Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
ANTHONY'EGO MICHAELA COLLINSA
przedstawiona w dniu 8 czerwca 2023 r. [1]

Sprawa C-178/22

Nieznani sprawcy
przy udziale:
Procura della Repubblica presso il Tribunale di Bolzano

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Tribunale di Bolzano (trybunał w Bolzano, Włochy)]

Odesłanie prejudycjalne – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Poufność komunikacji – Dostawcy usług łączności elektronicznej – Dyrektywa 2002/58/WE – Artykuł 1 ust. 3 i art. 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 11 oraz art. 52 ust. 1 – Wniosek prokuratora o udzielenie dostępu do danych w celu prowadzenia dochodzenia w sprawie kradzieży kwalifikowanej telefonu komórkowego i karania tego przestępstwa – Definicja „poważnego przestępstwa" mogącego uzasadniać poważną ingerencję w prawa podstawowe – Zakres uprzedniej kontroli służącej zapewnieniu przestrzegania wymogu popełnienia poważnego przestępstwa – Zasada proporcjonalności

I. Wprowadzenie

1. Procura della Repubblica presso il Tribunale di Bolzano [prokuratura przy trybunale w Bolzano, Włochy, zwana dalej „prokuraturą (Bolzano)"] występuje do Tribunale di Bolzano (trybunału w Bolzano, Włochy) o udzielenie dostępu do danych zatrzymywanych przez dostawców usług łączności elektronicznej na podstawie uregulowania krajowego umożliwiającego w szczególności namierzenie i zidentyfikowanie źródła oraz odbiorcy komunikatów wymienianych przy użyciu telefonów komórkowych.

2. W związku z tym wnioskiem Tribunale di Bolzano (trybunał w Bolzano) zwraca się do Trybunału Sprawiedliwości o dokonanie wykładni art. 15 ust. 1 dyrektywy 2002/58/WE [2]. Przepis ten zezwala państwom członkowskim na wprowadzenie w ustawodawstwie wyjątków od

[1] Język oryginału: angielski.

[2] Dyrektywa 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 – wyd. spec. w jęz. polskim, rozdz. 13, t. 29, s. 514), zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11).

ustanowionego w owej dyrektywie [3] obowiązku zapewnienia poufności łączności elektronicznej. W wyroku Prokuratuur [4] Trybunał orzekł, że dostęp do danych umożliwiających wyciągnięcie precyzyjnych wniosków na temat życia prywatnego użytkownika, zapewniony na mocy środków przyjętych na podstawie art. 15 ust. 1 dyrektywy 2002/58, stanowi poważną ingerencję w prawa podstawowe i zasady zagwarantowane w art. 7, 8, i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą") [5]. Takiego dostępu nie można udzielać w celach zapobiegania „ogółowi przestępstw" oraz dochodzenia, wykrywania i karania „ogółu przestępstw". Można go przyznać jedynie w postępowaniach mających na celu zwalczanie „poważnej przestępczości" [6]; ponadto musi on być uzależniony od służącej zapewnieniu przestrzegania tego wymogu uprzedniej kontroli sądu lub niezależnego organu administracyjnego [7]. Tribunale di Bolzano (trybunał w Bolzano) zwraca się do Trybunału o wyjaśnienie dwóch aspektów wyroku Prokuratuur, dotyczących pojęcia „poważnej przestępczości" oraz zakresu uprzedniej kontroli, którą sąd powinien przeprowadzić na podstawie przepisu prawa krajowego zobowiązującego go do udzielenia dostępu do danych zatrzymywanych przez dostawców usług łączności elektronicznej.

II. Ramy prawne

A. Prawo Unii

3. Artykuł 5 dyrektywy 2002/58, zatytułowany „Poufność komunikacji", stanowi:

„1. Państwa członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. […]

[…]".

4. Artykuł 6 dyrektywy 2002/58, zatytułowany „Dane o ruchu", brzmi:

„1. Dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, bez uszczerbku dla przepisów ust. 2, 3 i 5 niniejszego artykułu oraz art. 15 ust. 1.

[…]

[3] Zobacz art. 5 dyrektywy 2002/58. Zagwarantowana w art. 5 ust. 1 dyrektywy 2002/58 ochrona poufności łączności elektronicznej znajduje zastosowanie do środków stosowanych przez podmioty inne niż użytkownicy, niezależnie od tego, czy są to podmioty publiczne, czy też prywatne. Wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 36 i przytoczone tam orzecznictwo.

[4] Wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152 (zwany dalej „wyrokiem Prokuratuur").

[5] Niezależnie od długości okresu, na jaki wniesiono o dostęp do takich danych, oraz ilości i rodzaju danych dostępnych przez taki okres.

[6] Lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego. Zobacz wyrok Prokuratuur, pkt 35, 39, 45. Zobacz także wyroki: z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 56; 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, pkt 140.

[7] Wyrok Prokuratuur, pkt 48–52.

5. Przetwarzanie danych o ruchu, zgodnie z ust. 1–3 i 4, musi być ograniczone do osób działających z upoważnienia dostawców publicznych sieci łączności i publicznie dostępnych usług łączności elektronicznej, zajmujących się naliczaniem opłat lub ruchem, obsługą klienta, systemem wykrywania nadużyć finansowych, marketingiem usług łączności elektronicznej lub świadczeniem usług tworzących wartość dodaną, oraz musi być ograniczone do celów niezbędnych przy takich działaniach.

[…]".

5. Artykuł 9 dyrektywy 2002/58, zatytułowany „Dane dotyczące lokalizacji inne niż dane o ruchu", stanowi:

„1. W przypadku gdy dane dotyczące lokalizacji inne niż dane o ruchu, odnoszące się do użytkowników lub abonentów publicznych sieci łączności lub publicznie dostępnych usług łączności elektronicznej, mogą być przetwarzane, przetwarzanie może mieć miejsce tylko wówczas gdy dane te są anonimowe, lub za zgodą użytkowników lub abonentów, w zakresie i przez okres niezbędny do świadczenia usługi tworzącej wartość dodaną. Przed uzyskaniem zgody użytkowników lub abonentów dostawca usług musi ich poinformować o rodzaju danych dotyczących lokalizacji innych niż dane o ruchu, które będą przetwarzane, o celach i okresie ich przetwarzania oraz o tym, czy dane zostaną przekazane stronie trzeciej do celów świadczenia usługi tworzącej wartość dodaną. Użytkownicy lub abonenci mają możliwość odwołania w każdej chwili swojej zgody na przetwarzanie danych dotyczących lokalizacji innych niż dane o ruchu.

[…]".

6. Artykuł 15 ust. 1 dyrektywy 2002/58 ma następujące brzmienie:

„Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego ([np.] bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE[8]. W tym celu państwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej".

B. Prawo krajowe

7. Artykuł 132 ust. 3 decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali (dekretu ustawodawczego nr 196 z dnia 30 czerwca 2003 r. ustanawiającego kodeks ochrony danych osobowych)[9], ostatnio zmieniony art. 1 decreto-legge 30 settembre 2021 n. 132 – Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP, convertito con modificazioni nella legge 23 novembre 2021 n. 178

[8] Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. 1995, L 281, s. 31).

[9] Dodatek zwyczajny nr 123 do GURI nr 174 z dnia 29 lipca 2003 r., s. 11.

(dekretu z mocą ustawy nr 132 z dnia 30 września 2021 r.[10], przekształconego ze zmianami w ustawę nr 178 z dnia 23 listopada 2021 r.)[11] (zwany dalej „art. 132 ust. 3 dekretu ustawodawczego nr 196/2003"), stanowi:

3. „W przewidzianym w ustawie okresie zatrzymywania (to znaczy 24 miesiące od dnia komunikatu), jeśli istnieją wystarczające przesłanki popełnienia przestępstw, w odniesieniu do których ustawa przewiduje karę dożywotniego pozbawienia wolności lub karę pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata, określoną zgodnie z art. 4 Codice di procedura penale (kodeksu postępowania karnego), a także przestępstw groźby karalnej i nękania lub niepokojenia osób za pomocą telefonu, w przypadku gdy groźba karalna, nękanie i niepokojenie są poważne, o ile są one istotne dla ustalenia okoliczności faktycznych, dane pozyskuje się za uprzednią zgodą sądu wydaną w drodze uzasadnionego postanowienia na wniosek prokuratury lub na wniosek obrońcy oskarżonego, osoby objętej postępowaniem przygotowawczym, pokrzywdzonego oraz innych osób prywatnych;

[…]".

3 quater „Dane pozyskane z naruszeniem przepisów ust. 3 i 3 bis nie mogą być wykorzystane".

8. Artykuł 4 kodeksu postępowania karnego, zatytułowany „Zasady ustalania właściwości", brzmi:

„W celu ustalenia właściwości bierze się pod uwagę karę przewidzianą w ustawie w odniesieniu do każdego popełnionego przestępstwa lub usiłowania przestępstwa. Nie bierze się pod uwagę ciągłości popełnienia przestępstwa, recydywy i okoliczności popełnienia przestępstwa, z wyjątkiem okoliczności obciążających, w odniesieniu do których ustawa przewiduje karę innego rodzaju niż zwykła kara za przestępstwo, oraz okoliczności o skutku szczególnym".

9. Zdaniem sądu odsyłającego przestępstwo kradzieży kwalifikowanej może być ścigane z urzędu przez prokuraturę[12]. Zgodnie z art. 625 Codice penale (kodeksu karnego) osoba uznana winną kradzieży kwalifikowanej podlega karze szczególnej pozbawienia wolności od dwóch do sześciu lat i karze grzywny w wysokości od 927 EUR do 1500 EUR. Artykuł 624 kodeksu karnego stanowi, że osoba uznana winną kradzieży mniejszej wagi, która jest ścigana na wniosek pokrzywdzonego, podlega karze pozbawienia wolności od sześciu miesięcy do trzech lat i karze grzywny w wysokości od 154 EUR do 516 EUR.

III. Postępowania główne i pytanie prejudycjalne

10. Prokuratura wszczęła przeciwko nieznanym sprawcom dwa postępowania karne w sprawie kradzieży kwalifikowanej telefonu komórkowego na podstawie art. 624 i 625 kodeksu karnego[13]. Aby zlokalizować sprawców, wystąpiła ona do sądu odsyłającego, w trybie art. 132 ust. 3 dekretu ustawodawczego nr 196/2003, o „[…] wydanie zgody na pozyskanie od wszystkich operatorów telefonicznych wszystkich danych będących w ich posiadaniu wraz z metodami śledzenia i lokalizacji (w szczególności dotyczących użytkowników i ewentualnie kodów IMEI osób

[10] GURI nr 234 z dnia 30 września 2021 r., s. 1.

[11] GURI nr 284 z dnia 29 listopada 2021 r., s. 1.

[12] Zgodnie z prawem włoskim przestępstwa kradzieży będące przedmiotem postępowania przygotowawczego przed sądem odsyłającym uznaje się za przestępstwa w typie kwalifikowanym.

[13] Pierwsza kradzież została popełniona w dniu 27 października 2021 r. (numer referencyjny RGNR 9228/2021). Druga kradzież miała miejsce w dniu 20 listopada 2021 r. (numer referencyjny RGNR 9794/2021). Do obu kradzieży telefonów komórkowych doszło w Bolzano, zaś właściciele tych urządzeń zgłosili owe przestępstwa na posterunku Carabinieri (policji).

wywoływanych/wywołujących, odwiedzanych/odbieranych stron, czasu i długości wywołania/połączenia oraz wskazania odpowiednich stacji przekaźnikowych lub anten, użytkowników i numerów IMEI będących nadawcami/odbiorcami wiadomości SMS lub MMS oraz, w miarę możliwości, ogólnych danych odpowiednich odbiorców) przychodzących i wychodzących rozmów/komunikatów telefonicznych oraz wykonanych połączeń, w tym w roamingu, nawet w przypadku połączeń bez naliczania opłat (nieodebranych połączeń), od dnia kradzieży do dnia sporządzenia wniosku".

11. Sąd odsyłający zastanawia się, czy art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 jest zgodny z art. 15 ust. 1 dyrektywy 2002/58, tak jak ów przepis został zinterpretowany w wyroku Prokuratuur. Zauważa on, że w dniu 7 września 2021 r. Corte suprema di cassazione (najwyższy sąd kasacyjny, Włochy)[14] orzekł, iż ponieważ sądy krajowe mogą swobodnie określać przestępstwa stanowiące „poważne zagrożenie dla bezpieczeństwa publicznego lub inne formy poważnej przestępczości", wyrok Prokuratuur nie podlegał bezpośredniemu stosowaniu przez sądy krajowe. W następstwie wyroku Corte suprema di cassazione (najwyższego sądu kasacyjnego) ustawodawca włoski przyjął dekret z mocą ustawy nr 132 z dnia 30 września 2021 r., w którego art. 132 ust. 3 do poważnych przestępstw, w przypadku których możliwe jest pozyskanie wyciągów telefonicznych, zaliczono między innymi przestępstwa, za które ustawa przewiduje „karę pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata […]".

12. Zdaniem sądu odsyłającego ustanowiony w art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 próg służący kwalifikowaniu przestępstw jako poważnych prowadzi do objęcia zakresem tego pojęcia przestępstw, których szkodliwość społeczna jest niewielka i które mogą być ścigane jedynie na wniosek[15]. W związku z tym na podstawie tego przepisu dostęp do wyciągów telefonicznych można uzyskać w przypadku kradzieży rzeczy o małej wartości, takich jak telefon komórkowy lub rower. Oznacza to, że próg ustanowiony w art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 narusza zasadę proporcjonalności w rozumieniu art. 52 ust. 1 karty, która to zasada zawsze wymaga dokonania wyważenia między wagą przestępstwa będącego przedmiotem postępowania przygotowawczego a ograniczeniem w korzystaniu z prawa podstawowego. Ściganie tak drobnych przestępstw nie może stanowić uzasadnienia dla ograniczenia w korzystaniu z praw podstawowych do poszanowania życia prywatnego, ochrony danych osobowych oraz wolności wypowiedzi i informacji[16].

13. Sąd odsyłający wyjaśnia, że zakres swobody sądów włoskich w zakresie odmowy wydania zgody na dostęp do wyciągów telefonicznych jest bardzo ograniczony, ponieważ taka zgoda musi zostać udzielona w przypadku istnienia „wystarczających przesłanek popełnienia przestępstw" oraz jeżeli taka zgoda jest „istotna dla ustalenia okoliczności faktycznych". W szczególności sądy nie są właściwe do oceny wagi przestępstwa będącego przedmiotem postępowania przygotowawczego. Tej oceny dokonał ustawodawca, gdy postanowił, w sposób ogólny i bez rozróżnienia między różnymi rodzajami przestępstw, że dostępu do wyciągów telefonicznych

[14] Cass. Pen. Sez. II, n. 33116, ud. 7.9.2021, est. Pellegrino.

[15] Sąd odsyłający wskazuje, że „dotyczy to na przykład przestępstwa włamania, które zgodnie z art. 614 kodeksu karnego jest zagrożone karą od roku do czterech lat pozbawienia wolności. Innymi przestępstwami, których górna granica ustawowego zagrożenia nie stoi na przeszkodzie uzyskaniu wyciągów telefonicznych, ściganych na wniosek ze względu na znikomą szkodliwość społeczną, są przestępstwa przewidziane w art. 633 kodeksu karnego (squatting – zajęcie opuszczonej nieruchomości zazwyczaj bez zgody właściciela: kara pozbawienia wolności od roku do trzech lat i kara grzywny w wysokości od 103 EUR do 1032 EUR) lub w art. 640 kodeksu karnego (oszustwo mniejszej wagi: kara pozbawienia wolności od sześciu miesięcy do trzech lat i kara grzywny w wysokości od 51 EUR do 1032 EUR)".

[16] Zobacz art. 7, 8, 11 karty.

należy udzielać w szczególności w kontekście postępowań przygotowawczych w sprawach wszystkich przestępstw zagrożonych karą pozbawienia wolności, której górna granica zagrożenia wynosi nie mniej niż trzy lata.

14. W tych okolicznościach Tribunale di Bolzano (trybunał w Bolzano) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującym pytaniem prejudycjalnym:

„Czy art. 15 ust. 1 [dyrektywy 2002/58] sprzeciwia się uregulowaniu krajowemu zawartemu w [art. 132 ust. 3 dekretu ustawodawczego nr 196/2003], [który] […] stanowi, co następuje:

»W przewidzianym w ustawie okresie zatrzymywania, jeśli istnieją wystarczające przesłanki popełnienia przestępstw, w odniesieniu do których ustawa przewiduje karę dożywotniego pozbawienia wolności lub karę pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata, określoną zgodnie z art. 4 [kodeksu postępowania karnego], a także przestępstw groźby karalnej i nękania lub niepokojenia osób za pomocą telefonu, w przypadku gdy groźba karalna, nękanie i niepokojenie są poważne, o ile są one istotne dla ustalenia okoliczności faktycznych, dane pozyskuje się za uprzednią zgodą sądu wydaną w drodze uzasadnionego postanowienia na wniosek prokuratury lub na wniosek obrońcy oskarżonego, osoby objętej postępowaniem przygotowawczym, pokrzywdzonego oraz innych osób prywatnych«?”.

IV. Postępowanie przed Trybunałem

15. Uwagi na piśmie zostały przedstawione przez rządy czeski, estoński, Irlandię, rządy francuski, włoski, cypryjski, węgierski, niderlandzki, austriacki i polski oraz przez Komisję Europejską.

16. Na rozprawie w dniu 21 marca 2023 r. te zainteresowane strony oraz prokuratura (Bolzano) przedstawiły swe wystąpienia ustne i udzieliły odpowiedzi na pytania Trybunału.

V. Ocena

A. W przedmiocie dopuszczalności

17. Rząd włoski i Irlandia podnoszą, że część wniosku o wydanie orzeczenia w trybie prejudycjalnym jest niedopuszczalna. Ze stanu faktycznego przedstawionego w postanowieniu odsyłającym wynika, że wniosek o udzielenie dostępu został złożony w związku z postępowaniami przygotowawczymi dotyczącymi kwalifikowanych kradzieży telefonów komórkowych. Irlandia podkreśla, że prokuratura może ścigać to przestępstwo z urzędu. Istnienie owego uprawnienia jest pochodną stanowiska, zgodnie z którym to przestępstwo, ze względu na swój charakter i swoje skutki, wpływa na społeczeństwo w ujęciu ogólnym. Wniosek o wydanie orzeczenia w trybie prejudycjalnym jest zatem hipotetyczny w zakresie, w jakim odnosi się również do przestępstw, które mogą być ścigane wyłącznie na wniosek. Rząd włoski wskazuje, że sąd odsyłający wspomina o szeregu przestępstw, które pozostają bez znaczenia dla zawisłych przed nim spraw. Rząd włoski i Komisja podnoszą, że – wbrew zamieszczonej we wniosku wzmiance o „karze pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata” – zgodnie z art. 625 kodeksu karnego przestępstwo kradzieży kwalifikowanej jest zagrożone karą pozbawienia wolności od dwóch do sześciu lat. Komisja proponuje zatem, aby Trybunał przeformułował pytanie prejudycjalne. Rząd francuski również

zwraca się do Trybunału o przeformułowanie tego pytania. Uważa on, że o ile Trybunał może dokonywać wykładni przepisów prawa Unii, o tyle nie jest właściwy do oceny zgodności przepisów prawa krajowego z prawem Unii.

18. Literalne brzmienie pytania prejudycjalnego postawionego przez sąd odsyłający wzywa Trybunał do wypowiedzenia się w przedmiocie zgodności przepisu prawa krajowego z prawem Unii. Samo w sobie nie stoi to na przeszkodzie dostarczeniu sądowi odsyłającemu elementów wykładni prawa Unii, w tym przypadku art. 15 ust. 1 dyrektywy 2002/58, które umożliwią mu rozstrzygnięcie o zgodności z tym przepisem każdego uregulowania krajowego analizowanego w toczącym się przed nim postępowaniu [17].

19. Z wniosku o wydanie orzeczenia w trybie prejudycjalnym jasno wynika, że prokuratura (Bolzano) wystąpiła z wnioskiem o udzielenie dostępu do danych w szczególności w celu prowadzenia postępowania przygotowawczego w sprawie dwóch czynów stanowiących przestępstwo kradzieży kwalifikowanej telefonu komórkowego na podstawie art. 625 kodeksu karnego oraz w celu karania tego przestępstwa. W tych okolicznościach zawarte we wniosku wzmianki o innych przestępstwach, w tym nawiązania do art. 624 kodeksu karnego (kradzież mniejszej wagi) [18], nie mają znaczenia dla rozstrzygnięcia wniosków przedłożonych sądowi odsyłającemu [19]. W zakresie, w jakim pytanie prejudycjalne dotyczy złożonego przez prokuraturę (Bolzano) wniosku o udzielenie dostępu do danych w celu przeprowadzenia postępowania przygotowawczego w sprawie popełnienia przestępstw kradzieży kwalifikowanej, nie jest ono hipotetyczne. W związku z tym moja ocena kwestii stosowania art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 będzie się ograniczać do opisanych przez sąd odsyłający okoliczności faktycznych związanych z kradzieżami kwalifikowanymi telefonów komórkowych.

B. Co do istoty

1. Uwagi wstępne

20. U podstaw rozpatrywanego odesłania leży wniosek prokuratury (Bolzano) o udzielenie dostępu do danych zatrzymywanych przez dostawców usług łączności elektronicznej. Jego przedmiotem nie jest zatrzymywanie tych danych ani zgodność takiego zatrzymywania z prawem na podstawie w szczególności art. 15 ust. 1 dyrektywy 2002/58 [20]. Do tych danych zaliczają się informacje o przychodzących i wychodzących komunikatach [21] wymienianych przy użyciu skradzionych telefonów komórkowych oraz dane dotyczące lokalizacji [22]. Choć te dane nie

[17] Zobacz analogicznie wyrok z dnia 17 marca 2021 r., Consulmarketing, C-652/19, EU:C:2021:208, pkt 33. Zgodnie z utrwalonym orzecznictwem w ramach procedury ustanowionej w art. 267 TFUE do Trybunału należy udzielenie sądowi krajowemu odpowiedzi, która pozwoli mu rozstrzygnąć zawisły przed nim spór. W tym celu Trybunał może przeformułować przedłużone mu pytania. Wyrok z dnia 25 lipca 2018 r., Dyson, C-632/16, EU:C:2018:599, pkt 47 i przytoczone tam orzecznictwo.

[18] Osoba, która popełnia przestępstwo kradzieży mniejszej wagi, podlega karze pozbawienia wolności w wymiarze od sześciu miesięcy do trzech lat, co oznacza, że zastosowanie znajduje art. 132 ust. 3 dekretu ustawodawczego nr 196/2003.

[19] Co się tyczy wzmianek dotyczących tego, że na art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 można się powoływać w postępowaniach przygotowawczych w sprawach przestępstw, które nie są poważnymi przestępstwami, zob. pkt 35–39 niniejszej opinii.

[20] Wniosek o wydanie orzeczenia w trybie prejudycjalnym opiera się więc na założeniu, że zatrzymywanie danych objętych wnioskiem jest zgodne z prawem. Zatrzymywanie danych objętych zakresem stosowania dyrektywy 2002/58 oraz dostęp do nich stanowią odrębne ingerencje w prawa podstawowe zagwarantowane w art. 7, 8 i 11 karty i wymagają odrębnego uzasadnienia na podstawie jej art. 52 ust. 1. Zobacz podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 47. W pkt 29–33 wyroku Prokuratuur omówiono przepisy regulujące zatrzymywanie takich danych.

[21] Artykuł 2 lit. d) dyrektywy 2002/58 stanowi, że „komunikat" „oznacza każdą informację wymienianą lub przekazaną między określoną liczbą stron za pośrednictwem usług publicznie dostępnej łączności elektronicznej […]".

[22] Artykuł 2 lit. c) dyrektywy 2002/58 stanowi, że „dane dotyczące lokalizacji" „oznaczają wszelkie dane […] wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług łączności elektronicznej".

obejmują treści komunikatów, to umożliwiają wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane są udostępniane, zaś dostęp do nich jawi się jako „poważna" ingerencja w ich prawa podstawowe [23]. Ingerencja, z jaką wiąże się dostęp do takich danych, może być uzasadniona celem [24], o którym mowa w art. 15 ust. 1 dyrektywy 2002/58, polegającym na zapobieganiu „poważnym przestępstwom", ich dochodzeniu, wykrywaniu i karaniu, ale już nie na zapobieganiu ogółowi przestępstw oraz dochodzeniu, wykrywaniu i karaniu ogółu przestępstw. Przy dokonywaniu wykładni art. 15 ust. 1 dyrektywy 2002/58 Trybunał wiąże wagę ingerencji w prawa podstawowe danej osoby z wagą przestępstwa będącego przedmiotem dochodzenia [25].

2. Przysługująca państwom członkowskim kompetencja do określania „poważnych przestępstw"

21. Dyrektywa 2002/58 odnosi się do działalności dostawców usług łączności elektronicznej w zakresie przetwarzania danych osobowych [26]. Artykuł 1 ust. 3 dyrektywy 2002/58 w sposób wyraźny wyłącza z zakresu jej stosowania działalność państwa w określonych dziedzinach, takich jak bezpieczeństwo publiczne, obronność, bezpieczeństwo państwa i prawo karne. Rodzaje działalności, o których mowa w art. 15 ust. 1 dyrektywy 2002/58, pokrywają się zasadniczo z rodzajami działalności wymienionymi w jej art. 1 ust. 3; zalicza się do nich działalność państwa w dziedzinie prawa karnego, która jest wyraźnie wyłączona z zakresu stosowania dyrektywy 2002/58 [27]. Istnieje zatem oczywisty związek między działalnością państwa, która jest wyłączona z zakresu stosowania dyrektywy 2002/58 na mocy jej art. 1 ust. 3, a środkami ustawodawczymi, jakie państwa członkowskie mogą uchwalić na podstawie jej art. 15 ust. 1 [28].

22. Pomimo istnienia tego oczywistego związku Trybunał konsekwentnie wskazuje, że skoro art. 15 ust. 1 dyrektywy 2002/58 wyraźnie upoważnia państwa członkowskie do uchwalenia opisanych w nim środków ustawodawczych, owe środki wchodzą w zakres stosowania tej dyrektywy. Z tego orzecznictwa wynika, że pojęcie „działalności", w tym „działalności państwa w dziedzinie prawa karnego" wspomnianej w art. 1 ust. 3 dyrektywy 2002/58, nie obejmuje środków ustawodawczych, o których mowa w jej art. 15 ust. 1 [29].

[23] Wyrok Prokuratuur, pkt 34, 35. Zobacz analogicznie wyrok z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 59–62. Do sądu krajowego należy ocena, czy dostęp do danych, o których mowa, stanowi „poważną" ingerencję w prawa podstawowe osób, których dane te dotyczą. Niniejsza opinia opiera się na założeniu, że ingerencja, z jaką wiąże się dostęp do danych opisanych w pkt 10 niniejszej opinii, jest poważna.

[24] Wykaz celów zawartych w art. 15 ust. 1 dyrektywy 2002/58 ma charakter wyczerpujący. Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 90.

[25] Zobacz podobnie opinia rzecznika generalnego H. Saugmandsgaarda Øe w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300, pkt 79–82 i przytoczone tam orzecznictwo). Jeśli chodzi o cel polegający na zwalczaniu przestępczości, dostęp może co do zasady zostać przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też popełnienie poważnego przestępstwa bądź też zaangażowanych w taki czy inny sposób w takie przestępstwo. Wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 105.

[26] Zobacz podobnie art. 3 dyrektywy 2002/58, który stanowi, że ma ona zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej. Zobacz także wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 70, 74; zob. także analogicznie opinia rzecznika generalnego M. Szpunara w sprawie La Quadrature du Net i in. (Dane osobowe i walka z naruszeniami praw własności intelektualnej) (C-470/21, EU:C:2022:838, pkt 38).

[27] 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, pkt 97.

[28] W celu zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania przestępstwom kryminalnym, ich dochodzenia, wykrywania i karania, jak również zapobiegania przypadkom niedozwolonego używania systemów łączności elektronicznej, ich dochodzenia, wykrywania i karania.

[29] 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, pkt 98. Wyrok z dnia 6 października 2020 r., Privacy International, C-623/17, EU:C:2020:790, pkt 38 i przytoczone tam orzecznictwo.

23. Ani w art. 2 dyrektywy 2002/58, który zawiera szereg definicji do celów stosowania owego aktu prawnego, ani też w żadnym innym przepisie dyrektywy 2002/58, w tym w jej art. 15 ust. 1, nie zdefiniowano pojęcia „przestępstw kryminalnych". W dyrektywie 2002/58 nie zamieszczono wykazu „przestępstw kryminalnych"[30]. Definicji tego pojęcia próżno także szukać w orzecznictwie dotyczącym wykładni art. 15 ust. 1 dyrektywy 2002/58[31].

24. Mimo braku takich definicji dyrektywa 2002/58 nie przewiduje, że każde państwo członkowskie określa „przestępstwa kryminalne" zgodnie ze swoim prawem krajowym[32]. W myśl utrwalonego orzecznictwa Trybunału zarówno względy jednolitego stosowania prawa Unii, jak i zasada równości wymagają, aby przepisowi prawa Unii, który nie odsyła wyraźnie do prawa państw członkowskich dla określenia swojego znaczenia i zakresu, nadawać zwykle w całej Unii autonomiczną i jednolitą wykładnię. W kontekście wykładni art. 15 ust. 1 dyrektywy 2002/58 termin „przestępstwa kryminalne" można, przynajmniej co do zasady, uznać za autonomiczne pojęcie prawa Unii, które podlega jednolitej wykładni na terytorium wszystkich państw członkowskich[33].

25. Dziesięć państw członkowskich, które przedstawiły Trybunałowi swoje uwagi, oraz Komisja jednomyślnie twierdzą jednak, że to do każdego państwa członkowskiego należy określenie „przestępstw kryminalnych", w tym poważnych przestępstw, o których w art. 15 ust. 1 dyrektywy 2002/58 wspomniano przez odniesienie do prawa krajowego.

26. Zgadzam się z tymi uwagami z przedstawionych poniżej powodów.

27. Po pierwsze, Trybunał wyjaśnił już, że w kontekście art. 15 ust. 1 dyrektywy 2002/58 to do państw członkowskich należy określenie ich podstawowych interesów bezpieczeństwa i podjęcie odpowiednich środków zmierzających do zapewnienia ich bezpieczeństwa wewnętrznego i zewnętrznego[34]. Wydaje się więc, że Trybunał, choć nie stwierdził tego wyraźnie, uznał, iż pojęcie „bezpieczeństwa narodowego" zawarte w art. 15 ust. 1 dyrektywy 2002/58 nie stanowi autonomicznego pojęcia prawa Unii mimo braku jego definicji lub jakiegokolwiek wyraźnego

[30] Zobacz natomiast: art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. 2002, L 190, s. 1 – wyd. spec. w jęz. polskim, rozdz. 19, t. 6, s. 34), zmienionej decyzją ramową Rady 2009/299/WSiSW z dnia 26 lutego 2009 r. (Dz.U. 2009, L 81, s. 24), w którym to przepisie wymieniono przestępstwa stanowiące podstawę do przekazania na mocy europejskiego nakazu aresztowania; załącznik II do dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.U. 2016, L 119, s. 132), w którym wymieniono „poważne przestępstwa", o których mowa w art. 3 pkt 9 tej dyrektywy.

[31] Dyrektywa 2002/58 nie posługuje się takimi terminami jak „ogół przestępstw", „poważne przestępstwa" czy też „przestępstwo (przestępstwa)". Można je odnaleźć w orzecznictwie Trybunału, który nie przedstawia ich definicji ani nie podaje żadnych kryteriów, które mogliby zastosować ustawodawcy krajowi w celu ich zdefiniowania. Zobacz na przykład wyroki: z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 115, 125; z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 54, 56, 63. Zobacz także w tym względzie pkt 45 wyroku Prokuratuur.

[32] Zobacz natomiast art. 1 ust. 1 dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 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 zmieniającej dyrektywę 2002/58 (Dz.U. 2006, L 105, s. 54), który stanowił, że „[c]elem niniejszej dyrektywy jest zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, *określonych w ustawodawstwie każdego państwa członkowskiego*" (wyróżnienie moje). Wyrokiem z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238), Trybunał stwierdził nieważność dyrektywy 2006/24.

[33] Zobacz także analogicznie wyrok z dnia 7 września 2022 r., Staatssecretaris van Justitie en Veiligheid (Charakter prawa pobytu na podstawie art. 20 TFUE), C-624/20, EU:C:2022:639, pkt 19, 20.

[34] 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, pkt 99, 136.

odesłania do prawa państw członkowskich [35]. Nie dostrzegam powodu, dla którego to samo podejście nie miałoby być stosowane w odniesieniu do przysługującej państwom członkowskim kompetencji do określania „przestępstw kryminalnych" lub „poważnych przestępstw" na potrzeby stosowania art. 15 ust. 1 dyrektywy 2002/58. Zawarte w tym przepisie pojęcia „przestępstw kryminalnych", „bezpieczeństwa publicznego" i „bezpieczeństwa narodowego" można uznać za noscitur a sociis („znane ze względu na kontekst, w jakim się pojawiają"), ponieważ wydaje się, że prawodawcy Unii przyświecał zamiar, aby każde z nich było traktowane podobnie, w tym jeśli chodzi o sposób ich definiowania [36].

28. Po drugie, art. 4 ust. 2 TUE zobowiązuje Unię do poszanowania tożsamości narodowej państw członkowskich, która jest nierozerwalnie związana z ich podstawowymi strukturami politycznymi i konstytucyjnymi. W preambule karty również uznano, że choć Unia przyczynia się do ochrony i rozwoju wspólnych wartości, to szanuje przy tym między innymi różnorodność kultur i tradycji narodów Europy. Określanie przestępstw i kar [37] odzwierciedla narodowe uwarunkowania i tradycje, które nie tylko znacząco różnią się od siebie w poszczególnych państwach członkowskich, lecz także ulegają istotnej ewolucji w czasie, w następstwie zmian społecznych [38].

29. W tym kontekście można zauważyć, że przy określaniu przestępstw i kar państwa członkowskie w różnym stopniu uwzględniają różnorodne czynniki. Dokonana przez państwa członkowskie ocena „wagi" danego przestępstwa często, o ile nie zawsze, przekłada się na stopień dotkliwości nakładanej kary. Długość kary polegającej na pozbawieniu wolności może wynikać z analizy szeregu czynników, w tym percypowanej samoistnej „wagi" danego przestępstwa oraz jego względnej „wagi" w porównaniu z innymi przestępstwami. Nie wskazano żadnych powodów, dla których państwa członkowskie miałyby nie wykonywać tej kompetencji lub też dla których przy określaniu „przestępstw kryminalnych", „poważnych przestępstw" lub „ogółu przestępstw" należałoby w rozpatrywanym kontekście zastosować inne podejście.

30. Kompetencja państw członkowskich w dziedzinie prawa karnego nie narusza kompetencji, która w niektórych przypadkach przysługuje Unii, na przykład w zakresie ustanawiania norm minimalnych odnoszących się do określania przestępstw lub kar w dziedzinach szczególnie poważnej przestępczości o wymiarze transgranicznym, wynikających z rodzaju lub skutków tych

[35] Ponadto art. 4 ust. 2 TUE stanowi, że bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego. Okoliczność, że środek krajowy został przyjęty w celu ochrony bezpieczeństwa narodowego, nie prowadzi do niemożności stosowania prawa Unii i nie zwalnia państw członkowskich z konieczności przestrzegania tego prawa. 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, pkt 99, 135.

[36] Znaczenie celu ochrony bezpieczeństwa narodowego przeważa wprawdzie nad znaczeniem celu polegającego na zwalczaniu poważnej przestępczości, co oznacza, że może on stanowić uzasadnienie dla poważniejszych ingerencji w prawa podstawowe, ale nie wpływa na przysługujące państwom członkowskim prawo do określenia „przestępstw kryminalnych" lub „poważnych przestępstw kryminalnych". 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, pkt 136.

[37] A także okoliczności łagodzących i obciążających.

[38] Rzecznik generalny H. Saugmandsgaard Øe uznał, że ustawodawstwo karne i normy postępowania karnego należą do kompetencji państw członkowskich, nawet jeśli na ich porządek prawny mogą jednak mieć wpływ przepisy prawa Unii przyjęte w tej dziedzinie między innymi na podstawie art. 83 ust. 2 TFUE. W związku z tym nie istnieje przepis o charakterze generalnym, który dawałby zharmonizowaną definicję pojęcia „poważnego przestępstwa". Opinia w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300, pkt 95). Rzecznik generalny G. Pitruzzella wskazał, że określenie „poważnego przestępstwa" trzeba pozostawić uznaniu państw członkowskich. W różnych krajowych systemach prawnych to samo przestępstwo może bowiem podlegać karze mniej lub bardziej surowej. Również określenie okoliczności obciążających może różnić się w poszczególnych państwach członkowskich. Opinia w sprawie Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2020:18, pkt 91, 92). Z kolei rzecznik generalny M. Szpunar uznał, że „[p]ojęcie »poważnej przestępczości« należy […] interpretować w sposób autonomiczny. Nie może ono zależeć od koncepcji każdego państwa członkowskiego, gdyż w przeciwnym razie umożliwiłoby to obejście wymogów określonych w art. 15 ust. 1 dyrektywy 2002/58 w zależności od tego, czy państwa członkowskie przyjmują mniej lub bardziej szeroką koncepcję walki z poważną przestępczością". Opinia w sprawie La Quadrature du Net i in. (Dane osobowe i walka z naruszeniami praw własności intelektualnej) (C-470/21, EU:C:2022:838, pkt 74).

przestępstw lub ze szczególnej potrzeby wspólnego ich zwalczania [39]. Niemniej jednak prawodawca Unii nie ustanowił norm dotyczących określania przestępstw kryminalnych, o których mowa w art. 15 ust. 1 dyrektywy 2002/58 [40]. Jak już bowiem wskazano [41], z treści art. 1 ust. 3 dyrektywy 2002/58 wynika, że przy przyjmowaniu tej dyrektywy prawodawcy Unii nie przyświecał zamiar wykonania jakichkolwiek kompetencji w dziedzinie prawa karnego.

31. Te dwa powody w sposób wystarczający wyjaśniają, dlaczego – mimo że krajowe środki ustawodawcze uchwalone na podstawie art. 15 ust. 1 dyrektywy 2002/58 w celu dochodzenia i karania przestępstw kryminalnych są objęte zakresem stosowania tego aktu – państwa członkowskie zachowują kompetencję do określania „przestępstw kryminalnych", w tym „poważanych przestępstw", oraz do ustanawiania kar grożących osobom dopuszczającym się takich czynów [42].

3. Standard kontroli przeprowadzanej w przypadku skorzystania z przewidzianej w art. 15 ust. 1 dyrektywy 2002/58 możliwości odstąpienia od zasady poufności

32. Trybunał podkreślił, że możliwość odstąpienia [43] między innymi od zasady poufności zagwarantowanej w art. 5 ust. 1 dyrektywy 2002/58 podlega wykładni zawężającej, tak aby nie stało się to regułą i tym samym pozbawiało ową zasadę znaczenia [44]. W związku z tym korzystanie z tej możliwości powinno się odbywać w poszanowaniu w szczególności zasady równoważności [45] i skuteczności [46]. W takim przypadku należy również zapewnić zgodność z ogólnymi zasadami prawa Unii, w tym z zasadą proporcjonalności [47], oraz z art. 7, 8, 11 [48] i art. 52 ust. 1 karty [49]. Cel polegający na zwalczaniu poważnej przestępczości należy zawsze pogodzić z korzystaniem z praw podstawowych, na które wywiera ono wpływ. Prawa ustanowione w art. 7, 8 i 11 karty nie

[39] Artykuł 83 ust. 1 akapit pierwszy TFUE. Zobacz także wyrok z dnia 21 października 2021 r., Okrazhna prokuratura – Varna, C-845/19 i C-863/19, EU:C:2021:864, pkt 32.

[40] Zobacz analogicznie wyrok Prokuratuur, pkt 41, 42. Trybunał orzekł, że w braku uregulowań Unii w tej dziedzinie oraz zgodnie z zasadą autonomii proceduralnej „wyłącznie do prawa krajowego należy co do zasady określenie przepisów dotyczących dopuszczalności i oceny, w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstw, informacji i dowodów uzyskanych w wyniku takiego uogólnionego i niezróżnicowanego zatrzymywania danych sprzecznego z prawem Unii". Podstawą prawną dyrektywy 2002/58 jest art. 114 TFUE (dawny art. 95 WE), a nie na przykład art. 83 ust. 1 akapit pierwszy TFUE. Z kolei podstawami prawnymi dyrektywy 2016/681 są art. 82 ust. 1 akapit drugi lit. d) TFUE (współpraca wymiarów sprawiedliwości w sprawach karnych) i art. 87 ust. 2 lit. a) TFUE (współpraca policyjna).

[41] Zobacz pkt 21 niniejszej opinii.

[42] Zobacz analogicznie wyrok z dnia 23 października 2007 r., Komisja/Rada, C-440/05, EU:C:2007:625, pkt 66, 70, 71 i przytoczone tam orzecznictwo. Zobacz także wyrok z dnia 28 kwietnia 2011 r., El Dridi, C-61/11 PPU, EU:C:2011:268, pkt 53.

[43] Artykuł 15 ust. 1 dyrektywy 2002/58 stanowi, że państwa członkowskie „mogą uchwalić" środki ustawodawcze, które ograniczają niektóre prawa i obowiązki przewidziane tą dyrektywą.

[44] Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 89. Rzecznik generalny H. Saugmandsgaard Øe uznał, że „mimo iż każde państwo członkowskie ma prawo ocenić, jaki próg kary będzie adekwatny dla scharakteryzowania poważnego przestępstwa, ma ono jednak obowiązek nieustanawiania tego progu na poziomie tak niskim w porównaniu ze zwykłym poziomem kar stosowanych w tym państwie, że wyjątki od zakazu przechowywania i wykorzystywania danych osobowych przewidziane w art. 15 ust. 1 będą co do zasady bezużyteczne […]". Opinia w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300, pkt 114).

[45] Nic nie wskazuje na to, że rozpatrywane uregulowanie włoskie nie jest zgodne z tą zasadą.

[46] Wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 127.

[47] Zobacz także motyw 11 dyrektywy 2002/58.

[48] Zobacz także motyw 2 dyrektywy 2002/58.

[49] Wyroki: z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 89; 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, pkt 111–113. Zobacz także opinia rzecznika generalnego H. Saugmandsgaarda Øe w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300, pkt 116–120). W wyroku z dnia 8 marca 2022 r., Bezirkshauptmannschaft Hartberg-Fürstenfeld (Bezpośrednia skuteczność) (C-205/20, EU:C:2022:168, pkt 31), Trybunał przypomniał, że zasada proporcjonalności wiąże państwa członkowskie przy wprowadzaniu w życie prawa Unii. W tym kontekście państwa członkowskie muszą przestrzegać art. 49 ust. 3 karty, jeżeli ustanawiają sankcje karne, nawet w braku przepisów Unii harmonizujących te sankcje.

stanowią prerogatyw o charakterze absolutnym, zaś ich wykonywanie powinno być rozważane z uwzględnieniem ich funkcji społecznej [50]. W związku z tym art. 52 ust. 1 karty stanowi, że ograniczenia w korzystaniu z tych praw, które są przewidziane ustawą, muszą szanować istotę tych praw oraz, zgodnie z zasadą proporcjonalności, muszą być konieczne i muszą rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób. Oznacza to, że krajowe środki ustawodawcze uchwalone na podstawie art. 15 ust. 1 dyrektywy 2002/58 muszą rzeczywiście odpowiadać wyłącznie jednemu z celów wyliczonych w tym przepisie. Powinny one się opierać na obiektywnych kryteriach, być prawnie wiążące oraz ustanawiać jasne i dokładne reguły określające materialne i proceduralne warunki regulujące dostęp do danych udzielany właściwym organom krajowym przez dostawców usług łączności elektronicznej [51].

33. Aby zapewnić pełne poszanowanie tych warunków w praktyce, dostęp właściwych organów krajowych do zatrzymywanych danych powinien, co do zasady [52], być uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego [53] i następować po złożeniu przez owe organy uzasadnionego wniosku oraz powiadomieniu zainteresowanych osób [54]. Zgodnie z utrwalonym orzecznictwem przy przeprowadzaniu uprzedniej kontroli sąd lub niezależny organ administracyjny powinien pogodzić poszczególne wchodzące w grę interesy i prawa w celu zagwarantowania właściwej równowagi pomiędzy wymogami dochodzenia a potrzebą zapewnienia prawa podstawowego do poszanowania życia prywatnego i ochrony danych osobowych zainteresowanych osób [55].

34. W niniejszej sprawie w art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 określono warunki, których spełnienie obliguje sąd krajowy do zobowiązania dostawców usług łączności elektronicznej do udzielenia prokuraturze, na złożony przez nią wniosek, dostępu do danych. Nie ulega wątpliwości [56], że art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 określa w sposób jasny i dokładny okoliczności i warunki, w jakich sąd krajowy może zobowiązać dostawców usług łączności elektronicznej do udzielenia takiego dostępu. Sąd odsyłający uważa jednak, że kryterium kary „pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata", jest nazbyt szerokie, ponieważ skutkuje uwzględnieniem przestępstw takich jak kradzież mniejszej wagi, których szkodliwość społeczna jest nieznaczna.

35. O ile art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 potencjalnie dotyczy szerokiego wachlarza przestępstw, o tyle w ramach niniejszego postępowania Trybunałowi nie przedstawiono żadnych dowodów świadczących o tym, że obejmuje on tak dużą liczbę przestępstw, iż skutkuje przekształceniem udzielanego na jego podstawie dostępu do danych

[50] Artykuł 52 ust. 1 karty. 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, pkt 120.

[51] Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 117–119. Zobacz także 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, pkt 110, 129–133.

[52] Na przykład w art. 132 ust. 3 bis dekretu ustawodawczego nr 196/2003 ustanowiono szczególne zasady dostępu do danych w pilnych przypadkach. W opinii w sprawie La Quadrature du Net i in. (Dane osobowe i walka z naruszeniami praw własności intelektualnej) (C-470/21, EU:C:2022:838, pkt 99–105) rzecznik generalny M. Szpunar uznał, że uprzednia kontrola jest wymagana jedynie wówczas, gdy ma miejsce poważna ingerencja w życie prywatne użytkowników usług łączności elektronicznej. Przeprowadzenie uprzedniej kontroli jest konieczne, ponieważ w kontekście niniejszego postępowania do poważnej ingerencji dochodzi ze względu na charakter danych, o dostęp do których wnosi prokuratura.

[53] Wymóg przeprowadzenia uprzedniej kontroli wyłania się nie z dyrektywy 2002/58, lecz z orzecznictwa Trybunału: wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 120, 121 i przytoczone tam orzecznictwo.

[54] Wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in., C-203/15 i C-698/15, EU:C:2016:970, pkt 120, 121.

[55] Wyrok Prokuratuur, pkt 52.

[56] Z zastrzeżeniem wyniku weryfikacji dokonanej przez sąd odsyłający.

z wyjątku w regułę [57]. Ustanowiony w tym przepisie próg kary pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata, nie wydaje się nadmiernie niski [58]. Analogicznie w art. 3 pkt 9 dyrektywy 2016/681 [59] „poważną przestępczość" zdefiniowano jako „przestępstwa wymienione w załączniku II, które na mocy prawa krajowego państwa członkowskiego podlegają karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat" [60]. Trybunał orzekł jednak, że ponieważ art. 3 pkt 9 dyrektywy 2016/681 odnosi się nie do minimalnego, lecz do maksymalnego wymiaru kary, nie jest wykluczone, iż odpowiednie „dane […] mogą być przetwarzane w celu zwalczania przestępstw, które, mimo że spełniają kryteria określone we wskazanym przepisie co do swojej wagi, stanowią – ze względu na specyfikę krajowego systemu karnego – nie przestępstwa poważne, a zwyczajne" [61].

36. Trzyletni wymiar kary, o którym mowa w art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 odnosi się do maksymalnego wymiaru kary, co oznacza, że ów przepis może znaleźć zastosowanie do przestępstw takich jak kradzież mniejszej wagi [62]. Należy zatem zbadać, w jaki sposób art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 jest stosowany w praktyce. Z zastrzeżeniem weryfikacji, która powinna zostać przeprowadzona przez sąd odsyłający, wydaje się, że w art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 ustanowiono, w zależności od charakteru przestępstw będących przedmiotem postępowania przygotowawczego, dwa różne standardy uprzedniej kontroli przeprowadzanej przez sąd odsyłający.

37. W ramach pierwszego z tych standardów kontroli wymaga się [63], aby sądy krajowe udzieliły prokuraturze dostępu do danych zatrzymywanych przez dostawców usług łączności elektronicznej, o ile takie dane są istotne w celu ustalenia okoliczności faktycznych oraz jeśli istnieją wystarczające przesłanki popełnienia przestępstw groźby karalnej i nękania lub niepokojenia osób za pomocą telefonu, w przypadku gdy groźba karalna, nękanie i niepokojenie są poważne. Oznacza to, że sąd krajowy powinien przeprowadzić indywidualną ocenę wagi danego przestępstwa i zweryfikować, czy prowadzenie dochodzenia w sprawie tego przestępstwa oraz jego karanie uzasadniają ograniczenie praw o charakterze ogólnym, zagwarantowanych w art. 7, 8 i 11 karty, oraz praw o charakterze szczególnym, ustanowionych w art. 5, 6 i 9 dyrektywy 2002/58. Standard ten wymaga przeprowadzenia w danej sprawie indywidualnej oceny, czy ingerencja w te prawa jest proporcjonalna do celu interesu publicznego, jakim jest zwalczanie przestępczości.

[57] Zobacz analiza zawarta w opinii rzecznika generalnego H. Saugmandsgaarda Øe w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300, pkt 116–120). Ocena tej kwestii należy w ostatecznym rozrachunku do sądu odsyłającego.

[58] Sama okoliczność, że w jednym państwie członkowskim przestępstwa i system kar określono odmiennie niż w innym państwie członkowskim, nie może mieć wpływu na proporcjonalność danego uregulowania. Zobacz analogicznie wyrok z dnia 8 lipca 2010 r., Sjöberg i Gerdin, C-447/08 i C-448/08, EU:C:2010:415, pkt 38.

[59] Dyrektywa 2016/681 dotyczy przekazywania i przetwarzania danych pasażerów w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

[60] Trybunał orzekł, że wymogi wynikające z tego przepisu, odnoszące się do charakteru i surowości stosowanej kary, mają na celu, co do zasady, ograniczyć zastosowanie systemu utworzonego na mocy dyrektywy 2016/681 do przestępstw wystarczająco poważnych, by uzasadnić ingerencję w prawa podstawowe zagwarantowane w art. 7 i 8 karty. Wyrok z dnia 21 czerwca 2022 r., Ligue des droits humains, C-817/19, EU:C:2022:491, pkt 150.

[61] Trybunał orzekł zatem, że państwa członkowskie powinny zapewnić, aby system utworzony na podstawie dyrektywy 2016/681 był stosowany jedynie do zwalczania poważnej przestępczości i nie obejmował zwyczajnych przestępstw. Wyrok z dnia 21 czerwca 2022 r., Ligue des droits humains, C-817/19, EU:C:2022:491, pkt 151, 152. Przedmiot i zakres stosowania dyrektywy 2016/681, która przewiduje między innymi wymianę danych PNR między państwami członkowskimi, nie pokrywają się z przedmiotem i zakresem stosowania dyrektywy 2002/58. Z powyższego wynika, że przepisy tych dyrektyw należy oceniać odrębnie i indywidualnie. W tym względzie oraz inaczej niż ma to miejsce w przypadku art. 15 ust. 1 dyrektywy 2002/58 pojęcie „poważnej przestępczości" zawarte w dyrektywie 2016/681 jest autonomicznym pojęciem prawa Unii. Zobacz: motyw 12, art. 3 pkt 9 dyrektywy 2016/681; załącznik II do tej dyrektywy.

[62] Zobacz analogicznie wyrok z dnia 21 czerwca 2022 r., Ligue des droits humains, C-817/19, EU:C:2022:491, pkt 151.

[63] W oryginalnej wersji językowej użyto sformułowania „i dati sono acquisiti".

38. Z kolei w ramach drugiego standardu kontroli, który jest istotny w kontekście niniejszego postępowania, wymaga się[64], aby sądy krajowe udzieliły prokuraturze dostępu do danych zatrzymywanych przez dostawców usług łączności elektronicznej, o ile takie dane są istotne w celu ustalenia okoliczności faktycznych oraz jeśli istnieją wystarczające przesłanki popełnienia przestępstwa zagrożonego między innymi karą pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata. W tym przypadku rola sądu krajowego sprowadza się do sprawdzenia, czy te obiektywne warunki zostały spełnione; nie ma on natomiast żadnej możliwości przeprowadzenia indywidualnej oceny wchodzących w grę interesów[65]. Kontrola na podstawie art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 jest zatem przeprowadzana przez sąd krajowy w oderwaniu od jakiegokolwiek rzeczywistego związku z konkretnymi okolicznościami zawisłej przed nim sprawy.

39. Choć sądy krajowe mogą nie być właściwe do kontroli określania przestępstw przez ustawodawcę lub do kontroli dokonywanych przez niego wyborów dotyczących przypisywania im konkretnej wagi[66], musi im jednak przysługiwać właściwość do przeprowadzenia indywidualnej oceny lub też oceny, czy udzielenie, na podstawie środków ustawodawczych uchwalonych zgodnie z art. 15 ust. 1 dyrektywy 2002/58, dostępu do danych wrażliwych, umożliwiających wyciągnięcie precyzyjnych wniosków na temat życia prywatnego użytkownika, który stanowi tym samym poważną ingerencję w prawa podstawowe zagwarantowane w art. 7, 8 i 11 oraz w art. 52 ust. 1 karty, jest proporcjonalne.

40. Z powyższego wynika, iż na podstawie środków uchwalonych zgodnie z art. 15 ust. 1 dyrektywy 2002/58 nie można udzielić dostępu do danych wrażliwych, chyba że (i) dane przestępstwo osiąga próg wagi ustalony zawczasu przez ustawodawcę krajowego oraz (ii) sąd lub inny niezależny organ administracyjny uzna, po przeprowadzeniu indywidualnej oceny lub kontroli czy też oceny lub kontroli, iż ingerencja w prawa podstawowe, z jaką wiąże się ten dostęp, jest proporcjonalna, w świetle celu interesu publicznego polegającego na zwalczaniu przestępczości w konkretnej sprawie. W niektórych przypadkach dostępu do takich danych nie można jednak udzielić nawet wówczas, gdy przestępstwo osiąga próg wagi określony prawem krajowym.

41. W niniejszej sprawie przestępstwo kradzieży kwalifikowanej uznaje się za „poważne” w świetle prawa krajowego, ponieważ jest ono zagrożone w szczególności karą pozbawienia wolności od dwóch do sześciu lat, co oznacza, iż próg wagi ustalony w art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 jest osiągnięty[67]. Wydaje się, że przy stosowaniu środków uchwalonych na podstawie art. 15 ust. 1 dyrektywy 2002/58 sądy włoskie nie mogą zakwestionować dokonanej w prawie krajowym klasyfikacji kradzieży kwalifikowanej jako „poważnego przestępstwa”. Jeżeli nie osiągnięto progu ustanowionego w prawie krajowym, sąd odsyłający nie może udzielić dostępu do danych objętych wnioskiem[68].

[64] Użycie trybu oznajmującego w art. 132 ust. 3 dekretu ustawodawczego nr 196/2003 („i dati sono acquisiti”) oznacza, co musi zostać zweryfikowane przez sąd odsyłający, że sąd krajowy udziela dostępu do przedmiotowych danych, o ile spełnione są przewidziane w tym przepisie obiektywne warunki.

[65] Na rozprawie prokuratura (Bolzano) i rząd włoski przedstawiły odmienne stanowiska co do roli sądu krajowego i zakresu uprzedniej kontroli na podstawie art. 132 ust. 3 dekretu ustawodawczego nr 196/2003. O ile prokuratura (Bolzano) podniosła, że przed udzieleniem dostępu do takich danych sąd krajowy powinien przeprowadzić indywidualne badanie proporcjonalności tego dostępu, o tyle rząd włoski podkreślił, iż sąd krajowy jest związany, zgodnie z art. 101 Costituzione della Repubblica Italiana (konstytucji Republiki Włoskiej) i art. 1 kodeksu karnego, zasadą legalności, w związku z czym nie może on dokonywać, jak ujął to rząd włoski, twórczej wykładni prawa. Dokonanie wykładni mających zastosowanie przepisów prawa krajowego należy do sądu odsyłającego.

[66] Chyba że zezwala na to prawo krajowe oraz z zastrzeżeniem poszanowania w szczególności art. 49 karty.

[67] Kara pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata.

[68] Artykuł 52 ust. 1 karty stanowi, że wszelkie ograniczenia w korzystaniu z prawa uznanego w karcie muszą być przewidziane ustawą. Wynika stąd, że sądy krajowe są co do zasady związane ustawodawstwem krajowym przewidującym takie ograniczenia.

42. Jeżeli próg ustanowiony przez ustawodawcę krajowego jest osiągnięty, sąd odsyłający powinien, zgodnie z art. 15 ust. 1 dyrektywy 2002/58, skontrolować, czy – w świetle wszystkich okoliczności rozpatrywanego przypadku – ingerencja w prawa podstawowe, z jaką wiąże się udzielenie dostępu do danych wrażliwych, jest proporcjonalna do celu interesu publicznego polegającego na zwalczaniu przestępczości. W tym względzie sąd odsyłający powinien uwzględnić i wyważyć wszystkie wchodzące w grę prawa i interesy, w tym w szczególności uszczerbek dla przysługującego ofierze przestępstwa prawa własności chronionego na podstawie art. 17 karty, oraz okoliczność, że telefony komórkowe mogą zawierać szczególnie wrażliwe informacje dotyczące życia prywatnego, zawodowego i finansowego ich właścicieli [69]. Dostęp do takich danych może stanowić jedyny skuteczny i pozostający w dyspozycji środek służący prowadzeniu dochodzenia w sprawie analizowanych przestępstw, ich karaniu, jak również zapewnieniu, że ich – póki co nieznani – sprawcy nie pozostaną bezkarni. Pod uwagę należy wziąć także prawa osób trzecich [70].

43. Jeśli chodzi o prawa osób trzecich, z akt sprawy przed sądem odsyłającym zdaje się wynikać [71], że prokuratura (Bolzano) wniosła o udostępnienie danych dotyczących komunikatów wymienianych przy użyciu skradzionych telefonów komórkowych począwszy od dnia 29 października 2021 r. (w odniesieniu do pierwszej kradzieży, popełnionej w dniu 27 października 2021 r.) [72] oraz od dnia 20 listopada 2021 r. (w odniesieniu do drugiej kradzieży popełnionej właśnie w tym dniu) [73]. Jeżeli wziąć pod uwagę te daty, okazuje się, że wnioski o udzielenie dostępu jedynie w bardzo ograniczonym zakresie wpływają na prawa ofiar przestępstw, które zagwarantowano w szczególności w art. 7, 8 i 11 karty [74]. W swoich uwagach na piśmie rząd włoski również stwierdził, że postępowania krajowe dotyczą wyłącznie danych przydatnych do ustalenia tożsamości sprawcy (sprawców) poszczególnych kradzieży. W przypadku zidentyfikowania połączeń z osobami trzecimi, które nie są związane z kradzieżą, odnośne dane zostałyby zniszczone zgodnie z art. 269 kodeksu postępowania karnego [75]. Wreszcie art. 132 ust. 3 quater dekretu ustawodawczego nr 196/2003 stanowi, że dane pozyskane z naruszeniem jego ust. 3 i 3 bis nie mogą być wykorzystane [76].

[69] W telefonach komórkowych mogą się znajdować zdjęcia, dane dotyczące zdrowia, wyciągi bankowe, hasła itp. Kradzież telefonu komórkowego może zatem narazić na szwank tożsamość cyfrową jego właściciela, zaś jej skutki mogą znacząco wykraczać poza samą tylko utratę wartości pieniężnej urządzenia. Sąd odsyłający powinien więc również uwzględnić i wyważyć ewentualny uszczerbek dla praw przysługujących ofierze przestępstwa, w szczególności na podstawie art. 7, 8 i 17 karty.

[70] Takich jak ofiary domniemanego przestępstwa.

[71] Z zastrzeżeniem wyniku weryfikacji dokonanej przez sąd odsyłający.

[72] Numer referencyjny RGNR 9228/2021.

[73] Numer referencyjny RGNR 9794/2021.

[74] Chociaż dane mogą się odnosić do komunikatów przekazywanych ofierze przestępstwa po dacie kradzieży, to jednak w rzeczywistości nie odnoszą się one do komunikatów przekazywanych przez ofiarę przestępstwa ani do danych dotyczących jej lokalizacji.

[75] Według rządu włoskiego mająca zastosowanie wersja art. 269 ust. 2 kodeksu postępowania karnego stanowiła, że „[…] nagrania są przechowywane do chwili wydania wyroku kończącego postępowanie w sprawie. W interesie poufności zainteresowane strony mogą jednak zwrócić się do sędziego, który wydał zgodę na przejęcie lub je zatwierdził, o zniszczenie nagrań, które nie zostały włączone do akt sprawy” (ponieważ są one nieistotne). O ile dostęp do danych dotyczących osób postronnych jest nieograniczony, o tyle wydaje się, z zastrzeżeniem weryfikacji, której dokonanie należy do sądu odsyłającego, że prawo krajowe ogranicza wykorzystywanie tych danych.

[76] W odesłaniu prejudycjalnym nie wyjaśniono ani dokładnego znaczenia tego przepisu, ani kwestii jego stosowania w praktyce.

VI. Wnioski

44. W świetle powyższych rozważań proponuję Trybunałowi, by na pytanie prejudycjalne przedstawione przez Tribunale di Bolzano (trybunał w Bolzano, Włochy) odpowiedział następująco:

Artykuł 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 (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., oraz art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej

należy interpretować w ten sposób, że nie stoją one na przeszkodzie uregulowaniu krajowemu zobowiązującemu sąd do udzielenia prokuraturze dostępu do danych zatrzymywanych zgodnie z prawem przez dostawców usług łączności elektronicznej i umożliwiających wyciągnięcie precyzyjnych wniosków na temat życia prywatnego użytkownika, o ile takie dane są istotne w celu ustalenia okoliczności faktycznych i jeśli istnieją wystarczające przesłanki popełnienia poważnego przestępstwa określonego w prawie krajowym, które jest zagrożone karą pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata. Przed udzieleniem dostępu sąd krajowy powinien przeprowadzić indywidualną ocenę, czy ingerencja w prawa podstawowe, z jaką wiąże się udzielenie takiego dostępu, jest proporcjonalne w świetle, w szczególności, wagi konkretnego przestępstwa i okoliczności faktycznych sprawy.