

*Marek Chrabkowski*

Wyższa Szkoła Administracji i Biznesu, Gdynia

m.chrabkowski@wsaib.pl

## Dane bilingowe jako dowód w postępowaniu w sprawach o wykroczenia

DOI: <http://dx.doi.org/10.12775/SIT.2017.027>

### 1. Wstęp

Dziennikarka Dorota Gajos-Kaniewska w swoim artykule prasowym przedstawiła kulisy postępowania w sprawie o wykroczenie, które rozpatrywane było w I instancji przez Sąd Rejonowy w Mińsku Mazowieckim oraz w II instancji przez Sąd Okręgowy w Siedlcach<sup>1</sup>. Sąd *meriti* uznał pozwaną za winną wykroczenia z art. 97 k.w., polegającego na rozmawianiu przez telefon komórkowy, wymagający trzymania słuchawki i mikrofonu w rękę, podczas kierowania samochodem, za co wymierzył jej karę grzywny w wysokości 200 zł. Obwiniona odwołała się od wyroku, zarzucając w apelacji błąd w ustaleniach faktycznych. Skarżąca konsekwentnie zaprzeczała, że dopuściła się zarzucanego jej wykroczenia, i jej zdaniem sąd

---

<sup>1</sup> D. Gajos-Kaniewska, *Sąd: nie będzie mandatu za używanie komórki podczas jazdy, bo policja nie zadbała o dowody*, „Rzeczpospolita” 14.11.2016, <http://www.rp.pl/Prawo-drogowe/311149999-Sad-nie-bedzie-mandatu-za-uzywanie-komorki-podczas-jazdy-bo-policja-nie-zadbala-o-dowody.html#ap-1> (dostęp: 17.11.2016 r.).

I instancji nie zebrał dowodów, które by to potwierdzały<sup>2</sup>. W wyroku z 26 października 2016 r. Sąd Okręgowy w Siedlcach<sup>3</sup> po rozpoznaniu apelacji uznał jej zasadność i uniewinnił pozwaną. W uzasadnieniu tego orzeczenia stwierdzono, że jedynym dowodem oskarżenia jest zeznanie policjanta przeprowadzającego kontrolę. Wprawdzie potwierdził on, że obwiniona rozmawiała przez telefon, trzymając urządzenie w ręce, ale zdaniem sądu ustalenie w takiej sytuacji, jak było faktycznie, wymagało zażądania od operatora sieci telefonii komórkowej informacji, czy nawiązano połączenie z telefonu i jaki czas trwała rozmowa. W ocenie Sądu Okręgowego w Siedlcach dowód ten był niezbędny, zwłaszcza że zdarzenie miało miejsce we wrześniu około godz. 19.40, a więc o zmierzchu, a pojazdy obwinionej i świadka były wówczas w ruchu. Wymienione okoliczności nasunęły wątpliwości sądu *ad quem*, czy faktycznie obwiniona trzymała w trakcie kierowania pojazdem przy uchu telefon komórkowy, który nie był podświetlony, a jeśli tak czy prowadziła rozmowę telefoniczną. Sąd odwoławczy zwrócił się więc do operatora sieci o ujawnienie danych chronionych tajemnicą telekomunikacyjną. Przedsiębiorca nie przekazał żądanych informacji, ponieważ dane o połączeniach przechowywane są w jego systemach przez 12 miesięcy, a okres ten upłynął przed wpływieniem sądowego wezwania. Powstałe wątpliwości zostały rozstrzygnięte na korzyść obwinionej, i na tej podstawie Sąd Okręgowy w Siedlcach uniewinnił ją od popełnienia wykroczenia zarzucanego jej we wniosku o ukaranie.

W przedstawionej sprawie sąd *ad quem* nie miał wątpliwości co do możliwości sięgnięcia w sprawie o wykroczenie po dane chronione tajemnicą telekomunikacyjną. Nie pojawiły się one również u przedsiębiorcy telekomunikacyjnego, który był skłonny przekazać sądowi żądane dane i nie uczynił tego tylko z powodu ich usunięcia

---

<sup>2</sup> Uzasadnienie wyroku Sądu Okręgowego w Siedlcach z 26 października 2016 r., sygn. akt. II Ka 426/16, [http://orzeczenia.siedlce.so.gov.pl/content/\\$N/15301500001006\\_II\\_Ka\\_000426\\_2016\\_Uz\\_2016-10-26\\_001](http://orzeczenia.siedlce.so.gov.pl/content/$N/15301500001006_II_Ka_000426_2016_Uz_2016-10-26_001) (dostęp: 18.10.2017 r.).

<sup>3</sup> Wyrok Sądu Okręgowego w Siedlcach z 26 października 2016 r., sygn. akt. II Ka 426/16, [http://orzeczenia.siedlce.so.gov.pl/content/\\$N/15301500001006\\_II\\_Ka\\_000426\\_2016\\_Uz\\_2016-10-26\\_001](http://orzeczenia.siedlce.so.gov.pl/content/$N/15301500001006_II_Ka_000426_2016_Uz_2016-10-26_001) (dostęp: 18.10.2017 r.).

z pamięci serwerów w związku z upływem ustawowego okresu retencji tego typu danych. Przedstawiona sprawa skłania do refleksji nad zakresem wykorzystywania danych chronionych tajemnicą korespondencji. W związku z tym przeprowadzono badania, których celem było udzielenie odpowiedzi na następujące pytanie badawcze: czy sąd, prowadząc postępowanie w sprawie o wykroczenie, jest uprawniony do dowodowego wykorzystania danych chronionych tajemnicą telekomunikacyjną? Brak wątpliwości po stronie Sądu Okręgowego w Siedlcach, że może takich danych zażądać, i przedsiębiorcy telekomunikacyjnego, że powinien takie dane udostępnić, zdecydowały o przyjęciu następującej hipotezy badawczej: sąd jako organ prowadzący postępowanie w sprawie o wykroczenie na etapie jurysdykcyjnym jest uprawniony do uzyskania od przedsiębiorcy telekomunikacyjnego danych bilingowych, jeżeli dane te mają znaczenie dla rozstrzyganej sprawy, a przedsiębiorca telekomunikacyjny jest zobowiązany takie dane sądowi udostępnić.

Przyjęta hipoteza badawcza zdeterminowała strukturę publikacji. W artykule w odrębnych śródtytułach przedstawiono zagadnienia dotyczące:

- kwestii doprecyzowujących zakres terminu „dane bilingowe”;
- kształtu uniwersalnego standardu europejskiego w zakresie gromadzenia i przetwarzania danych bilingowych;
- możliwości udostępniania danych bilingowych na żądanie sądu rozstrzygającego sprawę o wykroczenie.

Badania przeprowadzono z wykorzystaniem metod badawczych w postaci: krytycznej analizy literatury, badania prawa i badania dokumentów w formie analizy orzecznictwa sądowego. Wnioski z przeprowadzonych badań zostały zawarte w zakończeniu.

## 2. Dane bilingowe

Tajemnica telekomunikacyjna jest zaliczana do szeroko rozumianej tajemnicy przedsiębiorstwa<sup>4</sup>. W Ustawie z 16 lipca 2004 r. Prawo

---

<sup>4</sup> A. Michalak, *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, Kraków 2006, s. 55.

telekomunikacyjne (dalej: pr.tel.)<sup>5</sup> nie zawarto definicji legalnej tej tajemnicy<sup>6</sup>. Jej zakres został wskazany w formie zamieszczonego w art. 159 ust. 1 pr.tel. katalogu, który obejmuje:

- dane dotyczące użytkownika;
- treść indywidualnych komunikatów;
- dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;
- dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
- dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

Dodatkowo dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną<sup>7</sup>:

- nazwisk i imion;
- imion rodziców;
- miejsca i daty urodzenia;
- adresu miejsca zamieszkania i adresu korespondencyjnego, jeżeli jest on inny niż adres miejsca zamieszkania;
- numeru ewidencyjnego PESEL – w przypadku obywatela Rzeczypospolitej Polskiej;

---

<sup>5</sup> Tekst jednolity: Dz.U. z 2017 r., poz. 1907.

<sup>6</sup> S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych*, Opole 2006, s. 265.

<sup>7</sup> Art. 161 ust. 2 pr.tel.

- nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego UE albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu;
- zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych.

Dane te, jako dotyczące użytkownika, objęte są również tajemnicą telekomunikacyjną. Oprócz tych informacji, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych<sup>8</sup>. Te dane, również jako informacje o użytkowniku, objęte są tajemnicą telekomunikacyjną, a dodatkowo w odniesieniu do instrumentów finansowych również tajemnicą bankową.

Przedsiębiorcy telekomunikacyjni w związku z realizacją zadań na rzecz bezpieczeństwa i obronności państwa, a także bezpieczeństwa i porządku publicznego zobligowani są do przechowywania przez okres 12 miesięcy następujących danych chronionych tajemnicą telekomunikacyjną, które są niezbędne do<sup>9</sup>:

- ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
  - inicjującego połączenie;
  - do którego kierowane jest połączenie;
- określenia:
  - daty i godziny połączenia oraz czasu jego trwania;
  - rodzaju połączenia;
  - lokalizacji telekomunikacyjnego urządzenia końcowego.

Systematyzując rodzaje danych gromadzonych przez przedsiębiorców telekomunikacyjnych, które objęte są tajemnicą telekomunikacyjną, można dokonać ich podziału na:

---

<sup>8</sup> Art. 161 ust. 3 pr.tel.

<sup>9</sup> Art. 180c ust. 1 pr.tel.

- dane dotyczące treści przekazu telekomunikacyjnego;
- dane towarzyszące przekazowi telekomunikacyjnemu, w tym:
  - dane transmisyjne;
  - dane o próbach uzyskania połączenia;
  - dane lokalizacyjne;
- dane o abonencie.

Dane o abonencie wraz z danymi towarzyszącymi przekazowi telekomunikacyjnymi, które nie zawierają treści przekazu, a służą m.in. do rozliczenia świadczonych usług i wystawienia rachunku, dalej określane będą zbiorczą nazwą „dane bilingowe”. Informacje te łącznie z treścią przekazu stanowią kompletny zbiór danych chronionych tajemnicą telekomunikacyjną. Zaproponowany dychotomiczny podział danych objętych tajemnicą telekomunikacyjną ułatwi przedstawienie wyników badań w dalszej części publikacji, ponieważ przepisy prawne, regulujące dostęp organów państwa do tajemnicy telekomunikacyjnej, wprowadzają inny stopień ochrony dla samej treści przekazu telekomunikacyjnego, a inny w stosunku do danych bilingowych. Należy podkreślić, że poziomy ochrony danych wchodzących w zakres danych bilingowych, tj. o abonencie i danych towarzyszących przekazowi, są zbliżone, więc istnieje uzasadnienie dla łącznego ich rozpatrywania.

Bez względu na rodzaj danych objętych tajemnicą telekomunikacyjną podmiot uczestniczący w wykonywaniu działalności telekomunikacyjnej w sieciach publicznych oraz podmioty z nim współpracujące są obowiązane do jej zachowania, a do tego są zobowiązane do zachowania należytej staranności, w zakresie uzasadnionym względami technicznymi lub ekonomicznymi, przy zabezpieczaniu urządzeń telekomunikacyjnych, sieci telekomunikacyjnych oraz zbiorów danych przed ujawnieniem tajemnicy telekomunikacyjnej<sup>10</sup>. Ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej<sup>11</sup>. Treści lub dane objęte tą tajemnicą mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas,

---

<sup>10</sup> Art. 160 ust. 1 i 2 pr.tel.

<sup>11</sup> Art. 159 ust. 3 pr.tel.

gdy czynności te dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów prawa<sup>12</sup>.

### 3. Uniwersalny standard europejski w zakresie gromadzenia i przetwarzania danych bilingowych

W Polsce organy państwa mają łatwiejszy dostęp do danych bilingowych niż do treści przekazów. To zróżnicowanie nie znajduje uzasadnienia w orzecznictwie Europejskiego Trybunału Praw Człowieka w Strasburgu, który uznaje wykaz połączeń za integralną część telefonicznego porozumiewania się i mimo że jest czymś innym niż podsłuch, to jego ujawnienie może zagrozić prawom wymienionym w art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności<sup>13</sup>. W uzasadnieniu swojego stanowiska trybunał ten stwierdził, że ogólny billing rozmów telefonicznych wykorzystywany do innych celów niż związane z księgowym rozliczeniem świadczonych usług, nawet gdy odbywa się bez przechwytywania informacji, stanowi ingerencję w życie prywatne. W cenie tego organu na podstawie danych zawartych w billingu umożliwia się władzom wydedukowanie informacji, które nie są dla nich przeznaczone. Trafnie więc wyrażono obawę, że przetwarzanie tzw. „neutralnych” danych może być dotkliwie w takim samym stopniu jak przetwarzanie danych intymnych.

Uniwersalny standard europejski w zakresie gromadzenia i przetwarzania danych bilingowych przez władze publiczne został wyraźnie podkreślony przez Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 8 kwietnia 2014 r. w połączonych sprawach *High Court of Ireland* i *Verfassungsgerichtshof* z Austrii<sup>14</sup>. W sprawie tej

---

<sup>12</sup> Art. 161 ust. 1 pr.tel.

<sup>13</sup> Wyrok ETPCz z 2 sierpnia 1984 r. w sprawie *Malone przeciwko Zjednoczonemu Królestwu*, sygn. 8691/79, Legalis (dostęp: 25.10.2017 r.).

<sup>14</sup> Wyrok Trybunału Sprawiedliwości UE z 8 kwietnia 2014 r., sygn. akt C-293/12 i C-594/12, Legalis (dostęp: 16.10.2017 r.).

przedmiotem kontroli były przepisy dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE<sup>15</sup>. W wyroku tym Trybunał Sprawiedliwości UE orzekł o nieważności całej dyrektywy z uwagi na naruszenie praw podstawowych zagwarantowanych w art. 7 i 8 Karty praw podstawowych Unii Europejskiej<sup>16</sup>, które dotyczą prawa do ochrony życia prywatnego oraz prawa do ochrony danych osobowych.

Jak wynika z uzasadnienia wyroku Trybunału Sprawiedliwości UE, z uwagi na duże znaczenie środków komunikacji elektronicznej we współczesnym świecie, dane zatrzymywane na podstawie kontrolowanej dyrektywy dają krajowym organom ścigania dodatkowe możliwości wyjaśniania okoliczności poważnych przestępstw. Stanowią tym samym cenne narzędzie przy prowadzeniu czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych. Zdaniem Trybunału Sprawiedliwości UE, zatrzymywanie tego rodzaju danych należy uznać za odpowiednie dla realizacji celów zakładanych przez kontrolowaną dyrektywę. Trybunał dostrzegł, że rzeczywisty cel dyrektywy, czyli ułatwienie walki z poważnymi przestępstwami, można uznać za uzasadniony w ramach interesu ogólnego Unii Europejskiej. Zastrzeżenia Trybunału Sprawiedliwości wzbudziły natomiast inne kwestie, wśród których wskazano:

- objęcie przepisami dyrektywy osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, nawet pośredni i daleki, z poważnymi przestępstwami;
- brak wymagań co do wykazania przez organy państwa związku między danymi, które mają być zatrzymywane, a zagrożeniem dla bezpieczeństwa publicznego, w szczególności dyrektywa nie ograniczała się do zatrzymywania danych dotyczących kręgu osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem lub z innych powodów przyczynić się

---

<sup>15</sup> Dz. Urz. UE L 105 z 2006 r., s. 54–63.

<sup>16</sup> Dz. Urz. UE C 326 z 2012 r., s. 391–407.

do zapobiegania poważnym przestępstwom, ich wykrywania i ścigania;

- brak określenia obiektywnego kryterium, które gwarantowałyby, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać tylko w celu zapobiegania przestępstwom oraz wykrywania i ścigania przestępstw, co z uwagi na zakres oraz wagę ingerencji w prawa podstawowe ustanowione w art. 7 i art. 8 Karty praw podstawowych UE można uznać za wystarczająco poważne, aby tego rodzaju ingerencję uzasadnić;
- brak gwarancji proceduralnych zapobiegających nadużyciom, zwłaszcza że nie wprowadzono obowiązku uzyskania uprzedniej zgody sądu lub innego niezależnego organu na udostępnianie czy wykorzystywanie danych bilingowych.

Podkreślając wyjątkowości uprawnień organów państwa do przetwarzania danych bilingowych Trybunał Sprawiedliwości UE stwierdził, że samo odesłanie do kategorii „poważnych przestępstw” określonych w ustawodawstwie niektórych państw członkowskich, jest niewystarczające z punktu widzenia zasady proporcjonalności. Uniwersalny standard europejski w zakresie gromadzenia i przetwarzania danych bilingowych przez władze publiczne dopuszcza przetwarzanie danych bilingowych przez organy państwa w sprawach przestępstw ale – jak zaznaczono wcześniej – nie wszystkich. Dotyczy tylko tych, które zaliczane są do kategorii przestępstw poważnych. Ocena ciężaru gatunkowego czynów przestępnych uzasadniająca sięgnięcie po dane bilingowe nie może być intuicyjna, ale powinna wynikać z precyzyjnego wskazania ustawodawcy, np. w formie katalogu przestępstw – tak jak to uczyniono w przypadku przepisów regulujących operacyjny dostęp do treści przekazu telekomunikacyjnego w ramach kontroli operacyjnej. To ustawowe wskazanie typów przestępstw nie może być też nazbyt szerokie, ponieważ będzie narażone na zarzut naruszenia zasady proporcjonalności<sup>17</sup>. Ograniczenie uprawnień organów państwa do uzyskiwania

---

<sup>17</sup> W wyroku ETPCz z 10 lutego 2009 r. *Iordachi i inni przeciwko Mołdawii*, skarga nr 25198/02, uznano niedopuszczalność stosowania podsłuchów i kontroli korespondencji w postępowaniach dotyczących bliżej nieokreślonej grupy

danych bilingowych jedynie do przypadków poważnych przestępstw wyklucza możliwość pozyskiwania tych danych w sprawach innych czynów zabronionych, które w polskim systemie prawnym zaliczyć można do drobnych występków, wykroczeń skarbowych, wykroczeń, deliktów administracyjnych czy cywilnych.

#### 4. Udostępnianie danych bilingowych na potrzeby postępowań w sprawach o wykroczenia

Uniwersalny standard europejski w zakresie gromadzenia i przetwarzania danych bilingowych przez władze publiczne przewiduje dostęp do danych bilingowych tylko na potrzeby spraw dotyczących poważnych przestępstw. Kolejnym krokiem w prowadzonych badaniach było więc sprawdzenie, czy polskie prawo w zakresie spraw o wykroczenia mieści się w granicach tego standardu. W pierwszej kolejności analizie poddano przepisy Prawa telekomunikacyjnego. Zgodnie z art. 179 ust. 3 wskazanej ustawy przedsiębiorca telekomunikacyjny jest zobowiązany do realizacji zadań na rzecz bezpieczeństwa i obronności państwa oraz bezpieczeństwa i porządku publicznego, w ramach których wymaga się od niego m.in.:

- zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania, umożliwiających jednoczesne i wzajemnie niezależne:
  - uzyskiwanie przez organy operacyjne<sup>18</sup> dostępu do posiadanych przez przedsiębiorcę danych bilingowych;
  - utrwalanie przez uprawnione organy operacyjne danych bilingowych;
- utrwalania na rzecz sądu i prokuratora danych bilingowych.

---

poważnych przestępstw (ang. *very serious and exceptionally serious crimes*), potencjalnie obejmującej ponad połowę przestępstw wymienionych w mołdawskim kodeksie karnym.

<sup>18</sup> Ustawodawca wśród uprawnionych organów operacyjnych wymienia: Policję, Straż Graniczną, Agencję Bezpieczeństwa Wewnętrznego, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Centralne Biuro Antykorupcyjne i Krajową Administrację Skarbową.

Dyspozycja art. 179 ust. 3 pkt 2 pr.tel. nie precyzuje rodzaju spraw, w których sąd lub prokurator może zażądać od przedsiębiorcy telekomunikacyjnego danych bilingowych, co nie oznacza, że każdy sąd i każdy prokurator, bez względu na rodzaj prowadzonej sprawy, może zwrócić się do przedsiębiorcy telekomunikacyjnego o utrwalenie, a następnie udostępnienie danych bilingowych. Dane chronione tajemnicą telekomunikacyjną podobnie jak dane chronione tajemnicą państwową, służbową, zawodową, funkcyjną lub inną prawnie określoną mogą być udostępniane wyłącznie na zasadach określonych w odrębnych ustawach kompetencyjnych.

Mając na uwadze przedmiot badań, należy wskazać, że aktem prawnym regulującym tryb postępowania dowodowego w sprawach o wykroczenia jest Ustawa z 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (k.p.w.)<sup>19</sup>. W komentarzach do tej ustawy problem udostępniania danych bilingowych nie jest poruszany, a uwagi autorów skupiają się co najwyżej na trybie postępowania z danymi niejawnymi zabezpieczonymi podczas przeszukania<sup>20</sup>. Analiza przepisów Kodeksu postępowania w sprawach o wykroczenia prowadzi do konstatacji, że w sprawach prowadzonych w oparciu o tę procedurę wykorzystywać danych bilingowych nie wolno. Wniosek ten wynika wprost z dyspozycji art. 44 § 5 k.p.w. Zamieszczono w nim katalog przepisów, regulujących przeszukiwanie i zatrzymanie przedmiotów, które znajdują zastosowanie przy czynnościach procesowych realizowanych na potrzeby postępowań w sprawach o wykroczenia. W katalogu tym pominięto art. 218 k.p.k. Zgodnie z brzmieniem art. 44 § 5 k.p.w przy przeprowadzaniu przeszukania i zatrzymania przedmiotów w sprawach o wykroczenia stosuje się odpowiednio przepisy art. 217, 221–234 i 236 k.p.k. Brak art. 218 k.p.k., który zobowiązuje urzędy, instytucje i podmioty prowadzące działalność pocztową lub działalność telekomunikacyjną, urzędy celno-skarbowe oraz instytucje i przed-

---

<sup>19</sup> Tekst jednolity: Dz.U. z 2016 r., poz. 1713 ze zm.

<sup>20</sup> Zob. W. Kotowski, B. Kurzępa, *Kodeks postępowania w sprawach o wykroczenia. Komentarz*, Warszawa 2016, Legalis, art. 44; P. Gensikowski, *Kodeks postępowania w sprawach o wykroczenia. Komentarz*, Warszawa 2016, Legalis, art. 44.

siębiorstwa transportowe do wydania sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i art. 180d pr.tel., jeżeli mają znaczenie dla toczącego się postępowania, statuuje wyraźny zakaz dowodowy w postępowaniu w sprawach o wykroczenia, korespondujący z uniwersalnym standardem europejskim w zakresie gromadzenia i przetwarzania danych bilingowych. Pominięcie art. 218 k.p.k. należy uznać za celowe działanie ustawodawcy, który w ten sposób ograniczył zakres postępowania dowodowego, wyłączając dane bilingowe ze spektrum dopuszczalnych dowodów w sprawach o wykroczenia. Jest to czytelny sygnał z jego strony, że odtajnianie tego rodzaju danych może mieć miejsce w przypadkach poważniejszych, dotyczących czynów o większym ciężarze gatunkowym.

Wejście w posiadanie informacji objętych tajemnicą telekomunikacyjną na podstawie art. 41 § 3 zd. 1 k.p.w. byłoby obejściem zakazu dowodowego wykorzystania danych bilingowych w sprawie o wykroczenie. Zgodnie z przytoczonym przepisem osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „zastrzeżone” lub „poufne” lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd zwolni te osoby od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej. W takim przypadku na postanowienie sądu służy zażalenie<sup>21</sup>. W tym samym artykule zamieszczono *expressis verbis* wyjątki od tej reguły, zabraniając sądowi zwalniania od obowiązku zachowania tajemnicy statystycznej oraz związanej z wykonywaniem zawodu adwokata, radcy prawnego, lekarza lub dziennikarza<sup>22</sup>. Jak trafnie zauważył Maciej Rogalski przepis ten odnosi się jednak wyłącznie do obowiązków świadka, a nie do obowiązków przedsiębiorcy telekomunikacyjnego lub innego podmiotu zobowiązanego do udostępniania korespondencji i nie może on stanowić podstawy do żądania danych bilingowych przez zwolnienie z tajemnicy zwią-

---

<sup>21</sup> Art. 41 § 3 zd. 2 k.p.w.

<sup>22</sup> Art. 41 § 4 k.p.w.

zanej z wykonywaniem zawodu lub sprawowaniem funkcji, gdyż w sprawach o wykroczenia nie ma zastosowania – ani wprost, ani *per analogiam* – art. 218 § 1 k.p.k.<sup>23</sup> „Przepisu tego, przewidującego zwolnienie z tajemnicy komunikowania się w sprawach karnych, nie można stosować odpowiednio do spraw o wykroczenia, gdyż zgodnie z art. 1 § 2 k.p.w. w postępowaniach w sprawach o wykroczenia przepisy Kodeksu postępowania karnego stosuje się jedynie wówczas, gdy KPW [Kodeks postępowania w sprawach o wykroczenia – M. C.] wyraźnie tak stanowi. Nie można więc na podstawie art. 41 § 3 k.p.w. żądać wydania danych bilingowych, gdyż wykraczałoby to poza ramy przepisu pozwalającego na zwolnienie świadka z tajemnicy zawodowej czy związanej z wykonywaną funkcją. Należy też wskazać, że zwolnienie z tajemnicy musi dotyczyć okoliczności wynikających z zeznań świadka składanych przed organem prowadzącym czynności i nie może oznaczać żądania przedstawienia np. wykazu połączeń telefonicznych. Trzeba bowiem odróżnić składanie zeznań na okoliczności objęte tajemnicą związaną z wykonywaniem zawodu lub zajmowaną funkcją, gdy świadek został zwolniony z zachowania tych tajemnic, od przedkładania konkretnych informacji na piśmie w formie określonego dokumentu. Ponadto czym innym jest tajemnica zawodowa lub związana z zajmowaną funkcją, a czym innym – tajemnica telekomunikacyjna. Ustawodawca nie przewidział możliwości zwolnienia z tajemnicy telekomunikacyjnej w ramach postępowań dotyczących wykroczeń”<sup>24</sup>.

Przytoczone argumenty prowadzą do wniosku, że sąd nie jest uprawniony do zwalniania świadków z obowiązku zachowania tajemnicy telekomunikacyjnej. Po pierwsze, taka interpretacja byłaby sprzeczna z uniwersalnym standardem europejskim w zakresie gromadzenia i przetwarzania danych bilingowych. Po drugie, gdyby takie uprawnienie przysługiwało sądowi, to ustawodawca nie zrezygnowałby z możliwości wykorzystania w procedurze wykroczeniowej art. 218 k.p.k. przynajmniej w części dotyczącej danych bilingowych. Nie uczynił tego, ponieważ ingerencja w tajemnicę

---

<sup>23</sup> M. Rogalski, *Kontrola korespondencji*, Warszawa 2016, Legalis.

<sup>24</sup> Ibidem.

telekomunikacyjną, przy deliktach o charakterze głównie porządkowym, naruszyłyby zasadę proporcjonalności.

## 5. Podsumowanie

Na podstawie przeprowadzonych badań ustalono, że sąd jako organ prowadzący postępowanie w sprawie o wykroczenie na etapie jurysdykcyjnym nie jest uprawniony do uzyskania od przedsiębiorcy telekomunikacyjnego danych towarzyszących przekazowi telekomunikacyjnemu, nawet jeżeli dane te mają znaczenie dla rozstrzyganej sprawy. Zgodnie z uniwersalnym standardem europejskim organy państwa mają prawo do uzyskiwania danych bilingowych tylko w przypadkach poważnych przestępstw. Polski ustawodawca wykluczył możliwość pozyskiwania danych bilingowych w sprawach o wykroczenia. Świadczy o tym pominięcie w treści art. 44 § 5 k.p.w. jednego z przepisów Kodeksu postępowania karnego zobowiązującego m.in. instytucje i podmioty prowadzące działalność pocztową lub telekomunikacyjną do wydania sądowi lub prokuratorowi danych bilingowych, jeżeli mają znaczenie dla toczącego się postępowania. Ten zabieg legislacyjny nie pozostawia wątpliwości co do niedopuszczalności sięgania w sprawach o wykroczenie po te dane. Ten zakaz dowodowy koresponduje z uniwersalnym standardem europejskim w zakresie gromadzenia i przetwarzania danych bilingowych. Ustawodawca celowo ograniczył zakres postępowania dowodowego, sygnalizując, że odtajnianie tego rodzaju danych może mieć miejsce w przypadkach spraw poważniejszych i dotyczyć czynów o większym niż wykroczenia ciężarze gatunkowym. Formułując wnioski *de lege ferenda*, należy zasignalizować, że Kodeks postępowania w sprawach o wykroczenia powinien zostać uzupełniony o przepis, z którego *expressis verbis* wynikałby zakaz dowodowy obejmujący dane chronione tajemnicą telekomunikacyjną, tak aby w przyszłości nie dochodziło do błędnego interpretowania prawa i wykorzystywania danych bilingowych w postępowaniach wykroczeniowych.

## **STRESZCZENIE**

### Dane bilingowe jako dowód w postępowaniu w sprawach o wykroczenia

Postępowanie w sprawach o wykroczenia rzadko jest przedmiotem zainteresowania przedstawicieli doktryny, chociaż sprawy dotyczące tego typu czynów zabronionych są dość powszechne i budzą zaciekawienie dużej części społeczeństwa, chociażby z uwagi na popularność postępowania mandatowego. W jednym z artykułów prasowych zasygnalizowano, że w sprawie dotyczącej wykroczenia drogowego organy orzekające wystąpiły do przedsiębiorcy telekomunikacyjnego o udostępnienie danych towarzyszących przekazowi telekomunikacyjnemu, który zainicjowany był przez abonenta, występującego w tej sprawie w charakterze obwinionego. W związku z powyższym przeprowadzono badania zmierzające do ustalenia, czy na etapie jurysdykcyjnym postępowania w sprawach o wykroczenia dopuszczalne jest sięganie przez sąd po dane bilingowe chronione tajemnicą telekomunikacyjną. Badania zostały przeprowadzone z wykorzystaniem metod badawczych stosowanych w naukach prawnych.

**Słowa kluczowe:** tajemnica telekomunikacyjna; dowody w sprawie o wykroczenie; dane bilingowe; wykroczenie drogowe; postępowanie sądowe

## **SUMMARY**

### Billing data as evidence in proceedings in cases of misdemeanor

Cases concerning misdemeanours are common. These cases evoke curiosity among large parts of society, because people are often punished for minor violations of the law. The proceedings in cases of misdemeanours is rarely of interest to representatives of science. In one of the newspaper articles it was pointed out that, in a case involving a misdemeanor by traffic of road authorities of the Member State requested that billing data from the telecommunications entrepreneur. In view of the above, research has been carried out to establish whether at the stage of judicial, the authorities of the Member State shall have the right to require billing data, which are protected by telecommunications secrecy. Studies have been carried out

with the use of research methods which are normal research methods, which are characteristic in legal sciences.

**Keywords:** telecommunications secrecy; the evidence in the case of misdemeanor; billing data; traffic offence; court proceedings

## BIBLIOGRAFIA

- Gajos-Kaniewska D., *Sąd: nie będzie mandatu za używanie komórki podczas jazdy, bo policja nie zadbała o dowody*, „Rzeczpospolita” 14.11.2016, <http://www.rp.pl/Prawo-drogowe/311149999-Sad-nie-bedzie-mandatu-za-uzywanie-komorki-podczas-jazdy-bo-policja-nie-zadbala-o-dowody.html#ap-1> (dostęp: 17.11.2016 r.).
- Gensikowski P., *Kodeks postępowania w sprawach o wykroczenia. Komentarz*, Warszawa 2016, Legalis.
- Hoc S., *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych*, Opole 2006.
- Kotowski W., Kurzępa B., *Kodeks postępowania w sprawach o wykroczenia. Komentarz*, Warszawa 2016, Legalis.
- Michalak A., *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, Kraków 2006.
- Rogalski M., *Kontrola korespondencji*, Warszawa 2016, Legalis.