Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 20 września 2022 r.*

Odesłanie prejudycjalne – Jednolity rynek usług finansowych – Nadużycia na rynku – Wykorzystanie informacji poufnych – Dyrektywa 2003/6/WE – Artykuł 12 ust. 2 lit. a) i d) – Rozporządzenie (UE) nr 596/2014 – Artykuł 23 ust. 2 lit. g) i h) – Uprawnienia nadzorcze i śledcze Autorité des marchés financiers (AMF) – Cel interesu ogólnego polegający na ochronie integralności rynków finansowych Unii Europejskiej i zaufania publicznego do instrumentów finansowych – Możliwość uzyskania przez AMF zapisów danych o ruchu przechowywanych przez operatora usług łączności elektronicznej – Przetwarzanie danych osobowych w sektorze łączności elektronicznej – Dyrektywa 2002/58/WE – Artykuł 15 ust. 1 – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 11 oraz art. 52 ust. 1 – Poufność komunikacji – Ograniczenia – Ustawodawstwo przewidujące uogólnione i niezróżnicowane zatrzymywanie danych o ruchu przez operatorów usług łączności elektronicznej – Możliwość ograniczenia przez sąd krajowy skutków w czasie stwierdzenia nieważności dotyczącego krajowych przepisów ustawowych niezgodnych z prawem Unii – Wyłączenie

W sprawach połączonych C-339/20 i C-397/20

mających za przedmiot wnioski o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożone przez Cour de cassation (trybunał kasacyjny, Francja) postanowieniami z dnia 1 kwietnia 2020 r., które wpłynęły do Trybunału, odpowiednio, w dniach 24 lipca 2020 r. i 20 sierpnia 2020 r., w postępowaniach karnych przeciwko:

VD (C-339/20),

SR (C-397/20),

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis i I. Ziemele, prezesi izb, T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (sprawozdawca), N. Piçarra, L. S. Rossi i A. Kumin, sędziowie,

rzecznik generalny: M. Campos Sánchez-Bordona,

sekretarz: R. Şereş, administratorka,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 14 września 2021 r.,

* Język postępowania: francuski.

rozważywszy uwagi, które przedstawili:

– w imieniu VD – D. Foussard i F. Peltier, avocats,

– w imieniu SR – M. Chavannes i P. Spinosi, avocats,

– w imieniu rządu francuskiego – A. Daniel, E. de Moustier, D. Dubois, J. Illouz i T. Stéhelin, w charakterze pełnomocników,

– w imieniu rządu duńskiego – N. Holst-Christensen, N. Lykkegaard i M. Søndahl Wolff, w charakterze pełnomocników,

– w imieniu rządu estońskiego – A. Kalbus i M. Kriisa, w charakterze pełnomocników,

– w imieniu Irlandii – M. Browne, A. Joyce i J. Quaney, w charakterze pełnomocników, których wspierał D. Fennelly, BL,

– w imieniu rządu hiszpańskiego – L. Aguilera Ruiz, w charakterze pełnomocnika,

– w imieniu rządu polskiego – B. Majczyna, w charakterze pełnomocnika,

– w imieniu rządu portugalskiego – P. Barros da Costa, L. Inez Fernandes, L. Medeiros i I. Oliveira, w charakterze pełnomocników,

– w imieniu Komisji Europejskiej – S. L. Kalėda, H. Kranenborg, T. Scharf i F. Wilman, w charakterze pełnomocników,

– w imieniu Europejskiego Inspektora Ochrony Danych – A. Buchta, M. Guglielmetti, C.-A. Mamier i D. Nardi, w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 18 listopada 2021 r.,

wydaje następujący

Wyrok

1 Wnioski o wydanie orzeczenia w trybie prejudycjalnym dotyczą zasadniczo wykładni art. 12 ust. 2 lit. a) i d) dyrektywy Parlamentu Europejskiego i Rady 2003/6/WE z dnia 28 stycznia 2003 r. w sprawie wykorzystywania poufnych informacji i manipulacji na rynku (nadużyć na rynku) (Dz.U. 2003, L 96, s. 16) oraz art. 23 ust. 2 lit. g) i h) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenia w sprawie nadużyć na rynku) oraz uchylającego dyrektywę 2003/6 i dyrektywy Komisji 2003/124/WE, 2003/125/WE, 2004/72/WE (Dz.U. 2014, L 173, s. 1), w związku z 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 (dyrektywy o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (Dz.U. 2009, L 337, s. 11) (zwanej dalej „dyrektywą 2002/58”), interpretowanych w świetle art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”).

2 Wnioski te zostały przedstawione w ramach postępowań karnych wszczętych przeciwko VD i SR, w których oskarżono ich o wykorzystywanie i ukrywanie informacji poufnych, współsprawstwo, korupcję i pranie pieniędzy.

Ramy prawne

Prawo Unii

Dyrektywa 2002/58

3 Motywy 2, 6, 7 i 11 dyrektywy 2002/58 mają następujące brzmienie:

„(2) Niniejsza dyrektywa dąży do poszanowania fundamentalnych praw i jest zgodna z zasadami uznanymi w szczególności przez [kartę]. W szczególności niniejsza dyrektywa zmierza do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 [karty].

[…]

(6) Internet przekształca tradycyjne struktury rynkowe przez udostępnienie ogólnej, globalnej infrastruktury dostarczającej szerokiego spektrum usług łączności elektronicznej. Usługi łączności elektronicznej ogólnodostępne za pośrednictwem [I]nternetu stwarzają nowe możliwości użytkownikom, ale również powodują powstanie nowych zagrożeń dotyczących ich danych osobowych i prywatności.

(7) W przypadku publicznych sieci łączności należy wprowadzić szczególne przepisy prawne, wykonawcze i techniczne w celu ochrony podstawowych praw i wolności osób fizycznych oraz uzasadnionego interesu osób prawnych, w szczególności w odniesieniu do zwiększonej pojemności automatycznego przechowywania i przetwarzania danych odnoszących się do abonentów i użytkowników.

[…]

(11) Niniejsza dyrektywa, podobnie jak dyrektywa 95/46/WE [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)], nie odnosi się do kwestii ochrony podstawowych praw i wolności związanych z działalnością, która nie jest regulowana prawem wspólnotowym. Dyrektywa nie zmienia zatem istniejącej równowagi między prawem do prywatności osoby fizycznej a [przysługującą państwom członkowskim możliwością] podejmowania środków, określonych w art. 15 ust. 1 niniejszej dyrektywy, niezbędnych do ochrony bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając gospodarczy dobrobyt państwa, gdy działania dotyczą zagadnień bezpieczeństwa państwa) i wykonywania prawa karnego. Wskutek tego niniejsza dyrektywa nie wpływa na możliwości państw członkowskich do zgodnego z prawem przejmowania danych w łączności elektronicznej lub podejmowania innych środków, jeżeli jest to konieczne dla któregokolwiek z tych celów i zgodne z europejską Konwencją o ochronie praw człowieka i podstawowych wolności [podpisaną w Rzymie dnia 4 listopada 1950 r.], dla której wykładnię stanowi orzecznictwo Europejskiego Trybunału Praw Człowieka. Środki tego rodzaju muszą być właściwe,

współmierne do zamierzonego celu i niezbędne w ramach społeczeństwa demokratycznego oraz powinny podlegać stosownym zabezpieczeniom zgodnie z europejską Konwencją o ochronie praw człowieka i podstawowych wolności”.

4 Artykuł 1 dyrektywy 2002/58, zatytułowany „Zakres i cel”, stanowi:

„1. Niniejsza dyrektywa harmonizuje przepisy państw członkowskich wymagane dla zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej.

2. Przepisy niniejszej dyrektywy dookreślają i uzupełniają dyrektywę [95/46] zgodnie z celami przedstawionymi w ust. 1. Ponadto zapewniają ochronę uzasadnionych interesów abonentów będących osobami prawnymi.

3. Niniejsza dyrektywa nie ma zastosowania do działalności, która wykracza poza zakres [traktatu FUE], takiej jak działalność określona w tytułach V i VI [traktatu UE], ani w żadnym wypadku do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (włączając dobrobyt gospodarczy państwa, gdy działalność odnosi się do spraw bezpieczeństwa państwa) i działalności państwa w dziedzinie prawa karnego”.

5 Artykuł 2 tej dyrektywy, zatytułowany „Definicje”, stanowi w akapicie drugim lit. b):

„Stosuje się […] następujące definicje:

[…]

b) »dane o ruchu« oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi”.

6 Zgodnie z art. 5 wspomnianej dyrektywy, zatytułowanym „Poufność komunikacji”:

„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. Niniejszy ustęp nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu, bez uszczerbku dla zasady poufności.

2. Ustęp 1 nie dotyczy jakichkolwiek przypadków prawnie dozwolonego rejestrowania komunikatów i związanych z nimi danych o ruchu stosowanego w zgodnej z prawem praktyce handlowej do celów zapewnienia dowodów transakcji handlowej lub do celów łączności w działalności handlowej.

3. Państwa członkowskie zapewniają, aby przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika było dozwolone wyłącznie pod warunkiem, że dany abonent lub użytkownik wyraził zgodę zgodnie

z dyrektywą [95/46] po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. Nie stanowi to przeszkody dla każdego technicznego przechowywania danych ani dostępu do nich jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej, lub gdy jest to ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika".

7 Artykuł 6 dyrektywy 2002/58, zatytułowany „Dane o ruchu", stanowi:

„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.

2. Można przetwarzać dane o ruchu niezbędne do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich. Przetwarzanie takie jest dozwolone tylko do końca okresu, w którym rachunek może być zgodnie z prawem zakwestionowany lub w którym należy uiścić opłatę [lub w którym można dochodzić jego zapłaty].

3. Do celów wprowadzania na rynek usług łączności elektronicznej lub świadczenia usług tworzących wartość [dodaną], dostawca publicznie dostępnych usług łączności elektronicznej może przetwarzać dane określone w ust. 1, w zakresie i przez czas niezbędny dla tego rodzaju usług lub wprowadzania ich na rynek, jeżeli abonent lub użytkownik, których dane dotyczą, uprzednio wyraził na to zgodę. Użytkownicy lub abonenci mają w każdej chwili możliwość odwołania swojej zgody na przetwarzanie danych o ruchu.

[…]

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.

[…]".

8 Artykuł 9 tej dyrektywy, zatytułowany „Dane dotyczące lokalizacji inne niż dane o ruchu", przewiduje w ust. 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. […]".

9 Artykuł 15 dyrektywy 2002/58, zatytułowany „Stosowanie niektórych przepisów dyrektywy [95/46]”, stanowi w ust. 1:

„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 (i.e. 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]. 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 [TUE]”.

Dyrektywa 2003/6

10 Motywy 1, 2, 12, 37, 41 i 44 dyrektywy 2003/6 mają następujące brzmienie:

„(1) Prawdziwy jednolity rynek usług finansowych ma zasadnicze znaczenie dla wzrostu gospodarczego i tworzenia miejsc pracy we Wspólnocie.

(2) Zintegrowany i wydajny rynek wymaga uczciwości rynkowej. Sprawne działanie rynków papierów wartościowych oraz zaufanie społeczne do rynków to warunki niezbędne do wzrostu gospodarczego i dobrobytu. Nadużycia na rynku mają negatywny wpływ na integralność rynków finansowych oraz zaufanie społeczne do papierów wartościowych i instrumentów pochodnych.

[…]

(12) Nadużycia na rynku polegają na wykorzystywaniu poufnych informacji i manipulacjach na rynku. Cel przepisów wymierzonych przeciwko wykorzystywaniu poufnych informacji jest taki sam jak cel przepisów wymierzonych przeciwko manipulacjom na rynku: zapewnienie integralności rynków finansowych Wspólnoty i zwiększenie zaufania inwestorów do tych rynków. […]

[…]

(37) Wspólny minimalny zestaw skutecznych narzędzi i uprawnień właściwych organów każdego państwa członkowskiego zagwarantuje skuteczność nadzoru. Przedsiębiorstwa rynkowe i wszystkie podmioty aktywne gospodarczo powinny także przyczyniać się, na swoich poziomach, do integralności rynku.[…]

[…]

(41) Ponieważ cel zaproponowanych działań, a mianowicie zapobieganie nadużyciom na rynku w formie wykorzystywania poufnych informacji i manipulacji na rynku, nie może być w wystarczającym stopniu osiągnięty przez państwa członkowskie i dlatego, ze względu na zakres i skutki środków, może zostać w wyższym stopniu osiągnięty na poziomie

Wspólnoty, Wspólnota może przyjąć środki zgodnie z zasadą pomocniczości wymienioną w art. 5 [TUE]. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(44) Niniejsza dyrektywa respektuje prawa podstawowe i stosuje się do zasad uznanych w szczególności w [karcie], w szczególności w jej art. 11 i w art. 10 [europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności]. […]”.

11 Artykuł 11 tej dyrektywy stanowi:

„Bez uszczerbku dla kompetencji organów sądowych każde państwo członkowskie wyznacza jeden właściwy organ administracyjny w celu zapewnienia stosowania przepisów przyjętych zgodnie z niniejszą dyrektywą.

[…]”.

12 Zgodnie z art. 12 wspomnianej dyrektywy:

„1. Właściwe organy są wyposażone w uprawnienia nadzorcze i śledcze niezbędne do wypełniania ich funkcji. […]

2. Bez uszczerbku dla art. 6 ust. 7 uprawnienia określone w ust. 1 niniejszego artykułu wykonywane są zgodnie z prawem krajowym i obejmują przynajmniej prawo do:

a) posiadania dostępu do każdego dokumentu w jakiejkolwiek formie oraz do otrzymywania kopii;

[…]

d) żądania wydania rejestrów połączeń telefonicznych i rejestrów przesyłu danych;

[…]”.

Rozporządzenie nr 596/2014

13 Rozporządzenie nr 596/2014 uchyliło i zastąpiło dyrektywę 2003/6 z dniem 3 lipca 2016 r.

14 Motywy 1, 2, 7, 24, 44, 62, 65, 66, 77 i 86 tego rozporządzenia mają następujące brzmienie:

„(1) Prawdziwy rynek wewnętrzny usług finansowych ma decydujące znaczenie dla wzrostu gospodarczego i tworzenia miejsc pracy w Unii.

(2) Spójność, efektywność i przejrzystość rynku finansowego wymaga integralności rynku. Sprawne działanie rynków papierów wartościowych oraz zaufanie społeczne do rynków to warunki niezbędne do wzrostu gospodarczego i dobrobytu. Nadużycia na rynku mają negatywny wpływ na integralność rynków finansowych oraz zaufanie społeczne do papierów wartościowych i instrumentów pochodnych.

[…]

(7) Nadużycie na rynku to pojęcie obejmujące bezprawne zachowanie na rynkach finansowych, a do celów niniejszego rozporządzenia należy je rozumieć jako wykorzystywanie informacji poufnych, bezprawne ujawnianie informacji poufnych oraz manipulacje na rynku. Zachowanie takie uniemożliwia pełną i właściwą przejrzystość rynku, która stanowi warunek konieczny do umożliwienia wszystkim podmiotom gospodarczym obrotu na zintegrowanych rynkach finansowych.

[…]

(24) Jeżeli osoba prawna lub fizyczna będąca w posiadaniu informacji poufnych nabywa lub zbywa albo usiłuje nabyć lub zbyć, na własny rachunek lub na rzecz osoby trzeciej, pośrednio lub bezpośrednio, instrumenty finansowe, których dotyczą dane informacje, powinno istnieć domniemanie, że osoba ta wykorzystała te informacje. Domniemanie to nie narusza prawa do obrony. Pytanie, czy dana osoba naruszyła zakaz wykorzystywania informacji poufnych lub usiłowała wykorzystać informacje poufne, należy analizować w świetle celu niniejszego rozporządzenia, jakim jest ochrona integralności rynku finansowego i podnoszenie zaufania inwestorów, które z kolei opiera się na zapewnieniu inwestorom równych warunków działania i ochrony przed nadużywaniem informacji poufnych.

[…]

(44) Cena wielu instrumentów finansowych jest ustalana na podstawie wskaźników referencyjnych. Faktyczna manipulacja lub usiłowanie manipulacji wskaźnikami referencyjnymi, w tym międzybankowymi stopami procentowymi, może mieć poważny wpływ na zaufanie do rynku i przynieść znaczne straty dla inwestorów lub rzeczywiste zakłócenia w gospodarce. […]

(62) Zestaw skutecznych narzędzi, uprawnień i zasobów dla właściwych organów każdego z państw członkowskich gwarantuje skuteczność nadzoru. Dlatego też w niniejszym rozporządzeniu przewidziano w szczególności minimalny zestaw uprawnień nadzorczych i uprawnień do czynności wyjaśniających, jakie należy powierzyć właściwym organom państw członkowskich zgodnie z prawem krajowym. Jeżeli wymaga tego prawo krajowe, uprawnienia te powinny być wykonywane na podstawie wniosku do właściwych organów sądowych. […]

[…]

(65) Istniejące nagrania rozmów telefonicznych i zapisy danych o ruchu firm inwestycyjnych, instytucji kredytowych i instytucji finansowych dokonujących transakcji i dokumentujących ich wykonanie oraz istniejące zapisy połączeń telefonicznych i danych o ruchu operatorów telekomunikacyjnych stanowią istotne, a niekiedy jedyne dowody przy wykrywaniu i udowadnianiu wykorzystywania informacji poufnych i manipulacji na rynku. Dzięki zapisom połączeń telefonicznych i danych o ruchu można zidentyfikować osobę odpowiedzialną za rozpowszechnienie fałszywych lub wprowadzających w błąd informacji lub ustalić, że dane osoby kontaktowały się w określonym czasie oraz że istnieje powiązanie między co najmniej dwiema osobami. Dlatego też właściwe organy powinny móc zażądać istniejących nagrań rozmów telefonicznych oraz zapisów komunikacji elektronicznej i danych o ruchu przechowywanych przez firmę inwestycyjną, instytucję kredytową lub instytucję finansową zgodnie z dyrektywą [Parlamentu Europejskiego

i Rady] 2014/65/UE [z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniającą dyrektywę 2002/92/WE oraz dyrektywę 2011/61/UE (Dz.U. 2014, L 173, s. 349)]. Dostęp do zapisów danych i połączeń telefonicznych jest konieczny do uzyskania dowodów i poszlak dotyczących prawdopodobnego wykorzystania informacji poufnych lub manipulacji na rynku, a zatem do wykrywania nadużyć na rynku i nakładania sankcji za ich popełnianie. Aby wprowadzić równe warunki działania w Unii, jeśli chodzi o dostęp do istniejących zapisów połączeń telefonicznych i danych o ruchu operatorów telekomunikacyjnych lub istniejących nagrań rozmów telefonicznych i zapisów danych o ruchu przechowywanych przez firmę inwestycyjną, instytucję kredytową lub instytucję finansową, właściwe organy powinny móc zażądać, zgodnie z prawem krajowym, istniejących zapisów połączeń telefonicznych i danych o ruchu operatorów telekomunikacyjnych, na ile zezwala na to prawo krajowe, oraz istniejących nagrań rozmów telefonicznych i zapisów danych o ruchu przechowywanych przez firmę inwestycyjną, jeżeli istnieje uzasadnione podejrzenie, że takie zapisy dotyczące przedmiotu inspekcji lub czynności wyjaśniających mogą mieć znaczenie w udowodnieniu wykorzystania informacji poufnych lub manipulacji na rynku z naruszeniem niniejszego rozporządzenia. Dostęp do zapisów połączeń telefonicznych i danych o ruchu operatorów telekomunikacyjnych nie obejmuje dostępu do treści komunikacji głosowej prowadzonej przez telefon.

(66) Niniejsze rozporządzenie określa minimalny zbiór uprawnień, jakie powinny posiadać właściwe organy, jednak uprawnienia te należy wykonywać w ramach całościowego systemu prawa krajowego, gwarantującego poszanowanie praw podstawowych, w tym prawa do prywatności. W odniesieniu do wykonywania tych uprawnień, które może stanowić poważną ingerencję w prawo do poszanowania życia prywatnego i rodzinnego, miru domowego i komunikowania się, państwa członkowskie powinny dysponować wystarczającymi i skutecznymi zabezpieczeniami przed nadużyciami, np. w formie wymogu uzyskania w stosowanych przypadkach uprzedniej zgody organów sądowych danego państwa członkowskiego. Państwa członkowskie powinny dać właściwym organom możliwość wykonywania takich uprawnień naruszających prywatność w zakresie niezbędnym do właściwego przeprowadzenia czynności nadzorczych w poważnych przypadkach, w których nie istnieją równoważne środki pozwalające na uzyskanie takich samych rezultatów.

[…]

(77) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w [karcie]. W związku z tym niniejsze rozporządzenie powinno być interpretowane i stosowane zgodnie z tymi prawami i zasadami. […]

[…]

(86) Ponieważ cel niniejszego rozporządzenia, a mianowicie zapobieganie nadużyciom na rynku w formie wykorzystywania informacji poufnych, bezprawnego ujawniania informacji poufnych i manipulacji na rynku, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na jego rozmiary i skutki możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 [TUE]. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu”.

15 Zgodnie z art. 1 wspomnianego rozporządzenia:

„Niniejsze rozporządzenie ustanawia wspólne ramy regulacyjne dotyczące wykorzystywania informacji poufnych, bezprawnego ujawniania informacji poufnych i manipulacji na rynku (nadużyć na rynku), a także środki mające zapobiegać nadużyciom na rynku w celu zapewnienia integralności rynków finansowych w Unii oraz poprawy ochrony inwestorów i zwiększenia zaufania do tych rynków".

16 Artykuł 3 tego samego rozporządzenia, zatytułowany „Definicje", stanowi w ust. 1 pkt 27:

„Do celów niniejszego rozporządzenia stosuje się następujące definicje:

[…]

27) »zapisy danych o ruchu« oznaczają zapisy danych o ruchu w rozumieniu art. 2 akapit drugi lit. b) dyrektywy [2002/58]".

17 Zgodnie z art. 14 rozporządzenia nr 596/2014, zatytułowanym „Zakaz wykorzystywania i bezprawnego ujawniania informacji poufnych":

„Zabrania się każdej osobie:

a) wykorzystywania informacji poufnych lub usiłowania wykorzystywania informacji poufnych;

b) rekomendowania innej osobie lub nakłaniania jej do wykorzystywania informacji poufnych; lub

c) bezprawnego ujawniania informacji poufnych".

18 Artykuł 22 tego rozporządzenia przewiduje:

„Bez uszczerbku dla kompetencji organów sądowych każde państwo członkowskie wyznacza jeden właściwy organ administracyjny do celów niniejszego rozporządzenia. […]".

19 Artykuł 23 wspomnianego rozporządzenia, zatytułowany „Uprawnienia właściwych organów", stanowi w ust. 2 i 3:

„2. W celu wykonywania swoich obowiązków wynikających z niniejszego rozporządzenia właściwe organy posiadają zgodnie z prawem krajowym co najmniej uprawnienia w zakresie nadzoru i czynności wyjaśniających do:

a) posiadania dostępu do każdego dokumentu i danych w jakiejkolwiek formie oraz do otrzymywania ich kopii;

[…]

g) żądania wydania istniejących nagrań rozmów telefonicznych, komunikacji elektronicznej lub zapisów danych o ruchu przechowywanych przez firmy inwestycyjne, instytucje kredytowe lub instytucje finansowe;

h) w przypadku uzasadnionego podejrzenia naruszenia i gdy takie rejestry mogą mieć znaczenie dla czynności wyjaśniających w sprawie naruszenia art. 14 lit. a) lub b) lub art. 15 – żądania, w zakresie dozwolonym prawem krajowym, wydania istniejących zapisów danych o ruchu przechowywanych przez operatora telekomunikacyjnego;

[…]

3. Państwa członkowskie gwarantują odpowiednie środki umożliwiające właściwym organom posiadanie wszystkich uprawnień w zakresie nadzoru i czynności wyjaśniających, koniecznych do wykonywania ich obowiązków.

[…]”.

Prawo francuskie

CPCE

20 Artykuł L. 34-1 code des postes et des communications électroniques (kodeksu pocztowego i łączności elektronicznej), w brzmieniu mającym zastosowanie do sporów w postępowaniach głównych, (zwanego dalej „CPCE”) stanowił:

„I. – Niniejszy artykuł ma zastosowanie do przetwarzania danych osobowych w związku z publicznym świadczeniem usług łączności elektronicznej; ma on zastosowanie w szczególności do sieci obejmujących urządzenia do zbierania danych i urządzenia do identyfikacji.

II. – Operatorzy łączności elektronicznej, a w szczególności osoby, których działalność polega na oferowaniu dostępu do usług internetowej komunikacji publicznej, są zobowiązani do usunięcia lub zanonimizowania wszystkich danych o ruchu, z zastrzeżeniem przepisów ust. III, IV, V i VI.

Osoby świadczące publicznie usługi łączności elektronicznej są zobowiązane ustanowić, z uwzględnieniem przepisów poprzedniego akapitu, procedury wewnętrzne umożliwiające ustosunkowanie się do żądań właściwych organów.

Osoby, które w ramach głównej lub dodatkowej działalności zawodowej oferują publicznie połączenie umożliwiające komunikację internetową za pośrednictwem dostępu do sieci, nawet bezpłatnie, są zobowiązane do przestrzegania przepisów mających zastosowanie do operatorów łączności elektronicznej na mocy niniejszego artykułu.

III. – Do celów wykrywania, stwierdzania i ścigania przestępstw kryminalnych lub uchybienia obowiązkowi określonemu w art. L. 336-3 code de la propriété intellectuelle (kodeksu własności intelektualnej) lub do celów zapobiegania naruszeniom systemów zautomatyzowanego przetwarzania danych, które są przewidziane i karane na mocy artykułów od 323-1 do 323-3-1 code pénal (kodeksu karnego), i jedynie w celu umożliwienia, w razie konieczności, udostępnienia sądowi lub wysokiej władzy, o której mowa w art. L. 331-12 kodeksu własności intelektualnej, lub krajowemu organowi ds. bezpieczeństwa systemów informatycznych określonemu w art. L. 2321-1 code de la défense (kodeksu obronności), działania zmierzające do usunięcia lub anonimizacji określonych kategorii danych technicznych mogą zostać odroczone na okres maksymalnie jednego roku. Wydany po zasięgnięciu opinii Commission nationale de l’informatique et des libertés (krajowej komisji ds. informatyki i wolności) konsultowany

z Conseil d'État (radą stanu, Francja) dekret określa, w granicach ustanowionych w ust. VI, te kategorie danych i okres ich zatrzymywania, w zależności od działalności operatorów i charakteru połączeń oraz warunków rekompensaty, w stosownych przypadkach, możliwych do ustalenia i wyszczególnionych kosztów dodatkowych świadczeń gwarantowanych z tego tytułu przez operatorów na żądanie państwa.

[…]

VI. – Dane zatrzymywane i przetwarzane zgodnie z warunkami określonymi w ust. III, IV i V dotyczą wyłącznie identyfikacji użytkowników usług świadczonych przez operatorów, cech technicznych komunikacji dostarczanej przez operatorów oraz lokalizacji urządzeń końcowych.

W żadnym wypadku nie mogą one odnosić się do treści wymienianej korespondencji lub do informacji, z którymi się zapoznano, w jakiejkolwiek formie, w ramach tej komunikacji.

Zatrzymywanie i przetwarzanie tych danych musi się odbywać zgodnie z przepisami ustawy nr 78-17 z dnia 6 stycznia 1978 r. dotyczącej informatyki, plików i swobód.

Operatorzy są zobowiązani do podjęcia wszelkich środków, aby zapobiec wykorzystaniu tych danych do celów innych niż przewidziane w niniejszym artykule".

21 Artykuł L. 34-1 code des postes et des communications électroniques (kodeksu pocztowego i łączności elektronicznej), w brzmieniu nadanym loi n° 2021-998, du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement (ustawą nr 2021-998 z dnia 30 lipca 2021 r. o zapobieganiu aktom terrorystycznym i o wywiadzie, JORF z dnia 31 lipca 2021 r., tekst nr 1), przewiduje w ust. II bis–III bis:

„II bis – Operatorzy łączności elektronicznej zobowiązani są zatrzymywać:

1) na potrzeby postępowania karnego, zapobiegania zagrożeniom bezpieczeństwa publicznego i ochrony bezpieczeństwa narodowego – informacje o tożsamości cywilnej użytkownika, do upływu pięciu lat od wygaśnięcia jego umowy;

2) w tych samych celach co wymienione w pkt 1 niniejszego ust. II bis – inne informacje dostarczone przez użytkownika w momencie zawarcia umowy lub utworzenia konta, jak również informacje dotyczące płatności, do upływu jednego roku, licząc od dnia wygaśnięcia jego umowy lub zamknięcia jego konta;

3) dla potrzeb walki z przestępczością i poważną przestępczością, zapobiegania poważnym zagrożeniom bezpieczeństwa publicznego i ochrony bezpieczeństwa narodowego – dane techniczne umożliwiające identyfikację źródła połączenia lub dane dotyczące urządzeń końcowych do upływu jednego roku od połączenia lub użycia urządzeń końcowych.

III. – Ze względów związanych z ochroną bezpieczeństwa narodowego, jeżeli zostanie stwierdzone jego poważne, aktualne lub przewidywalne zagrożenie, premier może w drodze dekretu nakazać operatorom łączności elektronicznej zatrzymywanie przez okres jednego roku niektórych kategorii danych o ruchu w uzupełnieniu do tych, o których mowa w ust. II bis pkt 3, oraz danych dotyczących lokalizacji określonych w dekrecie Conseil d'État (rady stanu).

Nakaz premiera, którego okres stosowania nie może przekroczyć jednego roku, może zostać przedłużony, jeżeli nadal są spełnione warunki jego wydania. Jego wygaśnięcie nie ma wpływu na okres przechowywania danych, o którym mowa w akapicie pierwszym niniejszego ust. III.

III bis. – Dane zatrzymywane przez operatorów na podstawie niniejszego artykułu mogą być przedmiotem nakazu szybkiego zatrzymania przez organy posiadające na mocy ustawy dostęp do danych dotyczących łączności elektronicznej w celu zapobiegania i zwalczania przestępczości, zapobiegania poważnym przestępstwom i zwalczania ich, a także zapobiegania innym poważnym naruszeniom przepisów, których przestrzeganie są one zobowiązane zapewnić, w celu uzyskania dostępu do tych danych, i zwalczania takich naruszeń".

22 Artykuł R. 10-13 CPCE ma następujące brzmienie:

„I. – Na mocy art. L. 34-1 ust. III operatorzy łączności elektronicznej zatrzymują do celów wykrywania, stwierdzania i ścigania przestępstw kryminalnych:

a) informacje umożliwiające identyfikację użytkownika;

b) dane dotyczące używanych końcowych urządzeń komunikacyjnych;

c) charakterystykę techniczną, jak również datę, godzinę i czas trwania połączenia;

d) dane dotyczące żądanych lub wykorzystywanych usług dodatkowych i ich dostawców;

e) dane umożliwiające identyfikację odbiorcy lub odbiorców połączenia.

II. – W przypadku usług telefonicznych operator zatrzymuje dane, o których mowa w ust. II, a ponadto dane, które pozwalają na identyfikację pochodzenia i lokalizacji połączenia.

III. – Okres zatrzymywania danych, o których mowa w niniejszym artykule, wynosi jeden rok, licząc od dnia ich zarejestrowania.

[…]".

LCEN

23 Artykuł 6 loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (ustawy nr 2004-575 z dnia 21 czerwca 2004 r. o zaufaniu do gospodarki cyfrowej, JORF z dnia 22 czerwca 2004 r., s. 11168), w brzmieniu mającym zastosowanie do sporów w postępowaniach głównych, (zwanej dalej „LCEN"), przewidywał:

„I. – 1. Osoby, których działalność polega na oferowaniu dostępu do usług internetowej łączności publicznej, informują swoich abonentów o istnieniu środków technicznych umożliwiających ograniczenie dostępu do niektórych usług lub ich wybór i proponują im co najmniej jeden z tych środków.

[…]

2. Osoby fizyczne lub prawne oferujące, nawet nieodpłatnie, do publicznego udostępniania za pomocą usług internetowej łączności publicznej, przechowywanie sygnałów, tekstów, obrazów, dźwięków lub wszelkiego rodzaju wiadomości dostarczonych przez odbiorców tych usług nie mogą ponosić odpowiedzialności cywilnej za działania lub informacje przechowywane na żądanie odbiorcy tych usług, jeżeli nie miały one rzeczywistej wiedzy na temat ich bezprawnego charakteru lub na temat faktów i okoliczności wskazujących na taki charakter, lub gdy z chwilą, w której osoby te zyskały taką wiedzę, zadziałały one niezwłocznie w celu wycofania tych danych lub uniemożliwienia dostępu do nich.

[…]

II. – Osoby, o których mowa w ust. I pkt 1 i 2, przechowują i zatrzymują dane umożliwiające identyfikację każdego, kto przyczynił się do stworzenia treści lub części treści usług, których są usługodawcami.

Zapewniają one osobom, które redagują usługę internetowej łączności publicznej, środki techniczne umożliwiające im spełnienie warunków identyfikacji przewidzianych w ust. III.

Organ sądowy może zażądać od usługodawców, o których mowa w ust. I pkt 1 i 2, przekazania danych wskazanych w akapicie pierwszym.

Przepisy art. 226-17, 226-21 i 226-22 kodeksu karnego mają zastosowanie do przetwarzania tych danych.

Dekret Conseil d'État (rady stanu), wydany po zasięgnięciu opinii krajowej komisji ds. informatyki i swobód, określa dane, o których mowa w akapicie pierwszym, oraz czas trwania i szczegółowe zasady ich zatrzymywania.

[…]".

CMF

24 Artykuł L. 621-10 code monétaire et financier (kodeksu pieniężnego i finansowego, zwanego dalej „CMF"), w brzmieniu mającym zastosowanie do sporów w postępowaniach głównych, stanowił w akapicie pierwszym:

„Gdy jest to niezbędne do prowadzenia czynności wyjaśniających lub kontroli, śledczy i kontrolerzy mogą żądać udostępnienia wszelkich dokumentów, niezależnie od nośnika, na jakim zostały one utrwalone. Śledczy mogą również żądać udostępnienia oraz przekazania danych zatrzymywanych i przetwarzanych przez operatorów telekomunikacyjnych na podstawie art. L. 34-1 [CPCE] i przez usługodawców, o których mowa w art. 6 ust. I pkt 1 i 2 [LCEN], oraz uzyskać ich kopię.

[…]".

25 Wyciągając konsekwencje ze stwierdzenia niezgodności z konstytucją art. L. 621-10 akapit pierwszy zdanie drugie CMF przez Conseil constitutionnel (radę konstytucyjną, Francja) w decyzji z dnia 21 lipca 2017 r., ustawodawca w drodze loi n° 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude (ustawy nr 2018-898 z dnia 23 października 2018 r.

o zwalczaniu nadużyć finansowych, JORF z dnia 24 października 2018 r., tekst nr 1) dodał do code monétaire et financier (kodeksu pieniężnego i finansowego) art. L. 621-10-2, który przewiduje:

„W celu wykrywania nadużyć na rynku określonych w rozporządzeniu [nr 596/2014] śledczy mogą żądać przekazania danych zatrzymywanych i przetwarzanych przez operatorów telekomunikacyjnych, na warunkach i w granicach określonych w art. L. 34-1 [CPCE], oraz przez usługodawców, o których mowa w art. 6 ust. I pkt 1 i 2 [LCEN].

Przekazanie danych, o których mowa w akapicie pierwszym niniejszego artykułu, wymaga uzyskania uprzedniego zezwolenia kontrolera wniosków o ujawnienie danych dotyczących połączeń.

Kontrolerem wniosków o dane dotyczące połączeń jest, na zmianę, członek Conseil d'État (rady stanu), czynny lub w stanie spoczynku, wybrany przez zgromadzenie ogólne Conseil d'État (rady stanu), a następnie sędzia Cour de cassation (trybunału kasacyjnego), czynny lub w stanie spoczynku, wybrany przez zgromadzenie ogólne tego trybunału. Jego zastępca, wywodzący się z drugiego sądu, jest powoływany na takich samych zasadach. Kontroler wniosków o dane dotyczące połączeń i jego zastępca są wybierani na nieodnawialny okres czterech lat.

[…]

W wykonywaniu swoich zadań kontroler wniosków o dane dotyczące połączeń nie może otrzymywać instrukcji od (ani zwracać się o nie do) Autorité des marchés financiers (urzędu rynków finansowych, Francja, zwanego dalej „AMF") ani żadnego innego organu. Jest on zobowiązany do zachowania tajemnicy zawodowej na warunkach określonych w art. L. 621-4 niniejszego kodeksu.

Sprawa jest kierowana do niego w drodze uzasadnionego wniosku sekretarza generalnego lub zastępcy sekretarza generalnego [AMF]. Wniosek ten zawiera informacje potwierdzające jego zasadność.

Zezwolenie jest dołączane do akt dochodzeniowych.

Śledczy wykorzystują dane przekazane przez operatorów telekomunikacyjnych i usługodawców, o których mowa w akapicie pierwszym niniejszego artykułu, wyłącznie w ramach dochodzenia, z tytułu którego otrzymali zezwolenie.

Dane dotyczące połączeń odnoszące się do okoliczności faktycznych będących przedmiotem przedstawienia zarzutów przez kolegium [AMF] zostają zniszczone w terminie sześciu miesięcy od wydania ostatecznej decyzji komisji ds. sankcji lub sądów odwoławczych. W przypadku porozumienia administracyjnego sześciomiesięczny termin rozpoczyna bieg od wykonania porozumienia.

Dane dotyczące połączeń odnoszące się do okoliczności faktycznych, które nie były przedmiotem przedstawienia zarzutów przez kolegium [AMF], zostają zniszczone z upływem terminu jednego miesiąca od dnia wydania decyzji kolegium.

W przypadku przekazania sprawozdania z dochodzenia procureur de la République financier (prokuratorowi finansowemu, Francja) lub w przypadku wszczęcia postępowania karnego przez procureur de la République financier (prokuratora finansowego) […] dane dotyczące połączeń przekazywane są procureur de la République financier (prokuratorowi finansowemu) i nie są zatrzymywane przez [AMF].

Szczegółowe zasady stosowania niniejszego artykułu określa dekret Conseil d'État (rady stanu)".

Postępowania główne, pytania prejudycjalne i postępowanie przed Trybunałem

26 Aktem oskarżenia z dnia 22 maja 2014 r. wszczęto wobec VD i SR sądowe postępowanie przygotowawcze w przedmiocie czynów mających znamiona przestępstwa polegającego na wykorzystywaniu i ukrywaniu informacji poufnych. Postępowanie to zostało następnie rozszerzone pierwszym uzupełniającym aktem oskarżenia z dnia 14 listopada 2014 r., w którym dokonano kwalifikacji przestępstwa współsprawstwa.

27 W dniach 23 i 25 września 2015 r. AMF przekazał sędziemu śledczemu pewne informacje, jakimi dysponował w ramach dochodzenia, które prowadził na podstawie art. L. 621-10 CMF, w szczególności dane osobowe pochodzące z rozmów telefonicznych przeprowadzonych przez VD i SR, które śledczy AMF zgromadzili na podstawie art. L. 34-1 CPCE od operatorów usług łączności elektronicznej.

28 W związku z zawiadomieniem dokonanym następnie przez AMF dochodzenie zostało rozszerzone, w drodze trzech uzupełniających aktów oskarżenia z dni 29 września 2015 r., 22 grudnia 2015 r. i 23 listopada 2016 r., w których dokonano kwalifikacji korupcji i prania pieniędzy.

29 VD i SR zostali postawieni w stan oskarżenia odpowiednio w dniach 10 marca i 29 maja 2017 r. pod zarzutem wykorzystywania informacji poufnych i prania pieniędzy w przypadku pierwszego z nich oraz wykorzystywania informacji poufnych w przypadku drugiego.

30 Ponieważ ich oskarżenie było oparte na danych o ruchu dostarczonych przez AMF, VD i SR wnieśli osobno do cour d'appel de Paris (sądu apelacyjnego w Paryżu, Francja) skargi, podnosząc w szczególności zarzut dotyczący zasadniczo naruszenia art. 15 ust. 1 dyrektywy 2002/58, interpretowanego w świetle art. 7, 8, 11 i art. 52 ust. 1 karty. Ściślej rzecz ujmując, opierając się na orzecznictwie wynikającym z wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), VD i SR kwestionowali fakt, że w celu zgromadzenia wspomnianych danych organ ten oparł się na art. L. 621-10 CMF i art. L. 34-1 CPCE, podczas gdy przepisy te z jednej strony nie były zgodne z prawem Unii w zakresie, w jakim przewidywały uogólnione i niezróżnicowane zatrzymywanie danych dotyczących połączeń, a z drugiej strony nie określały żadnych ograniczeń w zakresie uprawnień śledczych AMF do uzyskania dostępu do zatrzymanych danych.

31 Dwoma wyrokami cour d'appel de Paris (sądu apelacyjnego w Paryżu) z dnia 20 grudnia 2018 r. i z dnia 7 marca 2019 r. sąd ten oddalił skargi VD i SR. Z informacji zawartych we wnioskach o wydanie orzeczenia w trybie prejudycjalnym wynika, że w celu oddalenia zarzutu dotyczącego zasadniczo naruszenia art. 15 ust. 1 dyrektywy 2002/58, interpretowanego w świetle art. 7, 8, 11 i art. 52 ust. 1 karty, sędziowie orzekający co do istoty oparli się w szczególności na fakcie, że art. 23 ust. 2 lit. h) rozporządzenia nr 596/2014, dotyczący nadużyć na rynku, umożliwia

właściwym organom uzyskanie – w zakresie dozwolonym prawem krajowym – istniejących zapisów danych o ruchu przechowywanych przez operatorów usług łączności elektronicznej w przypadku uzasadnionego podejrzenia naruszenia zakazu wykorzystywania informacji poufnych na mocy art. 14 lit. a) i b) tego rozporządzenia i gdy takie zapisy mogą mieć znaczenie dla czynności wyjaśniających w sprawie tego naruszenia.

32 VD i SR wnieśli odwołanie od tych wyroków do sądu odsyłającego, podnosząc zarzut naruszenia w szczególności postanowień karty i przepisów dyrektywy 2002/58, o których mowa w poprzednim punkcie.

33 Co się tyczy dostępu do danych dotyczących połączeń, sąd odsyłający powołuje się na decyzję Conseil constitutionnel (rady konstytucyjnej) z dnia 21 lipca 2017 r., z której wynika, że przewidziane w prawie francuskim postępowanie w sprawie dostępu do danych osobowych zatrzymanych przez śledczych AMF nie jest zgodne z prawem do poszanowania prywatności, które jest chronione przez art. 2 Deklaracji praw człowieka i obywatela z 1789 r., i podkreśla, że chociaż ustawodawca krajowy zastrzegł uprawnienie do uzyskania takich danych w ramach dochodzenia dla upoważnionych urzędników, którzy są związani tajemnicą zawodową, i nie przyznał im uprawnienia do przymusowej egzekucji, to jednak nie przewidział w tym postępowaniu żadnej innej gwarancji zapewniającej zrównoważone pogodzenie między prawem do prywatności a zapobieganiem naruszeniom porządku publicznego i wykrywaniem sprawców przestępstw, w związku z czym art. L. 621-10 CMF akapit pierwszy zdanie drugie należy uznać za sprzeczny z francuską konstytucją.

34 Sąd odsyłający wskazuje ponadto z jednej strony, że Conseil constitutionnel (rada konstytucyjna) uznała, iż biorąc pod uwagę „oczywiście zbyt daleko idące" konsekwencje, jakie natychmiastowe uchylenie tego przepisu mogłoby mieć dla toczących się postępowań, należało odroczyć datę uchylenia na dzień 31 grudnia 2018 r., a z drugiej strony, że ustawodawca krajowy, wyciągając konsekwencje ze stwierdzenia niezgodności z konstytucją art. L. 621-10 akapit pierwszy CMF, wprowadził do tego kodeksu art. L. 621-10-2.

35 Sąd odsyłający, przypominając rozważania zawarte w pkt 125 wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), uważa, że nieważność art. L. 621-10 akapit pierwszy zdanie drugie CMF, mającego zastosowanie w chwili zaistnienia okoliczności faktycznych w postępowaniu głównym, nie może wynikać z tego stwierdzenia niezgodności z konstytucją, zważywszy na odroczenie skutków uchylenia tego przepisu. Uważa on jednak, że przysługujące śledczym AMF na podstawie tego przepisu uprawnienie do uzyskania danych dotyczących połączeń bez uprzedniej kontroli ze strony sądu lub niezależnego organu administracyjnego nie jest zgodne z wymogami wynikającymi z art. 7, 8 i 11 karty, tak jak interpretuje je Trybunał.

36 W tych okolicznościach jedyne pytanie, jakie się nasuwa w tym zakresie, dotyczy możliwości odroczenia w czasie skutków uchylenia art. L. 621-10 CMF, nawet jeżeli nie jest on zgodny z kartą.

37 W odniesieniu do zatrzymywania danych dotyczących połączeń sąd odsyłający wskazuje przede wszystkim, że chociaż art. L. 34-1 ust. II CPCE ustanawia zasadniczy obowiązek, zgodnie z którym operatorzy świadczący usługi łączności elektronicznej muszą usunąć lub poddać anonimizacji wszelkie dane dotyczące ruchu, to jednak obowiązkowi temu towarzyszą pewne wyjątki, w tym wyjątek przewidziany w ust. III tego przepisu, dotyczący „celów wykrywania, stwierdzania i ścigania przestępstw kryminalnych". W odniesieniu do tych szczególnych celów operacje usuwania lub anonimizacji pewnej liczby danych są odraczane o rok.

38 Wyjaśnia on w tym względzie, że pięć kategorii danych, których dotyczą w szczególności warunki określone w art. L. 34-1 ust. III CPCE, to kategorie wymienione w art. R. 10-13 CPCE. Te dane o połączeniach są generowane lub przetwarzane w następstwie połączenia i odnoszą się do okoliczności tego połączenia i do użytkowników usługi, ale nie dostarczają żadnej wskazówki co do treści danych połączeń.

39 Następnie, przypominając pkt 112 wyroku z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970), zgodnie z którym art. 15 ust. 1 dyrektywy 2002/58, w związku z art. 7, 8, 11 i art. 52 ust. 1 karty, należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania przestępczości uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej, sąd odsyłający zauważa, że w ramach spraw w postępowaniach głównych AMF miał dostęp do danych zatrzymywanych przez operatorów usług łączności elektronicznej w związku z podejrzeniami wykorzystywania informacji poufnych i nadużyć na rynku, które mogą być objęte szeregiem poważnych kwalifikacji karnych. Dostęp ten był uzasadniony potrzebą krzyżowego sprawdzenia przez ten organ, dla zapewnienia skuteczności prowadzonego przezeń dochodzenia, różnych danych zatrzymanych na pewien okres czasu w celu uaktualnienia informacji poufnych krążących między wieloma rozmówcami, które ujawniły istnienie bezprawnych praktyk w tej dziedzinie.

40 Zdaniem sądu odsyłającego dochodzenia prowadzone przez AMF odpowiadają obowiązkom nałożonym na państwa członkowskie w art. 12 ust. 2 lit. d) dyrektywy 2003/6 i w art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014, interpretowanym w świetle art. 1 tego rozporządzenia, w tym w szczególności obowiązkowi przekazania istniejących zapisów danych o ruchu przechowywanych przez operatorów usług łączności elektronicznej.

41 Ponadto sąd ten podkreśla z jednej strony, odnosząc się do motywu 65 wspomnianego rozporządzenia, że te dane dotyczące połączeń stanowią istotny, a czasami jedyny dowód pozwalający na wykrycie i wykazanie wykorzystywania informacji poufnych, ponieważ pozwalają one na ustalenie tożsamości osoby, która doprowadziła do rozpowszechnienia nieprawdziwych lub wprowadzających w błąd informacji, lub udowodnienie, że dane osoby kontaktowały się w określonym momencie.

42 Z drugiej strony sąd odsyłający cytuje motyw 66 tego samego rozporządzenia, z którego wynika, że wykonywanie uprawnień przyznanych organom właściwym w sprawach finansowych może stanowić ingerencję w prawo do poszanowania życia prywatnego i rodzinnego, miru domowego i komunikowania się oraz że w związku z tym państwa członkowskie powinny dysponować wystarczającymi i skutecznymi zabezpieczeniami przed nadużyciami, ograniczając te uprawnienia jedynie do przypadków, w których są one niezbędne do właściwego przeprowadzenia czynności nadzorczych w poważnych przypadkach, w których państwa te nie dysponują równoważnymi środkami pozwalającymi na uzyskanie takich samych rezultatów. Jego zdaniem z motywu tego wynika, że pewne przypadki nadużyć na rynku należy uznać za poważne naruszenia.

43 Sąd ten podkreśla ponadto, że w ramach spraw w postępowaniach głównych informacje poufne, które mogą charakteryzować materialny element niedozwolonych praktyk w dziedzinie rynku, były z natury swojej ustne i tajne.

44 W świetle powyższych rozważań sąd odsyłający zastanawia się nad pogodzeniem art. 15 ust. 1 dyrektywy 2002/58, interpretowanego w świetle art. 7, 8, 11 i art. 52 ust. 1 karty, z wymogami wynikającymi z art. 12 ust. 2 lit. d) dyrektywy 2003/6 i art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014.

45 Wreszcie, na wypadek gdyby Trybunał uznał, że rozpatrywane w postępowaniach głównych ustawodawstwo odnoszące się do zatrzymywania danych dotyczących połączeń nie jest zgodne z prawem Unii, pojawia się pytanie o tymczasowe utrzymanie w mocy skutków tego ustawodawstwa w celu uniknięcia niepewności prawnej i umożliwienia użycia zgromadzonych i zatrzymanych uprzednio danych do celów wykrywania i ścigania wykorzystywania informacji poufnych.

46 W tych okolicznościach Cour de cassation (trybunał kasacyjny) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi, które zostały sformułowane w identyczny sposób w sprawach C-339/20 i C-397/20:

„1) Czy art. 12 ust. 2 lit. a) i d) dyrektywy [2003/6], podobnie jak art. 23 ust. 2 lit. g) i h) rozporządzenia [nr 596/2014], który zastąpił ten pierwszy przepis z dniem 3 lipca 2016 r., interpretowany w świetle motywu 65 tego rozporządzenia, nie oznaczają z uwagi na poufny charakter wymienianych informacji oraz ogólny zakres osób, których prawa mogłyby zostać naruszone, możliwości nałożenia przez krajowego prawodawcę na operatorów łączności elektronicznej obowiązku czasowego zatrzymywania wszystkich danych o połączeniach w celu umożliwienia organowi administracji, o którym mowa w art. 11 dyrektywy [2003/6] i art. 22 rozporządzenia [nr 596/2014], w sytuacji gdy w stosunku do pewnych osób ujawni się uzasadnione podejrzenie, że podejmują działania polegające na wykorzystywaniu informacji poufnych i manipulacji na rynku, uzyskania od operatora istniejących zapisów danych o ruchu w przypadkach, w których istnieją podstawy do założenia, że owe zapisy związane z przedmiotem dochodzenia mogą okazać się istotne dla uzyskania dowodu na przebieg naruszenia poprzez umożliwienie w szczególności prześledzenia kontaktów nawiązanych przez zainteresowanych przed pojawieniem się podejrzeń?

2) W wypadku gdyby odpowiedź Trybunału […] [na pytanie pierwsze] była taka, że skłoniłaby Cour de cassation (sąd kasacyjny) do uznania, że francuskie przepisy dotyczące zatrzymywania danych o połączeniach nie są zgodne z prawem Unii, czy skutki tych przepisów mogłyby zostać tymczasowo utrzymane w celu uniknięcia niepewności prawa i umożliwienia wykorzystania uprzednio zebranych i zatrzymanych danych w jednym z celów określonych przez to ustawodawstwo?

3) Czy sąd krajowy może tymczasowo utrzymać w mocy skutki przepisów pozwalających funkcjonariuszom niezależnego organu administracyjnego odpowiedzialnego za prowadzenie dochodzeń w sprawie nadużyć na rynku na zażądanie przekazania danych o połączeniach bez uprzedniej kontroli sądu lub innego niezależnego organu administracyjnego?”.

47 Postanowieniem prezesa Trybunału z dnia 17 września 2020 r. sprawy C-339/20 i C-397/20 zostały połączone do celów przeprowadzenia pisemnego i ustnego etapu postępowania oraz wydania wyroku.

48 W dniu 21 kwietnia 2021 r. Conseil d'État (rada stanu, Francja) wydała wyrok w sprawie French Data Network i in. (nr 393099, 394922, 397844, 397851, 424717, 424718), w którym orzekła w szczególności w przedmiocie zgodności z prawem Unii określonych przepisów krajowych, mających znaczenie w ramach postępowań głównych, a mianowicie art. L. 34-1 CPCE i art. R. 10-13 CPCE.

49 Na wezwanie Trybunału uczestnicy rozprawy w niniejszych sprawach mieli możliwość wypowiedzenia się na temat ewentualnego wpływu tego wyroku Conseil d'État (rady stanu) na niniejsze odesłania prejudycjalne.

50 Przedstawiciel rządu francuskiego wskazał na rozprawie, że w wyroku tym Conseil d'État (rada stanu) uznała zasadniczo za niezgodne z prawem przepisy umożliwiające wdrożenie uogólnionego i niezróżnicowanego zatrzymywania danych dotyczących połączeń dla celów zwalczania przestępczości z wyjątkiem zatrzymywania adresów IP i danych dotyczących tożsamości cywilnej użytkowników sieci łączności elektronicznej, wyciągając w ten sposób konsekwencje z wyroku 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). Wyjaśnił on jednak, że w ramach postępowania kontradyktoryjnego Conseil d'État (rada stanu) musiała rozpatrzyć zarzut rządu francuskiego, zgodnie z którym taka wykładnia prawa Unii stoi w sprzeczności z normami rangi konstytucyjnej, a mianowicie takimi, które służą zapobieganiu naruszeniom porządku publicznego, w szczególności bezpieczeństwu osób i mienia oraz wykrywaniu sprawców przestępstw kryminalnych.

51 Przedstawiciel rządu francuskiego wyjaśnił w tym względzie, że Conseil d'État (rada stanu) dwukrotnie odrzuciła ten zarzut. Z jednej strony przyznała ona wprawdzie, że uogólnione i niezróżnicowane zatrzymywanie danych dotyczących połączeń stanowi warunek decydujący o powodzeniu dochodzeń w sprawach karnych i że żadna inna metoda nie może tego skutecznie zastąpić. Z drugiej strony Conseil d'État (rada stanu) uznała jednak, opierając się w szczególności na pkt 164 wyroku 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), że szybkie zatrzymywanie danych jest dozwolone przez prawo Unii również wtedy, gdyby to szybkie zatrzymywanie dotyczyło danych pierwotnie zatrzymywanych do celów ochrony bezpieczeństwa narodowego.

52 Ponadto przedstawiciel rządu francuskiego wyjaśnił, że w następstwie wyroku Conseil d'État (rady stanu) z dnia 21 kwietnia 2021 r. w sprawie French Data Network i in. (nr 393099, 394922, 397844, 397851, 424717, 424718) ustawodawca krajowy wprowadził ust. III bis do art. L. 34-1 kodeksu pocztowego i łączności elektronicznej, jak wspomniano w pkt 21 niniejszego wyroku.

W przedmiocie pytań prejudycjalnych

Uwagi wstępne

53 W pierwszej kolejności należy przypomnieć, że po złożeniu rozpatrywanych w niniejszym postępowaniu wniosków o wydanie orzeczenia w trybie prejudycjalnym Conseil d'État (rada stanu) ogłosiła wyrok z dnia 21 kwietnia 2021 r. w sprawie French Data Network i in. (393099, 394922, 397844, 397851, 424717, 424718), dotyczący w szczególności zgodności z prawem Unii art. L. 34-1 CPCE oraz art. R. 10-13 CPCE.

54 Tymczasem, jak zauważył rzecznik generalny w pkt 42 opinii i jak wynika również z wyjaśnień udzielonych przez sąd odsyłający, przedstawionych w pkt 27, 37 i 38 niniejszego wyroku, artykuły te stanowią „kluczowe przepisy" w ramach stosowania art. L. 621-10 CMF, który jest przedmiotem spraw w postępowaniach głównych.

55 Podczas rozprawy przed Trybunałem przedstawiciel rządu francuskiego, po podkreśleniu zmian legislacyjnych, jakim został poddany art. L. 34-1 CPCE w następstwie uściśleń dokonanych przez Trybunał w wyroku 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), o których wspomniano w pkt 21 niniejszego wyroku, wskazał zasadniczo, że w celu rozstrzygnięcia sporów w postępowaniach głównych sąd odsyłający będzie zobowiązany, zgodnie z zasadą stosowania prawa w czasie zapisaną w art. 7 i 8 Deklaracji praw człowieka i obywatela z 1789 r., do uwzględnienia przepisów krajowych w brzmieniu mającym zastosowanie do okoliczności faktycznych będących przedmiotem postępowania głównego, które sięgają lat 2014 i 2015, w związku z czym wyrok Conseil d'État (rady stanu) z dnia 21 kwietnia 2021 r. w sprawie French Data Network i in. (393099, 394922, 397844, 397851, 424717 i 424718) nie może być w żadnym razie brany pod uwagę przy analizie rozpatrywanych w niniejszym postępowaniu wniosków o wydanie orzeczenia w trybie prejudycjalnym.

56 Zgodnie z utrwalonym orzecznictwem w ramach postępowania, o którym mowa w art. 267 TFUE, wyłącznie do sądu krajowego, przed którym toczy się spór i który wobec tego musi przyjąć na siebie odpowiedzialność za wydane orzeczenie, należy ocena, w świetle konkretnych okoliczności sprawy, zarówno niezbędności orzeczenia prejudycjalnego do wydania wyroku, jak i istotnego charakteru pytań skierowanych do Trybunału. W konsekwencji, jeśli zadane pytania dotyczą wykładni prawa Unii, Trybunał jest co do zasady zobowiązany do wydania orzeczenia (zob. podobnie wyrok z dnia 8 września 2010 r., Winner Wetten, C-409/06, EU:C:2010:503, pkt 36 i przytoczone tam orzecznictwo).

57 Odmowa udzielenia odpowiedzi na pytanie prejudycjalne zadane przez sąd krajowy jest możliwa jedynie wtedy, gdy żądana wykładnia prawa Unii w sposób oczywisty nie ma żadnego związku ze stanem faktycznym lub przedmiotem sporu w postępowaniu głównym lub też gdy problem ma charakter hipotetyczny albo gdy Trybunałowi nie przedstawiono okoliczności faktycznych i prawnych koniecznych do tego, aby mógł odpowiedzieć na zadane mu pytania w użyteczny sposób (zob. podobnie wyrok z dnia 19 listopada 2009 r., Filipiak, C-314/08, EU:C:2009:719, pkt 42 i przytoczone tam orzecznictwo).

58 W niniejszej sprawie z postanowień odsyłających wynika, że pytania pierwsze i trzecie dotyczą bezpośrednio nie art. L. 34-1 CPCE i art. R. 10-13 CPCE, lecz art. L. 621-10 CMF, na podstawie którego AMF zażądał od operatorów świadczących usługi łączności elektronicznej przekazania danych o ruchu związanych z połączeniami telefonicznymi wykonanymi przez VD i SR, na podstawie których zostali oni postawieni w stan oskarżenia i których dopuszczalność jako dowodów jest kwestionowana w ramach postępowań głównych.

59 Ponadto należy zauważyć, że poprzez pytania drugie i trzecie przedstawione w niniejszych sprawach, które stanowią kontynuację pytania pierwszego w obu sprawach, sąd odsyłający dąży zasadniczo do ustalenia, czy w przypadku gdyby rozpatrywane ustawodawstwo krajowe odnoszące się do zatrzymywania i dostępu do danych dotyczących połączeń okazało się niezgodne z prawem Unii, skutki te nie mogłyby jednak zostać tymczasowo utrzymane w mocy, tak aby uniknąć niepewności prawnej i umożliwić wykorzystanie danych zatrzymanych na podstawie tego ustawodawstwa do celów wykrywania i ścigania przypadków wykorzystywania informacji poufnych.

60 W świetle powyższych okoliczności, a także tych przedstawionych przez rzecznika generalnego w pkt 44–47 opinii, należy stwierdzić, że niezależnie od wyroku Conseil d'État (rady stanu) z dnia 21 kwietnia 2021 r. w sprawie French Data Network i in. (393099, 394922, 397844, 397851, 424717, 424718) oraz decyzji Conseil constitutionnel (rady konstytucyjnej) z dnia 25 lutego 2022 r. (nr 2021-976/977), w której uznano częściowo za niekonstytucyjny art. L. 34-1 CPCE w brzmieniu wskazanym w pkt 20 niniejszego wyroku, odpowiedź Trybunału na zadane pytania pozostaje niezbędna dla rozstrzygnięcia sporów w postępowaniach głównych.

61 W drugiej kolejności należy zauważyć, że na rozprawie przed Trybunałem przedstawiciel VD zakwestionował zastosowanie ratione temporis rozporządzenia nr 596/2014, podnosząc zasadniczo, że okoliczności faktyczne sprawy w postępowaniu głównym miały miejsce przed wejściem w życie tego rozporządzenia. W związku z tym jedynie przepisy dyrektywy 2003/6 mają jego zdaniem znaczenie dla analizy pytań zadanych przez sąd odsyłający.

62 W tym względzie należy przypomnieć, że zgodnie z utrwalonym orzecznictwem nowy przepis stosuje się od wejścia w życie aktu, który go wprowadza, i choć nie stosuje się go do sytuacji prawnych powstałych i ostatecznie zakończonych pod rządami dawnej ustawy, stosuje się go do przyszłych skutków tych sytuacji oraz do nowych sytuacji prawnych. Inaczej jest tylko – i to z zastrzeżeniem zasady niedziałania wstecz aktów prawnych – jeżeli wraz z nowym przepisem zostają wydane przepisy szczególne, które określają konkretnie jego warunki stosowania w czasie (zob. podobnie wyrok z dnia 15 stycznia 2019 r., E.B., C-258/17, EU:C:2019:17, pkt 50 i przytoczone tam orzecznictwo, a także z dnia 14 maja 2020 r., Azienda Municipale Ambiente, C-15/19, EU:C:2020:371, pkt 57).

63 Tymczasem, jak wskazano w pkt 26–29 niniejszego wyroku, o ile sytuacje prawne rozpatrywane w postępowaniach głównych rzeczywiście powstały przed wejściem w życie rozporządzenia nr 596/2014, które uchyliło i zastąpiło dyrektywę 2003/6 z dniem 3 lipca 2016 r., o tyle postępowania główne były kontynuowane po tej dacie, tak że od tej daty przyszłe skutki tych sytuacji zgodnie z zasadą przypomnianą w poprzednim punkcie niniejszego wyroku są regulowane przepisami rozporządzenia nr 596/2014.

64 Wynika z tego, że przepisy rozporządzenia nr 596/2014 mają zastosowanie w niniejszej sprawie. Ponadto nie ma potrzeby dokonywania rozróżnienia pomiędzy przywołanymi przez sąd odsyłający przepisami wynikającymi z dyrektywy 2003/6 i rozporządzenia nr 596/2014, ponieważ mają one zasadniczo podobny zakres na potrzeby wykładni, jakiej Trybunał będzie musiał dokonać w niniejszych sprawach.

W przedmiocie pytania pierwszego

65 Poprzez pytanie pierwsze w niniejszych sprawach sąd odsyłający zmierza zasadniczo do ustalenia, czy art. 12 ust. 2 lit. a) i d) dyrektywy 2003/6 i art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014, w związku z art. 15 ust. 1 dyrektywy 2002/58 oraz w świetle art. 7, 8, 11 i art. 52 ust. 1 karty należy interpretować w ten sposób, że sprzeciwiają się one środkom ustawodawczym takim jak środek będący przedmiotem postępowań głównych, który przewiduje zapobiegawczo do celów zwalczania przestępstw polegających na nadużyciach na rynku, do których zalicza się wykorzystywanie informacji poufnych, uogólnione i niezróżnicowane zatrzymywanie danych o ruchu przez okres jednego roku od dnia zapisu.

66 Strony w postępowaniach głównych oraz zainteresowani, którzy przedstawili Trybunałowi uwagi na piśmie, wyrazili rozbieżne opinie w tym względzie. Zdaniem rządu estońskiego, Irlandii oraz rządów hiszpańskiego i francuskiego art. 12 ust. 2 lit. a) i d) dyrektywy 2003/6, a także art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014 upoważniają ustawodawcę krajowego w sposób dorozumiany, lecz konieczny do ustanowienia uogólnionego i niezróżnicowanego obowiązku zatrzymywania danych przez operatorów świadczących usługi łączności elektronicznej, aby umożliwić organowi właściwemu w sprawach finansowych wykrywanie i karanie wykorzystywania informacji poufnych. Ponieważ, jak wynika z motywu 65 rozporządzenia nr 596/2014, zapisy te stanowią istotne, a niekiedy jedyne dowody przy wykrywaniu i udowadnianiu wykorzystywania informacji poufnych i manipulacji na rynku, taki obowiązek zatrzymywania jest niezbędny zarówno dla zapewnienia skuteczności czynności śledczych i ścigania prowadzonych przez wspomniany organ, a tym samym skuteczności art. 12 ust. 2 lit. a) i d) dyrektywy 2003/6 oraz art. 23 ust. 2 lit. h) rozporządzenia nr 596/2014, jak również dla spełnienia celów interesu ogólnego, którym służą te instrumenty, polegających na zapewnieniu integralności rynków finansowych Unii i wzmocnieniu zaufania inwestorów do tych rynków.

67 VD, SR, rząd polski i Komisja Europejska podnoszą natomiast, że przepisy te – jako że ograniczają się do określenia ram uprawnienia do żądania od podmiotów świadczących usługi łączności elektronicznej udostępniania „istniejących" zapisów danych o ruchu posiadanych przez tych operatorów – regulują jedynie kwestię dostępu do tych danych.

68 W tym względzie należy przypomnieć w pierwszej kolejności, że zgodnie z utrwalonym orzecznictwem przy dokonywaniu wykładni przepisu prawa Unii należy nie tylko odwołać się do jego brzmienia, lecz także wziąć pod uwagę jego kontekst oraz cele regulacji, której część on stanowi, a także uwzględnić w szczególności genezę tego uregulowania (zob. podobnie wyrok z dnia 17 kwietnia 2018 r., Egenberger, C-414/16, EU:C:2018:257, pkt 44).

69 Co się tyczy brzmienia przepisów, o których mowa w pytaniach pierwszych, należy stwierdzić, że podczas gdy art. 12 ust. 2 lit. d) dyrektywy 2003/6 odnosi się do uprawnienia organu właściwego w sprawach finansowych do „żądania wydania rejestrów połączeń i rejestrów przesyłu danych", art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014 odsyła do uprawnienia tego organu do żądania wydania z jednej strony „zapisów danych o ruchu przechowywanych przez firmy inwestycyjne, instytucje kredytowe lub instytucje finansowe", a z drugiej strony „żądania, w zakresie dozwolonym prawem krajowym, wydania istniejących zapisów danych o ruchu przechowywanych przez operatora telekomunikacyjnego".

70 Z brzmienia tych przepisów wynika więc jednoznacznie, że ograniczają się one do zakreślenia ram uprawnienia wspomnianego organu do „żądania" lub „żądania wydania" danych, którymi dysponują ci operatorzy, co odpowiada dostępowi do tych danych. Ponadto odwołanie się do zapisów „istniejących", takich jak „przechowywane" przez wspomnianych operatorów, sugeruje, że prawodawca Unii nie zamierzał regulować możliwości ustanowienia przez ustawodawcę krajowego obowiązku przechowywania takich zapisów.

71 W tym względzie należy przypomnieć, że zgodnie z utrwalonym orzecznictwem wykładnia przepisu prawa Unii nie może skutkować pozbawieniem wszelkiej skuteczności jasnego i precyzyjnego brzmienia tego przepisu. W związku z tym, jeżeli znaczenie przepisu prawa Unii wynika jednoznacznie z samego jego brzmienia, Trybunał nie może odejść od tej wykładni (wyrok z dnia 25 stycznia 2022 r., VYSOČINA WIND, C-181/20, EU:C:2022:51, pkt 39 i przytoczone tam orzecznictwo).

72 Za wykładnią przedstawioną w pkt 70 niniejszego wyroku przemawia zarówno kontekst, w jaki wpisują się art. 12 ust. 2 lit. a) i d) dyrektywy 2003/6 i art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014, jak i cele uregulowania, którego część stanowią te przepisy.

73 Co się tyczy kontekstu, w jaki wpisują się te przepisy, należy zauważyć, że o ile zgodnie z art. 12 ust. 1 dyrektywy 2003/6 i art. 23 ust. 3 rozporządzenia nr 596/2014 interpretowanym w świetle motywu 62 tego rozporządzenia prawodawca Unii zamierzał zobowiązać państwa członkowskie do podjęcia niezbędnych środków w celu zapewnienia, aby organy właściwe w sprawach finansowych dysponowały zestawem narzędzi, kompetencji i odpowiednich zasobów, jak również uprawnień nadzorczych i śledczych niezbędnych do zapewnienia skuteczności ich zadań, o tyle przepisy te nie mówią nic o tym, czy państwa członkowskie mogą w tym celu nałożyć na operatorów usług łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, ani o warunkach, na jakich dane te powinny być zatrzymywane przez tych operatorów w celu przekazania ich w stosownych przypadkach właściwym organom.

74 W drodze art. 12 ust. 2 dyrektywy 2003/6 i art. 23 ust. 2 rozporządzenia nr 596/2014 prawodawca Unii zamierzał jedynie przyznać organowi właściwemu w sprawach finansowych, w celu zapewnienia skuteczności jego zadań śledczych i nadzorczych, klasyczne uprawnienia śledcze, takie jak te, które umożliwiają temu organowi dostęp do dokumentów, przeprowadzanie inspekcji i przeszukań, a także wydawanie nakazów lub zakazów wobec osób podejrzanych o popełnienie naruszeń w postaci nadużyć na rynku, do których zalicza się w szczególności wykorzystywanie informacji poufnych.

75 Ponadto należy stwierdzić, że przepisy rozporządzenia nr 596/2014, które szczegółowo regulują kwestię zatrzymywania danych, a mianowicie art. 11 ust. 5 akapit ostatni, ust. 6 akapit drugi, ust. 8 i ust. 11 lit. c), art. 17 ust. 1 akapit pierwszy, art. 18 ust. 5 oraz art. 28 tego rozporządzenia, nakładają taki obowiązek zatrzymywania wyłącznie na podmioty finansowe wymienione w art. 23 ust. 2 lit. g) tego rozporządzenia i dotyczą zatem wyłącznie danych odnoszących się do transakcji finansowych i usług świadczonych przez te konkretne podmioty.

76 Co się tyczy celów realizowanych przez rozpatrywane uregulowanie, należy zauważyć, że z motywów 2 i 12 dyrektywy 2003/6 z jednej strony oraz z art. 1 rozporządzenia nr 596/2014 interpretowanego w świetle jego motywów 2 i 24 z drugiej strony wynika, iż celem tych instrumentów jest zapewnienie integralności rynków finansowych Unii i zwiększenie zaufania inwestorów do tych rynków, które to zaufanie opiera się w szczególności na tym, że będą one traktowane na równych zasadach i chronione przed bezprawnym wykorzystywaniem informacji poufnych. Zakaz wykorzystywania informacji poufnych ustanowiony w art. 2 ust. 1 dyrektywy 2003/6 i w art. 8 ust. 1 rozporządzenia nr 596/2014 ma zatem na celu zagwarantowanie równości stron transakcji giełdowej poprzez uniknięcie sytuacji, w której jedna z nich, posiadająca informacje poufne i znajdująca się w związku z tym w uprzywilejowanej sytuacji w stosunku do pozostałych inwestorów, osiąga w ten sposób korzyść ze szkodą dla innych inwestorów, którzy nie posiadają takich informacji (zob. podobnie wyrok z dnia 15 marca 2022 r., Autorité des marchés financières, C-302/20, EU:C:2022:190, pkt 43, 65, 77 i przytoczone tam orzecznictwo).

77 O ile zgodnie z motywem 65 rozporządzenia nr 596/2014 zapisy danych o połączeniach stanowią istotny, a niekiedy jedyny dowód pozwalający na wykrycie i udowodnienie wykorzystywania informacji poufnych lub manipulacji na rynku, o tyle motyw ten odnosi się jedynie do zapisów „przechowywanych” przez operatorów usług łączności elektronicznej, a także do uprawnienia organu właściwego w sprawach finansowych do „zażądania” od tych operatorów udostępnienia „istniejących” danych. Z motywu tego nie wynika zatem w żaden sposób, że prawodawca Unii

zamierzał w drodze tego rozporządzenia przyznać państwom członkowskim uprawnienie do nałożenia na operatorów świadczących usługi łączności elektronicznej uogólnionego obowiązku zatrzymywania danych.

78 W świetle powyższych rozważań należy stwierdzić, że ani dyrektywy 2003/6, ani rozporządzenia nr 596/2014 nie można interpretować w ten sposób, że mogą one stanowić podstawę prawną ogólnego obowiązku zatrzymywania zapisów danych o ruchu przechowywanych przez operatorów usług łączności elektronicznej w celu wykonywania uprawnień powierzonych organowi właściwemu w sprawach finansowych na podstawie dyrektywy 2003/6 i rozporządzenia nr 596/2014.

79 W drugiej kolejności należy przypomnieć, że – jak wskazał zasadniczo rzecznik generalny w pkt 53 i 61 opinii – dyrektywa 2002/58 jest uregulowaniem stanowiącym punkt odniesienia w dziedzinie zatrzymywania i, bardziej ogólnie, przetwarzania danych osobowych w sektorze łączności elektronicznej, wobec czego wykładnia dokonana przez Trybunał w świetle tej dyrektywy stosuje się również do zapisów danych o ruchu przechowywanych przez operatorów usług łączności elektronicznej, których organy właściwe w sprawach finansowych w rozumieniu art. 11 dyrektywy 2003/6 i art. 22 rozporządzenia nr 596/2014 mogą zażądać od tych operatorów.

80 Zgodnie bowiem z art. 1 ust. 1 dyrektywy 2002/58 przewiduje ona między innymi harmonizację przepisów krajowych wymaganych do zapewnienia równego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej, który obejmuje również sektor telekomunikacji.

81 Ponadto z art. 3 tej dyrektywy wynika, że ma ona zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii, włącznie z publicznymi sieciami łączności obsługującymi urządzenia służące do gromadzenia danych i identyfikacji. W konsekwencji należy uznać, że dyrektywa ta reguluje działalność dostawców takich usług, wśród których znajdują się między innymi operatorzy telekomunikacyjni (zob. podobnie 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 93 i przytoczone tam orzecznictwo).

82 W świetle powyższych rozważań należy uznać, jak stwierdza zasadniczo rzecznik generalny w pkt 62 i 63 opinii, że ocena zgodności z prawem przetwarzania zapisów przechowywanych przez operatorów usług łączności elektronicznej w rozumieniu art. 12 ust. 2 lit. d) dyrektywy 2003/6 i art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014 powinna być dokonywana w świetle przesłanek przewidzianych w dyrektywie 2002/58, a także wykładni tej dyrektywy w orzecznictwie Trybunału.

83 Wykładnię tę potwierdza art. 3 ust. 1 pkt 27 rozporządzenia nr 596/2014 w zakresie, w jakim przewiduje on, że zapisy danych o ruchu dla celów tego rozporządzenia oznaczają zapisy w rozumieniu art. 2 akapit drugi lit. b) dyrektywy 2002/58.

84 Ponadto zgodnie z motywem 44 dyrektywy 2003/6, jak również z motywami 66 i 77 rozporządzenia nr 596/2014, cele tych aktów powinny być realizowane z poszanowaniem praw podstawowych i zasad uznanych w karcie, w tym prawa do prywatności. W tym względzie prawodawca Unii wyraźnie wskazał w motywie 66 rozporządzenia nr 596/2014, że w celu wykonywania uprawnień przyznanych organowi właściwemu w sprawach finansowych na mocy

tego rozporządzenia, które mogą stanowić poważną ingerencję w prawo do poszanowania życia prywatnego i rodzinnego, miru domowego i komunikowania się, państwa członkowskie powinny dysponować wystarczającymi i skutecznymi zabezpieczeniami przed nadużyciami, na przykład w formie wymogu uzyskania w stosowanych przypadkach uprzedniej zgody organów sądowych danego państwa członkowskiego. Państwa członkowskie powinny dać właściwym organom możliwość wykonywania takich naruszających prywatność uprawnień wyłącznie w zakresie niezbędnym do właściwego przeprowadzenia czynności nadzorczych w poważnych przypadkach, w których nie istnieją równoważne środki pozwalające na uzyskanie takich samych rezultatów. Wynika z tego, że stosowanie środków regulowanych przez dyrektywę 2003/6 i rozporządzenie nr 596/2014 nie może w żadnym razie naruszać ochrony danych osobowych przyznanej na podstawie dyrektywy 2002/58 (zob. podobnie i analogicznie wyroki: z dnia 29 stycznia 2008 r., Promusicae, C-275/06, EU:C:2008:54, pkt 57; z dnia 17 czerwca 2021 r., M.I.C.M., C-597/19, EU:C:2021:492, pkt 124 i przytoczone tam orzecznictwo).

85 W konsekwencji art. 12 ust. 2 lit. a) i d) dyrektywy 2003/6 oraz art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014 należy interpretować w ten sposób, że nie zezwalają one na uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji w celu zwalczania przestępstw w postaci nadużyć na rynku, a w szczególności wykorzystywania informacji poufnych, przy czym zgodność z prawem Unii przepisów krajowych przewidujących takie zatrzymywanie należy oceniać na podstawie art. 15 ust. 1 dyrektywy 2002/58, odczytywanego w świetle art. 7, 8, 11 i art. 52 ust. 1 karty, tak jak interpretowany jest on w orzecznictwie Trybunału.

86 Co się tyczy badania zgodności takiego uregulowania krajowego z tymi ostatnimi przepisami, należy przypomnieć, że – jak wynika zasadniczo z łącznej lektury pkt 53, 54 i 58 niniejszego wyroku – o ile głównym przepisem leżącym u podstaw odesłań prejudycjalnych rozpatrywanych w niniejszym postępowaniu jest art. L. 621-10 CMF, na podstawie którego AMF zażądał od operatorów usług łączności elektronicznej przekazania danych o ruchu dotyczących połączeń telefonicznych wykonanych przez VD i SR, na podstawie których postawiono ich w stan oskarżenia, o tyle należy jednak stwierdzić, że – jak wskazał rzecznik generalny w pkt 42 opinii – to art. L. 34-1 CPCE i art. R. 10-13 CPCE są „kluczowymi przepisami" w ramach stosowania tegoż art. L. 621-10 CMF.

87 Z wyjaśnień przedstawionych przez sąd odsyłający, streszczonych w pkt 27, 37 i 38 niniejszego wyroku, wynika bowiem z jednej strony, że śledczy AMF zgromadzili rozpatrywane dane o ruchu na podstawie art. L. 34-1 CPCE, w brzmieniu mającym zastosowanie do sporów w postępowaniach głównych, którego ust. III poddał zasadniczy obowiązek przewidziany w ust. II, zgodnie z którym operatorzy świadczący usługi łączności elektronicznej muszą usunąć lub poddać anonimizacji wszelkie dane o ruchu, szeregowi wyjątków, w tym wyjątkowi dotyczącemu „celów wykrywania, stwierdzania i ścigania przestępstw kryminalnych". W odniesieniu do tych szczególnych celów operacje usuwania lub anonimizacji pewnej liczby danych były odroczone o rok.

88 Z drugiej strony sąd ten wyjaśnia, że pięć kategorii danych, których dotyczy art. L. 34-1 ust. III CPCE, w brzmieniu znajdującym zastosowanie w sporach w postępowaniach głównych, to kategorie wymienione w art. R. 10-13 CPCE, a mianowicie informacje umożliwiające identyfikację użytkownika, dane dotyczące używanych końcowych urządzeń komunikacyjnych, charakterystyka techniczna, jak również data, godzina i czas trwania każdego komunikatu, dane dotyczące żądanych lub używanych usług dodatkowych i ich dostawców i w końcu dane umożliwiające identyfikację odbiorcy lub odbiorców połączenia. Ponadto z art. R. 10-13 ust. II CPCE,

w brzmieniu mającym zastosowanie do sporów w postępowaniach głównych, wynika, że w przypadku usług telefonicznych dani operatorzy mogli również zatrzymywać dane umożliwiające identyfikację pochodzenia i lokalizacji połączenia.

89 Wynika z tego, że uregulowanie rozpatrywane w postępowaniach głównych odnosi się do wszystkich środków łączności telefonicznej i obejmuje wszystkich użytkowników tych środków, bez zróżnicowania czy wprowadzania wyjątku w tym względzie. Ponadto uregulowanie to zobowiązuje operatorów usług łączności elektronicznej do zatrzymywania w szczególności danych niezbędnych do ustalenia źródła połączenia i jego przeznaczenia, określenia daty, godziny, czasu trwania i rodzaju połączenia, wskazania wykorzystanego urządzenia komunikacyjnego, a także ustalenia położenia urządzeń końcowych i umiejscowienia połączeń, to jest danych, wśród których znajdują się w szczególności nazwisko i adres użytkownika, jak też numery telefonu nadawcy i odbiorcy połączenia.

90 W związku z tym dane, które zgodnie z rozpatrywanym uregulowaniem krajowym powinny być zatrzymywane na okres jednego roku, o ile nie obejmują treści danego połączenia, pozwalają w szczególności ustalić, kim jest osoba, z którą użytkownik środka komunikacji telefonicznej się łączył, i za pomocą jakiego środka nawiązano to połączenie, określić datę, godzinę i czas trwania połączeń oraz miejsce, z którego zostały nawiązane, oraz poznać lokalizację urządzeń końcowych bez konieczności realizacji połączenia. Co więcej, oferują one możliwość określenia częstotliwości połączeń użytkownika z pewnymi osobami w danym okresie. Należy więc uznać, że całokształt tych danych może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają. W szczególności dane te dają możność ustalenia profilu danych osób, która to informacja jest z punktu widzenia prawa do poszanowania życia prywatnego równie newralgiczna co sama treść komunikatów (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 45 i przytoczone tam orzecznictwo).

91 Jeśli chodzi o zamierzone cele, należy zauważyć, że rozpatrywane uregulowanie dotyczy – obok innych celów – wykrywania, stwierdzania i ścigania przestępstw kryminalnych, w tym nadużyć na rynku, do których zalicza się wykorzystywanie informacji poufnych.

92 W świetle okoliczności przedstawionych w pkt 86–91 niniejszego wyroku należy stwierdzić, że w rozpatrywanym uregulowaniu ustawodawca krajowy przewidział, w szczególności dla celów wykrywania, stwierdzania i ścigania przestępstw kryminalnych oraz zwalczania przestępczości, uogólnione i niezróżnicowane zatrzymywanie danych o ruchu przez okres jednego roku od dnia zapisu.

93 Tymczasem w szczególności z pkt 140–168 wyroku 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), a także z pkt 59–101 wyroku z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in. (C-140/20, EU:C:2022:258), wynika, że takie zatrzymywanie nie może być uzasadnione takimi celami na podstawie art. 15 ust. 1 dyrektywy 2002/58.

94 Z powyższego wynika, że uregulowanie krajowe, takie jak rozpatrywane w postępowaniach głównych, nakładające na operatorów usług łączności elektronicznej obowiązek zatrzymywania zapobiegawczo w celu zwalczania naruszeń w postaci nadużyć na rynku, do których zalicza się wykorzystywanie informacji poufnych, w sposób uogólniony i niezróżnicowany danych o ruchu

wszystkich użytkowników środków łączności elektronicznej, bez jakiegokolwiek zróżnicowania w tym względzie lub ustanowienia wyjątków i bez wykazania wymaganego związku, zgodnie z orzecznictwem przywołanym w poprzednim punkcie niniejszego wyroku, między danymi, które mają być zatrzymywane, a realizowanym celem, wykracza poza granice tego, co ściśle konieczne, i nie może być uznane za uzasadnione w społeczeństwie demokratycznym, jak tego wymaga art. 15 ust. 1 dyrektywy 2002/58, interpretowany w świetle art. 7, 8, 11 i art. 52 ust. 1 karty (zob. podobnie i analogicznie wyrok z dnia 6 października 2020 r., Privacy International, C-623/17, EU:C:2020:790, pkt 81).

95 W świetle powyższych rozważań na pierwsze pytania w sprawach C-339/20 i C-397/20 należy odpowiedzieć, że art. 12 ust. 2 lit. a) i d) dyrektywy 2003/6 oraz art. 23 ust. 2 lit. g) i h) rozporządzenia nr 596/2014, w związku z art. 15 ust. 1 dyrektywy 2002/58 oraz w świetle art. 7, 8, 11 i art. 52 ust. 1 karty, należy interpretować w ten sposób, że sprzeciwiają się one środkom ustawodawczym przewidującym zapobiegawczo w celu zwalczania przestępstw polegających na nadużyciach na rynku, do których zalicza się wykorzystywanie informacji poufnych, ogólne i niezróżnicowane zatrzymywanie danych o ruchu przez rok od dnia ich zapisu.

W przedmiocie pytań drugiego i trzeciego

96 Poprzez pytania drugie i trzecie w niniejszych sprawach, które należy rozpatrzyć łącznie, sąd odsyłający dąży zasadniczo do ustalenia, czy prawo Unii należy interpretować w ten sposób, że sąd krajowy może na podstawie prawa krajowego ograniczyć w czasie skutki stwierdzenia nieważności w odniesieniu do krajowych przepisów ustawowych, które z jednej strony nakładają na operatorów świadczących usługi łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, a z drugiej strony pozwalają na przekazywanie tych danych organowi właściwemu w sprawach finansowych bez uprzedniego zezwolenia sądu lub niezależnego organu administracyjnego, ze względu na niezgodność tych przepisów z art. 15 ust. 1 dyrektywy 2002/58 interpretowanego w świetle karty.

97 Na wstępie należy przypomnieć, że zasada pierwszeństwa prawa Unii ustanawia prymat prawa Unii nad prawem państw członkowskich. Zasada ta nakłada zatem na wszystkie organy państw członkowskich obowiązek zapewnienia pełnej skuteczności różnych norm prawa Unii, a prawo państw członkowskich nie może mieć wpływu na skuteczność przyznaną tym różnym normom na terytorium wspomnianych państw. Zgodnie z tą zasadą, w braku możliwości dokonania wykładni ustawodawstwa krajowego zgodnej z wymogami prawa Unii, sąd krajowy, do którego należy w ramach jego kompetencji stosowanie przepisów prawa Unii, jest zobowiązany zapewnić pełną skuteczność tych przepisów, w razie konieczności odstępując z własnej inicjatywy od stosowania wszelkich sprzecznych z nim przepisów prawa krajowego, nawet późniejszych, bez konieczności żądania lub oczekiwania na ich uprzednie usunięcie w drodze ustawodawczej lub w ramach innej procedury konstytucyjnej (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 118 i przytoczone tam orzecznictwo).

98 Jedynie Trybunał może w drodze wyjątku, kierując się nadrzędnymi względami pewności prawa, tymczasowo zawiesić wywierany przez prawo Unii skutek w postaci uchylenia przepisów prawa krajowego sprzecznych z prawem Unii. Takie ograniczenie w czasie skutków wykładni prawa Unii dokonanej przez Trybunał może zostać orzeczone jedynie w samym wyroku, w którym Trybunał rozstrzyga w przedmiocie wykładni, o którą się do niego zwrócono. Do naruszenia pierwszeństwa i jednolitego stosowania prawa Unii doszłoby, gdyby sądy krajowe były

uprawnione do przyznania, choćby tymczasowo, przepisom krajowym pierwszeństwa przed prawem Unii, z którym te przepisy są sprzeczne (wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 119 i przytoczone tam orzecznictwo).

99 Prawdą jest, iż w sprawie dotyczącej zgodności z prawem środków przyjętych z naruszeniem ustanowionego w prawie Unii obowiązku przeprowadzenia uprzedniej oceny oddziaływania przedsięwzięcia na środowisko i na teren chroniony Trybunał uznał, że sąd krajowy może wyjątkowo utrzymać w mocy skutki takich środków, w przypadku gdy prawo krajowe na to zezwala, jeżeli to utrzymanie w mocy jest uzasadnione nadrzędnymi względami związanymi z koniecznością uniknięcia rzeczywistego i poważnego zagrożenia polegającego na przerwaniu dostaw energii elektrycznej w danym państwie członkowskim, któremu nie można zaradzić za pomocą innych środków i rozwiązań alternatywnych, w szczególności w ramach rynku wewnętrznego, przy czym wspomniane utrzymanie w mocy może obejmować jedynie okres ściśle niezbędny do usunięcia tej niezgodności z prawem (zob. podobnie wyrok z dnia 29 lipca 2019 r., Inter-Environnement Wallonie i Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, pkt 175, 176, 179, 181).

100 Niemniej, w przeciwieństwie do pominięcia obowiązku proceduralnego takiego jak uprzednia ocena oddziaływania przedsięwzięcia, które wpisuje się w specyficzną dziedzinę ochrony środowiska, naruszenie art. 15 ust. 1 dyrektywy 2002/58, w związku z art. 7, 8, 11 i art. 52 ust. 1 karty, nie może być przedmiotem konwalidacji w drodze procedury analogicznej do tej, o której mowa w poprzednim punkcie (zob. podobnie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 121 i przytoczone tam orzecznictwo).

101 Utrzymanie w mocy skutków przepisów krajowych takich jak rozpatrywane w postępowaniach głównych oznaczałoby bowiem, że przepisy te w dalszym ciągu nakładają na dostawców usług łączności elektronicznej obowiązki, które są sprzeczne z prawem Unii i które powodują poważną ingerencję w prawa podstawowe osób, których dane są zatrzymywane (zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 122 i przytoczone tam orzecznictwo).

102 W konsekwencji sąd odsyłający nie może ograniczyć w czasie skutków stwierdzenia nieważności, którego ma on dokonać na podstawie prawa krajowego w odniesieniu do uregulowania krajowego rozpatrywanego w postępowaniu głównym (zob. analogicznie wyrok z dnia 5 kwietnia 2022 r., Commissioner of An Garda Síochána i in., C-140/20, EU:C:2022:258, pkt 123 i przytoczone tam orzecznictwo).

103 Należy ponadto uściślić, że ograniczenia w czasie skutków przyjętej wykładni nie dokonano w wyrokach z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (C-203/15 i C-698/15, EU:C:2016:970) i 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), w związku z czym, zgodnie z orzecznictwem przypomnianym w pkt 98 niniejszego wyroku, nie może ono nastąpić w wyroku Trybunału późniejszym od tych wyroków.

104 Wreszcie, biorąc pod uwagę fakt, że sąd odsyłający rozpatruje wnioski o uznanie za niedopuszczalne dowodów uzyskanych na podstawie danych o ruchu z tego względu, że rozpatrywane przepisy krajowe są sprzeczne z prawem Unii zarówno w odniesieniu do zatrzymywania danych, jak i dostępu do nich, należy ustalić wpływ stwierdzenia ewentualnej niezgodności art. L. 621-10 CMF, w brzmieniu mającym zastosowanie do okoliczności

faktycznych w postępowaniach głównych, z art. 15 ust. 1 dyrektywy 2002/58, w świetle art. 7, 8, 11 i art. 52 ust. 1 karty, na dopuszczalność dowodów podniesionych przeciwko VD i SR w ramach postępowań głównych.

105 W tym względzie wystarczy odesłać do orzecznictwa Trybunału, a w szczególności do zasad przypomnianych w pkt 41–44 wyroku z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej) (C-746/18, EU:C:2021:152), z którego wynika, że dopuszczalność ta jest zgodnie z zasadą autonomii proceduralnej państw członkowskich kwestią prawa krajowego, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

106 Co się tyczy tej ostatniej zasady, należy przypomnieć, że nakłada ona na krajowy sąd karny obowiązek nieuwzględniania informacji i dowodów uzyskanych w drodze uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji niezgodnego z prawem Unii lub też w drodze dostępu właściwego organu do tych danych z naruszeniem tego prawa w ramach postępowania karnego wszczętego przeciwko osobom podejrzanym o popełnienie przestępstw, jeżeli osoby te nie są w stanie skutecznie ustosunkować się do tych informacji i dowodów, należących do dziedziny niepodlegającej rozpoznaniu przez sąd i mogących mieć decydujący wpływ na ocenę okoliczności faktycznych [zob. podobnie wyrok z dnia 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C-746/18, EU:C:2021:152, pkt 44 i przytoczone tam orzecznictwo].

107 W świetle powyższych rozważań na pytania drugie i trzecie w niniejszych sprawach należy odpowiedzieć, że prawo Unii należy interpretować w ten sposób, iż sprzeciwia się ono temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego na mocy prawa krajowego ma on dokonać w odniesieniu do przepisów krajowych, które z jednej strony nakładają na operatorów świadczących usługi łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, a z drugiej strony pozwalają na przekazywanie tych danych organowi właściwemu w sprawach finansowych bez uprzedniego zezwolenia sądu lub niezależnego organu administracyjnego, ze względu na niezgodność tych przepisów z art. 15 ust. 1 dyrektywy 2002/58 interpretowanym w świetle karty. Dopuszczalność dowodów uzyskanych na podstawie krajowych przepisów ustawowych niezgodnych z prawem Unii podlega, zgodnie z zasadą autonomii proceduralnej państw członkowskich, prawu krajowemu, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.

W przedmiocie kosztów

108 Dla stron w postępowaniach głównych niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed sądem odsyłającym, do niego zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniach głównych, nie podlegają zwrotowi.

Z powyższych względów Trybunał (wielka izba) orzeka, co następuje:

1) **Artykuł 12 ust. 2 lit. a) i d) dyrektywy 2003/6/WE Parlamentu Europejskiego i Rady z dnia 28 stycznia 2003 r. w sprawie wykorzystywania poufnych informacji i manipulacji na rynku (nadużyć na rynku) oraz art. 23 ust. 2 lit. g) i h) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenia w sprawie nadużyć na rynku) i uchylającego dyrektywę 2003/6**

i dyrektywy Komisji 2003/124/WE, 2003/125/WE, 2004/72/WE, w związku z 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 (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., oraz w świetle art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej

należy interpretować w ten sposób, że:

sprzeciwiają się one środkom ustawodawczym przewidującym zapobiegawczo w celu zwalczania przestępstw polegających na nadużyciach na rynku, do których zalicza się wykorzystywanie informacji poufnych, ogólne i niezróżnicowane zatrzymywanie danych o ruchu przez rok od dnia ich zapisu.

2) **Prawo Unii należy interpretować w ten sposób, że sprzeciwia się ono temu, by sąd krajowy ograniczył w czasie skutki stwierdzenia nieważności, którego na mocy prawa krajowego ma on dokonać w odniesieniu do przepisów krajowych, które z jednej strony nakładają na operatorów świadczących usługi łączności elektronicznej uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu, a z drugiej strony pozwalają na przekazywanie tych danych organowi właściwemu w sprawach finansowych bez uprzedniego zezwolenia sądu lub niezależnego organu administracyjnego, ze względu na niezgodność tych przepisów z art. 15 ust. 1 dyrektywy 2002/58, zmienionej dyrektywą 2009/136, interpretowanym w świetle Karty praw podstawowych Unii Europejskiej. Dopuszczalność dowodów uzyskanych na podstawie krajowych przepisów ustawowych niezgodnych z prawem Unii podlega, zgodnie z zasadą autonomii proceduralnej państw członkowskich, prawu krajowemu, z zastrzeżeniem poszanowania w szczególności zasad równoważności i skuteczności.**

Podpisy