Sprawa C-350/21

Streszczenie wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonego zgodnie z art. 98 § 1 regulaminu postępowania przed Trybunałem

Data wpływu:

4 czerwca 2021 r.

Oznaczenie sądu odsyłającego:

Specializiran nakazatelen syd (Bułgaria)

Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym:

3 czerwca 2021 r.

Strona skarżąca:

Specializirana prokuratura

Przedmiot postępowania głównego

Zgodność z prawem Unii uregulowania krajowego umożliwiającego ogólne i niezróżnicowane zatrzymywanie wszystkich danych o ruchu przez okres 6 miesięcy w celu walki z ciężkimi formami przestępczości.

Przedmiot i podstawa prawna wniosku o wydanie orzeczenia w trybie prejudycjalnym

Wniosek o wydanie orzeczenia w trybie prejudycjalnym zostaje złożony na podstawie art. 267 akapit pierwszy lit. b) TFUE.

Pytania prejudycjalne

Czy prawo krajowe – art. 251b ust. 1 Zakon za elektronnite syobsztenija (ustawy o komunikatach elektronicznych), w którym przewidziano ogólne i niezróżnicowane zatrzymywanie wszystkich danych o ruchu (danych o ruchu i o lokalizacji użytkowników środków łączności elektronicznej) przez okres 6 miesięcy, w celu walki z ciężkimi formami przestępczości, w sytuacji gdy w tym prawie krajowym przewidziano określone gwarancje – jest zgodne z art. 15 ust. 1 w związku z art. 5 ust. 1 w związku z motywem 11 dyrektywy 2002/58/WE

DOKUMENT ROBOCZY

Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej)?

Czy prawo krajowe – art. 159a Nakazatełno-procesualen kodeks (kodeksu postępowania karnego), w którym nie ograniczono dostępu do danych o ruchu jedynie do sytuacji, gdy jest to ściśle niezbędne, i nie przewidziano prawa osób, do czyich danych o ruchu uzyskały dostęp organy postępowania karnego, do powiadomienia ich w tym względzie, gdy to powiadomienie nie będzie stać na przeszkodzie prowadzeniu postępowania karnego, odpowiednio, nie przewidziano na ich rzecz środka ochrony prawnej przed bezprawnym dostępem – jest zgodne z art. 15 ust. 1 w związku z art. 5 ust. 1 w związku z motywem 11 dyrektywy 2002/58?

Przepisy i orzecznictwo Unii Europejskiej

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. 2002, L 201, s. 37.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. 2016, L 119, s. 1.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. 2016, L 119, s. 89.

Wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland Ltd i Karntner Landesregierung, C-293/12 i C-594/12, ECLI:EU:C:2014:238, zwany dalej „wyrokiem Digital Rights Ireland i in.”.

Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige AB i Post- och telestyrelsen, C-203/15 i C-698/15, ECLI:EU:C:2016:970, zwany dalej „wyrokiem Tele2”.

Wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, zwany dalej „wyrokiem Ministerio Fiscal”.

Wyrok z dnia 6 października 2020 r., Privacy International, C-623/17, EU:C:2020:790, zwany dalej „wyrokiem Privacy International”.

DOKUMENT ROBOCZY

Wyrok z dnia 6 października 2020 r., La Quadrature du Net i in., C-511/18, C-512/18 i C-520/18, EU:C:2020:791, zwany dalej „wyrokiem La Quadrature du Net i in.”.

Wyrok z dnia 2 marca 2021 r., H.K., C-746/18, EU:C:2021:152, zwany dalej „wyrokiem H.K.”.

Prawo krajowe

Zakon za elektronnite syobsztenija (ustawa o komunikatach elektronicznych, zwana dalej „ZES”).

Nakazatełno-procesualen kodeks (kodeks postępowania karnego, zwany dalej „NPK”).

Zwięzłe przedstawienie okoliczności faktycznych i postępowania głównego

1 Specializirana prokuratura (wyspecjalizowana prokuratura) wniosła do sądu odsyłającego wniosek o udostępnienie danych o ruchu komunikatów w odniesieniu do pięciu osób. Wniosek dotyczy danych już zatrzymanych w okresie poprzedzających 6 miesięcy.

2 Prokurator twierdzi, że dwie z tych osób – NG i RZ – uczestniczyły w zorganizowanej grupie przestępczej prowadzącej działalność w zakresie wprowadzania do obrotu towarów akcyzowych (papierosów bez banderoli). W odniesieniu do trzeciej z tych osób – IG – twierdzi, że przyczynia się ona do utrzymania relacji między NG a osobami trzecimi, od których NG nabywa papierosy bez banderoli. W odniesieniu do czwartej z tych osób – PP – twierdzi, że uczestniczy ona w tej działalności. W odniesieniu do ostatniej z tych osób – SJ – twierdzi, że otrzymuje ona od NG papierosy bez banderoli, a ustalenia między nimi są dokonywane w ramach rozmów telefonicznych.

3 Prokurator twierdzi, że komunikaty między tymi osobami są przekazywane wyłącznie poprzez ich telefony komórkowe. Wskazuje konkretne numery telefoniczne pięciu podejrzanych.

4 Prokurator wskazuje, że żądane dane o ruchu będą wykorzystane w ramach ścigania karnego, w celu zapobieżenia, ujawnienia i dokumentowania działalności przestępczej. W związku z tym prokurator złożył wniosek o udostępnienie danych zgodnie z art. 159a ust. 1–6 NPK.

5 Sąd odsyłający, po zapoznaniu się z materiałami sprawy, ustalił, że można wywieść założenie, iż owe pięć osób jest ewentualnie zaangażowanych w rozpatrywaną działalność przestępczą, czyli wprowadzanie do obrotu papierosów bez banderoli w ramach zorganizowanej grupy przestępczej – objęte prawną kwalifikacją określoną w art. 321 w związku z art. 234 Nakazatelen

DOKUMENT ROBOCZY

kodeks (kodeksu karnego). Jest to ciężkie umyślne przestępstwo. Istnieją również dane, że wskazane przez prokuratora numery telefoniczne są wykorzystywane przez te osoby, ewentualnie również przy prowadzeniu tego rodzaju działalności. W odniesieniu do niektórych z tych osób i niektórych z tych numerów telefonicznych udzielano już zezwolenia na ujawnienie danych o ruchu.

6 Zgodnie z prawem krajowym złożony wniosek o zezwolenie na udostępnienie dostępu do już zatrzymanych danych o ruchu – wstecz za okres 6 miesięcy – powinien zostać uwzględniony.

7 W tych okolicznościach istnieją wątpliwości, czy ten krajowy akt sądu byłby zgodny z prawem Unii, które stoi na przeszkodzie ogólnemu i niezróżnicowanemu zatrzymywaniu danych o ruchu. A mianowicie na podstawie takiego ogólnego i niezróżnicowanego zatrzymywania danych o ruchu, które jest zgodne z prawem krajowym, wniosek prokuratora może zostać uwzględniony. W związku z tym, jeśli zostanie ustalone, że prawo krajowe, w którym przewidziano takie ogólne i niezróżnicowane zatrzymywanie danych o ruchu, jest niezgodne z prawem Unii, sąd odsyłający nie uwzględni tego wniosku.

Zwięzłe przedstawienie uzasadnienia wniosku o wydanie orzeczenia w trybie prejudycjalnym

W przedmiocie pytania pierwszego

8 Trybunał przyjął, że dyrektywa 2006/24 ma zastosowanie ogólnie do wszystkich osób, bez żadnego rozróżnienia, ograniczenia lub wyłączenia; w szczególności nie jest niezbędne, by konkretne osoby były podejrzane, aby zatrzymywać ich dane o ruchu, nie istnieje ograniczenie w odniesieniu do rejonu geograficznego lub okresu czasu lub kręgu osób (wyrok Digital Rights Ireland Ltd i in., pkt 57–59). Wskazano, że dyrektywa 2006/24 „nie wyznacza ogólnych granic swojego zakresu zastosowania” (wyrok Digital Rights Ireland Ltd i in., pkt 60). Ze względu na te cechy dyrektywy uznano ją za nieważną.

9 Trybunał przyjął, że uregulowanie krajowe, w którym przewidziano ogólne i niezróżnicowane zatrzymywanie wszystkich danych o ruchu – wobec absolutnie wszystkich osób, bez konieczności istnienia podejrzenia o popełnienie przestępstwa i bez uwzględnienia ewentualnej tajemnicy zawodowej i bez jakichkolwiek ograniczeń – nie jest zgodne z prawem Unii (wyrok Tele2, pkt 103, 105, 106).

10 Trybunał przyjął, że podobne uregulowanie prawne jest niezgodne z prawem Unii w zakresie, w jakim przewiduje ono zatrzymywanie danych o ruchu jako regułę, podczas gdy dyrektywa wymaga, by był to wyjątek (wyrok Tele2, pkt 89, 104). Trybunał uściślił, że zatrzymywanie danych o ruchu nie powinno być systematyczne i nieprzerwane, nawet w wypadku walki z ciężką przestępczością (wyrok La Quadrature du Net i in., pkt 142).

DOKUMENT ROBOCZY

11 Trybunał przyjął, że w prawie krajowym należy wskazać okoliczności i warunki, w których prewencyjne można zastosować środek związany z zatrzymywaniem danych, ponieważ w ten sposób zapewnia się ograniczenie zatrzymywania do absolutnej konieczności (wyrok Tele2, pkt 109). W pkt 110 tego wyroku ponownie ustanowiono wymóg przewidzenia materialnych przesłanek ograniczających zakres prewencyjnego zatrzymywania danych. W ten sposób ponownie potwierdzono, że nie należy zatrzymywać masowo wszystkich danych o ruchu.

12 Trybunał dopuszcza ogólne zatrzymywanie wszystkich danych o ruchu jedynie na określonym obszarze geograficznym, co do którego zakłada się, że istnieje na nim wysokie ryzyko przygotowania i popełnienia przestępstwa (wyrok Tele2, pkt 111; wyrok La Quadrature du Net i in., pkt 144, 150).

13 Dopuszcza się ogólne zatrzymywanie wszystkich danych o ruchu w wypadku istnienia zagrożenia dla bezpieczeństwa narodowego, jednakże chodzi o zarządzenie takiego zatrzymywania przez ograniczony okres czasu i przy istnieniu faktycznego i aktualnego lub przewidywalnego zagrożenia dla bezpieczeństwa narodowego (wyrok Privacy International, pkt 75, 76; wyrok La Quadrature du Net i in., pkt 137–139). A zatem Trybunał nie uznał jeszcze za zgodne z prawem Unii przewidzianego w prawie ogólnego zatrzymywania wszystkich danych przez nieograniczony okres czasu, przy uwzględnieniu przyszłych nieokreślonych potrzeb, bez istnienia podejrzeń, że taka konkretna potrzeba co do zasady istnieje.

14 Równocześnie określony w art. 251b ust. 1 ZES krajowy reżim prawny zatrzymywania danych o ruchu ma zastosowanie do absolutnie wszystkich komunikatów elektronicznych zrealizowanych na całym terytorium państwa, w każdej chwili, przez wszystkie osoby i nieprzerwanie, a jedynie przechowywanie zatrzymanych danych jest ograniczone do 6 miesięcy. Reżim ten został uznany wyraźnie za zgodny z konstytucją przez Konstitucjonnija syd (trybunał konstytucyjny), ponieważ przedstawiono argumenty w tym względzie, a następnie ponownie został uznany w sposób dorozumiany.

15 W związku z tym powstaje kwestia, czy prawo krajowe, art. 251b ust. 1 ZES, jest zgodne z prawem Unii. Pomimo że Trybunał wskazał już jasno, że takie ogólne zatrzymywanie danych o ruchu – w sytuacji gdy dyrektywa 2006/24 „nie wyznacza ogólnych granic swojego zakresu zastosowania" – jest niezgodne z prawem Unii, to nie miał jednak możliwości rozważenia argumentów bułgarskiego Konstitucjonnija syd ani dokonania oceny, czy nie należałoby uwzględnić tych argumentów.

W przedmiocie okresu przechowywania danych o ruchu

16 Trybunał przyjął, że art. 6 dyrektywy 2006/24 jest niezgodny z prawem Unii w zakresie, w jakim przewidziano w nim ten sam okres przechowywania (minimum 6 miesięcy) wszystkich rodzajów danych – bez rozróżnienia między

DOKUMENT ROBOCZY

nimi i bez wskazania, że określenie okresu powinno opierać się na obiektywnych kryteriach, tak aby zapewnić, że jest on ograniczony do tego, co jest ściśle niezbędne (wyrok Digital Rights Ireland i in. pkt 63, 64).

17 Podobnie sformułowano prawo krajowe – art. 251b ust. 1 ZES – w którym przewidziano ten sam okres przechowywania (6 miesięcy) wszystkich rodzajów danych o ruchu. W związku z tym powstaje wątpliwość, czy prawo krajowe jest zgodne z prawem Unii.

W przedmiocie wykorzystania już zatrzymanych danych w odniesieniu do ciężkich przestępstw

18 Trybunał przyjął odnośnie do systemu ustanowionego w dyrektywie 2006/24, że dostęp do zatrzymanych danych nie jest ograniczony według obiektywnych kryteriów – w zakresie, w jakim dyrektywa 2006/24 dopuszcza ten dostęp w wypadku ciężkich przestępstw, zgodnie z ich określeniem w prawodawstwie krajowym (wyrok Digital Rights Ireland i in., pkt 60). Wskazano, że dyrektywa nie ogranicza tego dostępu do „dokładnie określonych poważnych przestępstw", ponieważ pozostawiono to uznaniu każdego państwa członkowskiego (wyrok Digital Rights Ireland i in., pkt 61). W związku z tym stwierdzono nieważność tej dyrektywy.

19 Z drugiej strony Trybunał przyjął, że wystarcza, jeśli zatrzymane dane o ruchu odnoszą się do ciężkich przestępstw – bez ustanowienia dodatkowych wymagań dotyczących ich istoty (wyrok Tele2, pkt 102, 110, 115; w tym rozumieniu wyrok Ministerio Fiscal, pkt 56).

20 Zgodnie z prawem krajowym dostęp do już zatrzymanych danych o ruchu jest dopuszczalny w odniesieniu do każdego ciężkiego umyślnego przestępstwa, czyli jeśli za to przestępstwo przewidziano karę w wymiarze ponad 5 lat „pozbawienia wolności" i popełniono je umyślnie – z zamiarem bezpośrednim lub pośrednim (sprawca zamierzał lub dopuszczał wystąpienie szkodliwych skutków). Czy istnienie tego kryterium – umyślnego przestępstwa – jest wystarczające dla przyjęcia, że zapewniono przestrzeganie wymogu dotyczącego „dokładnie określonych poważnych przestępstw" w rozumieniu pkt 60 wyroku Digital Rights Ireland i in., czy też wymóg ten nie jest już aktualny, mając na względzie nowsze orzecznictwo Trybunału?

W przedmiocie wzmocnionej ochrony przy zatrzymywaniu danych o ruchu i dostępie do nich

21 Pomimo że pod niektórymi względami uregulowanie krajowe nie spełnia wymogów prawa Unii dotyczących zatrzymywania i wykorzystania danych o ruchu, to jednak pod innymi względami spełnia ono te wymogi, a nawet zapewnia wyższy poziom ochrony. Są to nowe okoliczności faktyczne, których nie rozpatrywał Trybunał, a mianowicie wzmocniona ochrona przy zatrzymaniu danych o ruchu, zarówno w okresie 6 miesięcy, w którym są one przechowywane, jak i w odniesieniu do wniosku o udzielenie dostępu do nich oraz niszczenia

DOKUMENT ROBOCZY

otrzymanych sprawozdań. W związku z tym powstaje kwestia, czy uregulowanie krajowe, rozpatrywane w całości, przy uwzględnieniu wszystkich określonych w nim gwarancji, spełnia jednak wymogi prawa Unii, w związku z czym krajowy reżim prawny określony w art. 251b ust. 1 ZES jest zgodny z art. 15 ust. 1 w związku z art. 5 dyrektywy 2002/58.

22 Uregulowanie krajowe jest podobne do uregulowania szwedzkiego, opisanego w pkt 15–19 wyroku Tele2, jeśli chodzi o istotę i okres zatrzymywania danych; w tym kontekście zgodnie z bułgarskim uregulowaniem prawnym dostęp do tych danych jest uzależniony od kontroli sądu, której nie przewidziano w uregulowaniu szwedzkim, a poza tym bułgarskie uregulowanie prawne przewiduje ten dostęp wyłącznie w wypadku popełnienia ciężkich przestępstw – w odróżnieniu od uregulowania szwedzkiego.

23 Trybunał wskazał warunki, w których zatrzymywanie danych może być uznane za zgodne z prawem Unii:

– zatrzymywanie danych o ruchu powinno opierać się na jasnych i dokładnych regułach regulujących zakres i zastosowanie środka związanego z zatrzymywaniem danych o ruchu (wyrok Tele2, pkt 109). Takie reguły istnieją w prawie krajowym;

– dostęp do zatrzymanych danych o ruchu powinien być realizowany na podstawie jasnych i dokładnych reguł, materialnych i proceduralnych reguł dostępu (wyrok Tele2, pkt 117, 118). Takie reguły wskazano w art. 159a NPK;

– wykluczono ogólny dostęp do wszystkich zatrzymanych danych, przewidując dostęp do danych określonych osób, podejrzanych o popełnienie przestępstwa (wyrok Tele2, pkt 119; wyrok La Quadrature du Net i in., pkt 161). Taki wymóg określono w art. 159a NPK, zgodnie z wykładnią i sposobem stosowania tego przepisu przez sąd krajowy;

– dostęp jest realizowany na podstawie uprzedniej kontroli sądu, po rozpatrzeniu uzasadnionego wniosku organów prowadzących postępowanie karne (wyrok Tele2, pkt 120). Przewidziano taką uprzednią kontrolę sądu;

– dostawcy usług łączności elektronicznej powinni przyjąć odpowiednie środki techniczne i organizacyjne, tak aby wykluczyć nadużycie danych lub bezprawny dostęp do danych (wyrok Tele2, pkt 122). Takie środki przewidziano w ZES, wzmacniając je dodatkowo poprzez udział Komisija za zasztita na licznite danni (komisji ds. ochrony danych osobowych) oraz Komisija kym Narodno sybranie (komisji działającej przy zgromadzeniu narodowym).

24 A zatem ta wzmocniona ochrona przyznaje niezbędne gwarancje, pomimo ogólnego i niezróżnicowanego zatrzymywania wszystkich danych o ruchu przez określony w art. 251b ust. 1 ZES okres 6 miesięcy.

DOKUMENT ROBOCZY

W przedmiocie pytania drugiego

W przedmiocie ograniczenia dostępu do danych o ruchu do „ściśle niezbędnego" dostępu

25 Trybunał przyjął, że niezbędne jest ograniczenie dostępu do tego, co jest „ściśle konieczne [niezbędne] do realizacji zamierzonego celu", biorąc pod uwagę uzasadnienie wniosku (wyrok Digital Rights Ireland i in., pkt 62). W pkt 65 tego wyroku ponownie wskazano, że dostęp do danych o ruchu skutkuje „wyjątkowo szeroką i mocną ingerencją w te podstawowe dla porządku prawnego Unii prawa," co wymaga ograniczenia ingerencji do tego, co jest „ściśle niezbędne".

26 Wymaga się ustanowienia w prawie krajowym jasnych i dokładnych reguł dotyczących umożliwienia dostępu do danych osobowych i danych o ruchu (wyrok Privacy International, pkt 68; wyrok La Quadrature du Net i in., pkt 132). W pkt 38 wyroku H.K. wskazano parametry odnoszące się do tego, co jest „ściśle niezbędne" – kategorie danych i czas trwania dostępu, ponieważ oceny należy dokonać w zależności od okoliczności danego wypadku. W pkt 68 wyroku Privacy International wskazano wymóg proporcjonalności.

27 W prawie krajowym – art. 159a NPK – nie przewidziano kryterium tego, co jest „ściśle konieczne [niezbędne] do realizacji zamierzonego celu". Orzecznictwo sądów wymaga, by istniały racjonalne podejrzenia dotyczące uczestnictwa w rozpatrywanej działalności przestępczej osób, o czyich dane o ruchu wnioskowano, zaś w prawie ustanowiono wymóg, by zezwolenie na ujawnienie takich danych o ruchu było ograniczone rozsądnym terminem, nie dłuższym niż 6 miesięcy. W związku z tym powstaje kwestia, czy te wymogi są wystarczające, aby przyjąć, że spełniono wymóg dotyczący tego, co jest „ściśle niezbędne".

W przedmiocie prawa do skutecznego środka prawnego zainteresowanych osób

28 Trybunał przyjął, że w europejskich uregulowaniach prawnych należy określić jasne i dokładne reguły dotyczące minimalnych wymagań, tak aby zainteresowanym osobom przysługiwała skuteczna ochrona przed nadużyciami i bezprawnym dostępem (wyrok Digital Rights Ireland i in., pkt 54). Brak takich reguł skutkował stwierdzeniem nieważności dyrektywy 2006/24.

29 Trybunał przyjął, że w prawie krajowym należy również określić minimalne wymogi w taki sposób, by osoby, których dane są zatrzymane, dysponowały wystarczającymi gwarancjami umożliwiającymi im skuteczną ochronę przed nadużyciami (wyrok Tele2, pkt 109; wyrok Privacy International, pkt 68). Trybunał przyjął, że zatrzymywanie danych o ruchu samo w sobie skutkuje naruszeniem praw określonych w art. 7 i 8 karty – przy czym nie ma znaczenia, czy skutkowało to trudnościami dla zainteresowanych osób i czy dane te zostały wykorzystane (wyrok Privacy International, pkt 70; wyrok La Quadrature du Net i in., pkt 115, 116).

DOKUMENT ROBOCZY

30 Trybunał przyjął, że w prawie krajowym należy przewidzieć informowanie zainteresowanych osób od chwili, w której informacja taka nie będzie narażać na szwank prowadzonych postępowań dochodzeniowo-śledczych, tak aby osoby te mogły wykonać swoje prawa (wyrok Tele2, pkt 121).

31 Ponadto konieczne jest określenie na poziomie krajowym sprawowanej przez niezależny organ kontroli przestrzegania poziomu ochrony przewidzianego w prawie Unii, tak aby zapewnić prawo zainteresowanych osób do złożenia wniosku do krajowych organów nadzoru w celu ochrony ich danych (wyrok Tele2, pkt 123).

32 W prawie krajowym przewidziano szereg reguł zapewniających bezpieczeństwo zatrzymanych danych o ruchu, lecz nie przewidziano prawa zainteresowanych osób do powiadomienia ich o tym, że w stosunku do nich nakazano ujawnienie zatrzymanych w okresie 6 miesięcy danych o ruchu, odpowiednio, nie przewidziano prawa do zaskarżenia przez nie zgodności z prawem zezwolenia sądu, o którym mowa w art. 159a ust. 4 NPK.

33 Podniesiono kwestię, czy określony przez Trybunał w pkt 54 wyroku Digital Rights Ireland i in. wymóg dotyczący skutecznej ochrony przed nadużyciami i bezprawnym dostępem odnosi się również do wypadków, w których zezwolenie zostało udzielone przez sąd, jednakże wyłącznie na podstawie wniosku prokuratora, bez uczestnictwa zainteresowanych osób. Czy zezwolenie sądu udzielone w takich okolicznościach stanowi wystarczającą gwarancję przeciwko nadużyciom i bezprawnym dostępem, w związku z czym zainteresowana osoba nie będzie powiadamiana o ujawnieniu jej danych o ruchu i nie będzie mogła zaskarżyć zgodności z prawem udzielonego zezwolenia?

DOKUMENT ROBOCZY