

OPINIA RZECZNIKA GENERALNEGO  
PEDRA CRUZA VILLALÓNA  
przedstawiona w dniu 14 kwietnia 2011 r.<sup>1</sup>

Spis treści

I — Wprowadzenie .....	I - 11964
II — Ramy prawne .....	I - 11967
A — Prawo Unii .....	I - 11967
1. Uregulowania dotyczące ochrony własności intelektualnej .....	I - 11967
a) Dyrektywa 2001/29 w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym ...	I - 11967
b) Dyrektywa 2004/48 w sprawie egzekwowania praw własności inte- lektualnej .....	I - 11968
2. Uregulowania dotyczące ochrony danych osobowych .....	I - 11969
a) Dyrektywa 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych .....	I - 11969
b) Dyrektywa 2002/58 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej .....	I - 11969
3. Uregulowania dotyczące handlu elektronicznego: dyrektywa 2000/31 .....	I - 11970
B — Prawo krajowe .....	I - 11970

<sup>1</sup> — Język oryginału: francuski.

III — Okoliczności faktyczne leżące u podstaw sporu w postępowaniu krajowym i pytania prejudycjalne .....	I - 11971
A — Okoliczności faktyczne i przebieg postępowania krajowego .....	I - 11971
B — Pytania prejudycjalne .....	I - 11974
C — Postępowanie przez Trybunałem .....	I - 11974
IV — Analiza .....	I - 11975
A — Uwagi wstępne .....	I - 11975
1. Przeformułowanie pierwszego pytania: EKPC i karta .....	I - 11975
2. Struktura odpowiedzi .....	I - 11977
3. Podejście czteroetapowe .....	I - 11978
B — Środek, o którego zastosowanie wniesiono (nakaz zaprzestania) i wymagany „system” (filtrowanie i blokowanie) .....	I - 11979
1. System filtrowania i blokowania .....	I - 11980
a) Mechanizm „filtrowania” .....	I - 11980
b) Mechanizm „blokowania” .....	I - 11982
2. Cechy środka w postaci nakazania .....	I - 11982
a) „Bez ograniczeń w czasie”: zakres stosowania środka <i>ratione temporis</i> .....	I - 11983
b) „Wszystkich połączeń elektronicznych, zarówno wchodzących, jak i wychodzących”: zakres stosowania środka <i>ratione materiae</i> .....	I - 11983
c) „W stosunku do wszystkich swoich klientów”: zakres stosowania środka <i>ratione personae</i> .....	I - 11984
d) „In abstracto i w celach zapobiegawczych”: funkcja zapobiegawcza i odstraszająca środka, o którego zastosowanie wniesiono .....	I - 11985
e) „Na wyłączny koszt”: obciążenie kosztami związanym z wykonaniem środka, o którego zastosowanie wniesiono .....	I - 11985
3. Wniosek pośredni .....	I - 11986

C — Kwalifikacja środka w świetle dyrektyw i art. 7, 8 i 11 karty: „ograniczenie” w rozumieniu art. 52 ust. 1 karty .....	I - 11988
1. „Interpretowane w szczególności w świetle art. 7 i 8 karty”: w przedmiocie poszanowania życia prywatnego i prawa do ochrony danych osobowych .....	I - 11989
a) Ochrona danych osobowych (art. 8 karty) .....	I - 11990
b) Tajemnica połączeń elektronicznych (art. 7 karty) .....	I - 11992
2. „Interpretowane w szczególności w świetle art. 11 karty”: w przedmiocie zagwarantowania wolności wypowiedzi i prawa do informacji .....	I - 11993
3. Wniosek pośredni .....	I - 11995
D — W przedmiocie wymogów ograniczenia korzystania z praw i wolności zagwarantowanych przez kartę, a w szczególności wymogu dotyczącego „jakości ustawy” (art. 52 ust. 1 karty) .....	I - 11995
E — „Na podstawie samego przepisu ustawowego”: badanie ustawodawstwa krajowego w świetle wymogu dotyczącego „jakości ustawy” (art. 52 ust. 1 karty) ...	I - 12000
V — Wnioski .....	I - 12004

## I — Wprowadzenie

1. Niniejsza sprawa stwarza Trybunałowi możliwość rozważenia kwestii naruszeń

prawa autorskiego i praw pokrewnych w Internecie, nielegalnego pobierania dzieł chronionych, zjawiska powszechnie określanego „piractwem” dzieł muzycznych, kinematograficznych, audiowizualnych oraz literackich oraz analizy problemu walki posiadaczy

I - 11964

tych praw lub ich następców prawnych z tym, co określa się jako plagę światową<sup>2</sup>. Trybunał w szczególności musi przedstawić swe stanowisko w nierozpatrywanej dotychczas kwestii skuteczności z punktu widzenia prawa Unii Europejskiej niektórych środków technicznych mających na celu walkę z piractwem, które – chociaż ich niezawodność nie została w pełni potwierdzona i stale są poddawane postępowi technologicznemu i zmianie praktyk – określane są jako odpowiednia możliwa

odpowieź na naruszenia praw własności intelektualnej codziennie popełniane w sieci.

2 — Nie trzeba dodawać, że problem piractwa w Internecie jest globalny, co doprowadziło do udzielenia zróżnicowanych odpowiedzi przez sądy, w zależności od kraju [czy to w odniesieniu do samych użytkowników Internetu, czy też usługodawców, dostawców dostępu do Internetu, dostawców hostingów, wydawców programów peer-to-peer lub usług [zob. m.in. sprawy: Napster (A&M Records v. Napster, 239 F.3d 1004, 9th Cir. 201); Grokster (Metro-Goldwyn-Mayer Studios v. Grokster, 125 S. Ct. 2764, 2005) w Stanach Zjednoczonych, sprawa Kazaa w Australii (Kazaa [2005] F. C. A. 1242) lub także sprawa PirateBay w Szwecji (Svea hovrätt), 26 listopada 2010 r. (sprawa nr B 4041-09)], czasami ustawowych [na przykład we Francji ustawa zwana Hadopi, od nazwy Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet, którą ustanawia (ustawa nr 2009-669 z dnia 12 czerwca 2009 r. wspierająca rozpowszechnianie i ochronę twórczości w Internecie, JORF n° 135 z dnia 13 czerwca 2009 r., s. 9666); w Hiszpanii Disposición final cuadragésima tercera de la Ley 2/2011, de 4 de marzo, de Economía Sostenible (BOE z dnia 5 marca 2011 r., s. 25033)], czasami sui generis [zob. np. *Joint Memorandum of Understanding on an approach to reduce unlawful file sharing*, podpisane w 2008 r. przez głównych dostawców dostępu do Internetu w Zjednoczonym Królestwie i przedstawicieli branży twórczej], szeroko komentowanych, których przytoczenie tutaj, nawet skrótowne, nie jest możliwe, oraz że sama debata wokół tego problemu ma charakter światowy i szczególnie kontrowersyjny; w odniesieniu do podejścia francuskiego zob. m.in. E. Derieux, A. Granchet, *La lutte contre le téléchargement illégal, Lois DADVSI et HADOPI*, Lamy Axe Droit 2010; w odniesieniu do podejścia bronionego przez Komisję zob. jej pierwsze sprawozdanie w sprawie stosowania dyrektywy 2000/31/WÉ Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego, z dnia 21 listopada 2003 r. [COM(2003) 702 wersja ostateczna, pkt 4.7]; jej sprawozdanie w sprawie stosowania dyrektywy 2004/48/WÉ Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej, z dnia 22 grudnia 2010 r. [COM(2010) 779 wersja ostateczna, pkt 3.3], a także komunikat z dnia 16 lipca 2008 r. „Europejska strategia w zakresie praw własności przemysłowej” [COM(2008) 465 wersja ostateczna, pkt 5.3]. Spośród prac prowadzonych przez Radę Europy uwzględnić także rekomendację CM/Rec(2008)6 Komitetu Ministrów Państw Członkowskich z dnia 26 marca 2008 r. na temat środków mających na celu promowanie przestrzegania wolności wypowiedzi i informacji w świetle filtrów internetowych oraz wytyczne mające na celu wsparcie dostawców usług internetowych z lipca 2008 r.; zob. także sprawozdanie OECD przedstawione w dniu 13 grudnia 2005 r. przez Working Party on the Information Economy, Digital Broadband Content: Music, DSTI/ICCP/IE(2004)12/FINAL.

2. Udzielenie odpowiedzi na pytania pre-judycjalne postawione w niniejszej sprawie Trybunałowi wymaga dokonania wykładni zarówno złożonego zbioru przepisów aktów prawa wtórnego, jak i postanowień prawa pierwotnego, a zwłaszcza Karty praw podstawowych Unii Europejskiej<sup>3</sup>, w świetle europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności<sup>4</sup>. Należy jednakże na wstępie wskazać, że w ramach niniejszej opinii nie zostaną poruszone wszystkie kwestie prawne i problemy techniczne<sup>5</sup>, które wiążą się z rozpatrywanymi środkami. Opierając się na samym sformułowaniu pytań postawionych przez sąd odsyłający, a także na terminach, za pomocą których ten sąd wyjaśnia stan prawny i faktyczny toczącego się przed nim postępowania, postaram się

3 — Zwanej dalej „kartą”.

4 — Zwanej dalej „EKPC”.

5 — A zatem z prawnego punktu widzenia nie zostaną zbadane kwalifikacja prawna rozpatrywanych naruszeń oraz znaczenie wyjątków dotyczących kopiowania prywatnego; z technicznego punktu widzenia nie można przeanalizować ani technik bezprawnego pobierania, ani środków, które można podjąć, aby mu zapobiec. Ogólnie rzecz biorąc, odwołam się w tym względzie do bogatej doktryny, która jest wynikiem potrzeby zrozumienia tego zjawiska na płaszczyźnie prawnej.

przedstawić mu użyteczną odpowiedź, skupiając się na jej najistotniejszych aspektach.

3. W tym zakresie do Trybunału zwrócono się przede wszystkim o konkretne wskazanie sądowi odsyłającemu, czy z punktu widzenia prawa unijnego sąd krajowy może przyjąć środek taki jak ten, o którego zastosowanie wniesiono w toczącym się przed nim postępowaniu, nakazujący dostawcy dostępu do Internetu<sup>6</sup> wprowadzenie systemu filtrowania i blokowania połączeń elektronicznych. Tymczasem ponieważ środek, o którego zastosowanie wniesiono, posiada zakres w pełni odmienny dla – z jednej strony – tego ISP, a z drugiej strony – użytkowników usług tego ISP, a szerzej internautów, należy uwzględnić tę podwójną perspektywę, mimo że postawione pytanie dotyczy w szczególności praw użytkowników.

4. Na wstępie należy także wyjaśnić, że niniejsza sprawa odróżnia się od sprawy *Promusicae*<sup>7</sup>, mimo że ich ramy prawne oraz kontekst

ogólny zawierają ewidentne podobieństwa. O ile niniejsza sprawa wymaga, jak w ww. sprawie *Promusicae*, pogodzenia wymogów związanych z ochroną poszczególnych praw podstawowych, o tyle pomiędzy sprawami tymi istnieją różnice, które jak podkreśla sam sąd odsyłający, wykluczają, by wnioski zawarte w wyroku w sprawie *Promusicae*, a zwłaszcza zasada słusznej równowagi praw, którą ustanawia, były wystarczające do wydania przez niego orzeczenia. W sprawie *Promusicae* zwrócono się bowiem do ISP o ujawnienie w ramach postępowania sądowego tożsamości i adresu fizycznego osób zidentyfikowanych przez ich adres IP<sup>8</sup> oraz daty i godziny połączenia. Chodziło zatem o przekazanie w ramach postępowania sądowego znanych i zidentyfikowanych danych. W postępowaniu przed sądem odsyłającym zażądano natomiast od ISP, aby wprowadził system filtrowania połączeń elektronicznych i blokowania plików elektronicznych mogących naruszać prawo własności intelektualnej. Nie wymaga się zatem interwencji *a posteriori*, po stwierdzeniu naruszenia praw autorskich lub praw pokrewnych, ale interwencji *a priori*, w celu uniknięcia takiego naruszenia, a w szczególności w celu wprowadzenia systemu mogącego uniemożliwić w sposób prewencyjny każde przyszłe naruszenie prawa własności intelektualnej<sup>9</sup>, zgodnie z zasadami,

6 — Zwani dalej „ISP”.

7 — Wyrok z dnia 29 stycznia 2008 r. w sprawie C-275/06, Zb.Orz. s. I-271, opinia rzecznik generalnej J. Kokott z dnia 18 lipca 2007 r.

8 — Adres IP jest niepowtarzalnym adresem, którego używają urządzenia służące do komunikowania zgodnie z protokołem internetowym w celu identyfikowania się i komunikowania między sobą w sieci informatycznej; zob. w szczególności Jon Postel ed., Internet Protocol, RFC 791, September 1981, <http://www.faqs.org/rfcs/rfc791.html>. Zobacz także opinia rzecznik generalnej J. Kokott w ww. sprawie *Promusicae*, pkt 30, 31.

9 — Prawdę mówiąc o ile, jak przedstawię, wymaga się od danego ISP, aby wprowadził rozwiązanie „zapobiegające” w zakresie walki z naruszeniami praw własności intelektualnej, o tyle jednak należy podkreślić, że jest on w niniejszym przypadku adresem nakazu przyjętego w odpowiedzi na stwierdzone naruszenia praw własności intelektualnej w ramach postępowania cywilnego.

w odniesieniu do których istnieje wiele niejasności, co przedstawię w dalszej części opinii.

5. Po przedstawieniu tych wyjaśnień naturalnie narzuca się jednak, że badanie sytuacji rozpatrywanej w postępowaniu krajowym należy przeprowadzić zasadniczo w kontekście praw podstawowych.

tyczących ochrony danych osobowych, i dyrektywy 2000/31/WE<sup>14</sup>, dotyczącej handlu elektronicznego, pomiędzy którymi istnieją złożone relacje. Ze względu na ten złożony charakter w części opinii dotyczącej ram prawnych sprawy przedstawię tylko przepisy niezbędne dla zrozumienia sporu w postępowaniu krajowym.

1. Uregulowania dotyczące ochrony własności intelektualnej

## II — Ramy prawne

### A — Prawo Unii

6. Do Trybunału skierowano przede wszystkim pytania w przedmiocie wykładni dyrektyw 2001/29/WE<sup>10</sup> i 2004/48/WE<sup>11</sup>, dotyczących ochrony własności intelektualnej, dyrektyw 95/46/WE<sup>12</sup> i 2002/58/WE<sup>13</sup>, do-

a) Dyrektywa 2001/29 w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym

7. Artykuł 8 dyrektywy 2001/29, zatytułowany „Sankcje i środki naprawcze”, stanowi:

„1. Państwa członkowskie przewidują stosowne sankcje i środki naprawcze w przypadku naruszenia praw i obowiązków wymienionych w niniejszej dyrektywie i podejmują wszelkie niezbędne środki w celu zapewnienia ich realizacji. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

10 — Dyrektywa Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. L 167, s. 10).

11 — Dyrektywa Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.U. L 157, s. 45; sprostowania: Dz.U. 2004, L 195, s. 16; Dz.U. 2007 L 204, s. 27).

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

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

14 — Dyrektywa Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego („dyrektywa o handlu elektronicznym”) (Dz.U. L 178, s. 1).

2. Każde państwo członkowskie podejmuje niezbędne środki w celu zapewnienia, aby podmiot praw autorskich, którego interesy zostaną naruszone przez czynności dokonane na jego terytorium, mógł wytoczyć powództwo o odszkodowanie i/lub wnioskować o wydanie nakazu i w miarę potrzeby, domagać się przepadku naruszonych dóbr, jak również urzędzeń, produktów lub części składowych określonych w art. 6 ust. 2.

3. Państwa członkowskie zapewnią, aby podmioty praw autorskich mogły wnioskować o wydanie nakazu przeciwko pośrednikom, których usługi są wykorzystywane przez stronę trzecią w celu naruszenia praw autorskich lub pokrewnych”.

b) Dyrektywa 2004/48 w sprawie egzekwowania praw własności intelektualnej

8. Artykuł 9 ust. 1 lit. a) dyrektywy 2004/48 stanowi:

„1. Państwa członkowskie zapewniają, że organy sądowe mogą, na żądanie wnioskodawcy: Niniejszy artykuł nie ma wpływu na możliwość wymagania od usługodawcy przez sąd lub organ administracyjny, zgodnie z systemem prawnym Państw Członkowskich, żeby przerwał on naruszenia prawa lub im zapobiegł.

a) wystawić przeciwko domniemanemu naruszającemu tymczasowy nakaz sądowy,

który ma zapobiec możliwym dalszym naruszeniom prawa własności intelektualnej, lub w razie kontynuowania domniemanych naruszeń tego prawa, tymczasowo tego zakazać i w miarę potrzeb poddać powtarzającej [okresowej] się karze pieniężnej, jeśli prawo krajowe takową przewiduje, lub w przypadku ich kontynuowania nakazać złożenie zabezpieczenia zapewniającego pokrycie strat poniesionych przez właściciela praw; na takich samych zasadach można również wystawić tymczasowy nakaz sądowy przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią do naruszania prawa własności intelektualnej; nakazy sądowe przeciwko pośrednikom, których usługi są wykorzystywane przez osobę trzecią do naruszania praw autorskich lub praw pokrewnych przewidzianych dyrektywą 2001/29/WE”.

9. Zgodnie z art. 11 dyrektywy 2004/48, zatytułowanym „Zakazy sądowe”:

„Państwa członkowskie zapewniają, że tam, gdzie podjęta została decyzja sądu stwierdzająca naruszenie prawa własności intelektualnej, organy sądowe mogą wydawać naruszającym zakaz kontynuacji naruszenia. Jeśli tak przewiduje prawo krajowe, niewypełnienie zakazu poddaje naruszającego, gdzie właściwe, powtarzalnej [okresowej] karze pieniężnej w celu zapewnienia zgodności z zakazem. Państwa członkowskie zapewniają też właścicielom [praw własności intelektualnej] możliwość składania wniosku o zakaz [wydanie

zakazu] wobec pośredników, z usług których korzysta strona trzecia do naruszania [przy naruszeniu] prawa własności intelektualnej, bez uszczerbku dla postanowień art. 8 ust. 3 dyrektywy 2001/29/WE”.

b) Dyrektywa 2002/58 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej

11. Artykuł 5 ust. 1 dyrektywy 2002/58, poświęcony poufności komunikacji, stanowi:

## 2. Uregulowania dotyczące ochrony danych osobowych

a) Dyrektywa 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

10. Artykuł 13 ust. 1 lit. g) dyrektywy 95/46 przewiduje:

„1. Państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianego w art. 6 ust. 1, art. 10, art. 11 ust. 1, art. 12 oraz 21, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia:

„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”.

12. Artykuł 15 ust. 1 dyrektywy 2002/58, który przewiduje stosowanie niektórych przepisów dyrektywy 95/46, stanowi:

[...]

g) ochrony osoby, której dane dotyczą, oraz praw i wolności innych osób”.

„Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu



praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. [1, 2, 3, 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/WE. W tym celu państwa członkowskie mogą między innymi uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej”.

3. Uregulowania dotyczące handlu elektronicznego: dyrektywa 2000/31

13. Artykuł 15 dyrektywy 2000/31, który zamyka sekcję IV, poświęconą odpowiedzialności usługodawców będących pośrednikami,

ustanawia zasadę braku ogólnego obowiązku w zakresie nadzoru w następujący sposób:

„1. Państwa członkowskie nie nakładają na usługodawców świadczących usługi określone w art. 12, 13 i 14 ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują, ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.

2. Państwa członkowskie mogą ustanowić w stosunku do usługodawców świadczących usługi społeczeństwa informacyjnego obowiązek niezwłocznego powiadamiania właściwych władz publicznych o rzekomych bezprawnych działaniach podjętych przez ich usługobiorców lub przez nich przekazanych informacjach lub obowiązek przekazywania właściwym władzom, na ich żądanie, informacji pozwalających na ustalenie tożsamości ich usługobiorców, z którymi mają umowy o przechowywanie”.

B — *Prawo krajowe*

14. Artykuł 87 § 1 loi du 30 juin 1994 relative au droit d’auteur et aux droits voisins (ustawa o prawie autorskim i prawach pokrewnych z dnia 30 czerwca 1994 r.)<sup>15</sup>, zmienionej

15 — *Moniteur belge* z dnia 27 lipca 1994 r., s. 19297.

ustawą z dnia 10 maja 2007 r. zapewniającą transpozycję art. 8 ust. 3 dyrektywy 2001/29 i art. 11 dyrektywy 2004/48, stanowi:

„Prezes tribunal de première instance i prezes tribunal de commerce [...] orzekają istnienie i nakazują zaprzestanie wszelkiego naruszenia praw autorskich lub praw pokrewnych.

Mogą oni również wydać nakaz zaprzestania przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią do naruszania praw autorskich lub pokrewnych”.

### **III — Okoliczności faktyczne leżące u podstaw sporu w postępowaniu krajowym i pytania prejudycjalne**

#### *A — Okoliczności faktyczne i przebieg postępowania krajowego*

15. Pismem procesowym z dnia 24 czerwca 2004 r. Société belge des auteurs compositeurs et éditeurs (Sabam) zwróciło się w trybie ustawy z dnia 30 czerwca 1994 r. o prawie autorskim i prawach pokrewnych do prezesa tribunal de première instance de Bruxelles (sądu pierwszej instancji w Brukseli), orzekającego w przedmiocie zastosowania środków tymczasowych, z wnioskiem o wydanie

nakazu zaprzestania określonych działań przez Scarlet Extended SA, będącą ISP<sup>16</sup>.

16. Sabam podniosło, że Scarlet, jako ISP, znajduje się w doskonałej pozycji, aby podjąć środki w celu spowodowania zaprzestania naruszeń prawa autorskiego dokonywanych przez jej klientów, internautów którzy nielegalnie pobierają dzieła zawarte w jej katalogu za pośrednictwem programów „peer-to-peer”, nie uiszczając opłat, co jest korzystne dla Scarlet, gdyż działanie takie może prowadzić do zwiększenia natężenia ruchu, a w związku z tym popytu na jej usługi.

17. Sabam przede wszystkim zażądało, aby stwierdzono istnienie naruszeń prawa autorskiego w odniesieniu do dzieł muzycznych zawartych w jego repertuarze, a w szczególności prawa do powielania i prawa do publicznego udostępniania, które wynikają z niedozwolonej wymiany, za pośrednictwem usług świadczonych przez Scarlet, elektronicznych plików muzycznych za pomocą programów peer-to-peer.

18. Następnie Sabam zażądało, by na Scarlet nałożono, pod groźbą okresowej kary pieniężnej, obowiązek spowodowania zaprzestania tych naruszeń poprzez uniemożliwienie lub zablokowanie wszelkich form wysyłania lub otrzymywania przez jej klientów za pośrednictwem programów peer-to-peer plików zawierających dzieła muzyczne bez zezwolenia podmiotów uprawnionych z tytułu praw autorskich.

<sup>16</sup> — Zwana dalej „Scarlet”.

19. Wreszcie Sabam zażądało od Scarlet, pod groźbą okresowej kary pieniężnej, przekazania w ciągu ośmiu dni od doręczenia orzeczenia, które zostanie wydane, opisu podjętych środków, publikacji tekstu na głównej stronie jej portalu internetowego, a także publikacji wspomnianego orzeczenia w dwóch wybranych przez nią dziennikach i tygodniku.

20. Orzeczeniem z dnia 26 listopada 2004 r. prezes tribunal de première instance de Bruxelles stwierdził istnienie zgłoszonych naruszeń prawa autorskiego. Jednakże przed wydaniem orzeczenia w przedmiocie wniosku o nakazanie zaprzestania naruszeń wyznaczył biegłego w celu zbadania, czy rozwiązania techniczne zaproponowane przez Sabam mogą być zrealizowane pod względem technicznym, czy umożliwiają filtrowanie wyłącznie bezprawnej wymiany plików elektronicznych i czy istnieją inne środki, za pomocą których można byłoby kontrolować używanie programów peer-to-peer i określić koszt rozpatrywanych środków.

21. W dniu 29 stycznia 2007 r. wyznaczony biegły przedłożył sprawozdanie, którego wnioski, przedstawione w postanowieniu odsyłającym, brzmią następująco:

„1. Sieć peer to peer jest przejrzystym środkiem pozwalającym na wymianę treści, niezależnym, zdecentralizowanym i wyposażonym w zaawansowane funkcje wyszukiwania i pobierania;

2. Z wyjątkiem rozwiązania proponowanego przez Audible Magic, wszystkie systemy zabezpieczeń mają uniemożliwić korzystanie z sieci peer to peer, niezależnie od treści, jakie są przekazywane;

3. Ponadto w perspektywie średnioterminowej (dwóch–trzech lat) nie da się zapewnić skuteczności działania systemów filtrujących aplikacje peer to peer ze względu na coraz szersze wykorzystanie kodowania w tego rodzaju aplikacjach;

4. System zabezpieczający proponowany przez spółkę Audible Magic jest jedynym, który próbuje rozwiązać konkretnie ten problem. System ten, przeznaczony w szczególności na potrzeby sektora oświaty, nie jest jednak z natury dostosowany do rozmiarów natężenia ruchu ISP. W związku z powyższym zastosowanie tej techniki przez ISP związane jest z wysokimi kosztami nabycia i eksploatacji w celu skompensowania tego niedostosowania;

5. Koszt ten należy ocenić w świetle okresu, przez jaki system będzie skuteczny, bowiem powyżej wspomniane kodowanie uczyni ten system również nieskutecznym w zakresie filtrowania przechodzącego ruchu;

6. Wewnętrzne metody dochodzenia, stosowane w ramach sieci peer to peer są trudniejsze do wdrożenia, ale dają lepsze wyniki. Metody te obejmują a priori tylko część wymiany plików, która jest niezgodna z prawem, i są w stanie uwzględnić kontekst, w jakim ta wymiana jest dokonywana;
7. Zresztą metody te nie są odporne ani wyraźnie mniej wrażliwe na kodowanie, ale naszym zdaniem stanowią najlepszą inwestycję w perspektywie średnio- i długoterminowej w celu zagwarantowania poszanowania praw autorskich z jednoczesnym poszanowaniem praw wszystkich użytkowników”.
22. W oparciu o to sprawozdanie biegłego prezes tribunal de première instance de Bruxelles wydał w dniu 29 czerwca 2007 r. drugi wyrok, w którym orzekł, że Scarlet ma doprowadzić do zaprzestania naruszeń praw autorskich, których istnienie zostało ustalone w wyroku z dnia 26 listopada 2004 r., poprzez uniemożliwienie przesyłania lub odbierania, w jakiegokolwiek formie, przez jej klientów plików elektronicznych zawierających utwory muzyczne z repertuaru Sabam za pomocą programów peer to peer, pod groźbą okresowej kary pieniężnej w wysokości 2500 EUR za każdy dzień w przypadku niewykonania przez Scarlet wyroku po upływie sześciu miesięcy.
23. W dniu 6 września 2007 r. Scarlet złożyła apelację od tego wyroku do Cour d'appel de Bruxelles (sądu apelacyjnego w Brukseli).
24. Pismem procesowym z dnia 7 grudnia 2007 r. Scarlet zwróciła się ponadto do preza tribunal de première instance de Bruxelles z wnioskiem o uchylenie, a co najmniej zawieszenie wykonania nałożonej na nią okresowej kary pieniężnej. Scarlet podniosła, że nie posiada fizycznej lub czasowej możliwości wykonania nakazu zaprzestania, ponieważ system Audible Magic nie działa i nie zostało ustalone, że dostawca dostępu do Internetu posiada techniczną możliwość filtrowania lub skutecznego blokowania ruchu peer-to-peer.
25. Prezes tribunal de première instance de Bruxelles oddalił ten wniosek postanowieniem z dnia 22 października 2008 r., stwierdzając, że skutek dewolutywny apelacji sprzeciwia się temu, by strony ponownie wносиły sprawę do rozparzenia przez ten sąd. Uznając, że rozwiązanie Audible Magic nie mogło zostać skutecznie wprowadzone w życie, stwierdził jednak, że Scarlet nie stosowała innych rozwiązań z zakresu filtrowania lub blokowania, a w związku z tym nie dowiodła, że nakaz zaprzestania nie mógł zostać wykonany. Niemniej jednak zawiesił on wykonanie okresowej kary pieniężnej do dnia 31 października 2008 r., aby umożliwić Scarlet wykorzystanie innych środków.

B — *Pytania prejudycjalne*

26. W tych okolicznościach Cour d'appel de Bruxelles postanowił zawiesić postępowanie i przedłożyć Trybunałowi następujące pytania prejudycjalne:

- „1. Czy dyrektywy 2001/29 i 2004/48, w związku z dyrektywami 95/46, 2000/31 i 2002/58, interpretowane w szczególności w świetle art. 8 i 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, pozwalają państwom członkowskim upoważnić sąd krajowy, który ma orzekać co do istoty sprawy i jedynie na podstawie przepisu stanowiącego, że »[sąd krajowy może] również wydać nakaz przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią do naruszania praw autorskich i pokrewnych«, do nakazania dostawcy dostępu do Internetu (w skrócie ISP) wprowadzenia, w stosunku do wszystkich swoich klientów, in abstracto i w celach zapobiegawczych, na wyłączny koszt ISP i bez ograniczeń w czasie, systemu filtrowania wszystkich połączeń elektronicznych, zarówno wchodzących, jak i wychodzących, przekazywanych za pośrednictwem jego usług, w szczególności przy zastosowaniu programów peer to peer, w celu zidentyfikowania w jego sieci przypadków przekazywania plików elektronicznych zawierających utwory muzyczne, kinematograficzne lub audiowizualne, co do których strona

powodowa rości sobie prawa, a następnie zablokowania transferu tych plików, bądź to na etapie próby ich pobrania, bądź na etapie ich wysłania?

2. W przypadku odpowiedzi twierdzącej na pytanie [pierwsze] – czy te dyrektywy nakładają na sąd krajowy mający orzekać w zakresie wniosku o wydanie nakazu przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią w celu naruszania prawa autorskiego, obowiązek zastosowania zasady proporcjonalności, w przypadku gdy sąd ten ma orzec co do skuteczności i efektu odstraszającego żądanego środka?».

C — *Postępowanie przez Trybunałem*

27. Scarlet, Sabam wspólnie z Belgian Entertainment Association Video (BEA Video) oraz Belgian Entertainment Association Video (BEA Music), podobnie jak Internet Service Provider Association (ISPA) oraz Królestwo Belgii, Republika Czeska, Królestwo Niderlandów, Rzeczpospolita Polska, Republika Finlandii oraz Komisja Europejska przedstawiły uwagi na piśmie.

28. Trybunał wysłuchał przedstawicieli Scarlet, Sabam, ISPA, a także Królestwa Belgii, Republiki Czeskiej, Republiki Włoskiej,

Królestwa Niderlandów, Rzeczypospolitej Polskiej oraz Komisji Europejskiej podczas rozprawy w dniu 13 stycznia 2011 r.

#### IV — Analiza

##### A — Uwagi wstępne

1. Przeformułowanie pierwszego pytania: EKPC i karta

29. Sąd odsyłający wskazuje, że jego pierwsze pytanie prejudycjalne dotyczy wykładni szeregu przepisów prawa wtórnego Unii „w świetle art. 8 i 10 EKPC”. W ten sposób może on z pewnością oprzeć się na art. 6 ust. 3 TUE, na mocy którego „[p]rawa podstawowe, zagwarantowane w [EKPC] [...], stanowią część prawa Unii jako zasady ogólne”. W tym zakresie konieczne jest jednak przedstawienie uwag wstępnych, w ramach których dokonam stosownego przeformułowania pytania.

30. Przede wszystkim tenże art. 6 TUE rozpoczyna się wyjaśnieniem w ust. 1 akapit pierwszy, że karta „ma taką samą moc prawną jak traktaty”, co Trybunał podkreślił w swych ostatnich orzeczeniach<sup>17</sup>. Ponieważ zatem prawa, wolności i zasady ustanowione w karcie mają, same z siebie, moc prawną, skądinąd nadrzędną, odwołanie do wspomnianych zasad ogólnych, pod warunkiem że te pierwsze można identyfikować z drugimi, nie jest już konieczne. Jest to pierwszy czynnik przemawiający na rzecz zbadania pytania raczej w świetle postanowień karty niż postanowień EKPC, *ceteris paribus*<sup>18</sup>.

31. Następnie art. 52 ust. 3 karty przewiduje, że „[w] zakresie w jakim zawiera [ona] prawa, które odpowiadają prawom zagwarantowanym w [EKPC], ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję”, uściślając że „[n]iniejsze postanowienie nie stanowi przeszkody, aby prawo Unii

17 — Zobacz m.in., jeśli chodzi o najnowsze wyroki, wyroki: z dnia 14 października 2010 r. w sprawie C-243/09 Fuß (pkt 66; z dnia 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09 Volker und Markus Schecke i Eifert, pkt 45 i nast.; a także w sprawach połączonych C-57/09 i C-101/09 B i D, pkt 78; z dnia 12 listopada 2010 r. w sprawie C-339/10 Asparuhov Estov, pkt 12; z dnia 23 listopada 2010 r. w sprawie C-145/09 Tsakouridis, pkt 52; z dnia 22 grudnia 2010 r. w sprawie DEB Deutsche Energiehandels- und Beratungsgesellschaft, pkt 30; w sprawie C-208/09 Sayn-Wittgenstein, pkt 52; w sprawach połączonych C-444/09 i C-456/09 Gavieiro Gavieiro i Iglesias Torres, pkt 75; a także w sprawie C-491/10 PPU Aguirre Zarraga; z dnia 1 marca 2011 r. w sprawie C-236/09 Association Belge des Consommateurs Test-Achats i in., pkt 16.

18 — Zobacz także podobnie opinia rzecznika generalnego Y. Bota z dnia 5 kwietnia 2011 r. w sprawie C-108/10 Scattolon.

przyznawało szerszą ochronę”<sup>19</sup>. Tymczasem w okolicznościach sporu w postępowaniu krajowym prawa zagwarantowane w art. 8 EKPC „odpowiadają” w rozumieniu art. 52 ust. 3 karty prawom zagwarantowanym w art. 7 („poszanowanie życia prywatnego i rodzinnego”) i 8 („ochrona danych osobowych”) karty, podobnie jak prawa zagwarantowane w art. 10 EKPC „odpowiadają” prawom zagwarantowanym w art. 11 karty („wolność wypowiedzi i informacji”), niezależnie od różnic dotyczących odpowiednio zastosowanych sformułowań i użytych pojęć<sup>20</sup>.

i wolności” szeregowi wymogów. Sam termin „ograniczenie” odpowiada z kolei terminom „ingerencja” użytym w art. 8 EKPC, oraz „ograniczenie” zastosowanemu w art. 10 EKPC, postanowieniach, w których wymieniono poszczególne wymogi, które odpowiadają także w dużej mierze wymogom ustanowionym w art. 52 ust. 1 karty i których wykładania dokonania przez Europejski Trybunał Praw Człowieka powinna być uwzględniona przez Trybunał<sup>21</sup>. Jednakże ponieważ wymogi te różnią się, wydaje mi się oczywiste, że postanowieniom karty należy nadać niezależną wykładnię<sup>22</sup>.

32. Wreszcie należy wskazać, że postanowienia EKPC zezwalające pod określonymi warunkami na zastosowanie środków ograniczających prawa i wolności w ten sposób zagwarantowane, w niniejszym przypadku jej art. 8 ust. 2 i art. 10 ust. 2, także znajdują odpowiednik, sformułowany w nieco odmienny sposób, w postanowieniu przekrojowym karty, wspólnym dla wszystkich praw i wolności, które gwarantuje, czyli w art. 52 ust. 1 zatytułowanym „Zakres i wykładnia praw i zasad”.

33. To ostatnie postanowienie poddaje „[w]szelkie ograniczenia w korzystaniu z praw

34. W konsekwencji i z wyżej wymienionymi zastrzeżeniami proponuję zmianę treści pytania sądu krajowego w ten sposób, by odesłanie do art. 8 i 10 EKPC zastąpić odwołaniem do „art. 7, 8 i 11 karty, w związku z jej art. 52 ust. 1, interpretowanych w razie konieczności w świetle art. 8 i 10 EKPC”.

19 — Zobacz wyrok z dnia 5 października 2010 r. w sprawie C-400/10 PPU McB., Zb.Orz. s. I-8965, pkt 53; ww. wyrok w sprawie DEB Deutsche Energiehandels-und Beratungsgesellschaft, pkt 35.

20 — Zobacz także w tym zakresie wyjaśnienia opracowane w celu ukierunkowania wykładni karty, zamieszczone w art. 52 ust. 7, a w szczególności wyjaśnienia dotyczące art. 7, art. 8, art. 11 i art. 52 karty.

21 — Jak przypomniał Trybunał w pkt 35 wyroku w ww. sprawie DEB Deutsche Energiehandels-und Beratungsgesellschaft, „znaczenie i zakres zagwarantowanych praw określa nie tylko tekst EKPC, ale także między innymi orzecznictwo Europejskiego Trybunału Praw Człowieka”, zgodnie z wyjaśnieniami przedstawionymi w celu ukierunkowania wykładni karty, o których mowa w jej art. 52 ust. 7.

22 — Zobacz w tym zakresie moją opinię z dnia 1 marca 2011 r. w sprawie C-69/10 Samba Diouf, w toku, pkt 42.

## 2. Struktura odpowiedzi

35. Scarlet i ISPA, a także rządy belgijski, czeski, włoski, niderlandzki, polski i fiński twierdzą, ogólnie rzecz biorąc, po przeprowadzeniu merytorycznej analizy stosownych przepisów, ale przy istnieniu różnic w zakresie podejścia do problemu, że prawo unijne sprzeciwia się przyjęciu środka takiego jak ten, o który wniesiono. Komisja jest zdania, że o ile rozpatrywane dyrektywy nie sprzeciwiają się same z siebie wprowadzeniu systemu filtrowania i blokowania takiego jak ten, którego się wymaga, o tyle konkretne zasady jego wdrożenia są sprzeczne z zasadą proporcjonalności. Twierdzi także zasadniczo, że ostatecznie to sąd krajowy pierwszej instancji naruszył wymogi wynikające z zasady proporcjonalności, ponieważ w odniesieniu do krajowych przepisów ustawowych jako takich nie można postawić żadnego zarzutu.

36. Z pewnością należy przypomnieć w tym względzie, że art. 52 ust. 1 karty wymaga, by wszelkie ograniczenia w korzystaniu z praw i wolności były dokonywane, oprócz poszanowania innych wymogów, z zastrzeżeniem zasady proporcjonalności. Poszanowanie zasady proporcjonalności konieczne jest bez wątpienia, w przypadku gdy pojawia się kwestia ograniczenia w rozumieniu tego postanowienia, czyli nie tylko na etapie stosowania in concreto tego postanowienia przez sędziego, co jest właśnie przedmiotem drugiego

pytania, ale także wcześniej, na etapie jego definiowania in abstracto – jego formułowania przez ustawodawcę. Moim zdaniem w tym aspekcie problemu argumentacja Komisji jest wadliwa.

37. W każdym razie, nie ma wątpliwości, że jakkolwiek „ustawa” powinna sama z siebie podlegać kontroli proporcjonalności, kontrolę tę można przeprowadzić dopiero po stwierdzeniu, w stosownym przypadku, samego „istnienia” wspomnianej ustawy. W tym względzie nie przez przypadek pierwszym z wymogów każdego ograniczenia w korzystaniu z praw i wolności uznanych przez kartę, ustanowionych w jej art. 52 ust. 1, jest, by było ono „przewidziane ustawą”. Tymczasem okazuje się, że sąd odsyłający zapytując, czy rozpatrywany środek może być przyjęty „jedynie na podstawie przepisu”, który przytacza, wzywa przede wszystkim do zbadania przestrzegania tego pierwszego wymogu. Analiza tego aspektu pytania jest moim zdaniem nieunikniona i ma charakter wstępny w stosunku do każdego innego aspektu<sup>23</sup>. W braku „ustawy” w rozumieniu art. 52 ust. 1 karty nie będzie trzeba w rzeczywistości badać kolejno wymogów, którym podlega każde ograniczenie korzystania z praw i wolności uznanych przez kartę, a zwłaszcza wymogu proporcjonalności. O ile Trybunał rzadko

23 — Takie było właśnie znaczenie pytania, które zadałem w sposób szczegółowy poszczególnym interwenientom podczas rozprawy.



miał okazję badać przestrzeganie tego wymogu<sup>24</sup>, o tyle jest on jednak wspólny dla art. 8 i 10 EKPC i w jego przedmiocie od dawna orzekał Europejski Trybunał Praw Człowieka, co doprowadziło do powstania bogatego orzecznictwa, do którego w związku z tym w szczególności trzeba będzie odwołać się w celu udzielenia pełnej, a przede wszystkim użytecznej odpowiedzi sądowi odsyłającemu.

przecząco, nie trzeba będzie badać drugiego pytania<sup>25</sup>.

### 3. Podejście czterostopowe

38. Cour d'appel de Bruxelles formułuje odeślanie prejudycjalne w formie dwóch pytań, przy czym drugie, dotyczące przestrzegania przez sądy krajowe zasady proporcjonalności, zostało przedłożone wyłącznie pomocniczo, na wypadek gdyby Trybunał odpowiedział twierdząco na pierwsze pytanie. To pozwala mi na stwierdzenie, że jeśli uznam, iż na pierwsze pytanie należy odpowiedzieć

39. W związku z tym samo sformułowanie pierwszego pytania prejudycjalnego, wyjątkowo bogate i precyzyjne, pozwoli mi na rozwinięcie argumentacji w oparciu bezpośrednio o poszczególne aspekty, które zawiera. W tym celu proponuję przedstawienie mojego rozumowania w czterech etapach.

40. W pierwszym rzędzie należy szczegółowo rozważyć charakter i cechy środka, o którego zastosowanie zwrócono się do sądu odsyłającego, a dokładniej środka polegającego na potwierdzeniu lub zniesieniu w postępowaniu odwoławczym – w niniejszym przypadku wprowadzenia systemu filtrowania i blokowania – odróżniając od cech zażądanego środka, czyli nakazu zaprzestania, cechy jego treści. Analiza tego środka powinna mi już pozwolić na udzielenie zasadniczej odpowiedzi na postawione pytanie, co najmniej z punktu widzenia praw i interesów Scarlet. Jednakże ponieważ co do zasady zwrócono się do mnie o udzielenie odpowiedzi na postawione pytanie z punktu widzenia praw podstawowych użytkowników usług

24 — W odniesieniu do zwykłego wymienienia tego wymogu zob. w szczególności wyroki: z dnia 21 września 1989 r. w sprawach połączonych 46/87 i 227/88 Hoechst przeciwko Komisji, Rec. s. 2859, pkt 19; z dnia 17 października 1989 r. w sprawie 85/87 Dow Benelux przeciwko Komisji, Rec. s. 3137, pkt 30 i nast.; z dnia 26 czerwca 1997 r. w sprawie C-368/95 Familiapress, Rec. 1997, s. I-3689, pkt 26; z dnia 11 lipca 2002 r. w sprawie C-60/00 Carpenter, Rec. s. I-6279, pkt 42; z dnia 1 lipca 2010 r. w sprawie C-407/08 P Knauf Gips przeciwko Komisji, Zb.Orz. s. I-6375, pkt 91; w odniesieniu do „kontroli” wymogu zob. ww. wyrok Volker und Markus Schecke i Eifert, pkt 66. Zobacz także ww. opinia rzecznik generalnej J. Kokott w sprawie Promusicae, pkt 53.

25 — W dalszej części rozważań będę odwoływał się zatem do pytania prejudycjalnego w liczbie pojedynczej.

Scarlet, a szerzej internautów, moje badanie będzie rozwinięte bardziej szczegółowo w tej perspektywie.

kwestia, czy z punktu widzenia użytkowników usług Scarlet, a szerzej internautów, środek, o którego zastosowanie wniesiono, może być przyjęty na podstawie jedynie przepisów ustawowych prawa krajowego przytoczonych przez sąd odsyłający.

41. Na podstawie tej analizy możliwe będzie, w drugim rzędzie, zbadanie zażądanego środka w świetle poszczególnych przytoczonych dyrektyw, a w szczególności istotnych postanowień karty, interpretowanych w stosownym przypadku w świetle odpowiadających im postanowień EKPC wymienionych przez sąd odsyłający. Pogłębiona analiza rozpatrywanego środka powinna w rezultacie umożliwić mi rozpatrzenie środka w perspektywie ograniczeń praw i wolności przewidzianych w art. 52 ust. 1 karty.

B — Środek, o którego zastosowanie wniesiono (*nakaz zaprzestania*) i wymagany „system” (*filtrowanie i blokowanie*)

42. Ponieważ zostanie ustalone, że środek ten stanowi „ograniczenie” korzystania z praw i wolności uznanych przez kartę w rozumieniu jej art. 52 ust. 1, należało będzie zbadać, w trzecim rzędzie, pod jakimi warunkami byłoby możliwe jego wprowadzenie, przy czym należy zwrócić szczególną uwagę na wymóg, by ograniczenie było „przewidziane ustawą”. Nie powinno być bowiem konieczne, w świetle sformułowania pytania prejudycjalnego i w celu udzielenia na nie użytecznej odpowiedzi, badanie, czy środek ten spełnia pozostałe wymogi przewidziane w tym postanowieniu.

43. W czwartym i w ostatnim rzędzie w świetle tych rozważań zostanie zbadana

44. W odniesieniu do tego aspektu sąd odsyłający zwraca się przede wszystkim do Trybunału zapytaniem, czy jest dozwolone, by sąd państwa członkowskiego „nakaza[ł] [ISP] wprowadzeni[e], w stosunku do wszystkich swoich klientów, in abstracto i w celach zapobiegawczych, na [jego] wyłączny koszt [...] i bez ograniczeń w czasie, systemu filtrowania wszystkich połączeń elektronicznych, zarówno wchodzących, jak i wychodzących, przekazywanych za pośrednictwem jego usług, w szczególności przy zastosowaniu programów peer to peer, w celu zidentyfikowania w jego sieci przypadków przekazywania plików elektronicznych zawierających utwory muzyczne, kinematograficzne lub audiowizualne, co do których strona powodowa rości sobie prawa, a następnie zablokowania transferu tych plików, bądź to na etapie próby ich pobrania, bądź na etapie ich wysłania” w formie nakazu zaprzestania.

45. W oparciu o terminy i wyrażenia zastosowanie w tej części pytania zbadam cechy zarówno samego systemu filtrowania i blokowania, jak i środka zakazu, o którego zastosowanie wniesiono.

a) Mechanizm „filtrowania”

## 1. System filtrowania i blokowania

46. „System”, jaki należałoby wprowadzić w życie, jest podwójny. Powinien gwarantować w pierwszym rzędzie filtrowanie wszystkich przekazów danych przechodzących przez sieć Scarlet, w celu wykrycia lub wyizolowania tych, które wiążą się z naruszeniem prawa autorskiego<sup>26</sup>. W oparciu o to filtrowanie system powinien zapewniać, w drugim rzędzie, blokowanie połączeń, które rzeczywiście prowadzą do naruszenia prawa autorskiego, czy to „na etapie próby ich pobrania”, czy też „na etapie ich wysłania”<sup>27</sup>. Ponieważ wydajność systemu filtrowania jest warunkiem skuteczności mechanizmu blokowania, te dwie operacje, chociaż ściśle powiązane, mają bardzo różny charakter, a zatem odmienne konsekwencje.

47. Sąd odsyłający wskazuje, że wymagany środek nakłada na Scarlet przede wszystkim obowiązek wprowadzenia w stosunku do wszystkich swoich klientów systemu filtrowania wszystkich połączeń elektronicznych, zarówno wchodzących, jak i wychodzących, przekazywanych za pośrednictwem jego usług, w szczególności przy zastosowaniu programów peer to peer. Wyjaśnia, że celem tego filtrowania jest „zidentyfikowani[e] [...] przypadków przekazywania plików elektronicznych zawierających utwory muzyczne, kinematograficzne lub audiowizualne, co do których [Sabam] rości sobie prawa”.

48. Przedmiot kontroli jest zdefiniowany właśnie jako umożliwienie filtrowania połączeń elektronicznych przechodzących przez usługi Scarlet, przychodzących i wychodzących. To filtrowanie powinno umożliwić jej zidentyfikowanie „plików elektronicznych” wysyłanych i otrzymywanych przez abonentów usług Scarlet, co do których można przypuszczać, że naruszają prawo autorskie lub prawa pokrewne. Kontrola, jaką należałoby wprowadzić, która obejmuje zatem etap filtrowania i etap identyfikacji, jest więc zdefiniowana zasadniczo w oparciu o wyniki, jakie powinna przynieść, w związku z celem blokowania plików uznanych za naruszające prawo własności intelektualnej. Powinna także móc

<sup>26</sup> — Zwany dalej „systemem filtrowania”.

<sup>27</sup> — Zwany dalej „mechanizmem blokowania”.

dostosować się do zmian technologicznych. Aby była skuteczna, musi być zarazem systematyczna, uniwersalna i ewolucyjna<sup>28</sup>.

piractwa<sup>29</sup>. Trybunał nie posiada w szczególności żadnej dokładnej informacji ani co do intensywności, ani co do zakresu kontroli, którą należałoby przeprowadzać.

49. Należy zaznaczyć, że ani sąd odsyłający, ani Sabam nie dostarczyły żadnej informacji co do konkretnych zasad, zgodnie z którymi ta kontrola może lub powinna być przeprowadzana, czy to w odniesieniu do technik filtrowania, czy też procedur identyfikacji plików, co do których istniało podejrzenie

50. O ile w tym względzie należy przypomnieć, że nie jest zadaniem Trybunału, ale wyłącznie sądu odsyłającego, w stosownym przypadku, zbadanie aspektów technicznych tej kwestii<sup>30</sup>, należy niemniej jednak wyjaśnić, że charakter filtrowania, jakiego należałoby

28 — W swych pismach procesowych Sabam podkreśla jednakże, że środek, o którego zastosowanie wniesiono, dotyczy tylko połączeń peer-to-peer. Wyrażenie „peer-to-peer” („każdy do każdego”) oznacza metodę komunikowania, zgodnie z którą komputery połączone w sieci w linii bezpośredniej, wymieniają za pośrednictwem programów używających specyficznych protokołów informacje, które mogą być plikami („file sharing”, rozpatrywany w niniejszej sprawie), ale także na przykład usługami telefonicznymi, takimi jak Skype. Tytułem przykładu można przytoczyć następujące protokoły i programy z zakresu „file sharing”: BitTorrent (Azureus, BitComet, Shareaza, MlDonkey), eDonkey (eDonkey2000, MlDonkey), FastTrack (Kazaa, Grokster, iMesh, MlDonkey), Gnutella (BearShare, Shareaza, Casbos, LimeWire, MlDonkey...), Gnutella2 (Shareaza, Trustyfiles, Kiwi Alpha, FileScope, MlDonkey...), OpenNap (Napster, Lopster, Teknap, MlDonkey); szerzej na temat peer-to-peer zob. m.in. R. Stevens, *Peer-to-Peer (P2P) Resource Sharing*, lipiec 2010 (na stronie internetowej Uniwersytetu w Oksfordzie, Information and Communications Technology, <http://www.ict.ox.ac.uk/oxford/rules/p2p.xml>). Sabam wyjaśnia, że celem środka jest „umożliwienie za pomocą programu peer-to-peer wysyłania lub odbierania w każdej formie [...] plików elektronicznych zawierających dzieła muzyczne z repertuaru Sabam”. Do sądu odsyłającego należy określenie, czym jest dokładnie ten system, a w szczególności czy system powinien także dostosowywać się do alternatywnych dla peer-to-peer sposobów wymiany plików, takich jak „streaming” (strumień danych) oraz „direct download” (pobieranie bezpośrednio poprzez na przykład RapidShare, MegaUpload). Trybunał, zobowiązany sformułowaniem pytania prejudycjalnego, które zostało do niego skierowane, oraz motywami postanowienia odsyłającego, powinien wyjść z założenia, że żądany system filtrowania i blokowania dotyczy w szczególności, a zatem nie wyłącznie, połączeń realizowanych za pomocą programów peer-to-peer.

29 — Jest to nieuchronna konsekwencja zasady „neutralności technologicznej” bronionej przez Sabam, na mocy której środek, o którego zastosowanie wniesiono, nie nakłada na Scarlet obowiązku wprowadzenia żadnej szczególnej technologii.

30 — Z całą ostrożnością, z jaką musi przyjąć człowiek, który nie jest profesjonalistą, wydaje się, że wprowadzenie systemu filtrowania i blokowania może opierać się na kilku mechanizmach wykrywania. Można rozróżnić: 1) wykrywanie używanego protokołu komunikacji: ponieważ każdy protokół peer-to-peer posiada własne mechanizmy zarządzające siecią i koordynujące dystrybucję ruchu, możliwe jest utworzenie filtrów, które wyszukują w każdym pakiecie IP śladu właściwego danemu protokołowi (podpis). Następnie możliwe jest, po wykryciu podpisu, bądź to zablokowanie, a także znaczne zwolnienie w celu zniechęcenia wszelkich połączeń używających tego protokołu, bądź wykorzystanie możliwości pogłębionej kontroli treści plików, aby zablokować wyłącznie te, które są zidentyfikowane jako naruszające prawo; 2) wykrywanie treści wymienianych plików: ten rodzaj systemu może albo wykrywać tatusz informatyczny umieszczony wcześniej w pliku, albo porównywać ślad informatyczny pliku z wcześniej ustalonymi śladami dzieł. System CopySense d’Audible Magic, na który powołano się w postanowieniu odsyłającym, jest tego rodzaju systemem; 3) wykrywanie zachowania uczestników spornej komunikacji: wykrywanie portów połączeń, wykrywanie otwarcia przez serwer lub klienta kilku połączeń z kilkoma innymi klientami; wykrywanie prób poszukiwania lub transferu plików, a nawet wykrywanie kryptonimu wymiany jako wskazówki usiłowania ominięcia środków wykrywania. Szerzej na temat poszczególnych rozważanych technik por. np. sprawozdanie Kahna-Brugidou z dnia 9 marca 2005 r. oraz sprawozdanie Olivennesa w sprawie rozwoju i ochrony dzieł kultury w nowych sieciach z dnia 23 listopada 2007 r., które zainspirowały ustawę Hadopi.

dokonywać, nie jest z pewnością pozbawiony skutków prawnych<sup>31</sup>.

b) Mechanizm „blokowania”

51. Sąd odsyłający wskazuje, że mechanizm blokowania powinien być uruchamiany bądź to „na etapie próby [...] pobrania”, bądź „na etapie [...] wysłania”, ale nie przedstawia żadnej informacji dodatkowej na temat modus operandi takiego mechanizmu. Sabam podkreśla, iż mechanizm, jaki należałoby wprowadzić, definiuje się przede wszystkim poprzez jego cel, jego zdolność do „uniemożliwi[enia] przesyłani[a] lub odbierani[a] przez jej klientów, w jakiegokolwiek formie, za pomocą programów peer to peer, plików elektronicznych zawierających utwory muzyczne z repertuaru Sabam”. Wyjaśnia, że chodzi o uniemożliwienie przekazywania niektórych informacji poprzez dostarczenie wiadomości zwanych „time out”, wskazujących na niemożliwość dokonania przekazania.

52. W rzeczywistości<sup>32</sup> niemożliwe jest opisanie sposobu konkretnego funkcjonowania,

31 — Niezależnie od zasady neutralności technologicznej bronionej przez Sabam wybór systemu, jaki należałoby wprowadzić, nie jest neutralny także z punktu widzenia technologicznego. Można na przykład rozsądnie twierdzić, że system filtrowania treści wszystkich połączeń będzie miał prawdopodobnie większy wpływ na sieć komunikacji niż filtrowanie wyłącznie wymienianych plików zgodnie z protokołem, którego podpis został zidentyfikowany.

32 — Jest to bezpośrednia konsekwencja idei neutralności technologicznej bronionej przez Sabam.

modus operandi, systemu filtrowania i mechanizmu blokowania, do wprowadzenia których zobowiązywałby środek, o którego zastosowanie wniesiono. Zakres wymaganego filtrowania, czyli zarówno osoby, które miałyby być kontrolowane, połączenia podlegające kontroli i intensywność kontroli, jaką należałoby przeprowadzać, jest jednocześnie bardzo ogólny i w części nieokreślony. W konsekwencji nie można określić a priori ani jego konkretnego wpływu na wymianę danych, ani jego ogólnego kosztu ekonomicznego, w szczególności kosztu instalacji i utrzymania.

2. Cechy środka w postaci nakazania

53. Charakter i główne cechy wymaganego systemu filtrowania i blokowania, tak jak zostały opisane, mają bezpośredni wpływ na sam charakter środka, o którego zastosowanie zwrócono się do sądu. Bardzo ogólny zakres systemu, jaki należałoby wprowadzić sprawia, że zakresy stosowania *ratione personae* i *ratione materiae* wymaganego środka w formie nakazu mają w konsekwencji charakter ogólny, podobnie jak jego zakres stosowania *ratione temporis*, jak wyjaśnia sąd odsyłający.

54. Środek, o którego zastosowanie wniesiono, posiada także inne cechy, które należy podkreślić. Z jednej strony nakładałby on na Scarlet, w celach zapobiegawczych,

zobowiązanie rezultatu pod groźbą okresowej kary pieniężnej, a z drugiej obciążałby ją kosztami wprowadzenia systemu filtrowania i blokowania. Środek ten definiuje się zatem także poprzez jego zasadniczy cel, którym jest przekazanie ISP odpowiedzialności prawnej i gospodarczej w zakresie walki z bezprawnym pobieraniem dzieł podlegających piractwu internetowemu. Poniżej przeanalizuję szczegółowo te cechy.

zdefiniowanego wyłącznie w oparciu o skuteczność jego rezultatów w świetle wyznaczonego celu polegającego na ochronie praw własności intelektualnej.

a) „Bez ograniczeń w czasie”: zakres stosowania środka *ratione temporis*

55. Sąd odsyłający wyjaśnia, że wniesiono o zastosowanie środka „bez ograniczeń w czasie”. Sabam ze swej strony potwierdziła w pismach procesowych, że nakaz, o który wniosła, nie powinien być przedmiotem ograniczenia w czasie, innego niż to, które jest nierozdzielnie związane z okresem obowiązywania samego prawa autorskiego. Podkreśla także ewolucyjny wymiar środka, który powinien być dostosowany do zmian technologicznych, a zatem powinien móc być przedmiotem dostosowania.

56. Środek, o którego zastosowanie wniesiono, nakładałby zatem na Scarlet i, jak zostanie przedstawione, szerzej – na ISP w ogólności zarówno stały, jak i nieustanny obowiązek projektowania, testowania, wprowadzania i uaktualniania systemu filtrowania i blokowania

b) „Wszystkich połączeń elektronicznych, zarówno wchodzących, jak i wychodzących”: zakres stosowania środka *ratione materiae*

57. Połączenia podlegające filtrowaniu i w stosownym przypadku blokowaniu nie są przedmiotem, jak zostało przedstawione, żadnego uszczegółowienia. Niemożliwe jest określenie, czy kontrola powinna dotyczyć wszystkich połączeń czy też tylko tych, które są dokonywane za pomocą programu *peer-to-peer*; jednakże wydaje się, że kontrola, jaką należałoby wprowadzić, powinna być zarazem systematyczna i uniwersalna, aby wywierała skuteczne środki.

58. W konsekwencji wymagany środek, przedstawiony jako zwykły nakaz skierowany do ISP w ramach postępowania cywilnego mającego na celu stwierdzenie i ukaranie naruszenia praw własności intelektualnej, a także naprawienie wynikającej z niego szkody, zmierza w rzeczywistości do wprowadzenia w sposób stały i nieustanny systematycznego i uniwersalnego systemu filtrowania wszystkich połączeń elektronicznych realizowanych za pośrednictwem usług wspomnianego ISP.

c) „W stosunku do wszystkich swoich klientów”: zakres stosowania środka *ratione personae*

wcześniejszego i dokładnego zindywidualizowania naruszenia prawa autorskiego.

59. Celem systemu, jaki należałoby wprowadzić jest (i jest to bezpośrednia konsekwencja kontroli powszechnego zakresu filtrowania połączeń) wychycenie zachowań wszystkich użytkowników usług rozpatrywanych ISP, a nie tylko jej abonentów. Jak wyjaśniła Sabam w swych pismach procesowych, nieistotne jest, że połączenie pochodzi od lub jest przeznaczone do klienta ISP. System, aby był skuteczny, powinien funkcjonować, zgodnie ze sformułowaniem pytania prejudycjalnego, bez uprzedniego indywidualizowania osób, które miałyby być sprawcami naruszeń prawa autorskiego, niezależnie od wszelkich stosunków umownych pomiędzy tymi osobami a ISP.

60. System, jaki miałby być wprowadzony, powinien móc zablokować wysyłanie przez każdego internautę korzystającego z usług Scarlet do każdego innego internauty, niezależnie od tego, czy korzysta on z usług Scarlet, każdego pliku, który miałby naruszać prawo, którego zarządzanie, gromadzenie i ochrona jest zadaniem Sabam. Jednakże powinien on także móc zablokować odebranie przez każdego internautę korzystającego z usług Scarlet wszelkiego pliku naruszającego prawo autorskie pochodzącego od każdego innego internauty, niezależnie od tego, czy korzysta on z usług Scarlet. System powinien umożliwiać zablokowanie każdego pliku, którego treść należy do repertuaru Sabam, bez

61. Należy podkreślić także inny bardzo istotny wymiar środka, o którego zastosowanie wniesiono. O ile jest jasne, że spór w postępowaniu krajowym toczy się wyłącznie pomiędzy Sabam a Scarlet, o tyle jednak z postanowienia odsyłającego oraz z pism procesowych poszczególnych interwenientów wynika, że zasięg sporu przekracza z pewnością interesy stron w postępowaniu krajowym. Rozstrzygnięcie sporu w postępowaniu krajowym zostanie niewątpliwie rozszerzone i uogólnione nie tylko na wszystkich ISP, ale także w szerszym zakresie na inne istotne podmioty działające w sektorze związanym z Internetem<sup>33</sup>, nie tylko w państwie członkowskim, które jest autorem pytań prejudycjalnych, ale we wszystkich państwach członkowskich, a nawet w innych państwach<sup>34</sup>. Sąd odsyłający zwraca się bowiem do Trybunału, jak już podkreśliłem, o wskazanie, czy prawo unijne sprzeciwia się temu, aby przyznano mu prawo do przyjęcia środka takiego jak ten, o którego wydanie wniesiono, a szerzej, czy sprzeciwia się temu, by podmioty praw mogły wzmocnić walkę z bezprawnym pobieraniem, powielając wnioski tego rodzaju we

33 — Do Trybunału zresztą skierowano identyczne pytanie prejudycjalne w ramach innego sporu pomiędzy Sabam a Netlog, platformą sieci społecznej; zob. sprawa C-360/10, w toku (Dz.U. C 288, 23 października 2010 r., s. 18).

34 — Decyzje sądów belgijskich miały bowiem istotne reperkusje poza Europą, co można stwierdzić po krótkim przeszukaniu danych w Internecie.

wszystkich państwach członkowskich i w innych państwach<sup>35</sup>.

62. W konsekwencji celem środka, o którego zastosowanie wniesiono, przedstawionego jako nakaz skierowany do zidentyfikowanej osoby prawnej, nakładający na nią obowiązek wprowadzenia systemu filtrowania i blokowania, jest w rzeczywistości trwały wpływ na niezidentyfikowaną liczbę osób prawnych lub fizycznych, ISP lub internautów, dostawców usług społeczeństwa informacyjnego i użytkowników tych usług.

d) „In abstracto i w celach zapobiegawczych”: funkcja zapobiegawcza i odstraszająca środka, o którego zastosowanie wniesiono

63. Sąd odsyłający podkreśla, że został wezwany do nałożenia na Scarlet wymaganego środka „in abstracto” i „w celach zapobiegawczych”, jednakże nie wyjaśnił, co dokładanie przez to rozumie. Można jednakże zakładać, że celem środka, o którego zastosowanie wniesiono, nie jest nałożenie na ISP obowiązku działania opartego na stwierdzeniu, in

concreto, przez sąd w ramach postępowania cywilnego rzeczywistego naruszenia, a także bezpośredniego zagrożenia naruszenia prawa autorskiego lub praw pokrewnych. Środek ten powinien zatem pełnić funkcję zapobiegawczą i odstraszającą<sup>36</sup>.

e) „Na wyłączny koszt”: obciążenie kosztami związanym z wykonaniem środka, o którego zastosowanie wniesiono

64. Sąd odsyłający wyjaśnia wreszcie, że koszty wprowadzenia systemu filtrowania i blokowania, o którego zastosowanie wniesiono, powinny być ponoszone przez dostawcę usług. Z tego punktu widzenia celem rozpatrywanego środka jest przeniesienie na Scarlet bez wątpienia znacznego ciężaru kosztów związanych z wszczęciem postępowania cywilnego, które zwykle jest wszczynane przez podmioty praw autorskich lub praw pokrewnych lub ich następców prawnych w celu uzyskania stwierdzenia naruszenia,

35 — Warto podkreślić znaczne korzyści, jakie płynęłyby dla posiadaczy praw lub ich następców prawnych, a w szczególności spółek zajmujących się wspólnym zarządzaniem prawami, zaangażowanych w walkę z nielegalnym pobieraniem treści, z upowszechnienia wprowadzania systemów filtrowania i blokowania, zakładając, że byłyby one rzeczywiście efektywne, na początku na płaszczyźnie proceduralnej i własnościowej, w stosunku do strategii polegającej na uzyskaniu na drodze sądowej wsparcia ISP w celu wykrywania i identyfikowania autorów naruszeń, aby następnie wszcząć przeciwko nim postępowanie karne.

36 — Sabam wyjaśnia w tym zakresie, że nie zamierza pozywać Scarlet jako podmiotu odpowiedzialnego za naruszenia własności intelektualnej lub ich autora, ale zniechęcić ją do świadczenia usług osobom trzecim w zakresie, w jakim osoby te wykorzystują je do naruszenia prawa autorskiego lub praw pokrewnych. Niemniej jednak należy w tym względzie przypomnieć, że w postępowaniu w pierwszej instancji skierowano przeciwko Scarlet nakaz zaprzestania działania pod groźbą okresowej kary pieniężnej, który jest przedmiotem apelacji w postępowaniu przed sądem odsyłającym, i że Sabam żąda potwierdzenia decyzji sądu pierwszej instancji oraz tłumaczenia i publikacji orzeczenia, jakie zostanie wydane, na jej stronie internetowej oraz w kilku dziennikach.



usankcjonowania i w stosownym przypadku naprawienia szkód wyrządzonych naruszeniem wspomnianych praw.

65. Bezpośredni ekonomiczny skutek rozpatrywanego środka<sup>37</sup>, który nie jest i w rzeczywistości<sup>38</sup> nie może być przedmiotem jakiegokolwiek oszacowania, jest poza tym wzmocniony okresowymi karami pieniężnymi, które mogą być związane ze środkiem, o którego zastosowanie wniesiono, a w szczególności sankcją mającą na celu ukaranie opóźnień we wprowadzaniu systemu filtrowania i blokowania.

### 3. Wniosek pośredni

66. Z powyższych rozważań wynika, że środek, o którego zastosowanie wniesiono, nakładając na ISP obowiązek wprowadzenia systemu filtrowania i blokowania, takiego jak opisany powyżej, okazuje się w rzeczywistości nowym „obowiązkiem” o charakterze ogólnym, który zostałby ostatecznie rozszerzony w trwały sposób na wszystkich ISP. Sam nie

posiada cech konkretności i indywidualności, których zwykle oczekuje się od odpowiedzi lub reakcji na zakładane specyficzne i określone zachowanie. W odpowiedzi na bardziej lub mniej zindywidualizowanie naruszenia prawa własności intelektualnej zwrócono się do sądu odsyłającego o przyjęcie środka, który, powtórzę, przez samą swą naturę ma mieć wyłącznie charakter ogólny pod każdym względem: osobowym, przestrzennym i czasowym.

67. Pozwolę sobie wskazać, że z tego punktu widzenia i o ile pytanie sądu odsyłającego powinno być rozpatrywane wyłącznie w perspektywie prawa i interesów Scarlet, można byłoby, na podstawie zasady legalności w jej najszerszym znaczeniu, odpowiedzieć na nie przecząco. Jak bowiem podkreślił Trybunał w ww. wyroku w sprawie Hoechst przeciwko Komisji<sup>39</sup>, „ingerencja władz publicznych w dziedzinę prywatnej działalności jakiegokolwiek osoby, czy to fizycznej, czy prawnej, musi mieć podstawę prawną i być uzasadniona względami określonymi w prawie”. Ten wymóg ochrony, uznany jako zasada ogólna prawa unijnego, jest korelatem zasad legalności i pewności prawa, które wynikają z idei

37 — Biegły wyznaczony przez prezesa tribunal de première instance de Bruxelles podkreśla ten aspekt pytania. Zobacz pkt 4 i 5 wniosków jego sprawozdania z dnia 29 stycznia 2007 r., cytowane w postanowieniu odsyłającym i przytoczone w pkt 21 powyżej.

38 — Ponownie – zasada neutralności technologicznej broniąca przez Sabam sprawia, że niemożliwe jest oszacowanie ex ante ogólnych kosztów wprowadzenia takiego systemu filtrowania i blokowania, niezależnie od tego, czy chodzi o koszty związane z opracowywaniem i testowaniem samego systemu, koszty inwestycyjne (skrzynki do filtrowania, rutery itd.), koszty inżynierskie i zarządzania projektem, czy też koszty utrzymania i monitoringu operacyjnego.

39 — Punkt 19.

państwa prawa<sup>40</sup>. Trybunał wielokrotnie orzekał, że zasada pewności prawa wymaga, by uregulowania nakładające obciążenia na jednostki<sup>41</sup>, wywierające dla nich negatywne skutki<sup>42</sup>, a także nakładające środki ograniczające mające znaczący wpływ na prawa i wolności określonych osób<sup>43</sup>, były na tyle jasne i precyzyjne, by zainteresowane osoby miały możliwość jednoznacznego poznania swoich praw i obowiązków i podjęcia w związku

z tym odpowiednich działań<sup>44</sup>. Tymczasem, jak wykażę w sposób szczegółowy poniżej<sup>45</sup>, przeprowadzając analizę z punktu widzenia użytkowników usług Scarlet, a szerzej internautów, krajowy przepis ustawowy, na podstawie którego może być nałożony obowiązek na Scarlet, nie spełnia między innymi tych wymogów.

40 — Warto przypomnieć, że na mocy art. 2 TUE Unia jest oparta między innymi na wartościach państwa prawa i że Trybunał od dawna potwierdza w swym orzecznictwie ideę „wspólnoty prawa”; zob. m.in. wyroki: z dnia 23 kwietnia 1986 r. w sprawie 294/83 *Les Verts* przeciwko Parlamentowi, Rec. s. 1339, pkt 23; z dnia 3 września 2008 r. w sprawach połączonych C-402/05 P i C-415/05 P *Kadi i Al Barakaat International Foundation* przeciwko Radzie i Komisji, Zb.Orz. s. I-6351, pkt 281. W odniesieniu do tych kwestii i z wszelkimi zastrzeżeniami, które wiążą się z wykorzystaniem koncepcji krajowych w prawie unijnym zob. m.in. C. Calliess, M. Ruffert, *ELIV/EGV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtscharta, Kommentar*, Beck 2007, s. 62; J. Schwarze, *Droit administratif européen*, Bruylant 2009, s. 219 i nast.; L. Azoulai, „Le principe de légalité”, w: J.B. Auby, J. Duthell de la Rochère, *Droit administratif européen*, Bruylant 2007, s. 394, zwłaszcza s. 399; D. Simon, „La Communauté de droit”, w: F. Sudre i H. Labayle, *Réalité et perspectives du droit communautaire des droits fondamentaux*, Bruylant 2000, s. 85, zwłaszcza s. 117 i nast.

41 — Zobacz wyroki: z dnia 9 lipca 1981 r. w sprawie 169/80 *Gondrand i Garancini*, Rec. s. 1931, pkt 17; z dnia 22 lutego 1989 r. w sprawach połączonych 92/87 i 93/87 *Komisja przeciwko Francji i Zjednoczonemu Królestwu*, Rec. s. 405, pkt 22; z dnia 13 lutego 1996 r. w sprawie C-143/93 *Van Es Douane Agenten*, Rec. s. I-431, pkt 27; z dnia 17 lipca 1997 r. w sprawie C-354/95 *National Farmers' Union i in.*, Rec. s. I-4559, pkt 57; z dnia 16 października 1997 r. w sprawie C-177/96 *Banque Indosuez i in.*, Rec. s. I-5659, pkt 27; z dnia 23 września 2003 r. C-78/01 *BGL*, Rec. s. I-9543, pkt 71; z dnia 20 listopada 1997 r. w sprawie C-338/95 *Wiener SI* Rec. s. I-6495, pkt 19.

42 — Zobacz w szczególności wyroki z dnia 7 czerwca 2005 r. w sprawie C-17/03 *VEMW i in.*, Zb.Orz. s. I-4983, pkt 80; z dnia 14 stycznia 2010 r. w sprawie C-226/08 *Stadt Papenburg*, Zb.Orz. s. I-131, pkt 45; z dnia 14 września 2010 r. w sprawie C-550/07 P *Akzo Nobel Chemicals et Akros Chemicals* przeciwko Komisji i in., Zb.Orz. s. I-8301, pkt 100; z dnia 2 grudnia 2010 r. w sprawie C-225/09 *Jakubowska*, Zb.Orz. s. I-12329, pkt 42.

43 — Wyrok z dnia 29 kwietnia 2010 r. w sprawie C-340/08 *M i in.*, Zb.Orz. s. I-3913, pkt 65.

68. Ponadto i zgodnie z podejściem zwykle słusznie bronionym między innymi przez Komisję, wydaje się jasne, że pomiędzy stwierdzonym naruszeniem praw własności intelektualnej a wymaganym środkiem nie istnieje związek proporcjonalności. Jednakże nie takie jest moim zdaniem pytanie główne w sprawie. Pojawia się pytanie, czy ten nowy „obowiązek” wprowadzenia systemu filtrowania i blokowania posiadający wyżej opisane cechy może, w świetle jego wpływu na prawa podstawowe użytkowników usług wspomnianych ISP, czyli internautów, być nałożony na

44 — Zobacz także wyroki: z dnia 30 stycznia 1985 r. w sprawie 143/83 *Komisja przeciwko Dani*, Rec. s. 427, pkt 10; z dnia 21 czerwca 1988 r. w sprawie 257/86 *Komisja przeciwko Włochom*, Rec. s. 3249, pkt 12; z dnia 16 czerwca 1993 r. w sprawie C-325/91 *Francja przeciwko Komisji*, Rec. s. I-3283, pkt 26; z dnia 1 października 2009 r. w sprawie C-370/07 *Komisja przeciwko Radzie*, Zb.Orz. s. I-8917, pkt 39; z dnia 11 listopada 2010 r. w sprawie C-152/09 *Grotes*, (Zb.Orz. s. I-11285, pkt 43; z dnia 22 grudnia 2010 r. w sprawie C-77/09 *Gowan Comércio*, Zb.Orz. s. I-13533, pkt 47. W odniesieniu do wymogu jasności i szczegółowości przepisów transponujących dyrektywy zob. m.in. wyroki: z dnia 20 października 2005 r. w sprawie C-6/04 *Komisja przeciwko Zjednoczonemu Królestwu*, Zb.Orz. s. I-9017, pkt 21; z dnia 10 maja 2007 r. w sprawie C-508/04 *Komisja przeciwko Austrii*, Zb.Orz. s. I-3787, pkt 73; z dnia 3 marca 2011 r. w sprawie C-50/09 *Komisja przeciwko Włochom*, Zb.Orz. s. I-873, pkt 46.

45 — Zobacz poniżej, część E, pkt 101 i nast.

ISP w formie nakazu i na podstawie prawnej, która zostanie przeze mnie zbadana.

*C — Kwalifikacja środka w świetle dyrektyw i art. 7, 8 i 11 karty: „ograniczenie” w rozumieniu art. 52 ust. 1 karty*

69. Pytanie prejudycjalne dotyczy wykładni przez Trybunał „dyrektywy 2001/29 i 2004/48, w związku z dyrektywami 95/46, 2001/31 i 2002/58, interpretowanych w świetle art. [7, 8, 11 i art. 52 ust. 1 karty]”. Co do zasady chodzi o określenie, czy w świetle obowiązującego ustawodawstwa krajowego te uregulowania prawne, składające się z prawa pierwotnego i wtórnego Unii, umożliwiają sądom państw członkowskich przyznanie w formie nakazu środka takiego jak ten opisany powyżej. Jednakże spór w postępowaniu krajowym należy zbadać przede wszystkim w świetle prawa pierwotnego, a prawo wtórne ma podlegać wykładni, gdyż rozpatrywany środek dotyczy bezpośrednio, jak przedstawię, praw i wolności zagwarantowanych w art. 7, 8 i 11 karty. To stwierdzenie wymaga przedstawienia kilku uwag wstępnych.

70. Należy przypomnieć, że dyrektywy przywołane w pytaniu stanowią ramy prawne, w które powinien wpisać się środek,

o którego zastosowanie wniesiono<sup>46</sup>, przy czym niektórzy uważają, że zezwalają one na przyjęcie tego środka lub nie stoją temu na przeszkodzie, a inni przeciwnie, twierdzą, że nie zezwalają one na jego przyjęcie, a nawet sprzeciwiają się temu<sup>47</sup>. W dyrektywach tych odwołano się, w mniej lub bardziej bezpośredni sposób, do praw podstawowych zagwarantowanych w EKPC, a obecnie także w karcie<sup>48</sup>. W wyroku w sprawie *Promusicae* Trybunał orzekł, że zadaniem państw członkowskich jest dbanie w ramach transponowania i stosowania tych dyrektyw o utrzymanie właściwej równowagi pomiędzy prawami podstawowymi, do których zagwarantowania przyczyniają się te dyrektywy.

71. Artykuły 7, 8 i 11 karty gwarantują odpowiednio, jak wiadomo, prawo do

46 — Tytułem przykładu art. 8 ust. 3 dyrektywy 2001/29 i art. 9 ust. 1 lit. a) dyrektywy 2004/48 nakładają na państwa członkowskie podwójny obowiązek ustanowienia mechanizmów sądowych mających na celu zapobieganie naruszeniom praw własności intelektualnej i ich karanie. Artykuł 15 ust. 1 dyrektywy 2000/31 nakłada na państwa członkowskie podwójny obowiązek powstrzymania się od działania: powinny one powstrzymać się od nakładania na „usługodawców” ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują, oraz ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność. Dyrektywy 95/46 i 2002/58 gwarantują, poprzez sam swój cel, prawo do ochrony danych osobowych. Artykuł 4 dyrektywy 2006/24 przewiduje, że państwa członkowskie podejmują środki w celu zagwarantowania, że dane zatrzymywane w myśl niniejszej dyrektywy są udostępniane jedynie właściwym organom krajowym, w szczególnych przypadkach i zgodnie z krajowym ustawodawstwem.

47 — Zobacz w tym względzie ww. opinię rzecznik generalnej J. Kokott w sprawie *Promusicae*, w której szczegółowo zbadano relacje, jakie istnieją pomiędzy poszczególnymi dyrektywami.

48 — Zobacz w szczególności motyw pierwszy, drugi, dziesiąty i trzydziesty siódmy dyrektywy 95/46/WE, motywy 3, 11, 24 dyrektywy 2002/58, motyw 9 dyrektywy 2000/31 oraz motywy 9, 25, a także art. 4 dyrektywy 2006/24.

poszanowania życia prywatnego i rodzinnego, prawo do ochrony danych osobowych i wolność wypowiedzi i informacji. Należy podkreślić, że w niniejszej sprawie wchodzi w grę także inne prawa podstawowe, w szczególności prawo własności, zagwarantowane w art. 17 ust. 1 karty, a dokładniej prawo do poszanowania własności intelektualnej, zagwarantowane w art. 17 ust. 2 karty, którego naruszenie z tego względu, że bezprawne pobieranie treści przez Internet przyjmuje ogromne rozmiary, znajduje się z pewnością w centrum sporu sądem postępowaniu krajowym. Jednakże w świetle środka, o którego zastosowanie wniesiono, i systemu filtrowania i blokowania, a także sformułowania postawionego pytania, należy rozpatrzyć głównie prawa zagwarantowane w art. 7, 8 i 11 karty, a prawo własności posiada tylko drugorzędne znaczenie, w zakresie w jakim wprowadzenie systemu miałyby nastąpić na wyłączny koszt ISP<sup>49</sup>.

karty, interpretowanego w świetle art. 8 ust. 2 i art. 10 ust. 2 EKPC. Gdyby wspomniany środek należało zakwalifikować jako takie ograniczenie<sup>50</sup>, należałoby wtedy zbadać, czy spełnia on poszczególne wymogi określone w tych postanowieniach.

1. „Interpretowane w szczególności w świetle art. 7 i 8 karty”: w przedmiocie poszanowania życia prywatnego i prawa do ochrony danych osobowych

73. Należy zbadać kolejno środek, o którego zastosowanie wniesiono, jako możliwe

72. Z uwzględnieniem tych okoliczności należy rozpatrzyć kwestię, czy środek, o którego zastosowanie wniesiono, może być zakwalifikowany jako „ograniczenie” praw i wolności w rozumieniu art. 52 ust. 1

49 — W zakresie w jakim systemy filtrowania i blokowania powinny być wprowadzone na wyłączny koszt ISP, wspomniany środek może być także postrzegany jako „pozbawienie” prawa własności w rozumieniu art. 17 karty, interpretowanego w świetle art. 1 protokołu 1 do EKPC oraz stosownego orzecznictwa Europejskiego Trybunału Praw Człowieka. Ten aspekt pytania nie zostanie jednak zbadany w niniejszej opinii.

50 — Lub także „ingerencja” w rozumieniu art. 8 EKPC albo „ograniczenie” w rozumieniu art. 10 EKPC. W odniesieniu do tych pojęć zob. m.in. W.J. Ganshof van der Meersch, *Réflexions sur les restrictions à l'exercice des droits de l'homme dans la jurisprudence de la Cour européenne de Strasbourg*, *Völkerrecht als Rechtsordnung – Internationale Gerichtsbarkeit – Menschenrechte*, Festschrift für H. Mosler, Springer 1983, s. 263; C.A. Kiss, „Les clauses de limitation et de dérogation dans la CEDH”, w: D. Turp, G. Beaudoin, *Perspectives canadiennes et européennes des droits de la personne*, Yvon Blais 1986, s. 119; B. Duarte, *Les restrictions aux droits de l'homme garantis par le Pacte international relatif aux droits civils et politiques et les Conventions américaine et européenne des droits de l'homme*, doktorat, uniwersytet w Lille II, 2005; J. Viljanen, *The European Court of Human Rights as a Developer of the General Doctrines of Human Rights Law. A Study of the Limitation Clauses of the European Convention on Human Rights*, doktorat, uniwersytet w Tampere, 2003; L.G. Loucaides, „Restrictions or limitations on the Rights guaranteed by the European Convention on Human Rights”, w: *The Finnish Yearbook of International Law*, vol. 3, s. 334.

ograniczenie z jednej strony prawa do ochrony danych osobowych oraz z drugiej strony prawa do poszanowania tajemnicy komunikacji. Ogólnie rzecz biorąc, jak niejednokrotnie stwierdziła Komisja<sup>51</sup>, możliwość pozostania anonimowym posiada podstawowe znaczenie w kontekście ochrony podstawowych praw do ochrony życia prywatnego w cyberprzestrzeni. Jednakże o ile wydaje się oczywiste, że dyrektywy 95/46 i 2002/58 należy interpretować w świetle art. 7 i 8 karty<sup>52</sup>, a w stosownym przypadku w świetle art. 8 EKPC<sup>53</sup>, o tyle związek pomiędzy prawem do ochrony danych osobowych (art. 8 karty) a systemem filtrowania i blokowania, którego wprowadzenia zażądano, jest o wiele mniej oczywisty<sup>54</sup>.

a) Ochrona danych osobowych (art. 8 karty)

74. Istnieje pewna trudność w zakresie konkretnej oceny wpływu systemu filtrowania i blokowania na prawo do ochrony danych osobowych. Pierwsza trudność polega na zidentyfikowaniu danych osobowych, o których mowa, ponieważ poza „adresem IP”<sup>55</sup> nie są one wyraźnie określone. Neutralność technologiczna, na którą powołuje się Sabam, powoduje bowiem, że niemożliwe jest określenie a priori, czy system, jaki należałoby wprowadzić, wiąże się z przetwarzaniem danych osobowych. Niemożliwe jest też a fortiori określenie, czy wymaga on gromadzenia i przetwarzania adresów IP.

51 — Komunikat Komisji do Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Stworzenie bezpieczniejszego społeczeństwa informacyjnego poprzez wzmocnienie bezpieczeństwa infrastruktury informacyjnej i walkę z przestępczością w cyberprzestrzeni – eEuropa 2002 [COM(2000) 890 wersja ostateczna, zwłaszcza s. 23].

52 — Zobacz w tym względzie w szczególności wyroki: z dnia 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 *Rundfunk*, Rec. s. I-4989, pkt 68; z dnia 16 grudnia 2008 r. w sprawie C-73/07 *Satakunnan Markkinapörssi i Satamedia*, Zb.Orz. s. I-9831; a także ww. wyrok w sprawie *Völker und Markus Schecke*, pkt 56 i nast. Zobacz także ww. opinię rzecznik generalnej J. Kokott w sprawie *Promusicae*, pkt 51 i nast.

53 — Zobacz w szczególności motyw drugi dyrektywy 95/46, motywy 1, 2, 7, 10, 11, 24, a także art. 1 ust. 1 dyrektywy 2002/58.

54 — *Scarlet i ISPA*, podobnie jak rządy belgijski, czeski i niemiecki, podnoszą co do zasady, że wprowadzenie takiego systemu filtrowania i blokowania doprowadziłoby ISP do przetwarzania danych osobowych z naruszeniem przepisów dyrektyw 95/46 i 2002/58. Sabam, rządy polski i fiński oraz Komisja twierdzą natomiast, że wprowadzenie takiego systemu nie jest sprzeczne z dyrektywami 95/46 i 2002/58. W odniesieniu do badania zakazów przetwarzania danych przewidzianych w tych dyrektywach zob. w szczególności ww. opinię rzecznik generalnej J. Kokott w sprawie *Promusicae*, pkt 64 i nast.

75. Druga trudność polega na określeniu, czy adresy IP stanowią dane osobowe. Dotychczas Trybunał miał okazję orzekać tylko co do przypadków, w których chodziło o dane imienne związane z adresami IP<sup>56</sup>. Natomiast nigdy nie miał jeszcze okazji zbadania,

55 — *Scarlet i ISPA* twierdzą, że adres IP właściwy dla każdego użytkownika Internetu stanowi dane osobowe, ponieważ umożliwia on zidentyfikowanie internautów. W związku z tym gromadzenie i przetwarzanie adresów IP internautów, koniecznych do identyfikacji tych ostatnich, a zatem funkcjonowania takiego systemu, stanowiłyby przetwarzanie danych osobowych, na co nie pozwalają dyrektywy.

56 — Wyżej wymieniony wyrok w sprawie *Promusicae*, pkt 45; postanowienie z dnia 19 lutego 2009 r. w sprawie C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, Zb.Orz. s. I-1227.

czy adres IP jako taki można uznać za dane osobowe<sup>57</sup>.

76. Ze swej strony Europejski Inspektor Ochrony Danych miał okazję wskazać<sup>58</sup>, że „monitorowanie zachowania użytkowników Internetu oraz w konsekwencji gromadzenie ich adresów IP kłóci się z prawem do poszanowania ich życia prywatnego i korespondencji”<sup>59</sup>. Grupa Robocza ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych, utworzona na mocy dyrektywy 95/46<sup>60</sup>, twierdzi także, że adresy IP stanowią

bez wątpienia dane osobowe w rozumieniu art. 2 lit. a) wspomnianej dyrektywy<sup>61</sup>.

77. Stanowiska te odpowiadają rzeczywistości prawnej wynikającej z art. 5 dyrektywy 2006/24/WE<sup>62</sup>, który zobowiązuje dostawców dostępu do Internetu między innymi do zatrzymania pewnych danych w celu dochodzenia, wykrywania i ścigania poważnych przestępstw. Po pierwsze, chodzi o „dane niezbędne do ustalenia źródła połączenia”, w tym nazwisko i adres abonenta lub zarejestrowanego użytkownika, któremu przyznany jest adres IP, a po drugie, dane niezbędne do ustalenia „dat[y] i godzin[y] zalogowania i wylogowania sesji internetowej na podstawie danej strefy czasowej włącznie z adresem (IP) [...], czy to dynamiczn[ym], czy statyczn[ym], przydzielonym przez dostawcę usług internetowych dla danej komunikacji”.

78. W tym kontekście adres IP może być zakwalifikowany jako dane osobowe, ponieważ umożliwia identyfikację osoby za pomocą

57 — Można zauważyć, że kwestia ta pojawia się pośrednio w sprawie C-461/10 *Bonnier i in.*, w toku (Dz.U. C 317, 20 listopada 2010 r., s. 24), w ramach której Trybunałowi zadano co do zasady pytanie, czy dyrektywa 2006/24, zmieniająca dyrektywę 2002/58, sprzeciwia się stosowaniu przepisu prawa krajowego, ustanowionego na podstawie art. 8 dyrektywy 2004/48, który do celów zidentyfikowania abonenta zezwala na nakazanie ISP przekazanie podmiotowi prawa autorskiego lub jego następcy prawnemu adresu IP, który posłużył do naruszenia wspomnianego prawa.

58 — Opinia Europejskiego Inspektora Ochrony Danych z dnia 22 lutego 2010 r. na temat bieżących negocjacji Unii Europejskiej w sprawie Umowy handlowej dotyczącej zwalczania obrotu towarami podrzobionymi (ACTA) (Dz.U. 2010, C 147, s. 1, pkt 24); opinia Europejskiego Inspektora Ochrony Danych z dnia 10 maja 2010 r. na temat wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, uchylającej decyzję ramową 2004/68/WSiSW (Dz.U. 2010, C 323, s. 6, pkt 11).

59 — Odwołuje się w tym zakresie do orzecznictwa Europejskiego Trybunału Praw Człowieka, decyzji z dnia 29 czerwca 2006 r. w sprawie *Weber i Saravia* przeciwko Niemcom, skarga nr 54934/00, Rec. 2006-XI, oraz wyroku z dnia 1 lipca 2008 r. w sprawie *Liberty i in.* przeciwko Zjednoczonemu Królestwu, skarga nr 58243. Należy jednak zauważyć, że te dwie sprawy nie dotyczą szczegółowo gromadzenia adresów IP w Internecie, ale nadzoru nad telekomunikacją.

60 — Zwana „grupą roboczą »art. 29«”.

61 — Zobacz w szczególności opinię 4/2007 z dnia 20 czerwca 2007 r. w sprawie koncepcji danych osobowych, WP 136, dostępna pod adresem <http://ec.europa.eu/justice/policies/privacy/>. Zobacz także, szerzej, zalecenie nr 3/97 z dnia 3 grudnia 1997 r. *Anonimowość w Internecie*, WP 6, oraz dokument roboczy zatytułowany „Poszanowanie życia prywatnego w Internecie – Zintegrowane podejście europejskie w zakresie ochrony danych osobowych on-line”, przyjęty w dniu 21 listopada 2000 r., WP 37, zwłaszcza s. 22.

62 — Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. L 105, s. 54).

numeru identyfikacyjnego lub każdej innej informacji właściwej dla tej osoby<sup>63</sup>.

wpływ na prawo do ochrony danych osobowych<sup>65</sup> w stopniu wystarczającym, by umożliwić zakwalifikowanie go jako ograniczenia w rozumieniu art. 52 ust. 1 karty.

79. A zatem zamiast rozważać kwestię statusu prawnego adresów IP, należy raczej określić, w jakich warunkach i do jakich celów mogą być one gromadzone, w jakich warunkach można dokonywać ich przetwarzania, a także przetwarzania danych osobowych, które z nich wynikają, a także pod jakimi warunkami można wymagać dokonania ich gromadzenia i przetwarzania<sup>64</sup>.

b) Tajemnica połączeń elektronicznych (art. 7 karty)

80. Należy uwzględnić, że system filtrowania i blokowania taki jak ten, którego wprowadzenia zażądano, niezależnie od przytoczonych powyżej wątpliwości na płaszczyźnie technologicznej, z pewnością może mieć

81. Wprowadzenie systemu filtrowania połączeń elektronicznych, takiego jak ten, którego zażądano, także nie jest bez wpływu na prawo do poszanowania tajemnicy korespondencji, a szerzej na prawo do poszanowania tajemnicy komunikowania się gwarantowanego przez art. 7 karty<sup>66</sup>, interpretowanego w świetle art. 8 EKPC oraz stosownego

63 — Takie jest na przykład podejście przyjęte przez Commission nationale de l'informatique et des libertés en France (krajową komisję ds. informatyki i wolności we Francji); zob. narada nr 2007–334 z dnia 8 listopada 2007 r. Szerzej na temat tych kwestii zob. np. M. González Pascual, „La Directiva de retención de datos ante el Tribunal Constitucional Federal alemán. La convergencia de jurisprudencias en la Europa de los Derechos: un fin no siempre deseable”, *REDE* 2010, nr 36, s. 591.

64 — W kwestii zakresu zakazu przechowywania i przekazywania danych o ruchu w rozumieniu dyrektywy 2002/58 i wyjątków od tego zakazu por. ww. opinię rzecznik generalny J. Kokott w sprawie Promusicae, pkt 64 i nast.

65 — Na mocy art. 11 dyrektywy 2006/24 między innymi dodano ust. 1a do art. 15 dyrektywy 2002/58, zgodnie z którym art. 15 ust. 1 dyrektywy 2002/58 nie stosuje się do danych, których zatrzymywanie jest wyraźnie wymagane na mocy dyrektywy 2006/24/WE. Artykuł 4 dyrektywy stanowi w niniejszym przypadku, że „[p]aństwa członkowskie podejmują środki w celu zagwarantowania, że dane zatrzymywane w myśl niniejszej dyrektywy są udostępniane jedynie właściwym organom krajowym, w szczególnych przypadkach i zgodnie z krajowym ustawodawstwem. Procedura oraz warunki uzyskiwania dostępu do zatrzymanych danych, w przypadkach gdy został spełniony wymóg konieczności oraz proporcjonalności, są określone w prawie krajowym każdego państwa członkowskiego, podlegając odpowiednim przepisom prawa Unii Europejskiej lub międzynarodowego prawa publicznego, w szczególności EKPC, zgodnie z interpretacją Europejskiego Trybunału Praw Człowieka”.

66 — Scarlet, popierana przez ISPA, podnosi, że wprowadzenie takiego systemu naruszałoby przepisy dyrektywy 2002/58 dotyczące tajemnicy połączeń elektronicznych, odwołując się w tym zakresie do motywu 26 oraz art. 5 teże dyrektywy.

orzecznictwa Europejskiego Trybunału Praw Człowieka.

82. Europejski Trybunał Praw Człowieka jeszcze nie miał okazji orzekać w przedmiocie zgodności z EKPC specyficznych środków z zakresu kontroli połączeń elektronicznych ani a fortiori systemu filtrowania i blokowania takiego jak ten, którego wprowadzenia zażądano. Można jednakże w świetle orzecznictwa dotyczącego podsłuchów telefonicznych<sup>67</sup> stwierdzić, że takie środki stanowiłyby ingerencję w rozumieniu art. 8 EKPC. Zresztą miał on okazję orzec, że gromadzenie i przechowywanie bez wiedzy danej osoby danych osobowych odnoszących się do użytkowania przez nią telefonu, poczty elektronicznej i Internetu stanowią „ingerencję” w korzystanie z prawa zainteresowanej osoby do poszanowania życia prywatnego i tajemnicy korespondencji w rozumieniu art. 8 EKPC<sup>68</sup>.

83. Ze swej strony art. 5 dyrektywy 2002/58<sup>69</sup> definiuje i gwarantuje tajemnicę komunikacji

67 — Odnosząc się wyraźnie do tego orzecznictwa zbadał on również środek dotyczący nagłośnienia mieszkania. Zobacz wyrok Europejskiego Trybunału Praw Człowieka z dnia 31 maja 2005 r. w sprawie Vetter przeciwko Francji, skarga nr 59842/00, pkt 27, odsyłający wyraźnie do rozumowania zawartego w wyrokach: z dnia 24 kwietnia 1990 r. w sprawie Huvig przeciwko Francji, skarga nr 11105/84, seria A, nr 176-B; z dnia 24 kwietnia 1990 r. w sprawie Kruslin przeciwko Francji, skarga nr 11801/85, seria A, nr 176-A.

68 — Wyrok Europejskiego Trybunału Praw Człowieka z dnia 3 kwietnia 2007 r. w sprawie Copland przeciwko Zjednoczonemu Królestwu, skarga nr 62617/00, §§ 43, 44.

69 — Należy zauważyć, że motyw 15 dyrektywy 2000/31 wyraźnie odsyła do art. 5 dyrektywy 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony życia prywatnego w sektorze telekomunikacji (Dz.U. 1998, L 24, s. 1), który został uchylony przez dyrektywę 2002/58.

i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. Przepis ten nakłada na państwa członkowskie w szczególności obowiązek wprowadzenia zakazu jakiegokolwiek kontroli lub przechwytywania tych połączeń, poza przypadkami przewidzianymi ustawowo zgodnie z art. 15 wspomnianej dyrektywy. Ten ostatni przepis pozwala państwom członkowskim na podjęcie środków ustawowych mających na celu ograniczenie zakresu prawa do poszanowania tajemnicy połączeń, w przypadku gdy to ograniczenie stanowi środek konieczny do zapewnienia między innymi zapobiegania przestępstwom oraz ich poszukiwania, wykrywania i ścigania. Środki, które mogą być przyjęte w tym zakresie, powinny w każdym wypadku być „zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej”.

2. „Interpretowane w szczególności w świetle art. 11 karty”: w przedmiocie zagwarantowania wolności wypowiedzi i prawa do informacji

84. Artykuł 11 karty, który gwarantuje nie tylko prawo do przekazywania informacji, ale



także prawo do ich otrzymywania<sup>70</sup>, bez wątpienia ma zastosowanie do Internetu<sup>71</sup>. Jak podkreślił Europejski Trybunał Praw Człowieka, „dzięki ich dostępności, a także zdolności do przechowywania i rozpowszechniania wielkich ilości danych, strony internetowe przyczyniają się w znacznym stopniu do poprawy publicznego dostępu do aktualności, a w sposób ogólny do ułatwienia przekazywania informacji”<sup>72</sup>.

zagwarantowanej w art. 11 ust. 1 karty<sup>73</sup>, niezależnie od zasad technicznych, zgodnie z którymi konkretnie przeprowadza się kontrolę połączeń, zakresu i dokładności dokonywanej kontroli oraz skuteczności i wiarygodności kontroli rzeczywiście przeprowadzanej, czyli kwestii, które jak podkreśliłem powyżej podlegają dyskusji.

85. Bez wątpienia, jak podkreśliła Scarlet, wprowadzenie systemu filtrowania i blokowania takiego jak ten, którego zażądano, a w szczególności mechanizmu blokowania, mogącego prowadzić do kontroli wszystkich połączeń elektronicznych obsługiwanych za jej pośrednictwem, stanowi z samej jego natury „ograniczenie” w rozumieniu art. 10 EKPC wolności komunikowania się

86. Jak podniosła Scarlet, łączony system filtrowania i blokowania będzie miał niewątpliwie wpływ na zgodne z prawem wymiany treści, a więc również na treść praw gwarantowanych w art. 11 karty, chociażby dlatego, że zgodny bądź niezgodny z prawem charakter danego połączenia, który zależy od zakresu rozpatrywanego prawa autorskiego, jest różny w poszczególnych krajach, a zatem wymyka się technice. W zakresie w jakim można dokonać oceny, nie wydaje się, by jakikolwiek system filtrowania i blokowania był w stanie zagwarantować, w sposób zgodny z wymogami ustanowionymi w art. 11 i art. 52 ust. 1 karty, blokowania wyłącznie tych wymian, które mogą być zidentyfikowane jako bezprawne.

70 — Na wzór art. 10 EKPC. Zobacz m.in. wyroki Europejskiego Trybunału Praw Człowieka: z dnia 26 listopada 1991 r. w sprawie *Observer i Guardian* przeciwko Zjednoczonemu Królestwu, skarga nr 13585/88, seria A, nr 216, § 59; z dnia 19 lutego 1998 r. w sprawie *Guerra* i in. przeciwko Włochom, skarga nr 14967/89, Rec. 1998-I, § 53.

71 — Można zauważyć, że Europejski Trybunał Praw Człowieka miał także okazję uwzględnić „moc” Internetu, który ponieważ per se jest dostępny dla wszystkich, wywiera znaczny skutek mnożnikowy w ramach przeprowadzanej przez niego oceny zgodności „ograniczenia” wolności wypowiedzi z wymogami ustanowionymi w art. 10 ust. 2 EKPC. Zobacz w szczególności wyroki Europejskiego Trybunału Praw Człowieka: z dnia 13 stycznia 2011 r. w sprawie *Mouvement Raëlien Suisse* przeciwko Szwajcarii, skarga nr 16354/06, §§ 54 i nast.; z dnia 16 lutego 2010 r. w sprawie *Akdaş* przeciwko Turcji, skarga nr 41056/04, § 28; z dnia 16 lipca 2009 r. w sprawie *Willem* przeciwko Francji, skarga nr 10883/05, §§ 36, 38.

72 — Wyrok Europejskiego Trybunału Praw Człowieka z dnia 10 maja 2009 r. w sprawie *Times Newspapers Limited* przeciwko Zjednoczonemu Królestwu, skargi nr 3002/03 i 23676/03, § 27. Trybunał w tym przypadku orzekł, że „utworzenie w Internecie archiwów, stanowiących zasadniczy aspekt roli odgrywanej przez strony internetowe” wchodzi w zakres zastosowania art. 10 EKPC.

73 — Można było podnieść, że przepisy z zakresu prawa własności intelektualnej państwa członkowskiego mogą stanowić same w sobie ograniczenie w rozumieniu art. 10 EKPC; zob. R. Danay, „Copyright vs. Free Expression: The Case of peer-to-peer File-sharing of Music in the United Kingdom”, in *Yale Journal of Law & Technology*, 2005–2006, vol. 8, nr 2, s. 32.

### 3. Wniosek pośredni

87. Z powyższych rozważań wynika, że żądany środek w zakresie, w jakim nakłada obowiązek wprowadzenia systemu filtrowania i blokowania połączeń elektronicznych takiego jak ten, który opisano powyżej, może mieć negatywny wpływ na korzystanie z praw i wolności chronionych na podstawie karty przeanalizowanych powyżej, a zatem powinien być zakwalifikowany w stosunku do użytkowników usług Scarlet, a szerzej użytkowników Internetu, jako „ograniczenie” w rozumieniu art. 52 ust. 1 karty<sup>74</sup>. Tymczasem ograniczenia w korzystaniu z praw podstawowych użytkowników, do jakich prowadziłoby wprowadzenie takiego systemu filtrowania i blokowania, są dopuszczalne tylko pod warunkiem, iż spełniają pewne wymogi, które zbadam poniżej.

*D — W przedmiocie wymogów ograniczenia korzystania z praw i wolności zagwarantowanych przez kartę, a w szczególności wymogu dotyczącego „jakości ustawy” (art. 52 ust. 1 karty)*

88. W karcie ustanowiono, używając już znanych sformułowań, wymogi, jakim podlega

każde ograniczenie w korzystaniu z praw i wolności, jakie ona gwarantuje, podobnie jak EKPC definiuje wymogi, po spełnieniu których, między innymi, każda ingerencja w prawo do życia prywatnego lub każde ograniczenie wolności wypowiedzi może być uznane za zgodne z prawem.

89. W art. 52 karty odwołano się do „potrzeb[...] ochrony praw i wolności innych osób” oraz wymogu, by każdy środek tego rodzaju spełniał „cel[e] interesu ogólnego” i był zgodny z zasadą proporcjonalności. O ile ochrona praw własności intelektualnej stanowi niewątpliwie cel interesu ogólnego, o czym świadczą dyrektywy 2001/29 i 2004/48, o tyle jednak żądany system filtrowania i blokowania znajduje w okolicznościach sporu w postępowaniu krajowym swe główne uzasadnienie w konieczności zapewnienia ochrony „praw i wolności innych osób”. „Potrzeb[a] ochrony praw” podmiotów praw autorskich lub praw pokrewnych znajduje się w centrum niniejszej sprawy i jest ona główną przyczyną postępowania cywilnego wszczętego przez Sabam przeciwko Scarlet.

90. Należy bowiem stanowczo podkreślić w tym miejscu, że prawo własności jest obecnie zagwarantowane w art. 17 karty, którego ustęp drugi, nie należy o tym zapominać, wyraźnie wyjaśnia, że „własność intelektualna podlega ochronie”. Należy także przypomnieć, że Trybunał wcześniej potwierdził, że prawo własności jest prawem podstawowym

<sup>74</sup> — Lub alternatywnie „ingerencja” w rozumieniu art. 8 EKPC.

stanowiącym część ogólnych zasad prawa<sup>75</sup> i uznał, że prawa autorskie stanowią część prawa własności<sup>76</sup>. Celem dyrektyw 2001/29 i 2004/48<sup>77</sup> jest zagwarantowanie wysokiego poziomu ochrony własności intelektualnej. Ponadto zgodnie z bogatym orzecznictwem Europejskiej Komisji i Europejskiego Trybunału Praw Człowieka własność intelektualna jest jako taka niezaprzeczalnie chroniona na podstawie art. 1 protokołu 1 do EKPC<sup>78</sup>.

91. Wreszcie Trybunał wskazał, że podstawową racją bytu prawa autorskiego jest powierzenie twórcy dzieł wynalazczych i oryginalnych wyłącznego prawa do eksploataowania tych dzieł<sup>79</sup>. Prawo autorskie i prawa pokrewne posiadają zatem charakter ekonomiczny, w zakresie w jakim wiążą się między innymi z możliwością handlowego eksploataowania wprowadzenia do obrotu dzieła chronionego

w formie w szczególności licencji przyznanych w zamian za opłaty<sup>80</sup>.

92. Istnieje zatem bez wątpienia „potrzeb[a] ochrony praw[a]” w rozumieniu art. 52 ust. 1 karty, która może uzasadniać „ograniczenie” innych praw i wolności w rozumieniu tegoż przepisu.

93. Po przedstawieniu powyższych wyjaśnień należy wskazać, że nie jest konieczne przeprowadzanie szczegółowego badania wszystkich wymogów dopuszczalności ograniczeń praw i wolności zagwarantowanych w karcie w celu dostarczenia sądowi odsyłającemu użytecznej odpowiedzi na jego pytanie. Sąd odsyłający bowiem stawia nam bardzo precyzyjne pytanie, czy ograniczenie w korzystaniu z praw i wolności, jakie zgodnie z tym, co zostało wyjaśnione powyżej, stanowiłoby wprowadzenie zażądanego systemu filtrowania i blokowania, może być dokonane „na podstawie jednego [krajowego] przepisu ustawowego”, który stanowi art. 87 § 1 loi du 30 juin 1994 relative au droit d’auteur et aux droits voisins, przytoczony zresztą przez sąd odsyłający w całości. Ten aspekt pytania prejudycjalnego wymaga przede wszystkim zbadania pierwszego wymogu określonego w art. 52 ust. 1 karty, a mianowicie wymogu, by ograniczenie było „przewidziane ustawą”,

75 — Zobacz m.in. wyrok z dnia 12 września 2006 r. w sprawie C-479/04 *Laserdisken*, Zb.Orz. s. I-8089, pkt 62.

76 — Wyżej wymieniony wyrok w sprawie *Laserdisken*, pkt 65.

77 — Zobacz w szczególności motywy 3, 4 dyrektywy 2001/29, a także motywy 1, 10 dyrektywy 2004/48.

78 — Zobacz m.in. decyzje Europejskiej Komisji Praw Człowieka: z dnia 4 października 1990 r. w sprawie *Smith Kline i French Laboratories Ltd. przeciwko Niderlandom*, skarga nr 12633/87, DR 66, s. 81; z dnia 11 stycznia 1994 r. w sprawie *A.D. przeciwko Niderlandom*, skarga nr 21962/93; wyroki Europejskiego Trybunału Praw Człowieka: z dnia 20 listopada 1995 r. w sprawie *British-American Tobacco Company Ltd przeciwko Niderlandom*, seria A nr 331, §§ 71, 72; z dnia 30 marca 1989 r. w sprawie *Chappel przeciwko Zjednoczonemu Królestwu*, skarga nr 10461/83, seria A, nr 152A, § 59; z dnia 11 stycznia 2007 r. w sprawie *Anheuser-Bush Inc. przeciwko Portugalii*, skarga nr 73049/01, §§ 71, 72; decyzja Europejskiego Trybunału Praw Człowieka z dnia 5 lipca 2005 r. w sprawie *Melnychuk przeciwko Ukrainie*, skarga nr 28743/03, § 3.

79 — Zobacz wyrok z dnia 17 maja 1988 r. w sprawie 158/86 *Warner Brothers i Metronome Video*, Rec. s. 2605, pkt 13.

80 — Zobacz wyroki: z dnia 20 stycznia 1981 r. w sprawach połączonych 55/80 i 57/80 *Musik-Vertrieb membran i K-tel International*, Rec. s. 147, pkt 12; z dnia 20 października 1993 r. w sprawach połączonych C-92/92 i C-326/92 *Phil Collins i in.*, Rec. s. I-5145, pkt 20.

który jest sformułowany w identyczny sposób w art. 8 ust. 2 i art. 10 ust. 2 EKPC. Badanie to zostanie przeprowadzone w świetle istotnych orzeczeń Europejskiego Trybunału Praw Człowieka interpretujących postanowienia tych dwóch ostatnich artykułów, na podstawie których, jak już podkreśliłem, powstał z czasem szczególnie bogaty zbiór orzecznictwa pozwalający na wyznaczenie granic tego wymogu.

94. Europejski Trybunał Praw Człowieka wielokrotnie orzekał, że postanowienia EKPC uzależniające ingerencję w korzystanie z prawa lub ograniczenie korzystania z wolności, jakie ona gwarantuje, od spełnienia wymogu, by ta ingerencja lub ograniczenie były „przewidziane ustawą”<sup>81</sup>, wymagają nie tylko, by środek miał podstawę ustawową jako taką, czyli miał „podstawę w prawie krajowym”, ale także nakładają obowiązek spełnienia wymogów dotyczących, przytaczając dosłownie zastosowane sformułowanie, „jakości

rozpatrywanej ustawy”<sup>82</sup>. Ta „ustawa” powinna być bowiem „wystarczająco dostępna i przewidywalna, czyli sformułowana w precyzyjny sposób, by jednostka była w stanie – bez potrzeby uzyskania profesjonalnych porad – dostosować swoje postępowanie”, „przewidzieć konsekwencje, jakie ustawa będzie miała wobec niej”<sup>83</sup>, „przewidzieć w rozsądnym stopniu w okolicznościach danej sprawy konsekwencje, jakie mogą wynikać z danego aktu”<sup>84</sup>.

95. „Ustawa” powinna być zatem wystarczająco jasna<sup>85</sup> i przewidywalna w odniesieniu do znaczenia i charakteru stosowanych środków<sup>86</sup> oraz określać wystarczająco jasno zakres i zasady wykonywania prawa

81 — Miedzy innymi P. van Dijk i in., *Theory and practice of the European Convention on Human Rights*, 4th ed., Intersentia 2006, s. 336; F.G. Jacobs, R.C.A. White, C. Ovey, *The European Convention on Human Rights*, 5th ed., Oxford University Press 2010, s. 315; D.J. Harris, M. O’Boyle, C. Warbrick, *Law of the European Convention on Human Rights*, 2nd ed., Oxford University Press 2009; C. Grabenwarter, *Europäische Menschenrechtskonvention: ein Studienbuch*, 3. Auf., Helbing & Lichtenhahn 2008, s. 112; F. Matscher, „Der Gesetzesbegriff der EMRK”, w: Adamovich, A. Kobzina, *Der Rechtsstaat in der Krise – Festschrift Edwin Loebenstein zum 80. Geburtstag*, Mainz 1991, s. 105; J. Gundel, *Beschränkungsmöglichkeiten*, in *Handbuch der Grundrechte*, Band. VI/1, Müller 2010, s. 471; R. Weiß, *Das Gesetz im Sinne der europäischen Menschenrechtskonvention*, Duncker & Humblot 1996.

82 — Zobacz m.in. L. Martín-Retortillo Baquer, „La calidad de la ley según la jurisprudencia del Tribunal europeo de derechos humanos”, w: *Derecho Privado y Constitución*, 2003, nr 17, s. 377; P. Wächsmann, „De la qualité de la loi à la qualité du système juridique”, w: *Libertés, Justice, Tolérance, Mélanges en hommage au doyen Gérard Cohen-Jonathan*, Bruylant, Bruxelles, vol. 2, s. 1687.

83 — Wyrok Europejskiego Trybunału Praw Człowieka z dnia 26 marca 1987 r. w sprawie Leander przeciwko Szwecji, skarga nr 9248/81, seria A, nr 116, § 50.

84 — Wyrok Europejskiego Trybunału Praw Człowieka z dnia 25 lutego 1992 r. w sprawie Margareta i Roger Andersson przeciwko Szwecji, skarga nr 12963/87, seria A nr 226-A, s. 25, § 75.

85 — Wyrok Europejskiego Trybunału Praw Człowieka z dnia 3 lipca 2007 r. w sprawie Tan przeciwko Turcji, skarga nr 9460/03, §§ 22–26; w tej sprawie Trybunał orzekał co do zgodności z zasadą jasności ustawy dotyczącej korespondencji osób zatrzymanych. Stwierdził, że uregulowanie, które powierza dyrektorom zakładów penitencjarnych na podstawie decyzji komisji dyscyplinarnej prawo do odmowy nadania, do ocenzurowania lub do zniszczenia każdego listu uznanego za „szkodliwy”, nie wskazuje z wystarczającą jasnością zakresu i zasad korzystania przez władze ze swobodnego uznania w rozpatrywanej dziedzinie.

86 — Zobacz m.in. ww. wyrok Europejskiego Trybunału Praw Człowieka w sprawie Krušlin przeciwko Francji, § 30; decyzja Europejskiego Trybunału Praw Człowieka z dnia 25 września 2006 r. w sprawie Coban przeciwko Hiszpanii, skarga nr 17060/02.

do ingerencji w korzystanie z praw zagwarantowanych przez EKPC<sup>87</sup>. Ustawa, która przyznaje uprawnienia dyskrecjonalne, nie jest sprzeczna z tym wymogiem, pod warunkiem że zakres i zasady wykonywania tych uprawnień są wystarczająco jasno określone z uwagi na uzasadnione interesy, które wchodzi w grę, w celu zapewnienia jednostce odpowiedniej ochrony przed arbitralnością<sup>88</sup>. Ustawa przyznająca uprawnienia dyskrecjonalne powinna zatem określać ich zakres<sup>89</sup>.

96. W konsekwencji ograniczenie jest dopuszczalne tylko w przypadku, gdy opiera się ono na podstawie ustawowej w prawie krajowym, która jest dostępna, jasna i przewidywalna<sup>90</sup>. Wszystkie te wymogi wynikają z idei rządów prawa<sup>91</sup>. Z tego wymogu rządów

prawa wynika<sup>92</sup> konieczność dostępności i przewidywalności ustawy dla danej osoby<sup>93</sup>.

97. Z wymogu, zgodnie z którym każde ograniczenie powinno być „przewidziane ustawą”, wynika zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka, że działania osób dysponujących władzą publiczną wpisują się w ramy określone uprzednio przez przepisy prawa, co „nakłada określone wymogi, które powinny być spełnione zarówno przez same przepisy prawa, jak i procedury

87 — Zobacz m.in. wyrok Europejskiego Trybunału Praw Człowieka z dnia 14 września 2010 r. w sprawie Sanoma Uitgevers przeciwko Niderlandom, skarga nr 38224/03, §§ 81, 82.

88 — Między innymi ww. wyrok w sprawie Margareta i Roger Andersson, § 75.

89 — Wyrok Europejskiego Trybunału Praw Człowieka z dnia 25 marca 1983 r. w sprawie Silver i in. przeciwko Zjednoczonemu Królestwu, skargi nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 i 7136/75, seria A, nr 61, § 88.

90 — Zobacz w tej kwestii pkt 53 ww. opinii rzecznik generalnej J. Kokott w sprawie Promusicae, przytaczający ww. wyrok w sprawie Österreichischer Rundfunk, pkt 76, 77.

91 — W odniesieniu do zwięzłego sformułowania poszczególnych kryteriów zob. m.in. wyrok Europejskiego Trybunału Praw Człowieka z dnia 25 maja 1998 r. w sprawie Kopp przeciwko Szwajcarii, skarga nr 23224/94, Rec. 1998-II, § 55.

92 — Wyrok Europejskiego Trybunału Praw Człowieka z dnia 30 lipca 1998 r. w sprawie Valenzuela Contreras przeciwko Hiszpanii, skarga nr 27671/95, Rec. 1998-V, § 46, odsyłający do wyroku z dnia 2 sierpnia 1984 r. w sprawie Malone, skarga nr 8691/79, seria A, nr 82, i do ww. wyroków: w sprawie Kruslin przeciwko Francji; w sprawie Kopp przeciwko Szwajcarii.

93 — Zasada rządów prawa, która jest zawarta w preambule do EKPC, zakłada, że prawo krajowe oferuje określoną ochronę przed arbitralnymi naruszeniami przez władzę publiczną praw, które ona gwarantuje. O ile zgodnie z tą zasadą „ingerencja władz w korzystanie przez jednostkę z praw może podlegać skutecznej kontroli” (wyrok Europejskiego Trybunału Praw Człowieka z dnia 6 września 1978 r. w sprawie Klass i in. przeciwko Niemcom, skarga nr 5029/71, seria A nr 28, s. 25–26, § 55; ww. wyrok w sprawie Malone, § 68; ww. wyrok w sprawie Silver i in., § 90), „wymaga ona między innymi, by ingerencja władzy wykonawczej w korzystanie przez jednostkę z praw podlegała skutecznej kontroli, którą zwykle powinna zapewniać, przynajmniej w ostatniej instancji, władza sądowa, ponieważ oferuje ona najlepsze gwarancje niezależności, bezstronności i słusznego procesu” (ww. wyrok Europejskiego Trybunału Praw Człowieka w sprawie Klass i in., § 55), wymaga także „minimalnego poziomu ochrony”, który nie zostałby osiągnięty, „gdyby swoboda uznania przyznana władzy wykonawczej była nieograniczona” (w odniesieniu do art. 8 EKPC – poza ww. wyrokami w sprawie Malone, § 68, i w sprawie Kruslin przeciwko Francji, § 30 – wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii, skarga nr 28341/95, Rec. 2000-V, § 55; z dnia 6 czerwca 2006 r. w sprawie Segerstedt-Wiberg i in. przeciwko Szwecji, skarga nr 62332/00, Rec. 2006-VII, § 76; z dnia 8 czerwca 2006 r. w sprawie Lupsa przeciwko Rumunii, skarga nr 10337/04, Rec. 2006-VII, § 34; decyzja Europejskiego Trybunału Praw Człowieka z dnia 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga nr 54934/00, Rec. 2006-XI, § 94; w odniesieniu do art. 10 EKPC, ww. wyrok w sprawie Sanoma Uitgevers, § 82), a także gdyby swoboda oceny przyznana sądowi była nieograniczona (wyrok Europejskiego Trybunału Praw Człowieka z dnia 24 kwietnia 1990 r. w sprawie Huvig przeciwko Francji, skarga nr 11105/84, seria A, nr 176-B, s. 55, § 29; ww. decyzja w sprawie Weber i Saravia przeciwko Niemcom, § 94; ww. wyrok w sprawie Liberty i in. § 62; wyrok z dnia 10 marca 2009 r. w sprawie Bykov przeciwko Rosji, skarga nr 4378/02, § 78).

mające na celu zobowiązanie do ich skutecznego przestrzegania”<sup>94</sup>.

zasięgnięcia porady przez zainteresowaną osobę w celu dokonania oceny, jakie konsekwencje wynikają w danym przypadku z konkretnego aktu<sup>96</sup>. Dotyczy to w szczególności profesjonalistów, którzy przyzwyczajeni są w ramach wykonywania swojego zawodu do zachowania szczególnej ostrożności.

98. Europejski Trybunał Praw Człowieka orzekł także, że zakres pojęcia przewidywalności i dostępności ustawy zależy w dużej mierze od treści danego aktu, dziedziny, jakiej on dotyczy, oraz rodzaju adresatów<sup>95</sup>. Przewidywalność ustawy nie wyklucza konieczności

99. Wreszcie Europejski Trybunał Praw Człowieka wyjaśnił, że termin „ustawa” należy rozumieć w jego ujęciu „materialnym”, a nie tylko w ujęciu formalnym, ponieważ może ono obejmować zarówno „prawo pisane”, jak i „prawo niepisane”, a także „prawo wypracowane” przez sądy<sup>97</sup>. Z tego punktu widzenia może być konieczne między innymi uwzględnienie w stosownym przypadku orzecznictwa. „Utrwalone orzecznictwo”, opublikowane, a zatem dostępne i uwzględniane przez sądy krajowe, jest w stanie w niektórych okolicznościach uzupełnić przepisy ustawowe oraz wyjaśnić je tak, aby stały się przewidywalne<sup>98</sup>.

94 — P. Wachsmann, *La prééminence du droit*, w: *Le droit des organisations internationales, Recueil d'études à la mémoire de Jacques Schwob*, s. 241, spéc. 263; zob. także G. Wiarda, *La Convention européenne des droits de l'homme et la prééminence du droit*, *Rivista di studi politici internazionali*, 1984, s. 452; K. Grabarczyk, *Les principes généraux dans la jurisprudence de la Cour européenne des droits de l'homme*, PUAM 2008, spéc. s. 194 i nast.; J.Y. Morin, „La prééminence du droit dans l'ordre juridique européen”, w: *Theory of International Law at the Threshold of the 21st Century. Essays in Honour of Krzysztof Skubiszewski*, Kluwer Law International, 1996, s. 643.

95 — Wyroki Europejskiego Trybunału Praw Człowieka z dnia 28 marca 1990 r. w sprawie Groppera Radio i in. przeciwko Szwajcarii, skarga nr 10890/84, seria A, nr 173, s. 26, § 68; z dnia 15 listopada 1996 r. w sprawie Cantoni przeciwko Francji, skarga nr 17862/91, Rec. 1996-V, § 35. Jak Trybunał podkreślił w odniesieniu do środka nadzoru poprzez GPS przemieszczania się danej osoby w miejscach publicznych, ściśle i utrwalone kryteria stosowane w specyficznym kontekście nadzoru telekomunikacji nie mogą być zastosowanie *mutatis mutandis* do wszystkich form ingerencji. Zobacz wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 września 2009 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05, § 66. W tej sprawie Trybunał kierował się zasadami ogólnymi, których należy przestrzegać, by „zapewnić odpowiednią ochronę przeciwko arbitralnej ingerencji w korzystanie z praw chronionych przez art. 8” EKPC. W tym przypadku, jak Trybunał przypomina, „gdy chodzi o potajemną kontrolę przez władze publiczne, brak kontroli publicznej i ryzyko nadużycia władzy wymagają, by prawo wewnętrzne oferowało ochronę przed ingerencją w korzystanie z praw zagwarantowanych przez art. 8”. „Trybunał powinien upewnić się, że istnieją stosowne i wystarczające gwarancje chroniące przed nadużyciami. Ta ocena zależy od całokształtu okoliczności sprawy, na przykład charakteru, zakresu i czasu trwania ewentualnych środków, przyczyn ich stosowania, władz właściwych do wydania upoważnienia do ich zastosowania, wykonywania i kontrolowania, rodzaju środka odwoławczego przewidzianego w prawie wewnętrznym”.

96 — Między innymi ww. wyroki: w sprawie Groppera Radio, § 68; w sprawie Tolstoy Miloslavsky, § 37.

97 — Zobacz m.in. wyroki Europejskiego Trybunału Praw Człowieka: z dnia 26 kwietnia 1979 r. w sprawie Sunday Times przeciwko Zjednoczonemu Królestwu (nr 1), skarga nr 6538/74, seria A nr 30, § 49; z dnia 13 lipca 1995 r. w sprawie Tolstoy Miloslavsky przeciwko Zjednoczonemu Królestwu, skarga nr 18139/91, seria A nr 316-B, § 37; ww. wyrok w sprawie Sanoma Uitgevers, § 83.

98 — Między innymi wyrok Europejskiego Trybunału Praw Człowieka z dnia 24 maja 1988 r. w sprawie Müller i in. przeciwko Szwajcarii, skarga nr 10737/84, seria A nr 133, § 29.

100. Podsumowując, zarówno w karcie, jak i w EKPC przyznano, że możliwe jest ograniczenie korzystania z praw i wolności, ingerencja w korzystanie z praw lub ograniczenie korzystania z wolności, które one gwarantują, pod warunkiem między innymi, że są one „przewidziane ustawą”. Europejski Trybunał Praw Człowieka, odwołując się głównie do zasady rządów prawa ustanowionej w preambule do EKPC, stworzył na podstawie tego wyrażenia i zasadniczo za pomocą pojęcia „jakości prawa”<sup>99</sup>, prawdziwą doktrynę, zgodnie z którą każde ograniczenie lub ingerencja powinny być uprzednio przedmiotem przepisu ustawowego, co najmniej w materialnym znaczeniu tego terminu, który jest wystarczająco jasny w świetle wyznaczonego celu, czyli zgodny z minimalnymi wymogami. To orzecznictwo powinno być uwzględniane przez Trybunał w ramach wykładni znaczenia odpowiednich postanowień karty.

E — „*Na podstawie samego przepisu ustawowego*”: *badanie ustawodawstwa krajowego w świetle wymogu dotyczącego „jakości ustawy” (art. 52 ust. 1 karty)*

101. Na tym etapie mojej analizy pozostało tylko udzielenie odpowiedzi na pytanie, czy podstawa ustawowa, którą sąd odsyłający zidentyfikował w systemie prawnym państwa członkowskiego, rzeczywiście może z punktu widzenia użytkowników usług ISP, a szerzej widzenia internautów, stanowić „ustawę” w rozumieniu orzecznictwa Europejskiego Trybunału Praw Człowieka, analizowanego powyżej, czego wymaga karta, dostosowanego w stosownym przypadku do specyficznych cech porządku prawnego Unii.

99 — Należy zauważyć, że orzecznictwo Europejskiego Trybunału Praw Człowieka stopniowo przyznawało pojęciu „jakości ustawy” znaczenie własne, dostosowane do realizacji celów wyznaczonych w EKPC, które je odróżnia od pojęć pokrewnych, o szerzej zakreślonej treści, które można znaleźć w prawie niektórych państw członkowskich; zob. m.in. L. Milano, *Contrôle de constitutionnalité et qualité de la loi*, *Revue du Droit public*, 2006, nr 3, s. 637; *La mauvaise qualité de la loi: Vagueness Doctrine at the French Constitutional Council*, *Hastings Constitutional Law Quarterly*, hiver 2010, nr 37, s. 243; M. Reicherzer, *Legitimität und Qualität von Gesetzen*, *Zeitschrift für Gesetzgebung*, 2004, s. 121; P. Wachsmann, *La qualité de la loi*, *Mélanges Paul Amselek*, s. 809; P. de Montalivet, „La »juridicisation« de la légistique. À propos de l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la Loi”, w: *La confection de la loi*, PUF 2005, s. 99; H. Moysan, „L'accessibilité et l'intelligibilité de la loi. Des objectifs à l'épreuve de la pratique normative”, *AJDA*, 2001, s. 428.

102. Na początku przypomnę dosłowną treść rozpatrywanego krajowego przepisu ustawy, czyli art. 87 § 1 akapit drugi loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, które sąd odsyłający przytoczył in extenso w samym pytaniu prejudycjalnym „[Prezes tribunal de première instance i prezes tribunal de commerce] mogą również wydać nakaz przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią do naruszania praw autorskich i pokrewnych”.

103. Po przedstawieniu tych wyjaśnień nie ulega wątpliwości, że prawo belgijskie zawiera „jedną” podstawę prawną odnośnie do wydania, w ramach postępowania cywilnego wszczętego w celu uzyskania stwierdzenia, ukarania i naprawienia szkody wynikającej z naruszenia prawa autorskiego lub praw pokrewnych, nakazu zaprzestania skierowanego, jak w sporze w postępowaniu krajowym, przeciwko ISP takiemu jak Scarlet, aby zagwarantować rzeczywiste zaprzestanie danego naruszenia. Problem podniesiony w pytaniu sądu odsyłającego nie dotyczy jednakże kwestii, czy właściwy sąd krajowy może w sposób ogólny wydać nakaz zaprzestania w takim kontekście i w takim celu, ale czy może w świetle wymogów wynikających z „jakości ustawy” w rozumieniu EKPC, a obecnie karty, nakazać zastosowanie środka, takiego jak ten, o którego zastosowanie wniesiono w niniejszym przypadku, na podstawie tego upoważnienia do wydania nakazu.

104. W tym kontekście należy najpierw przypomnieć moją uwagę początkową dotyczącą cech, a ostatecznie „charakteru” środka, o którego zastosowanie wniesiono.

105. Jak przedstawiłem powyżej, z punktu widzenia Scarlet i ISP obowiązek wprowadzenia na ich wyłączny koszt systemu filtrowania i blokowania takiego jak ten, który jest

rozpatrywany, jest, po pierwsze, tak charakterystyczny, a nawet niepowtarzalny, a z drugiej strony „nowy”, czyli nieoczekiwany, że może być dopuszczony wyłącznie w przypadku, gdy jest przewidziany w sposób wyraźny, uprzedni, jasny i dokładny w „ustawie” w rozumieniu karty. Tymczasem z trudem tylko można uznać, że przyjmując żądany środek na podstawie rozpatrywanego przepisu ustawowego, właściwy sąd krajowy działałby w granicach wyrażnie, uprzednio, jasno i dokładnie określonych przez „ustawę”, uwzględniając w szczególności przepisy art. 15 dyrektywy 2000/31<sup>100</sup>. Z punktu widzenia Scarlet wydanie przez sąd belgijski środka o takim charakterze było trudne do przewidzenia<sup>101</sup> i ze względu na jego potencjalne konsekwencje ekonomiczne prowadzi wręcz do arbitralności.

106. Z punktu widzenia użytkowników usług Scarlet, a szerzej internautów, żądany system filtrowania, niezależnie od zasad jego

100 — Artykuł 15 ust. 1 dyrektywy 2000/31 nakłada na państwa członkowskie podwójny obowiązek niepodejmowania działań. Państwa członkowskie powinny powstrzymać się od nakładania na „usługodawców” ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują, oraz ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność. Artykuł 12 ust. 1 dyrektywy 2000/31 nakłada na państwa członkowskie ponadto obowiązek zapewnienia, by dostawcy usług dostępu do sieci komunikacyjnej, a zatem między innymi ISP, nie byli odpowiedzialni za przekazywane informacje.

101 — W motywie 30 dyrektywy 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. zmieniającej dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz.U. L 337, s. 11–36) wyjaśniono także, że „[d]yrektywa 2002/22/WE nie wymaga od dostawców monitorowania informacji przekazywanych za pośrednictwem ich sieci lub podejmowania środków prawnych przeciwko ich klientom na podstawie takich informacji ani nie nakłada na dostawców odpowiedzialności za takie informacje”.



konkretnego funkcjonowania, miałyby mieć zastosowanie w sposób systematyczny i powszechny, stały i nieustanny, ale jego wprowadzeniu nie towarzyszy żadna szczególna gwarancja w odniesieniu do ochrony danych osobowych i poufności komunikacji. Ponadto mechanizm blokowania, niezależnie od zasad konkretnego funkcjonowania, także byłby stosowany bez wyraźnego ustanowienia na rzecz osób, których dotyczyłoby blokowanie, czyli internautów, możliwości sprzeciwienia się blokowaniu danego pliku lub podważenia jego zasadności.

107. Z trudnością mogłoby być inaczej, ponieważ celem rozpatrywanej ustawy krajowej w żaden sposób nie jest upoważnienie właściwych sądów krajowych do przyjęcia środka polegającego na filtrowaniu wszystkich połączeń elektronicznych abonentów ISP wykonujących działalność na terytorium danego państwa członkowskiego.

108. Narzuca się zatem wniosek, że rozpatrywany przepis prawa krajowego nie może w świetle art. 7, 8 i 11 karty, a w szczególności wymogów dotyczących „jakości ustawy”, a szerzej wymogów rządów prawa, być uznany za wystarczającą podstawę ustawową do wydania środka nakazu nakładającego obowiązek wprowadzenia systemu filtrowania

i blokowania takiego jak ten, którego zażądano w sporze przed sądem krajowym.

109. Zresztą z punktu widzenia „materialnego” pojęcia „ustawy” także należy stwierdzić, że w żaden sposób nie dowiedziono istnienia obszernego orzecznictwa sądów belgijskich, powtarzającego i uszczegóławiającego wykładnię oraz stosowanie rozpatrywanego przepisu prawa krajowego, zgodnie z prawem unijnym i prawem EKPC, pod względem żądanego środka, co umożliwiłoby stwierdzenie, że wymóg dotyczący przewidywalności ustawy został spełniony<sup>102</sup>.

110. W świetle powyższego stwierdzenia nie jest konieczne badanie wpływu prawa unijnego<sup>103</sup> na „jakość” krajowej podstawy prawnej. Rzecznik generalny J. Kokott podkreśliła w tym względzie w ww. opinii w sprawie *Promusicae*<sup>104</sup>, że „równowaga między poszczególnymi prawami podstawowymi winna zostać określona w pierwszym rzędzie przez prawodawcę”, lecz że „niemniej państwa członkowskie są także zobowiązane mieć ją na uwadze przy wykonywaniu kompetencji

102 — Zobacz w szczególności ww. wyrok Europejskiego Trybunału Praw Człowieka w sprawie *Chappel*, § 56. Zobacz także wyroki Europejskiego Trybunału Praw Człowieka: z dnia 15 lutego 2007 r. w sprawie *Bock i Palade* przeciwko Rumunii, skarga nr 21740/02, §§ 61–64; z dnia 14 lutego 2008 r. w sprawie *July i Libération* przeciwko Francji, skarga nr 20893/03, § 55; z dnia 5 lutego 2009 r. w sprawie *Brunet-Leconte* i in. przeciwko Francji, skarga nr 42117/04, § 42.

103 — W odniesieniu do uwzględnienia przez Europejski Trybunał Praw Człowieka prawa unijnego w ramach badania jakości ustawy zob. m.in. ww. wyrok Europejskiego Trybunału Praw Człowieka w sprawie *Cantoni*, § 30, i decyzja Europejskiego Trybunału Praw Człowieka z dnia 27 maja 2008 r. w sprawie *Marchiani* przeciwko Francji, skarga nr 30392/03.

104 — Punkt 56.

ustawowej pozostawionej im w ramach dokonywania transpozycji dyrektyw”.

111. W ten sposób została podkreślona bardzo delikatna kwestia „odpowiedzialności” odpowiednio Unii i państw członkowskich w świetle zbadanych wyżej wymogów rządów prawa w sytuacji, w której dyrektywy, wraz z krajowymi środkami mającymi na celu transpozycję, są przedmiotem stosowania prowadzącego do „ograniczenia” prawa zagwarantowanego lub wolności potwierdzonej w karcie. Jednakże sformułowanie pytania postanowionego przez sąd odsyłający, które dotyczy wyraźnie przepisów prawa krajowego mających na celu transponowanie dyrektyw 2001/29 i 2004/48 dotyczących ochrony prawa własności intelektualnej, pozwala, po uprzednim stwierdzeniu, że żadna z rozpatrywanych dyrektyw nie nakłada obowiązku wprowadzenia systemu filtrowania i blokowania takiego jak ten, którego zażądano w sporze przed sądem krajowym, na pozostawienie tymczasowo tego pytania na marginesie rozważań.

112. Wreszcie koncepcja, zgodnie z którą rozpatrywane dyrektywy, a w szczególności dyrektywa 2000/31, powinny być przedmiotem zaktualizowanej wykładni, uwzględniającej rozwój technologii i wykorzystanie Internetu, powinna w tym kontekście być odrzucona. O ile bezspornie wymóg przewidywalności nie wiąże się z koniecznością istnienia bezwzględnej pewności, jak wielokrotnie

orzekł Europejski Trybunał Praw Człowieka<sup>105</sup>, podejście broniące „żywej” wykładni aktów nie może zamaskować braku jakiegokolwiek krajowej podstawy ustawowej wymieniającej w sposób wyraźny system filtrowania i blokowania połączeń elektronicznych. Wykładnia prawa unijnego, a w szczególności art. 15 dyrektywy 2000/31, jako umożliwiającego przyjęcie środka takiego jak ten, o którego zastosowanie wniesiono, lub nie sprzeciwiającego się temu, byłaby niezgodna z wymogami „jakości ustawy” oraz naruszałaby zasady pewności prawa<sup>106</sup> i ochrony uzasadnionych oczekiwań.

113. Pozwolę sobie dodać kilka uwag końcowych. Karta, podobnie jak EKPC, wymagając, by każde „ograniczenie” praw i wolności (lub „ingerencja” w tej dziedzinie) było „przewidziane ustawą”, odsyła w sposób wyraźny do funkcji ustawy, prawa w ścisłym tego słowa znaczeniu, jako źródła *tranquillitas publica* w bardzo wrażliwej dziedzinie, która jest przedmiotem rozważań. W samej karcie nie tylko przewidziano, że ustawa powinna istnieć przed jakimkolwiek ograniczeniem prawa i wolności, ale także że ograniczenie to powinno szanować „istotę” tych praw i wolności, co wymaga w sposób praktycznie nie do pominięcia interwencji ustawodawcy

105 — Jak podkreśla Trybunał, „pewność, chociaż bardzo pożądana, łączy się czasami z nadmiernym brakiem elastyczności; tymczasem prawo powinno móc dostosować się do zmian sytuacji”; m.in. ww. wyrok w sprawie *Sunday Times*, § 49; wyrok Europejskiego Trybunału Praw Człowieka z dnia 18 maja 2004 r. w sprawie *Éditions Plon* przeciwko Francji, skarga nr 58148/00, Rec. 2004-IV, § 26.

106 — W odniesieniu do wykazywanego czasami przez Europejski Trybunał Praw Człowieka związku pomiędzy zasadą rządów prawa a zasadą „bezpieczeństwa sytuacji prawnych” zob. w szczególności wyroki Europejskiego Trybunału Praw Człowieka: z dnia 25 lipca 2002 r. w sprawie *Sovtransavto Holding* przeciwko Ukrainie, skarga nr 48553/99, Rec. 2000-VII, § 77; z dnia 8 listopada 2005 r. w sprawie *Timotiyeveich* przeciwko Ukrainie, skarga nr 63158/00, § 32. Zobacz także ww. doktorat K. Grabarczyka, *Les principes généraux dans la jurisprudence de la Cour européenne des droits de l'homme*, zwłaszcza s. 209 i nast., nr 583 i nast.

w określenie granicy pomiędzy ograniczeniem prawa a zasadniczo nienaruszalnym zakresem tej istoty. Podobnie w karcie przewidziano, że każde ograniczenie korzystania z praw i wolności, jakie uznaje, powinno być zgodne z zasadą proporcjonalności, konieczności i powinno rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. W świetle wszystkich tych wymogów moim zdaniem, ponownie, nie istnieje „ustawa” rozumiana jako prawo „stanowione”, czyli demokratycznie legitymowane. Tylko bowiem ustawa w znaczeniu parlamentarnym mogłaby umożliwić przystąpienie do badania pozostałych wymogów, które ustanawia art. 52 ust. 1 karty. W tym względzie można byłoby podnieść, że art. 52 ust. 1 karty obejmuje domyślny wymóg, aby ustawa była

„stanowiona”, w powiązaniu z intensywnością debaty publicznej. Jednakże rozpatrywanym tutaj wymogiem jest wyraźny wymóg ustawy jako „prawa istniejącego”. Stwierdziwszy, że wymóg ten nie został w niniejszym przypadku spełniony, można udzielić odpowiedzi na pierwsze pytanie postawione przez sąd odsyłający.

114. Podsumowując, proponuję, by Trybunał odpowiedział przecząco na pierwsze z pytań prejudycjalnych zadanych przez Cour d'appel de Bruxelles i w konsekwencji uznał, że nie ma potrzeby udzielania odpowiedzi na pytanie drugie, postawione pomocniczo.

## V — Wnioski

115. Podsumowując, proponuję Trybunałowi, aby odpowiedział w sposób następujący na pytanie zadane przez Cour d'appel de Bruxelles:

Dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym i 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej, w związku z dyrektywami 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, 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej i 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego („dyrektywa o handlu elektronicznym”), interpretowane w świetle art. 7, 8, 11 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, z uwzględnieniem art. 8 i 10 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, należy interpretować w ten sposób, że sprzeciwiają się one przyjęciu przez sąd krajowy jedynie na podstawie przepisu stanowiącego, że „[właściwe sądy mogą] również wydać nakaz przeciwko pośrednikowi, którego usługi są wykorzystywane przez osobę trzecią do naruszania praw autorskich i pokrewnych”, środka nakazującego „[dostawcy dostępu do Internetu] wprowadzenie, w stosunku do wszystkich swoich klientów, in abstracto i w celach zapobiegawczych, na wyłączny koszt tego dostawcy i bez ograniczeń w czasie, systemu filtrowania wszystkich połączeń elektronicznych, zarówno wchodzących, jak i wychodzących, przekazywanych za pośrednictwem jego usług, w szczególności przy zastosowaniu programów peer to peer, w celu zidentyfikowania w jego sieci przypadków przekazywania plików elektronicznych zawierających utwory muzyczne, kinematograficzne lub audiowizualne, co do których strona powodowa rości sobie prawa, a następnie zablokowania transferu tych plików, bądź to na etapie próby ich pobrania, bądź na etapie ich wysłania”.