsamiana z wartością, jaką dana osoba posiada w pojęciu innych ludzi tj. znaczeniem społecznym człowieka[4] .

Postępowanie prywatnoskargowe, w trybie którego dochodzi się ochrony prawnokarnej czci, jest odmianą postępowania uproszczonego uregulowaną w rozdziale 52 „Postępowanie w sprawach z oskarżenia prywatnego" ustawy z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. Nr 89, poz. 555, ze zm.; dalej: k.p.k.). Jedną z jego cech jest odformalizowanie aktu oskarżenia. Może on ograniczyć się do *„oznaczenia osoby oskarżonego, zarzucanego mu czynu oraz wskazania dowodów, na których opiera się oskarżenie"* (art. 487 k.p.k.) i stanowi *lex specialis* względem przepisów art. 332 i 333 k.p.k. ze względu na fakt, iż wnoszony bywa przez osoby niebędące prawnikami. Z oczywistych powodów musi pozwolić jednak w swej treści nie tylko na dookreślenie zarzucanego czynu i wskazanie dowodów, ale przede wszystkim na identyfikację osoby oskarżonego (analogicznie skądinąd, jak w przypadku identyfikacji pozwanego w procesie cywilnym), co może niekiedy napotkać na przeszkodę, gdy wnoszący akt oskarżenia nie może ustalić sprawcy przestępstwa[5]. W takiej sytuacji skorzystać może z prawa do wniesienia skargi do Policji, która ma obowiązek skargę przyjąć, zabezpieczyć dowody, a następnie przesłać ją do właściwego sądu (art. 488 k.p.k.). Prawo do uzyskania danych umożliwiających przeprowadzenie czynności przez Policję w takim przypadku jest niewątpliwie przesłanką usprawiedliwiającą przetwarzanie danych w sytuacji prowadzenia postępowania karnego w sprawie o przestępstwo prywatnoskargowe.

Pozostaje tylko nadmienić, że podstawą ich pozyskania może być tutaj, jak się wydaje, i przepis art. 23 ust. 2 u.o.d.o., stanowiący, iż przetwarzanie danych osobowych (a zatem i udostępnianie w myśl postanowień przepisu art. 7 pkt 2 u.o.d.o.) jest dopuszczalne również wówczas, gdy *„jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa"*. Pogląd ten podzielić trzeba tym bardziej, że zdaniem doktryny, posługując się tą przesłanką, *„uwzględniać należy przepisy należące do wielu dziedzin prawa, jak choćby prawa handlowego, bankowego, podatkowego, ubezpieczeń społecznych, a także procedur sądowych (karnej i cywilnej) oraz administracyjnej w zakresie przeprowadzania postępowania dowodowego"*[6].

Mariusz Czyżak
Doktor nauk prawnych. Urząd Komunikacji Elektronicznej

[4] M. Mozgawa, *Komentarz do art. 212 Kodeksu karnego*, stan prawny na 2013.01.01., LEX.

[5] P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz*, T. II, Wydawnictwo C.H.Beck, Warszawa 1999, s. 718.

[6] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, LEX 2011, komentarz do art. 23.