



**WYROK W IMIENIU
RZECZYPOSPOLITEJ POLSKIEJ**

Dnia 5 lutego 2008 r.

Naczelny Sąd Administracyjny w składzie:

Przewodniczący: Sędzia NSA Małgorzata Pocztarek

Sędziowie NSA f Janina Antosiewicz

Zygmunt Zgierski (spr.)

Protokolant

Aleksandra Żurawicka

po rozpoznaniu w dniu 5 lutego 2008 r.

na rozprawie w Izbie Ogólnoadministracyjnej

skargi kasacyjnej Generalnego Inspektora Ochrony Danych Osobowych

od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie

z dnia 10 października 2006 r. sygn. akt II SA/Wa 642/05

w sprawie ze skargi S. A. w Warszawie

na decyzję Generalnego Inspektora Ochrony Danych Osobowych

z dnia 14 stycznia 2005 r. nr GI-DEC-DS-7/05/24,25

w przedmiocie udostępnienia danych osobowych

uchyla zaskarżony wyrok i oddala skargę S. A. w Warszawie

Uzasadnienie

Zaskarżonym wyrokiem z dnia 10 października 2006 r. Wojewódzki Sąd Administracyjny w Warszawie uwzględnił skargę [...] S.A. i uchylił zaskarżoną decyzję Generalnego Inspektora Ochrony Danych Osobowych z dnia [...] oraz poprzedzającą ją decyzję tego organu z dnia [...] w przedmiocie udostępnienia danych osobowych.

W uzasadnieniu wyroku Sąd I instancji przytoczył następujące okoliczności faktyczne i prawne:

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął wniosek Komendanta Straży Miejskiej w B. o wydanie decyzji nakazującej [...] S.A. z siedzibą w W., udostępnienie Straży Miejskiej w B. danych osobowych abonenta telefonu komórkowego, użytkowanego w sieci [...] S.A. o numerze telefonicznym [...], w zakresie imienia, nazwiska oraz adresu zamieszkania. W motywach wniosku podano, iż Straż Miejska w B. prowadzi sprawę o popełnienie wykroczenia z art. 66 § 1 Kodeksu wykroczeń, polegającego na wywoływaniu fałszywych alarmów o pożarze, w celu uruchomienia akcji straży pożarnej. Abonent telefonu, z którego dokonano alarmu, należy do sieci telefonii komórkowej [...]. W oparciu o powyższą informację Straż Miejska w dniu 28 kwietnia 2004 r. zwróciła się do operatora [...] S.A. o udostępnienie danych osobowych abonenta, zaś [...] S.A. odmówił udostępnienia tych danych podnosząc, iż dane abonentów objęte są tajemnicą służbową w rozumieniu art. 266 kk i wobec tego brak jest podstaw do ich ujawnienia.

Decyzją z dnia [...] Generalny Inspektor Ochrony Danych Osobowych nakazał [...] S.A. udostępnienie Komendantowi Straży Miejskiej żądanych danych osobowych abonenta telefonu komórkowego, ze zbioru danych abonentów Spółki.

Po ponownym rozpatrzeniu sprawy na wniosek pełnomocnika [...] S.A., Generalny Inspektor Ochrony Danych Osobowych decyzją z dnia [...] utrzymał w mocy własną decyzję z dnia [...]. Według organu, umieszczenie przez ustawodawcę w Prawie telekomunikacyjnym przepisów regulujących kwestie przetwarzania danych osobowych użytkowników nie przesądza jeszcze o tym, iż przetwarzanie takich danych nie podlega reżimowi ustawy o ochronie danych osobowych na podstawie art. 5 tej ustawy. Przepis art. 161 ust. 1 zd. 2 Prawa telekomunikacyjnego normuje bowiem kwestię zbiegu przepisów Prawa telekomunikacyjnego z przepisami ustawy o ochronie danych osobowych i to w taki sposób, że przepisy obu tych aktów prawnych, w szczególności w zakresie przesłanek przetwarzania danych użytkowników, "uzupełniają się". Zdaniem organu, przepisy Prawa telekomunikacyjnego nie wyłączają w tym zakresie zastosowania przepisów ustawy o ochronie danych osobowych. Niezależnie od powyższego, w kontekście zastosowania do przetwarzanych danych objętych tajemnicą telekomunikacyjną, przepisów innych aktów prawnych niż Prawo telekomunikacyjne organ wskazał na przepis art. 159 ust. 2 pkt 4 tej ustawy, który przewiduje możliwość przetwarzania (szeroko pojętego wykorzystywania) danych użytkownika (nadawcy komunikatu) przez podmioty inne niż wynikałoby to bezpośrednio z przepisów tejże ustawy, pod warunkiem, że będzie to niezbędne z powodów przewidzianych przepisami odrębnymi.

Na gruncie przepisów ustawy o ochronie danych osobowych za okoliczność "usprawiedliwiającą" przetwarzanie danych uznaje się w szczególności sytuację, gdy przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (art. 23 ust. 1 pkt 4). Aby można było uznać, że przetwarzanie danych

odbyło się w oparciu o tę właśnie przesłankę, konieczne jest spełnienie łącznie trzech warunków. Mianowicie, działania muszą być prowadzone w interesie publicznym przy użyciu form niewładczych; zadania publiczne, w tym państwowe, muszą być określone prawem; przetwarzanie danych musi być niezbędne do wykonania zadań publicznych.

Organ orzekający powołując się na art. 10, 10a pkt 1, 11, 12 ust. 1 pkt 5 ustawy o strażach gminnych oraz art. 54 § 1 i art. 56 § 2 kpw, stwierdził, że w niniejszej sprawie Straż Miejska, realizując nałożone na nią zadania w zakresie ochrony porządku publicznego, prowadzi postępowanie w sprawie o popełnienie wykroczenia, zmierzające do ustalenia tożsamości osoby podejrzanej o popełnienie tegoż wykroczenia i skierowania wniosku o ukaranie do właściwego sądu. Udostępnienie Straży Miejskiej żądanych danych było i jest, w ocenie organu, niezbędne do zrealizowania zadań określonych w powołanych wyżej przepisach, a [...] S.A. jest jedynym podmiotem, który posiada wnioskowane informacje. Według GİODO, w rozpoznawanej sprawie spełnione zostały wszystkie okoliczności, określone w art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych i z tego też względu dozwolone jest udostępnienie danych abonenta w oparciu o ten przepis. Dodatkowo organ stwierdził, iż obok art. 23 ust. 1 pkt 4 ustawy, podstawę udostępnienia danych osobowych może stanowić art. 23 ust. 1 pkt 2, który legalizuje przetwarzanie danych, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku, wynikającego z przepisu prawa. Udostępnienie przedmiotowych danych jest warunkiem niezbędnym dla zrealizowania obowiązków (i uprawnień) nałożonych na Straż Miejską przez powyższe akty prawne.

Organ wyjaśnił przy tym, iż zgodnie z art. 161 zd. 2 Prawa telekomunikacyjnego oraz przepisami ustawy o ochronie danych osobowych, udostępnienie danych abonenta, będącego osobą podejrzaną o popełnienie wykroczenia, jest niezbędne do wykonania określonych prawem zadań realizowanych przez Straż Miejską dla dobra publicznego (zrealizowanie obowiązku wynikającego z przepisu prawa). Co więcej, z przepisów ustawy o strażach gminnych, pośrednio z kpw oraz bezpośrednio z przepisu art. 159 ust. 1 pkt 4 Prawa telekomunikacyjnego, wynika dla Straży Miejskiej uprawnienie do pozyskania danych abonenta, będących w posiadaniu operatora. Skoro więc, operator ma podstawę prawną do udostępnienia danych, to odmowa udostępnienia danych stanowi naruszenie prawa.

Powyższą decyzję [...] S.A. zaskarżył do Wojewódzkiego Sądu Administracyjnego w Warszawie. Zaskarżonej decyzji zarzucono naruszenie art. 10a ustawy o strażach gminnych, art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych, art. 57 § 1, art. 59 § 2 i art. 41 § 3 Kodeksu postępowania w sprawach o wykroczenia w zw. z art. 5 ustawy o ochronie danych osobowych, poprzez błędne przyjęcie, że w/w przepisy stanowią podstawę udostępnienia danych osobowych abonenta telefonu komórkowego.

Odpowiadając na skargę Generalny Inspektor Ochrony Danych Osobowych wniósł o jej oddalenie i podtrzymał argumentację zawartą w uzasadnieniu zaskarżonej decyzji.

Wspomnianym na wstępie wyrokiem z dnia 10 października 2006 r. Wojewódzki Sąd Administracyjny w Warszawie uchylił zaskarżoną decyzję z dnia 14 stycznia 2005 r. i poprzedzającą ją decyzję z dnia 4 października 2004 r.

Oceniając legalność wymienionych wyżej rozstrzygnięć, Sąd I instancji stwierdził, iż porównanie treści art. 159 ust. 1 pkt 1, art. 159 ust. 2 i ust. 3, art. 161 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800 ze zm.) z art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926

ze zm.) prowadzi do wniosku, iż przepisy ustawy - Prawo telekomunikacyjne przewidują dalej idącą ochronę danych osobowych objętych tajemnicą telekomunikacyjną, aniżeli przepisy ustawy o ochronie danych osobowych. W tej zaś sytuacji, zastosowanie znajduje przepis art. 5 ustawy o ochronie danych osobowych, regulujący relację zachodzącą między normami prawa wewnętrznego. Ustawodawca przyjmuje w tym ostatnim przepisie zasadę rozstrzygania zbiegu norm na korzyść tych norm, które przewidują wyższy poziom ochrony. Tak więc o zakresie i sposobie ochrony danych osobowych objętych tajemnicą telekomunikacyjną decydować będą przepisy Prawa telekomunikacyjnego, a nie ustawy o ochronie danych osobowych. Co więcej, analiza w/w aktów prawnych prowadzi do wniosku, iż brak jest w nich przepisów dopuszczających przetwarzanie danych osobowych objętych tajemnicą telekomunikacyjną przez straż gminną w toku czynności wyjaśniających prowadzonych przez Straż Miejską w sprawach o wykroczenia. W szczególności, przepisem dopuszczającym przetwarzanie danych osobowych objętych tajemnicą telekomunikacyjną nie jest przepis art. 10a.

Sąd I instancji zwrócił przy tym uwagę, iż przepisy innych ustaw, jak np. art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji (tj. Dz.U. z 2002 r. Nr 7, poz. 58 ze zm.), art. 10b ust. 1 ustawy z dnia 12 października 1960 r. o Straży Granicznej (tj. Dz.U. Nr 78, poz. 462 ze zm.), art. 36 ust. 1 ustawy z dnia 28 września 1991 r. o kontroli skarbowej (tj. Dz.U. z 2004 r. Nr 8, poz. 65 ze zm.), art. 30 ust. 1 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. Nr 123, poz. 1353 ze zm.), art. 28 ust. 1 pkt 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz.U. Nr 74, poz. 676 ze zm.), art. 27 ust. 1 pkt 1 ustawy z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych (Dz.U. Nr 139, poz. 1326 ze zm.), dopuszczają przetwarzanie przez te organy danych objętych tajemnicą telekomunikacyjną, a w szczególności danych identyfikacyjnych abonenta.

Ponadto Sąd I instancji podkreślił, że z treści art. 15 ust. 1 Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r., dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), (Official Journal L 201, 31/07/2002, s. 37) wynika, że państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia między innymi poufności komunikacji (art. 5 Dyrektywy), gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej.

W świetle powołanej dyrektywy oczywistym jest, według Sądu I instancji, brak podobnej, jak wskazane powyżej, regulacji dopuszczającej przetwarzanie danych osobowych objętych tajemnicą telekomunikacyjną w toku postępowania w sprawach o wykroczenia. Dyrektywa dopuszcza bowiem uchwalanie przez państwa członkowskie środków ustawodawczych w celu ograniczenia poufności komunikacji w związku z zapobieganiem, dochodzeniem, wykrywaniem i karaniem przestępstw.

Podsumowując WSA stwierdził, iż zaskarżona decyzja oraz poprzedzająca ją decyzja organu I instancji wydane zostały z naruszeniem art. 5 ustawy o ochronie danych osobowych w zw. z art. 159 ust. 1 pkt 1, art. 159 ust. 2 i ust. 3 oraz art. 161 ust. 1 ustawy Prawo telekomunikacyjne. Stwierdzone naruszenie prawa materialnego, miało istotny wpływ na

wynik sprawy i uzasadniało wyeliminowanie z obrotu prawnego w/w decyzji w oparciu o art. 145 § 1 pkt 1 lit. "a" Prawa o postępowaniu przed sądami administracyjnymi.

W skardze kasacyjnej od powyższego wyroku Generalny Inspektor Ochrony Danych Osobowych, reprezentowany przez radcę prawnego, wniósł o uchylenie zaskarżonego wyroku w całości i przekazanie sprawy do ponownego rozpoznania Wojewódzkiemu Sądowi Administracyjnemu w Warszawie.

Organ zarzucił naruszenie przepisów prawa materialnego - art. 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) w zw. z art. 159 ust. 1 pkt 1, ust. 2 i ust. 3 oraz art. 161 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800 ze zm.), poprzez ich niewłaściwe zastosowanie w sytuacji, gdy do udostępnienia danych osobowych abonenta telekomunikacyjnego powinny znaleźć zastosowanie przepisy art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych w zw. z art. 54 § 1 i 56 § 2 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz.U. Nr 106, poz. 1148 ze zm.) i art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. Nr 123, poz. 779 ze zm.) oraz art. 161 ust. 1 i art. 159 ust. 2 pkt 4 Prawa telekomunikacyjnego.

W uzasadnieniu skargi organ podniósł, iż niezasadne jest stanowisko Sądu I instancji, że przepisy Prawa telekomunikacyjnego zapewniają danym osobowym, stanowiącym tajemnicę telekomunikacyjną, dalej idącą ochronę niż regulacje ustawy o ochronie danych osobowych. Jego zdaniem, pomiędzy tymi ustawami nie zachodzi relacja wyłączenia, lecz uzupełnienia. W konsekwencji, nie można zgodzić się z oceną WSA, iż wobec brzmienia art. 5 ustawy o ochronie danych osobowych, niniejsza sprawa nie podlega reżimowi ustawy o ochronie danych osobowych. Bezzasadny jest więc zarzut, iż organ orzekając na podstawie art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych, naruszył art. 5 tejże ustawy.

Odwołując się do treści art. 161 ust. 1 Prawa telekomunikacyjnego (którego odpowiednikiem do dnia 2 września 2004 r. był art. 69 ust. 1 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne), GODO stwierdził, że gdyby przepis ten ograniczał się wyłącznie do zdania pierwszego, to oznaczałoby to, że omawiany akt prawny zezwala na przetwarzanie informacji telekomunikacyjnych wyłącznie wówczas, gdy przetwarzanie to dotyczy usługi świadczonej użytkownikowi albo gdy jest to niezbędne do jej wykonania. Nie można jednak pominąć zdania drugiego powołanego artykułu, z którego wynika, że przetwarzanie danych osobowych objętych tajemnicą telekomunikacyjną (w tym ich udostępnianie przez podmiot świadczący usługę telekomunikacyjną) jest również dopuszczalne na podstawie przepisów ustawowych w innych celach niż określone w zdaniu pierwszym. Oznacza to, że przetwarzanie w/w danych może odbywać się w oparciu o przesłanki i w celach ustanowionych w innych aktach prawnych rangi ustawowej. Z uwagi na istnienie w przepisach Prawa telekomunikacyjnego tego rodzaju odesłania, nie można zgodzić się z twierdzeniem, iż ustawa ta wprowadza dalej idącą ochronę danych użytkowników, niż ustawa o ochronie danych osobowych. Co więcej, nie ma jakichkolwiek podstaw, by uznać, że przetwarzanie danych osobowych w celach innych, niż wskazane w przepisie art. 161 ust. 1 zd. 1 Prawa telekomunikacyjnego, nie może odbywać się w oparciu o przesłanki określone w ustawie o ochronie danych osobowych. Przyjęcie odmiennego założenia oznaczałoby zarazem, że operator nie mógłby prowadzić w stosunku do użytkownika korzystającego z jego usługi marketingu innych własnych produktów lub usług. Powyższe działania, niewątpliwie dozwolone na podstawie art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, nie mogłyby bowiem zostać uznane za legalne w świetle art. 161 ust. 1 zd. 1

Prawa telekomunikacyjnego, który wyraźnie ogranicza możliwość wykorzystania danych użytkownika do sytuacji, gdy jest to związane z usługą świadczoną użytkownikowi bądź gdy jest to niezbędne do wykonania tej usługi. Innymi słowy, przepisy Prawa telekomunikacyjnego nie wyłączają w tym zakresie zastosowania przepisów ustawy o ochronie danych osobowych, w tym art. 23 tej ustawy. Podobna regulacja przewidziana była zresztą w art. 69 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne.

Ponadto w kontekście ewentualnego zastosowania do przetwarzania danych objętych tajemnicą telekomunikacyjną przepisów innych aktów prawnych niż Prawo telekomunikacyjne, organ zwrócił uwagę na treść art. 159 ust. 2 pkt 4 tej ustawy, co do którego w literaturze przedmiotu prezentowany jest pogląd, iż przepis ten dopuszcza nie tylko te reguły przetwarzania danych osobowych, które są przewidziane w Prawie telekomunikacyjnym, ale także reguły, wynikające z ustawy o ochronie danych osobowych i innych ustaw. Przesłanki legalności przetwarzania danych, określone zwłaszcza w art. 23 ustawy o ochronie danych osobowych, mają pełne zastosowanie w dziedzinie telekomunikacji i dotyczy to, między innymi, wykonywania określonych prawem zadań realizowanych dla dobra publicznego, przetwarzania danych niezbędnych do wypełnienia prawnie usprawiedliwionych celów administratora danych. Co istotne, przy przyjęciu takiej interpretacji art. 159 ust. 2 pkt 4 Prawa telekomunikacyjnego, przepis ten w pełni koresponduje z art. 159 ust. 3 w/w ustawy, a także z jej art. 161 ust. 1. Z powyższych rozważań wynika więc, że wydane przez GODO decyzje były zgodne z prawem.

Organ odnosząc się w następnej kolejności do stanowiska Sądu I instancji, iż art. 10a ustawy o strażach gminnych nie daje uprawnień strażom miejskim (gminnym) do przetwarzania danych stanowiących tajemnicę telekomunikacyjną, w celu przeprowadzenia czynności wyjaśniających w sprawie o wykroczenie stwierdził, że stanowisko to jest błędne. Według GODO, przepisy art. 10a, 10, 11 i 12 ustawy o strażach gminnych oraz art. 56 § 2 w zw. z art. 54 § 1 i art. 17 § 2 i § 3 Kodeksu postępowania w sprawach o wykroczenia gwarantują strażom gminnym (miejskim) prawo do przetwarzania informacji o osobach, w stosunku do których podejmowane są określone czynności o wykroczenia, i to bez zgody tych osób, jako niezbędny instrument służący umożliwieniu tym organom wypełnianie ich obowiązków.

Istota zagadnienia poddanego przez Komendanta Straży Miejskiej rozstrzygnięciu GODO wymagała oceny, czy w sytuacji, gdy jedynym podmiotem, w posiadaniu którego znajdują się informacje niezbędne dla skierowania przez Straż Miejską wniosku o ukaranie do sądu, jest operator telekomunikacyjny, Straż Miejska ma prawo pozyskać je od tego operatora i poddać procesowi dalszego przetwarzania dla realizacji jej ustawowych obowiązków. Odpowiedź na tak postawione pytanie oznaczała w istocie zajęcie stanowiska w sprawie społecznego znaczenia ścigania wykroczeń oraz poziomu ochrony prawnej, jaką przyznaje się danym osobom osoby podejrzanej o popełnienie wykroczenia w stosunku do poziomu ochrony prawnej interesu ogółu obywateli w przeciwdziałaniu czynom społecznie szkodliwym.

Według GODO, wobec faktu, iż uzyskanie przez Straż Miejską wnioskowanych przez nią danych osobowych stanowi niezbędny warunek realizacji ustawowych zadań tego podmiotu, a zarazem jedynym źródłem, z którego możliwe jest pozyskanie tych danych jest wyłącznie Spółka [...], zaistniały określone w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych okoliczności, umożliwiające Straży Miejskiej przetwarzanie danych, stanowiących tajemnicę telekomunikacyjną. Powołany przepis zezwala bowiem na przetwarzanie danych, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Przesłanki przetwarzania danych wymienione w art. 23 ust. 1 pkt 2 i 4 ustawy o

ochronie danych osobowych mają bowiem charakter rozłączny, co oznacza, że zaistnienie którejkolwiek z nich przesądza o legalności procesu przetwarzania danych. Takie stanowisko znalazło również potwierdzenie w wyroku NSA z dnia 28 stycznia 2003 r. sygn. akt II SA 2210/01. Dlatego też, według Generalnego Inspektora, z chwilą zwrócenia się przez Komendanta Straży Miejskiej o udostępnienie danych z jednoczesnym wskazaniem celu ich wykorzystania, po stronie operatora powstał obowiązek udostępnienia tych danych. Obawa operatora, że udostępniając te dane naraża się na sankcje określone w art. 266 § 1 Kodeksu karnego, nie znajduje żadnego usprawiedliwienia w obowiązujących przepisach prawa. Brzmienie art. 159 ust. 2 pkt 4 dowodzi bowiem, że tajemnica telekomunikacyjna nie ma charakteru bezwzględnie i zezwala na szeroko rozumiane wykorzystywanie danych osobowych użytkownika, znajdujących się w posiadaniu operatora, przez podmioty inne niż nadawca i odbiorca komunikatu, o ile jest to niezbędne z powodów określonych przepisami odrębnymi. Taka właśnie sytuacja, miała miejsce w rozpoznawanej sprawie.

Podsumowując, Generalny Inspektor stanął na stanowisku, iż udostępnienie przez Spółkę na rzecz Straży Miejskiej wnioskowanych danych osobowych mogło i powinno nastąpić na zasadach określonych w art. 161 ust. 1 zd. 2 Prawa telekomunikacyjnego. Zadośćuczynienie przez Spółkę żądaniu Straży Miejskiej nie oznaczałoby zatem bezprawnego naruszenia przez tę pierwszą tajemnicy telekomunikacyjnej, ani też nie mogłoby skutkować odpowiedzialnością karną na podstawie art. 266 § 1 Kodeksu karnego.

Generalny Inspektor uznał również za błędne odwołanie się przez Sąd I instancji do regulacji art. 15 ust. 1 Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. i stwierdził, że penalizacja i ściganie wykroczeń służy ochronie porządku i bezpieczeństwa publicznego. W takim ujęciu przepisy zezwalające strażom gminnym na przetwarzanie danych osobowych, stanowiących tajemnicę telekomunikacyjną w ramach postępowania w sprawach o wykroczenia, korespondują z postanowieniami Dyrektywy.

W odpowiedzi na skargę kasacyjną [...] S.A. wniósł o oddalenie skargi i orzeczenie o kosztach postępowania sądowego, według norm przepisanych.

Naczelny Sąd Administracyjny zważył, co następuje:

Zgodnie z art. 183 § 1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. Nr 153, poz. 1270 ze zm.), Naczelny Sąd Administracyjny rozpoznaje sprawę w granicach skargi kasacyjnej, bierze jednak z urzędu pod rozwagę nieważność postępowania. W niniejszej sprawie nie występują, enumeratywnie wyliczone w art. 183 § 2 ustawy przesłanki nieważności postępowania sądowoadministracyjnego i dlatego też, przy rozpoznawaniu sprawy, Naczelny Sąd Administracyjny związany był granicami skargi kasacyjnej.

Skarga kasacyjna Generalnego Inspektora Ochrony Danych Osobowych oparta została na zarzucie naruszenia prawa materialnego poprzez niewłaściwe zastosowanie przez Sąd I instancji art. 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) w zw. z art. 159 ust.1 pkt 1, ust. 2 i ust. 3 oraz art. 161 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800 ze zm.) w sytuacji, gdy do udostępnienia Straży Miejskiej danych osobowych abonenta telefonu komórkowego powinny znaleźć zastosowanie przepisy art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych w zw. z art. 54 § 1 i art. 56 § 2 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz.U. Nr 106, poz. 1148 ze zm.) i art.

10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. Nr 123, poz. 779 ze zm.) oraz art. 161 ust. 1 i art. 159 ust. 2 pkt 4 Prawa telekomunikacyjnego.

W ocenie Naczelnego Sądu Administracyjnego podniesiony zarzut jest w pełni usprawiedliwiony.

Istotą sporu w rozpoznawanej sprawie jest odpowiedź na pytanie, czy Spółka Akcyjna [...] była zobowiązana, a jeśli tak, to na jakiej podstawie prawnej, do udostępnienia danych osobowych abonenta telefonu komórkowego na żądanie Komendanta Straży Miejskiej w B., w tym celu, by Straż Miejska mogła poddać je procesowi dalszego przetwarzania dla realizacji jej ustawowych obowiązków.

Aby odpowiedzieć na tak postawione pytanie, należy w pierwszej kolejności określić relacje, jakie zachodzą pomiędzy przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) i przepisami ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800 ze zm.).

Stosownie do treści art. 1 ust. 2 w zw. z art. 7 pkt 2 pierwszej z wymienionych ustaw, przetwarzanie danych osobowych, a więc ich zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą.

Jeżeli jednak przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ochronę, niż wynika to z niniejszej ustawy, to w rozumieniu art. 5 ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw.

Przytoczony wyżej przepis określa relacje między normami prawa wewnętrznego i statuuje zasadę rozstrzygania zbiegu norm na korzyść tych norm, które przewidują wyższy poziom ochrony. W polskim systemie prawa istnieje wiele przepisów odrębnych, które odnoszą się do szeroko rozumianego przetwarzania danych osobowych. Zaliczyć do nich w szczególności należy przepisy ustawy Prawo telekomunikacyjne, gdzie w art. 161 ust. 1 w zw. z art. 159 ust. 1 pkt 1 ustawodawca unormował problematykę przetwarzania danych osobowych użytkownika objętych tajemnicą telekomunikacyjną.

Ustawa ta stanowi, że treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej "przetwarzaniem", dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych (art. 161 ust. 1).

Brzmienie zd. 2 ust. 1 art. 161 dowodzi, że przetwarzanie danych, stanowiących tajemnicę telekomunikacyjną, może się odbywać w oparciu o przesłanki określone w innych aktach prawnych rangi ustawowej. Odesłanie do przepisów ustawowych prowadzi, w ocenie Naczelnego Sądu Administracyjnego, do wniosku, iż w grę wchodzić tu będzie przede wszystkim regulacja przewidziana w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych - art. 10a pkt 1 oraz w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych - art. 23 ust. 1 pkt 2 i 4. Istnienie w przepisach Prawa telekomunikacyjnego tego rodzaju odesłania, pozwala zatem podzielić pogląd Generalnego Inspektora Ochrony Danych Osobowych, że pomiędzy omawianymi tu ustawami nie zachodzi relacja wyłączenia lecz uzupełnienia. Tym

samym nie można zgodzić się z oceną Sądu I instancji, iż brzmienie art. 5 ustawy o ochronie danych osobowych wyklucza niniejszą sprawę spod reżimu ustawy o ochronie danych osobowych.

Powołany wyżej przepis art. 23 ust. 1 ustawy o ochronie danych osobowych w punktach od 1 do 5 określa materialne przesłanki przetwarzania danych osobowych. Każda z wymienionych w nim okoliczności usprawiedliwiających przetwarzanie danych osobowych ma charakter autonomiczny i niezależny, choć oczywiście może zdarzyć się tak, że określone przetwarzanie danych będzie legalizowane więcej niż jedną przesłanką podaną w art. 23 ust. 1.

Stosownie do treści art. 23 ust. 1 pkt 2, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Zdaniem Naczelnego Sądu Administracyjnego, komentowany przepis dopuszcza w istocie rzeczy przetwarzanie danych osobowych, przewidując dwa warunki, które powinny być spełnione łącznie. Pierwszym warunkiem jest istnienie odpowiedniego przepisu prawa, który przyznaje podmiotowi uprawnienie lub nakłada na niego obowiązek. Drugim zaś, warunkiem jest niezbędność przetwarzania danych dla zrealizowania tego uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

W rozpoznawanej sprawie, jak trafnie podniosła strona wnosząca skargę kasacyjną, przesłanka ta została spełniona, albowiem uzyskanie przez Straż Miejską danych osobowych abonenta telefonu komórkowego, których jedynym dysponentem była Spółka [...], stanowiło niezbędny warunek realizacji ustawowych zadań tego podmiotu, określonych w przepisach ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych.

Omawiana przesłanka pokrywa się w dużej mierze, z drugą przesłanką, określoną w pkt 4 ust. 1 art. 23, która pozwala na przetwarzanie danych osobowych, gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla d o b r a p u b l i c z n e g o.

Wspomniane zadania publiczne, w imię których ma się odbywać przetwarzanie danych osobowych, muszą być określone prawem. Ustawa o ochronie danych osobowych nie definiuje jednak pojęcia "zadań realizowanych dla dobra publicznego", ani też nie określa bliżej podmiotów wykonujących te zadania publiczne. W ocenie Naczelnego Sądu Administracyjnego chodzi tu o zadania, które zostały zlecone przez prawo temu podmiotowi, który dane przetwarza. Mogą to być zadania z zakresu bezpieczeństwa publicznego, walki z przestępczością, udzielania pomocy ofiarom klęsk żywiołowych itd. Podmiotami wykonującymi zadania publiczne mogą zaś być organy państwowe, samorządowe, państwowe lub komunalne jednostki organizacyjne, a także podmioty wymienione w art. 3 ust. 2 ustawy o ochronie danych osobowych. Niewątpliwie do takich podmiotów można zaliczyć straż gminną (miejską), która w rozumieniu art. 6 ust. 1 ustawy o strażach gminnych jest jednostką organizacyjną gminy i w oparciu o art. 10 ust. 1 tej ustawy wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. Wykonywanie czynności podejmowanych przez Straż Miejską w postępowaniu w sprawach o wykroczenia ma na celu ochronę porządku publicznego. Wobec tego bezspornym jest, że również i druga z wymienionych wyżej przesłanek została w niniejszej sprawie spełniona, skoro uzyskanie przez Straż Miejską danych osobowych abonenta telefonu komórkowego, czyli osoby podejrzanej o popełnienie wykroczenia, było konieczne do wykonania określonych prawem zadań realizowanych przez Straż Miejską dla dobra publicznego.

Oceniając legalność przetwarzania danych określonych w art. 23 bez zgody osoby, której dane te dotyczą, należy mieć na uwadze, czy ujawnienie takich danych jest niezbędne; co więcej, winny być w takim wypadku wyważone interesy związane np. z realizacją zadań dla dobra publicznego i osoby, której dane dotyczą, przy uwzględnieniu celu ustawy o ochronie danych osobowych, którym jest ochrona prywatności w rozumieniu art. 47 Konstytucji RP. Przepis art. 23 ust. 1 pkt 2 i 4 dotyczy bowiem sytuacji, gdy dobro publiczne niejako "wyprzedza" autonomię jednostki w decydowaniu o przetwarzaniu dotyczących jej danych osobowych.

Przepisem rangi ustawowej zezwalającym na przetwarzanie danych osobowych stanowiących tajemnicę telekomunikacyjną jest także art. 10a pkt 1 ustawy o strażach gminnych w myśl, którego straż w celu realizacji zadań ustawowych może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia.

Powyższe unormowanie, jak trafnie zauważył autor skargi kasacyjnej, koresponduje ściśle z art. 10, 11 i 12 ustawy o strażach gminnych.

Otóż, zgodnie z przytoczonym już wcześniej art. 10 ust. 1 straż gminna wykonuje zadania w zakresie ochrony porządku publicznego, które przewidziane są przepisami rangi ustawowej i aktami prawa miejscowego. W związku z wykonywaniem zadań, których przykładowy katalog określony został w art. 11 ustawy, strażnik ma prawo między innymi do dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych - w trybie i zakresie określonych w Kodeksie postępowania w sprawach o wykroczenia (art. 12 ust. 1 pkt 5).

Po myśli art. 54 § 1 w zw. z art. 56 § 2 i art. 17 § 3 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz.U. Nr 106, poz. 1148 ze zm.) straż gminna (miejaska), a także inne organy, gdy ustawa tak stanowi, mogą w granicach swojej właściwości prowadzić czynności wyjaśniające w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie oraz zebrania danych niezbędnych do sporządzenia wniosku o ukaranie. Wniosek o ukaranie w rozumieniu art. 57 § 2 pkt 1 powinien zawierać imię i nazwisko oraz adres obwinionego, a także inne dane niezbędne do ustalenia jego tożsamości.

Wskazane przepisy nie tylko uprawniają, ale wręcz zobowiązują Straż Miejską do pozyskania wszelkich niezbędnych danych w celu ustalenia sprawcy wykroczenia, a następnie skierowania do sądu stosownego wniosku o ukaranie podmiotu w pełni zidentyfikowanego. Na gruncie rozpoznawanej sprawy takimi niezbędnymi danymi były właśnie chronione tajemnicą telekomunikacyjną dane osobowe abonenta telefonu komórkowego (imię, nazwisko i adres zamieszkania), podejrzanego o wywoływanie fałszywych alarmów o pożarze. Odmowa udostępnienia Straży Miejskiej żądanych danych osobowych użytkownika, w sytuacji gdy jedynymi danymi, jakimi dysponowała Straż był jego numer telefonu komórkowego, a Spółka [...] była jedynym dysponentem tych danych, stanowiła niewątpliwie przeszkodę w zrealizowaniu nałożonych na Straż Miejską obowiązków wynikających z przepisów prawa.

Z tego też powodu w pełni uzasadnione jest stanowisko Generalnego Inspektora Ochrony Danych Osobowych, iż z chwilą zwrócenia się przez Komendanta Straży Miejskiej z wnioskiem o udostępnienie danych osobowych abonenta telefonu komórkowego, po stronie operatora powstał obowiązek udostępnienia tych danych. Realizacja tego obowiązku w żadnym zakresie nie może też doprowadzić do naruszenia tajemnicy telekomunikacyjnej, która, co niewątpliwie, należy do podstawowych wolności i praw osobistych uregulowanych w Konstytucji RP. W art. 49 ustawy zasadniczej ustawodawca zagwarantował bowiem obywatelom wolność i ochronę tajemnicy komunikowania się. Tajemnica komunikowania się nie ma jednak charakteru bezwzględnego, co oznacza, iż jej ograniczenie może być ustanowione, podobnie jak w przypadku innych konstytucyjnych praw i wolności - tylko w ustawie i w sposób w niej określony.

W obecnie obowiązującej ustawy Prawo telekomunikacyjne, w art. 159 ust. 1 pkt 1-5, ustawodawca określił jakie dane objęte są tajemnicą telekomunikacyjną. Obejmuje ona zarówno treść indywidualnych komunikatów jak i dane dotyczące użytkownika, dane transmisyjne o lokalizacji oraz o próbach uzyskania połączenia. Zakres ochrony tajemnicy telekomunikacyjnej określony został w art. 159 ust. 2 i obejmuje zakaz zapoznawania się, utrwalania, przechowywania, przekazywania lub innego wykorzystywania treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu. W ust. 2 pkt 1 - 4 omawianego artykułu, ustawodawca sprecyzował warunki, w ramach których dozwolone jest naruszenie tajemnicy telekomunikacyjnej. Szeroko rozumiane wykorzystywanie danych osobowych objętych tajemnicą telekomunikacyjną dozwolone jest m. in., gdy jest to konieczne z innych powodów niż wymienione w pkt 1-3 przewidzianych ustawą lub przepisami odrębnymi.

Takimi przepisami odrębnymi, upoważniającymi między innymi do przetwarzania danych osobowych objętych tajemnicą telekomunikacyjną, są właśnie przepisy ustawy o ochronie danych osobowych oraz ustawy o strażach gminnych. Skoro więc, według art. 159 ust. 3 Prawa telekomunikacyjnego, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną, z wyjątkiem przypadków określonych ustawą, narusza obowiązek zachowania tajemnicy telekomunikacyjnej, to ziszczenie się przypadków przewidzianych w ustawie o strażach gminnych i ustawie o ochronie danych osobowych musi wyłączać odpowiedzialność przewidzianą w art. 266 § 1 Kodeksu karnego.

Innymi słowy, zadośćuczynienie przez Spółkę [...] żądaniu Straży Miejskiej udostępnienia danych osobowych abonenta telefonu komórkowego nie mogłoby prowadzić do naruszenia tajemnicy telekomunikacyjnej, ani też nie mogłoby skutkować odpowiedzialnością karną w trybie art. 266 § 1 Kodeksu karnego.

Rozważając na tle niniejszej sprawy problematykę przetwarzania danych osobowych należy też zwrócić szczególną uwagę na odnoszące się do tej kwestii regulacje prawa wspólnotowego.

Art. 5 lit. a i b Konwencji z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych stanowi, iż dane osobowe będące przedmiotem automatycznego przetwarzania powinny być: pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem; gromadzone dla określonych i usprawiedliwionych celów i nie mogą być wykorzystywane w sposób niezgodny z tymi celami. Odstąpienie od tych reguł, stosownie do art. 9 ust. 2 lit. a Konwencji, jest dopuszczalne tylko wówczas, gdy taką możliwość przewiduje prawo wewnętrzne strony, jako środek konieczny w społeczeństwie

demokratycznym dla ochrony państwa, interesów finansowych państwa lub dla utrzymania porządku i bezpieczeństwa publicznego oraz zwalczania przestępczości.

Podobne unormowanie zostało również przewidziane w przepisach Dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. UE. L. 02.2001.37). W art. 5 ust. 1 tej Dyrektywy uregulowana została zasada poufności komunikacji. W myśl tej zasady, państwa członkowskie zobowiązane są zapewnić, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. Wyjątek od tej zasady przewidziany został w art. 15 ust. 1, zgodnie z którym państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych między innymi w art. 5 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej (...).

Przepisy prawa wspólnotowego stanowią więc swoistą gwarancję właściwego przetwarzania danych osobowych. Spenalizowanie konkretnego czynu w Kodeksie wykroczeń oznacza niewątpliwie, że taki czyn narusza porządek i bezpieczeństwo publiczne.

Z tych to powodów nie można w ocenie Naczelnego Sądu Administracyjnego zgodzić się ze stanowiskiem Sądu I instancji, że Dyrektywa 2002/58/WE dopuszcza uchwalanie przez państwa członkowskie środków ustawodawczych jedynie w celu ograniczenia poufności komunikacji w związku z zapobieganiem, dochodzeniem i karaniem przestępstw, albowiem właśnie ochronie porządku i bezpieczeństwa publicznego służy penalizacja i ściganie wykroczeń.

Z zaprezentowanym stanowiskiem w pełni koresponduje również wyrok Naczelnego Sądu Administracyjnego z dnia 28 stycznia 2003 r. sygn. akt II SA 2210/01 (Lex 194468), który mimo, iż został wydany na gruncie poprzednio obowiązującej ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz.U. Nr 73, poz. 852), zachował swoją aktualność również na tle rozpoznawanej sprawy.

W wyroku tym NSA wyraził pogląd, że system ochrony danych osobowych tworzą powiązane ze sobą rozwiązania w sposób uwzględniający hierarchię chronionych dóbr i wartości. Wyrazem tego jest m.in. art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych, dopuszczający przetwarzanie danych, gdy na to zezwalają przepisy prawa i gdy jest to niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego. Podobnie art. 69 ust. 1 Prawa telekomunikacyjnego zezwala na przetwarzanie danych objętych tajemnicą telekomunikacyjną również w innych celach niż świadczenie usług abonenckich, gdy jest to dopuszczalne na podstawie przepisów ustawowych. Łącznie z treścią art. 10 ust. 1 ustawy o strażach gminnych i art. 19 § 1 k.p.w. powstaje z tych przepisów uprawnienie straży do żądania udostępnienia jej danych osobowych pozostających w dyspozycji ich administratora, gdy jest to stosownie uzasadnione okolicznościami sprawy.

W związku z tym, iż w niniejszej sprawie nie doszło do naruszenia przepisów postępowania, które mogłyby mieć istotny wpływ na wynik sprawy, a zachodzi jedynie naruszenie prawa

materialnego Naczelny Sąd Administracyjny uchylił zaskarżony wyrok i skargę [...] S.A. na decyzję Generalnego Inspektora Ochrony Danych Osobowych z dnia [...] oddalił (art. 188 i 151 Prawa o postępowaniu przed sądami administracyjnymi).

O kosztach postępowania kasacyjnego Sąd orzekł na podstawie art. 203 pkt 2 tej ustawy.