Zeszyt
48

PRZEMYSŁAW POLAŃSKI

# Odpowiedzialność prawna za treści rozpowszechniane w Internecie

# Legal liability for content disseminated over the Internet

Centrum Europejskie Natolin

PRZEMYSŁAW POLAŃSKI

# Odpowiedzialność prawna za treści rozpowszechniane w Internecie*

# Legal liability for content disseminated over the Internet

* Opracowanie jest rezultatem badań Autora przeprowadzonych w 2010 r. w ramach programu badań letnich w Europejskim Instytucie Uniwersyteckim we Florencji dzięki grantowi Centrum Europejskiego Natolin.

*redaktor prowadzący serii*
MARIAN STASIAK

*redakcja w języku polskim*
ELŻBIETA NOWICKA-ROŻEK

*tłumaczenie na język angielski*
JAROSŁAW BRZEZIŃSKI

*skład i druk*
BIGBIT WOJCIECH ZEYDLER-ZBOROWSKI

*projekt graficzny*
WOJCIECH SOBOLEWSKI

*wydawca / published by*
CENTRUM EUROPEJSKIE NATOLIN,
UL. NOWOURSYNOWSKA 84 · 02-797 WARSZAWA
TEL. 22 545 98 00 · FAX 22 649 12 99
FUNDACJA@NATOLIN.EDU.PL · WWW.NATOLIN.EDU.PL

ISSN 1732-0445
ISBN 978-83-62818-09-9

WARSZAWA 2012

# *Spis treści*

# *Table of contents*

# *1. Wprowadzenie*

W czerwcu 2010 r. upłynęło dziesięć lat od uchwalenia dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego,[1] która stworzyła ramy prawne rozwoju internetowej gospodarki w Unii Europejskiej. Dyrektywa ta została zaimplementowana do polskiego porządku prawnego w ustawie o świadczeniu usług drogą elektroniczną[2] oraz w kodeksie cywilnym.

W ciągu ostatniej dekady nie tylko gwałtownie wzrosła liczba użytkowników Internetu, która obecnie w Europie przekroczyła już 2/3 unijnej populacji, ale także rozwinęły się na ogromną skalę usługi oferowane w Internecie, które dyrektywa określa mianem usług społeczeństwa informacyjnego. W efekcie ponad 330 milionów[3] użytkowników Internetu w UE codziennie ma możliwość nie tylko dokonywania zakupów w sieci, wyszukiwania informacji, porównywania cen czy edukowania się, ale także aktywnego wypowiadania się na blogach, udostępniania własnych zdjęć czy filmów, wspólnego rozwoju encyklopedii, takich jak Wikipedia, czy uczestniczenia w zdalnych kursach „e-learningowych". W ciągu

[1] Dyrektywa 2000/31/WE z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym (dyrektywa o handlu elektronicznym), Dz. Urz. WE L 178 z 17.07.2000.

[2] Ustawa o świadczeniu usług drogą elektroniczną z 18 lipca 2002 r. (Dz. U. nr 144, poz. 1204 ze zm.). Dalej jako UsługiElektrU lub ustawa o świadczeniu usług drogą elektroniczną.

[3] Dokładnie 337,779,055 użytkowników w czerwcu 2010 r. Źródło: >>http://www.internetworldstats.com/ europa.htm<<, ostatni dostęp: 19.11.2010.

tego okresu świat Internetu w UE rozwinął się na ogromną skalę, przeobrażając się z ogromnego zbioru statycznych stron internetowych serwowanych użytkownikowi w gigantyczną sieć stron interaktywnych, na których użytkownicy mogą umieszczać własne treści.

W erze tzw. Web 2.0 użytkownicy interaktywnych serwisów stali się równocześnie autorami treści tam publikowanych, przeobrażając na ogromną skalę myślenie o rozwoju usług internetowych, jak i tworząc wyzwanie dla regulatorów rynku internetowego, którzy dekadę temu tworzyli rozwiązania prawne w odmiennej rzeczywistości. Dyrektywa o handlu elektronicznym stworzyła podstawy prawne rozwoju gospodarki elektronicznej, koncentrując się na ustanowieniu liberalnych zasad podejmowania działalności gospodarczej w sieci, gwarantując przy tym internetowym przedsiębiorcom korzystanie z zasady państwa pochodzenia, która w swym założeniu miała poddać działalność przedsiębiorcy tylko jednemu systemowi prawnemu w UE. Oprócz tych gwarancji dyrektywa o handlu elektronicznym stworzyła wiele istotnych mechanizmów harmonizujących prawo państw członkowskich[4] w obszarze obowiązków informacyjnych i reklamy internetowej, prawa umów elektronicznych, a także transponowała z USA mechanizm ograniczenia odpowiedzialności prawnej za przesyłane lub przechowywane treści pewnej kategorii przedsiębiorców dystrybuujących treści w Internecie.

Jednym z celów dyrektywy stało się usunięcie problemów powstających w związku z pojawiającymi się rozbieżnościami między ustawodawstwem oraz orzecznictwem państw członkowskich w dziedzinie odpowiedzialności usługodawców działających jako pośrednicy. Prawodawca europejski uznał, że stanowią one przeszkodę w sprawnym funkcjonowaniu rynku wewnętrznego, w szczególności krępując rozwój usług transgranicznych i powodując zakłócenia w konkurencji.[5] Nadrzędnym

[4] Szerzej na ten temat: P. POLAŃSKI, *Usługi…*

[5] Motyw 40 dyrektywy o handlu elektronicznym.

celem stało się więc wprowadzenie stanu równowagi między różnymi interesami oraz ustanowienie zasad, które mogłyby służyć jako podstawa norm i umów branżowych.[6]

Wprowadzenie zasad wyłączenia odpowiedzialności pośredników za treści przesyłane w Internecie miało na celu umożliwienie im swobodnego prowadzenia działalności w sieci. Chodzi o podmioty oferujące usługi dostępu do Internetu oraz transmisji danych w sieci (*mere conduit*), usługodawców buforowania danych (ang. *caching*) oraz dostawców usług przechowania i udostępnienia danych (ang. *hosting*). Zdejmując z nich ciężar aktywnego poszukiwania bezprawnych danych, przy jednoczesnym wyłączeniu lub ograniczeniu ich odpowiedzialności z tytułu przekazywanych informacji, prawodawca unijny nie zdecydował się na jasne objęcie tym reżimem podmiotów oferujących usługi wyszukiwania w Internecie czy specjalnego reżimu dla uczelni, jak uczynił to amerykański prawodawca w *Digital Millennium Copyright Act*.[7] Prawodawca europejski nie określił również procedury, którą miałby się posłużyć przedsiębiorca poinformowany o przechowywaniu bezprawnych treści, mającej na celu zablokowanie lub odblokowanie dostępu do kwestionowanych materiałów. Powyższe braki wywołują spore problemy w stosowaniu przepisów dyrektywy, jak i w implementujących je przepisach krajowych, co jest szczególnie widoczne na tle orzeczeń ETS w sprawach połączonych C-236/08, 237/08 i 238/08 dotyczących wyszukiwarki Google.

Celem niniejszego opracowania jest analiza bliżej adekwatności obowiązujących rozwiązań na tle obecnego stanu rozwoju Internetu w UE. W pierwszej części opracowania krótko zostanie omówione rozwiązanie amerykańskie, które stało się wzorcem dla rozwiązań unijnych. Następnie przeanalizowane zostanie rozwiązanie obecnie przyjęte w dyrektywie

---

[6] Motyw 41 dyrektywy o handlu elektronicznym.

[7] Zob. section 512 *Digital Millennium Copyright Act*.

i w ustawie o świadczeniu usług drogą elektroniczną w zakresie braku obowiązku filtrowania treści oraz wyłączenia odpowiedzialności za zwykły przekaz, buforowanie i wreszcie przechowywanie danych. W podsumowaniu sformułowane zostaną wnioski i postulaty dotyczące reformy reżimu odpowiedzialności pośredników internetowych w UE.

## *2. Odpowiedzialność pośredników w USA*

Rozwiązania dotyczące ograniczenia odpowiedzialności pośredników w Internecie zostały po raz pierwszy sformułowane i przyjęte w amerykańskiej ustawie *Digital Millennium Copyright Act* z 1998 r., która wyłącza lub ogranicza odpowiedzialność pośredników w Internecie jedynie w zakresie naruszeń prawa autorskiego. Wyłączenie odpowiedzialności pośredników z tytułu naruszenia dóbr osobistych ujęte jest odmiennie w *Communications Decency Act*. Oba rozwiązania wymagają choćby bardzo skrótowego omówienia.

### *2.1. „Digital Millennium Copyright Act" (DMCA)*

Intencją twórcy DMCA nie było wprowadzenie nowego reżimu odpowiedzialności za naruszenie praw autorskich w sieci, ale ograniczenie rodzącej się na gruncie istniejącego prawa amerykańskiego odpowiedzialności pośredników przesyłających treści w Internecie. Ograniczenie to obejmuje zarówno sprawstwo oraz współsprawstwo (ang. *direct liability*), jak i odpowiedzialność z tytułu przyczynienia się do naruszenia (ang. *contributory liability*) oraz odpowiedzialność za cudze czyny (ang. *vicarious liability*). Aby jednak usługodawca transmisji danych, „cachingu", „hostingu" czy wyszukiwania informacji mógł się powołać na stosowne przepisy, musi wykazać, że jest usługodawcą (ang. *service provider*), przy

czym DMCA zawiera dwie definicje dostawcy usług. Zgodnie z pierwszą, usługodawcą jest podmiot oferujący usługi transmisji treści wskazanych przez użytkownika.[8] Zgodnie z drugą, usługodawcą jest podmiot oferujący (1) usługi *online* lub (2) usługi dostępu do sieci, lub (3) usługi operatorskie sieci.[9] Druga definicja jest definicją znacznie szerszą i obejmuje swym zakresem wszystkie kategorie podmiotów wskazanych powyżej, w tym także podwykonawców działających na rzecz pośredników wskazanych kategorii.

Ograniczenia odpowiedzialności pośredników w DMCA obejmuje pięć kategorii pośredników:

1. Podmioty oferujące usługi przesyłania danych poprzez sieci telekomunikacyjne (ang. *Transitory Communications*),[10] co sprowadza się – w skrócie – do usług dostępu do Internetu oraz transmisji danych w sieciach telekomunikacyjnych. W Unii Europejskiej i w Polsce usługi te określa się jako usługi zwykłego przekazu (ang. *mere conduit*).
2. Podmioty oferujące usługę „cachingu" (ang. *System caching*),[11] czyli buforowania danych w celu umożliwienia ich szybszego pobierania. DMCA nakazuje konfigurowanie serwera w taki sposób, jak to się powszechnie praktykuje w branży IT. Odesłanie do standardów powszechnie stosowanych w obrocie może być interpretowane jako odesłanie do praktyk w Internecie, które dopiero się tworzą, przy czym głównymi instytucjami, od których oczekuje się wypracowania stosownych standardów, są IETF oraz W3C.[12]

---

[8] Na gruncie europejskim odpowiada tej definicji dostawca usług zwykłego przekazu (*mere conduit*).

[9] Section 512(k)(l)(B) as „a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A)."

[10] DMCA, Section 512(a).

[11] DMCA, Section 512(b).

[12] HR2281, s. 73.

3. Podmioty oferujące usługi przechowywania danych w systemach komputerowych lub w sieci komputerowej na żądanie użytkowników (ang. *Storage of information on systems or networks at direction of users*).[13] W dyrektywie o handlu elektronicznym usługę tę określa się mianem „hostingu", a w polskim prawie – przechowaniem danych na żądanie usługobiorcy. Wskazane wyżej rodzaje usług zostaną poddane analizie w dalszej części pracy.
4. Podmioty oferujące usługi wyszukiwania informacji (ang. *Information location tools*),[14] a w szczególności dostęp do treści w Internecie za pomocą hiperłączy dostarczanych użytkownikowi w wynikach wyszukiwania, katalogach stron czy indeksach zasobów. W tym miejscu warto podkreślić, że Unia Europejska nie wprowadziła tego wyłączenia do dyrektywy o handlu elektronicznym, co powoduje wiele wątpliwości interpretacyjnych, o czym najlepiej świadczy omawiany w dalszej części wywodu wyrok Trybunału Sprawiedliwości w sprawach C-236-238/08, w których stroną pozwaną jest wyszukiwarka Google.
5. Podmioty oferujące usługi edukacyjne (ang. *non-for-profit institutions of higher learning*). DMCA zawiera specjalną klauzulę, która umożliwia zastosowanie powyższych ograniczeń odpowiedzialności do uniwersytetów działających w charakterze pośredników w dostępie do treści *online*.[15] Specjalna pozycja uczelni związana jest z wyjątkową rolą, jaką odgrywają one w krzewieniu wiedzy i wspieraniu nieskrępowanej wymiany myśli w społeczeństwie. Aby móc się oprzeć na ograniczeniu odpowiedzialności, musi być spełniona jedna przesłanka natury ogólnej oraz trzy przesłanki szczegółowe. Co do przesłanki ogólnej, kryterium podstawowym jest funkcja wykładowcy podczas

[13] DMCA, Section 512(c).

[14] DMCA, Section 512(d).

[15] HR2281, s. 74.

naruszania prawa. Uczelnie nie poniosą odpowiedzialności tak jak zwykły pracodawca za naruszenie prawa dokonane przez wykładowców podczas wykonywania przez nich funkcji dydaktycznych i naukowych, natomiast naruszenia prawa związane z pełnieniem funkcji administracyjnych lub operatorskich przez tego samego wykładowcę zostanie w pełni przypisane uczelni. Jednakże nawet pełnienie funkcji dydaktycznych lub naukowych nie uchroni uczelni w przypadku, gdy naruszenie prawa dotyczyć będzie treści dydaktycznych lub naukowych formalnie rekomendowanych studentom w ciągu ostatnich 3 lat. Po drugie, w tym samym okresie uczelnia nie powinna otrzymać więcej razy niż dwukrotnie informacji o podejrzeniu popełnienia przez wykładowcę naruszania prawa autorskiego. Po trzecie, uczelnie powinny aktywnie promować działalność studentów, wykładowców i administracji uczelni zgodnie z prawem autorskim. Powyższe przesłanki uwzględnić należy dopiero wówczas, gdy uczelnia miałaby ponieść odpowiedzialność na gruncie obowiązującego prawa. Intencją prawodawcy nie było bowiem wprowadzenia nowego czy innego rodzaju odpowiedzialności dla uczelni w DMCA.[16]

Ustawodawstwo amerykańskie jako pierwsze wprowadziło zwolnienie wskazanych wyżej kategorii usługodawców od obowiązku aktywnego filtrowania aktywności użytkowników pod względem identyfikacji przypadków naruszenia prawa autorskiego.[17] Nie oznacza to jednak, że intencją prawodawcy amerykańskiego było zniechęcenie pośredników do monitoringu treści. Wręcz przeciwnie, zgodnie z uzasadnieniem w projekcie HR2281 sądy nie powinny odmówić przyznania ochrony pośrednikom tylko ze względu na podjęcie się przez nich filtrowania treści.[18] Idea ta została recypowana w art. 15 dyrektywy o handlu elektronicznym

[16] HR2281, s. 75.

[17] Section 512 (m) DMCA.

[18] HR2281, s. 73.

w stosunku do wszelkich typów naruszeń, a nie tylko w odniesieniu do naruszeń prawa autorskiego. Natomiast w DMCA podmiot praw autorskich może się domagać ujawnienia danych osobowych osób naruszających jego monopol od podmiotów objętych ograniczeniem lub wyłączeniem odpowiedzialności.[19]

Koncepcja ograniczenia odpowiedzialności na gruncie prawa autorskiego z tytułu pośredniczenia w przekazywaniu, przechowywaniu lub wyszukiwaniu danych sprowadza się do całkowitego wyłączenia odpowiedzialności odszkodowawczej (obejmującej także koszty sądowe oraz koszty reprezentacji prawnej)[20] oraz znacznego ograniczenia możliwości uzyskania zabezpieczenia roszczeń w drodze nakazu lub zakazu sądowego (ang. *Injunctive relief*). W przypadku gdy usługodawca nie będzie się w stanie powołać na jedno z omawianych ograniczeń, będzie wciąż mógł się chronić innymi podstawami prawnymi, na przykład koncepcją dozwolonego użytku (ang. *fair use*). Na tym tle warto dodać, iż na gruncie polskiej doktryny prawa autorskiego pojawił się pogląd o dopuszczalności wniesienia roszczenia o zaniechanie przeciwko omawianym kategoriom usługodawców internetowych.[21]

## *2.2. „Communications Decency Act" (CDA)*

Tak jak fundamentalne znaczenie dla określenia reguł wyłączenia odpowiedzialności za naruszenia prawa autorskiego w sieci ma DMCA, tak podobnie ogromne znaczenie w związku ze zniesławieniami w Internecie ma *Communications Decency Act*. Regulacja przyjęta w CDA umożliwiła pośrednikom ingerowanie w treści generowanye przez użytkowników serwisu bez obawy o bycia uznanym za wydawcę

[19] Section 512(h) DMCA.

[20] „Monetary relief is defined in subsection (k)(2) as encompassing damages, costs, attorneys' fees, and any other form of monetary payment.", HR2281, s. 73.

[21] J. BARTA, R. MARKIEWICZ, *Prawo autorskie*, Warszawa 2010, s. 311.

bezprawnych treści. Była to odpowiedź na głośne orzeczenie z 1995 r. w sprawie *Stratton Oakmont, Inc. v. Prodigy Services Co*,[22] w którym Sąd Najwyższy stanu Nowy Jork uznał, że dostawca usług dostępu do forum dyskusyjnego, w którym pełnił funkcję aktywnego moderatora, może być pociągnięty do odpowiedzialności za treści zamieszczane przez użytkowników tego forum.

Zgodnie z art. 230 CDA, „żaden dostawca usług lub użytkownik interaktywnej usługi komputerowej nie powinien być uznany za wydawcę (ang. *publisher*) lub przekaziciela (ang. *speaker*) jakiejkolwiek informacji dostarczanej przez innego dostawcę treści (ang. *information content provider*)."[23] Amerykańskie sądy rozwinęły trójstopniowy test mający ułatwić stosowanie omawianego przepisu prawa telekomunikacyjnego. Zgodnie z nim, aby pozwany mógł się skutecznie powołać na art. 230 CDA, musi wykazać, że:

1) jest dostawcą lub użytkownikiem interaktywnego systemu komputerowego;
2) nie występuje w roli wydawcy lub przekaziciela zniesławiających treści oraz
3) nie jest źródłem treści zniesławiających.

Omawiana regulacja zdecydowanie wzmocniła pozycję pośredników w dostępie do treści w sieci, w szczególności operatorów witryn wyświetlających treści zamieszczane przez ich użytkowników, którzy obecnie mogą swobodnie ingerować w zawartość komunikatów w celu eliminacji treści ewidentnie bezprawnych. Artykuł 230 stał się jednak źródłem kontrowersji ze względu na praktykę sądów amerykańskich, które stosują ten przepis bardzo liberalnie przez co w niektórych przypadkach ofiary pomówień nie mają szansy uzyskania odszkodowania od kogokolwiek,

[22] 1995 WL 323710 (N.Y. Sup. Ct. 1995).

[23] *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider* (s. 230 CDA).

w szczególności gdy brakuje informacji o źródle bezprawnych treści. Często podawanym przykładem jest sprawa *Zeran v. AOL*,[24] w której zniesławiony Zeran nie uzyskał odszkodowania od usługodawcy forum dyskusyjnego, mimo że AOL znacząco spóźnił się z usunięciem treści pomawiających. Omawiana regulacja ma szczególne znaczenie w kontekście regulacji odpowiedzialności za treści przechowywane w ramach usługi hostingu.

## *3. Brak obowiązku filtrowania treści w Unii Europejskiej*

Dyrektywa o handlu elektronicznym, podobnie jak DMCA, nie nakłada na usługodawców świadczących usługi zwykłego przekazu, „cachingu" i „hostingu" ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują, ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na działalność bezprawną. Jednakże 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 bądź
- obowiązek przekazywania właściwym władzom, na ich żądanie, informacji pozwalających na ustalenie tożsamości ich usługobiorców, z którymi mają umowy o przechowywanie danych.

Powyższe stanowisko prawodawcy europejskiego motywowane jest dość powszechnym przekonaniem, że podmioty te nie mogłyby praktycznie wykonywać swoich podstawowych funkcji, gdyby zostały

[24] 129 F.3d 327 (4th Cir. 1997).

obarczone obowiązkiem uprzedniej kontroli treści przekazywanych lub przechowywanych. Wolumen danych, które przetwarzają, jest tak duży, że prowadziłoby to do narzucenia nadmiernych i nieproporcjonalnych obowiązków na świadczących usługi, a w konsekwencji doprowadziłoby także do wzrostu cen dostępu do Internetu i usług *online*.[25] Wreszcie działania takie doprowadziłyby do wprowadzenia cenzury w Internecie, a przy tym – paradoksalnie – mogłyby znacząco osłabić pozycję prawną dostawców usług *online*, bowiem jakakolwiek ingerencja w przesyłane dane rodziłaby możliwość uznania ich za ingerujących w zawartość przetwarzanych danych, a w konsekwencji pozbawić ochrony na gruncie „oaz bezpieczeństwa" przewidzianych w dyrektywie oraz w ustawie o świadczeniu usług drogą elektroniczną.

Bez względu jednak na brak generalnego obowiązku nadzorowania treści, dyrektywa wyraźnie przewiduje możliwość filtrowania konkretnie wskazanych treści. Zgodnie z motywem 47 dyrektywy, „Państwa Członkowskie nie mogą nakładać na usługodawców obowiązku nadzoru jedynie w odniesieniu do obowiązków o charakterze ogólnym; nie dotyczy to obowiązków nadzoru mających zastosowanie do przypadków szczególnych oraz, w szczególności, nie ma wpływu na decyzje władz krajowych podjęte zgodnie z ustawodawstwem krajowym." Ponadto usługodawcy mają także w niektórych przypadkach obowiązek działania w celu zapobieżenia bezprawnej działalności lub wstrzymania jej.[26] I to właśnie ta możliwość jest przyczyną rosnącej niepewności prawnej w sieci. Przykładem mogą być wzajemnie sprzeczne orzeczenia sądów niemieckich dotyczących portalu *RapidShare*. W orzeczeniu Sądu Okręgowego w Dusseldorfie z 23 grudnia 2008 r. uznano, że *RapidShare* jest zobowiązany do zapobiegania piractwu oraz do stosowania bardziej skutecznych środków zapobiegających naruszeniu praw

[25] Por. *First Report…*

[26] Motyw 40 dyrektywy o handlu elektronicznym.

autorskich. Jednakże Sąd Apelacyjny w Dusseldorfie w wyroku wydanym 27 kwietnia 2010 r. uznał, że *RapidShare* nie jest odpowiedzialny za naruszenia praw autorskich ani jako sprawca bezpośredni, ani jako pomocnik.[27] Bez wątpienia w UE należałoby uporządkować reguły filtrowania treści, przy czym wprowadzenie obowiązku filtrowania nadsyłanej zawartości to dobre rozwiązanie,[28] pod warunkiem jednakże uprzedniego lepszego dookreślenia zakresu podmiotowego zastosowania tego obowiązku.

Polska implementowała art. 15 dyrektywy w jeszcze bardziej lakoniczny sposób, a mianowicie uznała, że podmiot, który świadczy usługi zwykłego przekazu, buforowania oraz hostingu nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych. Tym samym ustawa wyraźnie przesądziła, iż wyłączenie odpowiedzialności tych podmiotów nie jest zależne od zachowania aktów szczególnej staranności z ich strony w zakresie, w jakim dotyczy to samej kontroli przechowywanych lub przekazywanych danych.[29] Natomiast w polskiej implementacji dyrektywy brakuje wyraźnego wyłączenia obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność. Powstaje pytanie, czy w wyłączeniu obowiązku sprawdzania przetwarzanych danych zawiera się wyłączenie nakazu aktywnego poszukiwania treści bezprawnych. Skoro nie ma obowiązku sprawdzania danych, to tym bardziej nie istnieje obowiązek aktywnego poszukiwania takich treści. Niemniej – w celu uzyskania

---

[27] Za J. BARTA, R. MARKIEWICZ, *Prawo autorskie*, s. 333.

[28] Za wprowadzeniem takiego obowiązku opowiadają się J. BARTA i R. MARKIEWICZ, *op. cit.*, s. 333.

[29] Por. A. FRAŃ, *Komentarz do art. 15 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz. U. 02.144.1204), LEX/el. 2002. Bardzo podobnie, M. ŚWIERCZYŃSKI, [w:] J. GOŁACZYŃSKI, K. KOWALIK-BAŃCZYK, A. MAJCHROWSKA, M. ŚWIERCZYŃSKI, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Oficyna, 2009, *Komentarz do art. 15 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz. U. 02.144.1204).

jak najpełniejszej pewności prawnej – lepiej byłoby *de lege ferenda* wprowadzić precyzyjne wyłączenie obowiązku i w tym zakresie.

Zwolnienie z obowiązku aktywnego monitoringu treści przez pośredników przekazujących lub przechowujących dane ma znaczenie fundamentalne w zrozumieniu istoty reżimu odpowiedzialności tych podmiotów w Unii Europejskiej i Polsce. Wraz z upływem czasu możemy obserwować stopniowe przekształcanie powyższego modelu w kierunku stopniowego wprowadzania nakazu aktywnego filtrowania przesyłanych i przechowywanych danych. Najgłośniejszym przykładem, który znalazł naśladowców w Unii Europejskiej jest wprowadzony przez Francję obowiązek odcinania dostępu do Internetu internautom, którzy zostali trzykrotnie poinformowani o fakcie naruszenia przez nich prawa autorskiego (tzw. ustawa HADOPI).[30]

Obecnie w Parlamencie Europejskim toczy się gorąca dyskusja na temat przyjęcia nowej dyrektywy dotyczącej pornografii dziecięcej w Internecie.[31] Państwa członkowskie, takie jak Francja i Hiszpania, które wprowadziły do swojego ustawodawstwa nakaz aktywnego monitoringu naruszeń prawa autorskiego oraz hazardu w Internecie, konsekwentnie

---

[30] HADOPI to skrót od „Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet" (dosłownie: Wysoki Urząd do spraw rozpowszechniania utworów i ochrony praw w Internecie). Ustawa *Loi favorisant la diffusion et la protection de la création sur Internet* została uchwalona 13 maja 2009 roku przez francuskie Zgromadzenie Narodowe, ale 10 czerwca 2009 francuska Rada Konstytucyjna uznała niektóre przepisy ustawy za niezgodne z Konstytucją. 22 października 2009 Rada Konstytucyjna przyjęła zmienioną wersję ustawy dopuszczając kontrolę sądu przed odcięciem dostępu do Internetu. Zob. E. PFANNER, *France Approves Wide Crackdown on Net Piracy* (22.11.2009) dostępny na stronie: >>http://www. nytimes.com/2009/10/23/ technology/23net.html<<, ostatni dostęp: 12.12.2010.

[31] Zob. wniosek COM(2010)94 final, zawierający projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, uchylający decyzję ramową 2004/68/WSiSW, dostępny na stronie: >>http:// www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282010%290094_/com_com%282010%290094_pl.pdf<<, ostatni dostęp: 12.12.2010.

lobbują na rzecz objęcia obowiązkową blokadą stron zawierających materiały pornograficzne z udziałem dzieci. Z kolei rządy Niemiec i Rumunii opowiadają się za pozostawieniem państwom członkowskim swobody wyboru sposobu postępowania w tym zakresie.[32] Ostateczny kształt nowej dyrektywy ma zostać ustalony na początku 2011 r.

# *4. Wyłączenie odpowiedzialności za zwykły przekaz danych (ang. „mere conduit")*

## *4.1. Istota zwykłego przekazu*

Zwykły przekaz (*mere conduit*) oznacza usługę transmisji danych zainicjowaną przez użytkowników, realizowaną zaś przez operatorów infrastruktury Internetu. Zwykłym użytkownikom usługę tę oferują podmioty umożliwiające dostęp do sieci Internet, na przykład operatorzy sieci telefonii stacjonarnej i mobilnej, sieci kablowych czy telewizji satelitarnej (dostawcy usługi dostępu do Internetu – ang. *Internet service providers*). Z drugiej strony, dostawcy usługi dostępu do Internetu sami muszą korzystać z usług innych operatorów sieci Internetu, aby móc transmitować dowolny komunikat przesyłany z innego miejsca na Ziemi. Są to najczęściej najwięksi globalni operatorzy telekomunikacyjni, którzy łatwo mogliby zostać obarczeni odpowiedzialnością za treści bezprawne, których stają się faktycznymi dystrybutorami. W prawie amerykańskim usługodawcą tego typu usług (ang. *transitory communications*) jest podmiot oferujący usługi transmisji treści wskazanych przez użytkownika,

[32] Warto w tym miejscu dodać, że oczy opinii europejskiej skierowane są na Polskę, która nakłaniana jest przez organizacje pozarządowe chroniące obywatelskie wolności do poparcia stanowiska Niemiec i Rumunii. Zob. >>http://www.edri.org/files/angelilli_wd.pdf<<.

ich przekazywania oraz nawiązywania połączeń między końcówkami wskazanymi przez użytkownika, przy zachowaniu integralności zarówno przesyłanych, jak i wysyłanych treści.[33] W prawie europejskim nie mamy definicji podmiotu oferującego usługi transmisji danych.

## *4.2. Przesłanki wyłączenia odpowiedzialności za zwykły przekaz*

Uzasadnienie ograniczenia odpowiedzialności za tzw. zwykły przekaz (ang. *mere conduit*) wzorowane jest na wyłączeniu odpowiedzialności podmiotów oferujących usługi przewozowe czy kurierskie. Ponieważ trudno jest przypisać takim podmiotom odpowiedzialność za treści, które przesyłają podczas transportu paczek czy listów, pośrednicy w przekazie internetowym dość szybko postanowili wywalczyć dla siebie podobne gwarancje w przepisach prawa. Systemy prawne wielu państw, w tym prawo amerykańskie i prawo europejskie, przyznały w związku z tym ochronę pośrednikom technicznym przekazującym dane w sieciach telekomunikacyjnych oraz podmiotom oferującym ogółowi dostęp do Internetu (ang. ISP).

Konstrukcja prawna wyłączenia odpowiedzialności pośredników *mere conduit* w prawie unijnym nie jest jednolita i zawarta jest zarówno w dyrektywie o handlu elektronicznym, jak i w dyrektywie o harmonizacji prawa autorskiego w społeczeństwie informacyjnym. Obie dyrektywy tworzą ramy prawne właściwe dla odpowiedzialności pośredników w Internecie, co zostało potwierdzone w treści preambuły dyrektywy o handlu elektronicznym. Zgodnie z motywem 50 tej dyrektywy, ważne dla twórców obu instrumentów było to, aby te dwie regulacje weszły w życie

[33] Section 512(k)(1)(A) DMCA: „an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."

w tym samym czasie – w celu ustanowienia precyzyjnych ram prawnych właściwych dla odpowiedzialności pośredników w przypadku naruszenia na poziomie wspólnotowym prawa autorskiego i praw pokrewnych.

Pierwowzorem regulacji zawartej w dyrektywie o handlu elektronicznym stały się bez wątpienia uregulowania zawarte w art. 512 (a) DMCA, które w zasadniczej części zostały recypowane do jej treści. Zgodnie z ustawą amerykańską, dostawca usług telekomunikacyjnych nie ponosi odpowiedzialności prawnej za treść danych przesyłanych przez sieci telekomunikacyjne, będących jego własnością lub przez niego zarządzanych pod pięcioma warunkami:[34]

1) proces transmisji danych został zainicjowany przez inną osobę niż dostawca usług zwykłego przekazu;
2) transmisja danych i powiązane z nią etapy przekazu, takie jak przekierowywanie danych (ang. *routing*), ich krótkotrwałe zapisywanie

[34] „(a) TRANSITORY DIGITAL NETWORK COMMUNICATIONS. – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if –

„(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

„(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

„(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

„(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

„(5) the material is transmitted through the system or network without modification of its content.

w celu dalszego przekazu czy zapewnienie połączeń z siecią (ang. *provision of connections*) mają charakter techniczny i automatyczny, a zatem nie dochodzi do selektywnego przekazywania danych;

3) dostawca usługi zwykłego przekazu nie wybiera odbiorcy przekazu, z wyjątkiem przypadku automatycznej odpowiedzi na żądanie innej osoby (ang. *except as an automatic response to the request of another person*);
4) dostawca usługi zwykłego przekazu musi usunąć wszystkie kopie przekazywanych danych podczas dokonywania transmisji; DMCA wymaga w szczególności, by nikt poza odbiorcą danych nie mógł mieć dostępu do przekazywanych danych, a kopie danych dla samego odbiorcy nie powinny być przechowywane dłużej, niż jest to konieczne do ukończenia transmisji danych;
5) proces transmisji nie może prowadzić do modyfikacji przesyłanych danych.

Generalnie rzecz ujmując, dostawcy usług dostępu oraz transmisji danych w Internecie nie ponoszą odpowiedzialności, jeśli ich usługi mają charakter techniczny i automatyzowany, w rezultacie czego przesyłane dane nie są modyfikowane, ani selektywnie dobierane, a podmiot pośredniczący nie inicjuje transmisji, ani nie wybiera odbiorcy danych (z wyjątkiem „autorespondera"). Automatyzm musi również prowadzić do szybkiego usunięcia wszelkich kopii transmitowanych danych.

Powyższe rozwiązanie zostało w zasadniczej mierze zaakceptowane w prawie europejskim. Zgodnie z art. 12 (1) dyrektywy o handlu elektronicznym, państwa członkowskie mają zapewnić, aby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na transmisji w sieci telekomunikacyjnej informacji przekazanych przez usługobiorcę lub na zapewnianiu dostępu do sieci telekomunikacyjnej usługodawca nie był odpowiedzialny za przekazywane informacje, jeżeli:

a) nie jest inicjatorem przekazu;

b) nie wybiera odbiorcy przekazu oraz
c) nie wybiera oraz nie modyfikuje informacji zawartych w przekazie.

Wyłączenie odpowiedzialności obejmuje, w szczególności, automatyczne, pośrednie i krótkotrwałe przechowywanie przekazywanych informacji w zakresie, w jakim służy to wyłącznie wykonywaniu transmisji w sieci telekomunikacyjnej, oraz że okres przechowywania nie przekracza czasu rozsądnie koniecznego do transmisji (art. 12(2) dyrektywy). Jednakże dyrektywa nie wyłącza możliwości wymagania przez sąd lub organ administracyjny od usługodawcy przerwania naruszania prawa albo zapobieżenia temu (art. 12(3)).

Łatwo zauważyć zasadnicze podobieństwo rozwiązań unijnych w stosunku do amerykańskiego pierwowzoru i wniosku tego nie zmienia większa liczba przesłanek wyłączenia od odpowiedzialności przewidzianych w prawie amerykańskim. Zmiany wprowadzone w dyrektywie mają głównie charakter redakcyjny. W obu systemach prawnych podstawowym warunkiem wyłączenia odpowiedzialności jest neutralny charakter dokonywanych czynności przekazu. Powyższą interpretację wzmacniają wskazówki interpretacyjne zawarte w dyrektywie. Pierwsza z nich jasno wskazuje na wymóg, by działanie usługodawcy zwykłego przekazu miało „charakter czysto techniczny, automatyczny i bierny, który zakłada, że podmiot świadczący usługi społeczeństwa informacyjnego nie ma wiedzy o informacjach przekazywanych lub przechowywanych ani kontroli nad nimi."[35] A druga przesądza o tym, że wszelka współpraca z usługobiorcą w celu przekazywania bezprawnych treści wykracza poza działalność zwykłego przekazu. „Usługodawca, który współpracuje rozmyślnie z jednym ze swoich usługobiorców w celu bezprawnego działania, wykracza poza działalność 'zwykłego przekazu' lub 'buforowania' i w konsekwencji

[35] Motyw 42 preambuły do dyrektywy o handlu elektronicznym. Zobacz także wyrok w sprawie *Google*.

nie może korzystać z wyłączeń odpowiedzialności przewidzianych dla tego typu działalności."[36]

Różnice w ujęciu ograniczenia odpowiedzialności wynikają głównie z faktu, że DMCA wyłącza odpowiedzialność jedynie za naruszenia prawa autorskiego, podczas gdy dyrektywa 2000/31/WE wyłącza odpowiedzialność usługodawców zwykłego przekazu za dowolne treści, które transmitują. Jedynym bardziej zauważalnym elementem, który nie został jasno doprecyzowany w art. 12 dyrektywy, jest sytuacja, w której usługodawca automatycznie przesyła treści na żądanie innej osoby („autoresponder"), co stanowi dopuszczalny wyjątek od zasady zakazu inicjowania transmisji. Z kolei dyrektywa dopuszcza możliwość odstąpienia od zasady zakazu modyfikacji przekazywanych danych, gdy dotyczy to „(…) czynności o charakterze technicznym, które mają miejsce podczas przekazu, jeśli nie wpływają one na integralność informacji zawartej w przekazie",[37] co nie jest z kolei jasno wyrażone w przepisach DMCA. Wskazany powyżej wyjątek legalizuje zwyczajową praktykę modyfikowania nagłówków przesyłanych pakietów w celu umożliwienia dalszej transmisji. Natomiast istotne wątpliwości pojawiają się w związku z dopuszczalnością powołania się na powyższy motyw przez podmioty włączające do przesyłanych danych innych treści, takich jak np. komunikatów reklamowych, o czym będzie mowa dalej.

## *4.3. Integralność transmitowanych danych a głęboka analiza pakietów (ang. „Deep Packet Inspection")*

Jednym z najbardziej interesujących – a, niestety, zupełnie pomijanym w rozważaniach prawniczych – wątków w odniesieniu do wyłączenie odpowiedzialności dostawców usług zwykłego przekazu jest ocena

[36] Motyw 44 preambuły do dyrektywy o handlu elektronicznym.

[37] Motyw 43 preambuły do dyrektywy o handlu elektronicznym.

ich praktyk modyfikowania przesyłanych pakietów w świetle przesłanki zakazu modyfikacji treści przesyłanych komunikatów. Należy bowiem pamiętać, że prawdopodobnie zdecydowana większość dostawców usług internetowych korzysta z pomocy firm technologicznych oferujących narzędzia do analizy treści przesyłanych za pomocą infrastruktury danego pośrednika. Jest to pokłosie swoistego nakazu bycia gotowym do podjęcia się analizy przesyłanych danych, do czego bezpośrednio zobowiązuje sama dyrektywa o handlu elektronicznym. Zgodnie bowiem z art. 12 ust. 3 dyrektywy, sąd lub organ administracyjny może nakazać, by pośrednik w przekazie danych przerwał naruszenia prawa lub im zapobiegł, co w rezultacie oznacza, że powinien on zablokować dostęp konkretnemu numerowi IP lub zastosować mniej inwazyjne technologie umożliwiające filtrowanie przesyłanych danych.

*Deep Packet Inspection* to technologia umożliwiająca analizę w czasie rzeczywistym kompletnej zawartości przesyłanych pakietów. Badany jest przy tym nie tylko nagłówek przechwytywanego pakietu, ale także fragment treści komunikatu zawartego w pakiecie (ang. *payload*). W rezultacie pośrednik stosujący tego typu technologię może poznać treść przesyłanego komunikatu bądź też złożyć bardziej rozbudowaną wiadomość w całość i następnie dokonać jej analizy. Prostsza forma analizy pakietów (tzw. płytka analiza pakietów) wykorzystywana była od dawna w celu zabezpieczenia komunikacji elektronicznej (np. w urządzeniach typu *firewall*) poprzez analizę nagłówków pakietów w celu zablokowania lub przepuszczenia ruchu w zależności od adresu IP i portu. Jej ograniczeniem była jednak niemożność analizy samej treści, głównie ze względów na wolumen danych. Obecny postęp techniczny umożliwił filtrowanie danych w czasie rzeczywistym.

Co więcej, oferowane komercyjne rozwiązania sprzętowe są w stanie wywnioskować rodzaj przesyłanych informacji nawet w przypadku stosowania szyfrowania danych. W konsekwencji DPI ma obecnie wiele zastosowań, począwszy od kwestii bezpieczeństwa transmisji, monitoring

ruchu po ochronę praw autorskich, cenzurę, reklamę spersonalizowaną czy profilowanie konsumentów. Zastosowanie tego typu technologii w celu zwiększenia bezpieczeństwa w Internecie raczej nie budzi wątpliwości natury prawnej. Inaczej jednak sprawa wygląda w przypadku zastosowania DPI, na przykład w celach reklamowych.

Wykorzystywanie przez dostawców usługi zwykłego przekazu technologii typu DPI dla celów marketingowych może być podstawą do uchylenia wyłączenia odpowiedzialności z art. 12 UsługiElektrU oraz dyrektywy 2000/31/WE. W takiej sytuacji ISPs ingerują w wybór odbiorcy danych oraz naruszają integralność treści przesyłanych komunikatów. Aby bowiem móc dołączyć komunikaty reklamowe do treści pobieranych przez usługobiorcę, pośrednicy muszą zmienić chwilowo kierunek przesyłania danych, czyli odbiorcę danych, a co za tym idzie – naruszyć integralność przesyłanych danych. Jest to zjawisko związane z rozwojem sieci reklamowych w Internecie (tzw. *advertising networks*), które monitorują zachowania kupujących na tych stronach, które należą do ich systemu.

Zgodnie z dyrektywą 2000/31/WE, usługodawca może korzystać z wyłączenia w przypadku „zwykłego przekazu" jeżeli nie modyfikuje on informacji, które przekazuje, chyba że jest to czynność o charakterze technicznym, która nie wpływa na integralność informacji zawartej w przekazie.[38] Profilowanie użytkowników w celach marketingowych przy wykorzystaniu technologii DPI raczej trudno uznać za czynność techniczną, która nie wpływa na integralność informacji, bowiem przekaz zostaje wzbogacony o treści reklamowe, których dostawca treści nie umieścił w swoim serwisie. Warto w tym miejscu raz jeszcze przywołać motyw 42 dyrektywy 2000/31/WE, który wyraźnie stwierdza, że wyłączenia odpowiedzialności obejmują jedynie przypadki, w których „(…) działalność podmiotu świadczącego usługi społeczeństwa informacyjnego

[38] Motyw 43, Dyrektywa 2000/31/WE.

jest ograniczona do technicznego procesu obsługi i udzielania dostępu do sieci komunikacyjnej, w której informacje udostępniane przez osoby trzecie są przekazywane (…)," a działanie takie musi mieć charakter bierny i automatyczny, przy czym usługodawca nie może mieć kontroli nad danymi, ani wiedzy o nich. A przecież celem dostawców usług reklamowych (ang. *advertising networks*) jest właśnie kontrola nad jak największą liczbą danych o zachowaniach użytkowników Internetu[39] przechowywanych w plikach *cookie*. Podsumowując, dostawcy usług zwykłej transmisji danych utracą ochronę gwarantowaną im przez dyrektywę o handlu elektronicznym w sytuacji, gdy będą wykorzystywać systemy filtrowania treści do celów marketingowych, naruszając integralność przesyłanych danych poprzez wstawienie stosownych komunikatów reklamowych.

## *4.4. Ochrona usługodawców zwykłego przekazu na gruncie prawa autorskiego*

### *4.4.1. Dozwolony użytek publiczny w dyrektywie 2001/29/WE*

W odniesieniu do roszczeń opartych na prawie autorskim usługodawcy „zwykłego przekazu" w Unii Europejskiej mają do dyspozycji instrument prawny, który zapewnia im jeszcze dalej idącą ochronę niż dyrektywa 2000/31/WE o handlu elektronicznym. Dyrektywa 2001/29/WE dopuszcza bowiem *explicite* możliwość przekazywania treści naruszających prawo autorskie i prawa pokrewne w ramach usługi zwykłego przekazu. W tym kontekście rozwiązanie to idzie dalej niż model zaproponowany w amerykańskim DMCA i przyjęty w dyrektywie o handlu elektronicznym.

W motywie 33 dyrektywy 2001/29/WE czytamy: „Od wyłącznego prawa do zwielokrotniania utworu powinien być uczyniony wyjątek

[39] Szerzej na temat *advertising networks* zob. np. K.C. LAUDON, C.G. TRAVER, *E-commerce 2010: Business, Technology, Society*, 6 wydanie, Boston 2010, s. 8–15 i nast.

mający na celu zezwalanie na niektóre tymczasowe czynności zwielokrotniania, które mają charakter przejściowy lub dodatkowy, stanowią integralną i podstawową część procesu technologicznego i wykonywane są wyłącznie w celu albo skutecznej transmisji w sieci wśród osób trzecich przez pośrednika, albo umożliwienia legalnego wykorzystania utworu lub innego przedmiotu objętego ochroną. (…)."Artykuł 5 ust. 1 dyrektywy 2001/29/WE ujmuje ten cel w następujący sposób:

„Tymczasowe czynności zwielokrotniania określone w art. 2, które mają charakter przejściowy lub dodatkowy, które stanowią integralną i podstawową część procesu technologicznego i których jedynym celem jest umożliwienie: a) transmisji w sieci wśród osób trzecich przez pośrednika lub b) legalnego korzystania z utworu lub innego przedmiotu objętego ochroną, i które nie mają odrębnego znaczenia ekonomicznego, będą wyłączone z prawa do zwielokrotniania określonego w art. 2."

Zgodnie z powyższym przepisem czynności zwielokrotniania są dopuszczalne tylko wtedy, gdy kumulatywnie spełnionych jest pięć przesłanek, a mianowicie gdy:

- dana czynność ma charakter tymczasowy;
- ma ona charakter przejściowy i dodatkowy;
- stanowi integralną i podstawową część procesu technologicznego;
- jedynym celem tego procesu jest albo umożliwienie transmisji w sieci wśród osób trzecich przez pośrednika albo umożliwienie legalnego korzystania z utworu lub innego przedmiotu objętego ochroną i
- czynność ta nie ma odrębnego znaczenia ekonomicznego (tzn. żadnej wartości ekonomicznej).

Jednakże przy interpretacji art. 5 ust. 1 należy raz jeszcze sięgnąć do motywu 33 dyrektywy: „(…) O ile spełniają one te warunki, wyjątek ten obejmuje czynności pozwalające na przeglądanie, jak również czynności wprowadzania do pamięci podręcznej, w tym czynności, które umożliwiają skuteczne funkcjonowanie systemów transmisji, z zastrzeżeniem że

pośrednik nie zmieni informacji i nie będzie utrudniał legalnego wykorzystania technologii, powszechnie uznanej i stosowanej przez przemysł, w celu uzyskania danych w sprawie wykorzystania informacji. Korzystanie jest uważane za legalne, jeżeli zezwala na nie podmiot praw autorskich lub nie jest ono ograniczone przez prawo."

Biorąc powyższe pod uwagę, należy stwierdzić, że dyrektywa 2001/29/WE uznała za dopuszczalne na gruncie prawa autorskiego dokonywanie reprodukcji w ramach usług zwykłego przekazu przy spełnieniu dwóch dodatkowych warunków:

1) zachowania integralności danych przez dostawcę usługi zwykłego przekazu oraz
2) nieingerowania w zwyczajowo wykorzystywane techniki pozyskiwania danych o sposobach wykorzystywania informacji.

Pierwsza z przesłanek występuje w dyrektywie o handlu elektronicznym i została już szerzej omówiona wcześniej. Można także argumentować, że nie jest to w istocie odrębna przesłanka, bowiem zakaz naruszania integralności danych można wywieść z wymogu, aby „jedynym celem procesu było umożliwienie transmisji w sieci wśród osób trzecich przez pośrednika." Skoro jedynym celem ma być transmisja w sieci, to inne elementy, takie jak np. modyfikacja pakietów, wykraczają poza ten cel. Druga przesłanka pojawia się w dyrektywie o handlu elektronicznym, jako jedna z przesłanek wyłączających odpowiedzialność dostawcy usług buforowania (o czym szerzej poniżej). Wydaje się jednak, że ten drugi wymóg nie ma większego znaczenia praktycznego, bowiem usługodawcy transmisji danych raczej nie ingerują w procesy pozyskiwania danych np. o odwiedzinach określonego serwisu, aczkolwiek, jak widzieliśmy to na przykładzie technologii typu *Deep Packet Inspection*, czasami pośrednicy ingerują w dane dla celów marketingowych. W takim przypadku stracą również ochronę gwarantowaną im przez europejskie prawo autorskie. Podsumowując, dopiero przy spełnieniu tych dwóch dodatkowych

warunków będzie można mówić o dopuszczalności reprodukcji utworów w ramach usług zwykłego przekazu.

### *4.4.2. Znaczenie wyroku w sprawie „InfoPaq"*

Trybunał Sprawiedliwości w wyroku w sprawie *C-5/08 InfoPaq* dokonał dalszej wykładni powyższego przepisu i uznał, że powyższe przesłanki – jako wyjątki od reguły, jaką jest uzyskiwanie zgody na reprodukcję utworów – należy interpretować w sposób ścisły i zawężający.[40] Dodatkowym argumentem na rzecz przyjęcia tezy o obowiązku zastosowania zawężającej wykładni tego artykułu, jest – z jednej strony – wymóg zapewnienia autorom bezpieczeństwa prawnego w zakresie ochrony ich utworów, z drugiej zaś konieczność zastosowania tzw. testu trójstopniowego (art. 5 ust. 5), który zakłada, że dopuszczony przez dyrektywę wyjątek od zasady uzyskiwania zgody podmiotu wyłącznie uprawnionego znajduje zastosowanie tylko w niektórych szczególnych przypadkach, które nie naruszają normalnego wykorzystania dzieła lub innego przedmiotu objętego ochroną, ani nie powodują nieuzasadnionej szkody dla uzasadnionych interesów podmiotów praw autorskich.

W odniesieniu do wymogu tymczasowości w sprawie *C-5/08* firma Infopaq monitorująca prasę w Internecie utrzymywała, że czynności zwielokrotniania, których dotyczyło postępowanie przed sądem krajowym, spełniały przesłankę tymczasowego charakteru, ponieważ rezultaty reprodukcji fragmentów artykułów prasowych były usuwane po zakończeniu procesu elektronicznego wyszukiwania. Trybunał Sprawiedliwości wstępnie stwierdził, że „(…) dana czynność może zostać zakwalifikowana jako czynność 'tymczasowa' w rozumieniu drugiej przesłanki zawartej w art. 5 ust. 1 dyrektywy 2001/29 jedynie wtedy, gdy czas jej trwania ogranicza się do okresu, który jest niezbędny do prawidłowego funkcjonowania rozpatrywanego procesu technologicznego, przy czym proces

[40] Sprawa *C-5/08 Infopaq*, motyw 56.

ten musi być zautomatyzowany w taki sposób, by rezultaty tej czynności były usuwane automatycznie – bez ingerencji człowieka – z chwilą gdy spełniona została funkcja czynności polegająca na umożliwieniu realizacji wspomnianego procesu."[41]

Zastosowanie powyższych ustaleń do przypadku *InfoPaq* okazało się dużym wyzwaniem. TSUE zlecił sądowi krajowemu ustalenie, czy mamy do czynienia z rozwiązaniem technologicznym, które podlega wyjątkowi z art. 5 dyrektywy. Dodał przy tym dwie wskazówki. Po pierwsze, że „w postępowaniu przed sądem krajowym nie można z góry wykluczyć, że dwie pierwsze czynności zwielokrotniania, których dotyczy to postępowanie – a mianowicie tworzenie plików TIFF oraz plików tekstowych w wyniku przekształcenia plików TIFF – mogą zostać zakwalifikowane jako czynności tymczasowe, ponieważ ich rezultaty są usuwane z pamięci w sposób automatyczny." Po drugie, w odniesieniu do trzeciej czynności zwielokrotniania, a mianowicie reprodukcji w pamięci komputera wycinków zawierających 11 słów „(…) dokumenty przedstawione Trybunałowi nie pozwalają na dokonanie oceny w przedmiocie tego, czy proces technologiczny jest zautomatyzowany w taki sposób, że pliki te są usuwane z pamięci bez konieczności podjęcia działania ludzkiego i że ma to miejsce w krótkim czasie. Tak więc to na sądzie krajowym spoczywa zadanie zbadania, czy takie usuwanie zależy od woli osoby korzystającej ze zwielokrotnienia i czy nie istnieje ryzyko, że pliki te pozostaną w pamięci także po spełnieniu przez czynność funkcji polegającej na realizacji rozpatrywanego procesu technologicznego."

Analizując powyższe uzasadnienie, można dojść do wniosku, że na obecnym etapie rozwoju nowych technologii sędzia stoi przed zagadnieniami na tyle skomplikowanymi, że jego wiedza i doświadczenie nie wystarczają do wydania sprawiedliwego wyroku. Praca sędziego ogranicza się, niestety, do sformułowania bardzo ogólnych wskazówek interpretacyjnych,

[41] Sprawa C-5/08 *InfoPaq*, motyw 64.

których następnie Trybunał nie jest już w stanie zastosować do rozstrzygnięcia przedmiotowego problemu. Na przykład: dlaczego Trybunał sugeruje, że skanowanie dokumentu do formatu TIFF i następnie konwersja tego dokumentu do formatu tekstowego jest automatyczna i powoduje usunięcie reprodukowanych treści w sposób automatyczny, a z kolei reprodukcja 11 słów już automatyczna nie jest, podobnie jak proces usuwania tych wycinków? Oczywiście, można argumentować, że sędziowie są bardzo ostrożni w formułowaniu swoich sądów, delegując w istocie zastosowanie ogólnych wskazówek sądom krajowym, jak i wyraźnie zaznaczając, że powyższych kwalifikacji nie można wykluczyć.

### *4.4.3. Dozwolony użytek w polskim prawie autorskim*

Artykuł 5 ust 1 dyrektywy 2001/29/WE został implementowany do prawa polskiego w art. $23^1$ prawa autorskiego. Zgodnie z tym przepisem „nie wymaga zezwolenia twórcy przejściowe lub incydentalne zwielokrotnianie utworów, niemające samodzielnego znaczenia gospodarczego, a stanowiące integralną i podstawową część procesu technologicznego oraz mające na celu wyłącznie umożliwienie: 1) przekazania utworu w systemie teleinformatycznym między osobami trzecimi przez pośrednika lub 2) zgodnego z prawem korzystania z utworu." Do interpretacji powyższego przepisu należy stosować przedstawione wyżej uwagi.

W doktrynie dostrzeżono problem wzajemnej relacji art. 12 ustawy o świadczeniu usług drogą elektroniczną i art. $23^1$ prawa autorskiego, który implementuje omawiany przepis dyrektywy 2001/29/WE. Pojawił się w konsekwencji pogląd, że wspomniany art. $23^1$ prawa autorskiego jest przepisem szczególnym wobec art. 12 ustawy o świadczeniu usług drogą elektroniczną i wobec tego jest on jedyną przesłanką uchylenia odpowiedzialności usługodawcy zwykłego przekazu na gruncie prawa autorskiego.[42] Z tym stanowiskiem należy się zgodzić.

[42] J. BARTA, R. MARKIEWICZ, *Prawo autorskie*, Warszawa 2010, s. 312.

### *4.4.4. Nakaz ujawnienia danych osobowych użytkowników Internetu*

Artykuł 15 (2) daje wyraźnie sądom lub organom administracyjnym możliwość podejmowania działań lub uzyskiwania informacji od pośredników w zwykłym przekazie danych. Jednakże przywilej ten nie dotyczy podmiotów prywatnych. Jednym z najbardziej interesujących wyroków Trybunału Sprawiedliwości w tym kontekście było orzeczenie w sprawie *C-275/06 Promusicae v Telefonica*. Hiszpańska organizacja zbiorowego zarządzania domagała się od dostawcy usług internetowych ujawnienia danych osobowych subskrybentów, którzy we wskazanych przez niego dniach pobierali pliki muzyczne z sieci wymiany plików *Kazaa*. *Telefonica* odmówiła wydania danych osobowych użytkowników, argumentując, że transfer takich danych jest możliwy jedynie na potrzeby postępowań karnych, a nie cywilnych. Wobec tego do Trybunału Sprawiedliwości trafiło wiele pytań dotyczących nie tylko dyrektyw z zakresu nowych technologii, ale także praw podstawowych.

Trybunał Sprawiedliwości po długich rozważaniach doszedł do następującego wniosku: „Dyrektywy: 2000/31, 2001/29, 2004/48 i 2002/58 nie zobowiązują państw członkowskich do ustanowienia obowiązku przekazania danych osobowych w celu zapewnienia skutecznej ochrony praw autorskich w ramach postępowania cywilnego." Brak obowiązku przekazania danych organizacjom zbiorowego zarządzania został odczytany jako zwycięstwo sieci wymiany plików. Sędziowie jednak zawarli w tezie wyroku sugestię, aby sądy „(…) oparły się (one) na takiej wykładni tych dyrektyw, która pozwoli na zapewnienie odpowiedniej równowagi między poszczególnymi prawami podstawowymi chronionymi przez wspólnotowy porządek prawny" oraz nie opierały się „(…) na takiej wykładni tych dyrektyw, która pozostawałaby w konflikcie ze wspomnianymi prawami podstawowymi lub z innymi ogólnymi zasadami prawa wspólnotowego, takimi jak zasada proporcjonalności." Pomijając niejednoznaczność

tych wskazówek, można dojść do wniosku, że sądy krajowe mogą równie dobrze nakazać przekazanie takowych danych, jeżeli tylko uznają, że nie zostanie naruszona równowaga między prawem do prywatności i prawem do ochrony danych osobowych, a prawem własności i prawem do skutecznego dochodzenia swoich roszczeń przed sądem.

# *5. Wyłączenie odpowiedzialności za przechowywanie danych w celu przyspieszenia ich transmisji („caching")*

## *5.1. Istota „cachingu"*

*Caching* to usługa polegająca na czasowym przechowywaniu danych w systemie teleinformatycznym znajdującym się między usługobiorcą, a dostawcą treści w celu przyspieszenia dostępu do nich (buforowanie danych). Usługa ta jest z reguły dostępna w ramach usługi dostępu do Internetu bądź w ramach sieci korporacyjnych. W pierwszym przypadku dostawca usługi dostępowej tymczasowo zapisuje na swoim komputerze strony www i inne dane pobierane przez swoich subskrybentów po to, aby kolejni użytkownicy sięgający po te same zasoby mogli pobrać je bezpośrednio z serwera usługodawcy. W drugim przypadku podmiotem, który zapisuje dane, jest administrator sieci lokalnej, który przechowuje je i udostępnia użytkownikom swojej sieci z tzw. serwera proxy, którego funkcje obejmują – oprócz czasowego składowania danych – także m.in. filtrowanie treści oraz anonimowe korzystanie z Internetu przez osoby pracujące wewnątrz sieci lokalnej.[43]

[43] Zgodnie z motywem 14 dyrektywy o handlu elektronicznym, „(…) niniejsza dyrektywa nie może uniemożliwiać anonimowego korzystania z otwartych sieci, takich jak Internet."

## *5.2. Przesłanki wyłączenia odpowiedzialności za „caching"*

### *5.2.1. „Caching" w prawie amerykańskim*

Po raz pierwszy wyłączenie odpowiedzialności usługodawcy „cachingu" zostało wprowadzone w amerykańskim *Digital Millennium Copyright Act*. DMCA ujmuje usługę buforowania (ang. *caching*) jako pośrednie i tymczasowe przechowywanie danych w systemie teleinformatycznym lub w sieci komputerowej kontrolowanej lub zarządzanej przez lub w imieniu dostawcy usług. [44] Usługa ta jest scharakteryzowana w DMCA w następujący sposób:

1) dane udostępniane są przez dostawcę treści, który jest podmiotem różnym od usługodawcy buforowania;
2) dane transmitowane są poprzez system teleinformatyczny lub sieć komputerową od dostawcy treści do użytkownika na jego żądanie;
3) proces przechowywania danych ma charakter zautomatyzowany i techniczny, a jego celem jest udostępnienie danych użytkownikom systemu teleinformatycznego lub sieci komputerowej, którzy zażądają ponownie przesłania danych od dostawcy treści.[45]

---

[44] DMCA, Section 512(b).

[45] „(b) SYSTEM CACHING. – „(1) LIMITATION ON LIABILITY. – A service provider shall not be liable for monetary relief, or, except as provided In subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –

„(A) the material is made available online by a person other than the service provider;

„(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

„(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

DMCA wyłącza odpowiedzialność za naruszenie prawa autorskiego poprzez buforowanie bezprawnych danych w celu umożliwienia ich szybszego pobierania przez usługobiorców (ang. *System caching*) przy spełnieniu wielu warunków:

1) dane przesyłane są kolejnym użytkownikom bez modyfikacji ich treści (w stosunku do danych, które otrzymał pierwszy użytkownik);[46]
2) dostawca usługi buforowania stosuje się do zasad aktualizacji danych przyjętych przez dostawcę treści, w tym ich odświeżania zgodnie z powszechnie stosowanymi standardami przesyłania danych (ang. *a generally accepted industry standard data Communications protocol*), z wyłączeniem jednakże takich zasad przyjętych przez dostawcę treści, które uniemożliwiłyby lub znacznie utrudniły świadczenie usługi buforowania;[47]
3) dostawca usługi buforowania nie zakłóca funkcjonowania technologii, która umożliwiłaby dostawcy treści uzyskanie pewnych informacji od użytkowników swojego serwisu, w sytuacji gdyby ci użytkownicy pobrali dane bezpośrednio od dostawcy treści, pod warunkiem że stosowanie tej technologii:
   a) nie zakłóca w sposób istotny świadczenia usługi buforowania czy też funkcjonowania systemu teleinformatycznego usługodawcy,

[46] „(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A).

[47] „(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data Communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies.

b) jest zgodne z powszechnie stosowanymi standardami przesyłania danych (ang. *is consistent with generally accepted industry standard communications protocols*) oraz

c) nie prowadzi do pozyskania dodatkowych informacji z systemu teleinformatycznego dostawcy usługi buforowania w stosunku do tych, które dostawca treści otrzymałby bez pośrednictwa usługodawcy „cachingu";[48]

4) jeżeli dostawca treści wymaga spełnienia pewnych warunków przed świadczeniem usługi, takich jak uiszczenie płatności lub podanie hasła, dostawca usługi buforowania umożliwia dostęp do przechowywanych danych w znacznej mierze (ang. *in significant part*) tylko tym użytkownikom jego systemu teleinformatycznego lub sieci, którzy spełnili te wymagania i tylko zgodnie z tymi warunkami[49] oraz

5) dostawca usługi buforowania usunie lub uniemożliwi dostęp do treści udostępnionych przez dostawcę treści bez zgody podmiotu praw wyłącznych po uzyskaniu zawiadomienia (ang. *notification*):

---

[48] „(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology –

„(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

„(ii) is consistent with generally accepted industry standard communications protocols; and

„(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person.

[49] „(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and…

a) jeżeli kwestionowane dane zostały usunięte z pierwotnego źródła lub sąd nakazał ich blokadę, lub usunięcie oraz
b) strona zawiadamiająca potwierdzi w zawiadomieniu, że kwestionowane dane zostały usunięte z pierwotnego źródła lub dostęp do nich został zablokowany, bądź też że sąd nakazał ich blokadę lub usunięcie.[50]

### *5.2.2. „Caching" w dyrektywie o handlu elektronicznym*

Zgodnie z art. 13 dyrektywy o handlu elektronicznym buforowanie danych (ang. *caching*) ujęte jest jako świadczenie usługi społeczeństwa informacyjnego polegającej na automatycznym, pośrednim i krótkotrwałym przechowywaniu informacji dokonywanej w celu usprawnienia późniejszej transmisji informacji na żądanie innych usługobiorców.[51] Ujęcie zaproponowane w DMCA jest bardziej rozbudowane i lepiej opisuje istotę buforowania, które polega na tymczasowym przechowywaniu informacji transmitowanej od dostawcy treści do użytkownika

[50] „(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if – "(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and "(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

[51] Zgodnie z art. 13 ust. 1 dyrektywy, „Państwa Członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na transmisji w sieci telekomunikacyjnej informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny z tytułu automatycznego, pośredniego i krótkotrwałego przechowywania tej informacji dokonywanego w celu usprawnienia późniejszej transmisji informacji na żądanie innych usługobiorców (…)".

serwisu (usługobiorcy) wyłącznie w celu przyspieszenia dostępu kolejnych użytkowników do informacji. Warto w tym miejscu wskazać na różnicę w funkcji krótkotrwałego przechowywania informacji w tej usłudze oraz w usłudze zwykłego przekazu, o której mówi art. 12 ust. 2 dyrektywy, określanego czasami jako *routing* internetowy. Inny jest cel krótkotrwałego przechowywania w przypadku zwykłego przekazu, który właśnie ma umożliwić transmisję, a nie przyspieszenie dostępu do danych.

Podobnie jak w przypadku usługi zwykłego przekazu, konstrukcja prawna wyłączenia odpowiedzialności za przechowywanie danych w celu przyspieszenia ich transmisji (dalej jako buforowanie danych) stanowi dość wierną replikę rozwiązań przyjętych w *Digital Millennium Copyright Act*:

a) usługodawca nie modyfikuje informacji;
b) usługodawca przestrzega warunków dostępu do informacji;
c) usługodawca przestrzega zasad dotyczących aktualizowania informacji, określonych w sposób szeroko uznany i stosowany w branży;
d) usługodawca nie zakłóca dozwolonego posługiwania się technologią, szeroko uznaną i stosowaną w branży w celu uzyskania danych o korzystaniu z informacji oraz
e) usługodawca niezwłocznie usuwa lub uniemożliwia dostęp do przechowywanych informacji, gdy uzyska wiarygodną wiadomość, że informacje zostały usunięte z początkowego źródła transmisji lub dostęp do nich został uniemożliwiony albo gdy sąd lub organ administracyjny nakazał usunięcie informacji bądź uniemożliwienie dostępu do niej. Podobnie jak w przypadku usługi zwykłego przekazu, sądy lub organy administracyjne mogą żądać, aby usługodawca przerwał naruszenia prawa lub im zapobiegł.

Usługodawca może korzystać z wyłączenia dla „cachingu", jeżeli nie jest on związany z przekazywaną informacją, a więc nie może jej modyfikować. Interpretacja tej przesłanki powinna być identyczna jak w przypadku

usługi zwykłego przekazu.[52] Po pierwsze, zakaz modyfikacji przechowywanych danych nie obejmuje czynności o charakterze technicznym, które mają miejsce podczas przekazu, jeśli nie wpływają one na integralność informacji zawartej w przekazie.[53] Po drugie, działalność usługodawcy musi być ograniczona do technicznego procesu obsługi systemu czasowego przechowywania danych. Po trzecie, jego działanie musi przybierać charakter czysto techniczny, automatyczny i bierny, przez co rozumie się, że podmiot świadczący usługi społeczeństwa informacyjnego nie ma wiedzy o informacjach przekazywanych lub przechowywanych ani kontroli nad nimi.[54] Po czwarte, wyłączenie odpowiedzialności dostawcy usługi nie obejmuje sytuacji, w której usługodawca współpracuje rozmyślnie z jednym ze swoich usługobiorców w celu bezprawnego działania.[55]

Zarówno dyrektywa, jak i DMCA nakazują skonfigurowanie systemu do buforowania danych w taki sposób, jak to się powszechnie praktykuje w branży IT. Odesłanie do powszechnie stosowanych standardów w obrocie może być interpretowane jako odesłanie do zwyczajów w Internecie, które dopiero się tworzą, przy czym głównymi instytucjami, od których oczekuje się wypracowania stosownych standardów, są IETF oraz W3C.[56] Odesłania takie występują w odniesieniu do przesłanki przestrzegania zasad dotyczących aktualizowania informacji oraz niezakłócania dozwolonego posługiwania się technologią w celu uzyskania danych o korzystaniu z informacji. Różnice w wersjach europejskiej i amerykańskiej sprowadzają się – poza bardziej precyzyjnym określeniem istoty buforowania, jak

---

[52] Interesujące są rozważania rzecznika generalnego P. Madury, który w opinii do sprawy Google sugeruje możliwość zastosowania wyłączenia za buforowanie danych do usługodawców wyszukiwarek internetowych, a konkretnie dostawców usług tzw. naturalnego wyszukiwania. Patrz poniżej.

[53] Motyw 43 dyrektywy o handlu elektronicznym.

[54] Motyw 42 dyrektywy o handlu elektronicznym.

[55] Motyw 44 dyrektywy o handlu elektronicznym.

[56] Zob. HR2281, s. 73. Na temat zwyczajów w Internecie, patrz: P. POLAŃSKI, *Customary law of the Internet*, Hague 2007.

i obecnością procedury blokowania dostępu – do treści, a także lepszego dookreślenia wyjątków od przesłanek wyłączenia odpowiedzialności.

– Po pierwsze, w odniesieniu do przesłanki poszanowania zasady aktualizacji danych, prawodawca amerykański wyraźnie przewiduje, że reguły te mogą zostać pominięte przez usługodawcę „cachingu" w sytuacji, gdy ich zastosowanie uniemożliwiłoby lub znacznie utrudniło świadczenie usługi buforowania. W dyrektywie należałoby wykazać, że pominięcie tego typu reguł jest zwyczajowo praktykowane, co może istotnie utrudnić stosowanie tego wyłączenia w praktyce.

– Po drugie, w odniesieniu do przesłanki poszanowania zasady niezakłócania pozyskiwania przez dostawcę treści danych o korzystaniu z informacji DMCA wprowadza trzy wymogi, z których tylko jeden znajduje się w dyrektywie. Oba instrumenty odsyłają do zwyczajów branżowych w tym zakresie. Jednakże DMCA dopuszcza możliwość naruszenia tej zasady także w sytuacji, gdy – podobnie jak w poprzednim przypadku – znacząco utrudniłoby to świadczenie tej usługi, a także w sytuacji, gdyby dostawca treści pozyskiwał większą liczbę danych o korzystaniu z informacji niż w przypadku korzystania bezpośrednio z jego serwisu. Europejskim usługodawcom pozostaje dobra znajomość zwyczajów branżowych.

– Po trzecie, w odniesieniu do przesłanki poszanowania zasad dostępu do informacji prawodawca amerykański zawiera wskazówkę, iż dane, do których dostęp wymaga podania hasła lub uiszczenia płatności, mogą być udostępnione tylko tym użytkownikom jego systemu teleinformatycznego lub sieci, którzy spełnili te wymogi, i tylko zgodnie z warunkami dostępu. Prawodawca europejski jest bardziej lakoniczny, aczkolwiek trudno jest w tym przypadku mieć wątpliwości co do tego, czy tego typu dane mogą być udostępnione osobom innym niż uprawnione. Warto w tym miejscu jeszcze raz podkreślić, że mimo braku odesłania do norm branżowych, doszło w tym zakresie do wykształcenia się takich zwyczajów, jak zakaz buforowania zaszyfrowanych danych przez dostawcę usług czy też zakaz

przechowywania stron dostępnych po zalogowaniu. Do reguł tych powinien się stosować dostawca usługi buforowania.

Polska transpozycja art. 13 dyrektywy, choć się różni pod względem brzmienia, pozostaje co do zasady zgodna z celem dyrektywy 2000/31/WE. Wobec tego należy przy stosowaniu tego przepisu wziąć pod uwagę wszystkie uwagi zgłoszone powyżej.

## *5.3. „Caching" a prawo autorskie*

Podobnie jak w przypadku usług zwykłego przekazu, przy analizie wyłączenia odpowiedzialności za *caching* uwzględnić należy także omawiany już art. 5 ust. 1 dyrektywy o harmonizacji prawa w społeczeństwie informacyjnym. Warto przypomnieć, że spod prawa do reprodukcji wyłączone są przypadki tymczasowego zwielokrotnienia dzieła mające charakter przejściowy lub incydentalny, będące integralną i podstawową częścią procesu technologicznego, którego wyłącznym celem jest umożliwienie transmisji w sieci między osobami trzecimi poprzez pośrednika, jeżeli nie mają niezależnego znaczenia gospodarczego.

Dozwolony użytek wynikający z art. 5 ust. 1 dyrektywy i art. $23^1$ prawa autorskiego dotyczy zwielokrotnień tymczasowych, efemerycznych, czyli takich, które znikają po zakończeniu procesu transmisji. W polskiej implementacji tego przepisu dostrzeżono brak przesłanki tymczasowości, jednakże można ją wyprowadzić z przejściowego lub incydentalnego charakteru zwielokrotnienia.[57]

---

[57] W doktrynie można się spotkać z próbą definiowania zwielokrotnienia przejściowego, za które uważa się zwielokrotnienie krótkotrwałe, które jest kasowane automatycznie po wykorzystaniu lub po określonym czasie, natomiast za zwielokrotnienia incydentalne – takie zwielokrotnienie, które zdarza się jedynie przy okazji i podczas procesu technicznego. Por. P. ŻERAŃSKI, *Zakres dozwolonego użytku dostawcy usług internetowych w świetle art. 23[1] Prawa autorskiego w kontekście ustawy o świadczeniu usług drogą elektroniczną*, MoP 2008, nr 20, powołując się na: M. WELSER, [w:] *Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft*, Ergänzungsband zum Urheberrecht, (red.) A.-A. WANDTKE, Winfried Bullinger, Monachium 2002, s. 44.

Powstaje pytanie, czy przepis ten można stosować także do dostawców usługi buforowania. Odpowiedź pozytywna w tym zakresie umożliwiłaby usługodawcom uwolnienie się od konieczności spełnienia wielu przesłanek wyłączenia odpowiedzialności na gruncie dyrektywy o handlu elektronicznym i ustawy o świadczeniu usług drogą elektroniczną. Za takim ujęciem może przemawiać powoływany już wielokrotnie motyw 33 dyrektywy o harmonizacji prawa autorskiego, który stwierdza, że omawiany wyjątek obejmuje czynności wprowadzania do pamięci podręcznej, w tym czynności, które umożliwiają skuteczne funkcjonowanie systemów transmisji, z zastrzeżeniem że pośrednik nie zmieni informacji i nie będzie utrudniał legalnego wykorzystania technologii, powszechnie uznanej i stosowanej przez przemysł, w celu uzyskania danych w sprawie wykorzystania informacji. Wprowadzanie do pamięci podręcznej (ang. *cache*) w powiązaniu z funkcjonowaniem systemów transmisji może być odczytywane jako nakaz objęcia tym wyjątkiem usługi „cachingu". Ponadto prawodawca europejski wyraźnie wymaga respektowania zasady braku ingerencji w informacje o korzystaniu z danych przez użytkowników serwisu, co jest jednym z warunków wyłączenia odpowiedzialności za buforowanie danych na gruncie prawa amerykańskiego i europejskiego.

Na tak postawione pytanie należy jednak udzielić odpowiedzi przeczącej. Choć omawiany przepis dopuszcza tymczasową reprodukcję plików, czyni to jednak dla szczególnego przypadku wprowadzania danych do pamięci podręcznej użytkownika komputera (a właściwie jego systemu operacyjnego). Natomiast w odniesieniu do tymczasowych reprodukcji przez pośredników[58] wymaga, by związane one były wyłącznie z transmisją danych, czyli zwykłym przekazem plików.[59] „Caching" co do zasady nie jest wymagany do transmisji danych. Zdania

[58] P. ŻERAŃSKI zwraca uwagę na to, że nie można utożsamiać pojęcia pośrednika z usługodawcą w rozumieniu UsługiElektrU. P. ŻERAŃSKI, *op. cit.*

[59] Tak, słusznie J. BARTA, R. MARKIEWICZ, *op. cit.*, s. 312–313.

w tej kwestii są jednak nadal podzielone[60] i wskazana byłaby interwencja instytucji unijnej w celu usunięcia wątpliwości w tym zakresie. Nie wyklucza to także przyjęcia takiego sposobu stosowania omawianych przepisów, w którym najpierw sprawdza się możliwość zastosowania omawianego przypadku dozwolonego użytku publicznego, a w drugiej kolejności art. 13 dyrektywy i ustawy o świadczeniu usług drogą elektroniczną.

## *6. Wyłączenie odpowiedzialności za przechowywanie danych w celu ich udostępnienia („hosting")*[61]

Zagadnienie odpowiedzialności podmiotu oferującego usługi hostingu należy do najżywiej dyskutowanych w doktrynie prawa i orzecznictwie sądowym. Bez usług hostingu niemożliwy byłby gwałtowny rozwój stron internetowych, bowiem ich twórcy czy administratorzy potrzebują przestrzeni, na której mogą zapisać swoje utwory i udostępnić je użytkownikom sieci. Także pozostałe popularne usługi w Internecie, takie jak poczta elektroniczna czy wymiana plików w kontrowersyjnych sieciach *peer-to-peer* wymagają usługi hostingu do odebranej korespondencji czy udostępnionych plików. Z drugiej strony

---

[60] Za możliwością powołania się na dozwolony użytek opowiada się P. ŻERAŃSKI, *op. cit.*, „(…) zwielkorotnienia tymczasowe powstające w toku tych procesów mogą być objęte dozwolonym użytkiem z art. 23[1] PrAut.", a także K. GIENAS, *Systemy Digital Rights Management…*, *op. cit.*, s. 21, P. PODRECKI, [w:] *Prawo Internetu*, *op. cit.*, s. 47.

[61] Punkty 6.1 oraz 6.2 w nieco zmienionej formie zostały uprzednio opublikowane w artykule pod tytułem *Uwagi na temat odpowiedzialności usługodawcy hostingu w Internecie* (red. J. GOŁACZYŃSKI) *Informatyzacja postępowania sądowego i administracji publicznej*, Warszawa 2010, s. 299–312.

już samo pojęcie hostingu jest niejednolicie rozumiane w polskiej doktrynie. A jest to zagadnienie doniosłe prawnie, bowiem od jego zdefiniowania zależy wyznaczenie zakresu odpowiedzialności podmiotów świadczących tego typu usługi w Internecie na gruncie przepisów dyrektywy o handlu elektronicznym oraz ustawy o świadczeniu usług drogą elektroniczną.

W doktrynie mamy problem z interpretacją pojęcia hostingu, bowiem ani dyrektywa o handlu elektronicznym, ani ustawa o świadczeniu usług drogą elektroniczną nie definiują tego pojęcia. Natomiast oba instrumenty charakteryzują tę usługę jako przechowywanie danych, co jest ujęciem zbyt wąskim. *Hosting* oznacza z reguły odpłatną usługę polegającą na zdalnym udostępnieniu usługobiorcy przez czas określony umową lub czas nieokreślony zasobów systemu teleinformatycznego usługodawcy w celu przechowywania i udostępniania użytkownikom Internetu danych tam umieszczonych przez samego usługobiorcę lub użytkowników jego serwisu. Należy przy tym odróżnić *hosting* właściwy (klasyczny) od „hostingu" wirtualnego, o czym szerzej poniżej.

## *6.1. Istota „hostingu"*

Problematyka „hostingu" została uregulowana w art. 14 dyrektywy 2000/31/WE o handlu elektronicznym oraz w art. 14 ustawy o świadczeniu usług drogą elektroniczną, który stanowi implementację postanowień dyrektywy. Omawiana dyrektywa zwalnia – pod pewnymi warunkami, o których później – usługodawcę z odpowiedzialności karnej i cywilnoprawnej za „informacje przechowywane na żądanie usługobiorcy".[62] W omawianym przepisie mowa jest jedynie o przechowywaniu

[62] Podobnie wersja anglojęzyczna, która mówi o usłudze społeczeństwa informacyjnego, która „(…) is provided that consists of the storage of information provided by a recipient of the service".

informacji, a nie o jej udostępnianiu. Może więc budzić wątpliwości, w szczególności, czy istotą tej usługi jest także udostępnianie przechowywanych danych innym usługobiorcom.[63]

Dyrektywa o handlu elektronicznym nie zawiera legalnej definicji „hostingu".[64] Ponadto w dyrektywie o handlu elektronicznym samo pojęcie „hostingu" nie pojawia się w przepisie, tylko w tytule tego artykułu. Niewiele materiału do pogłębienia analizy pojęcia „hostingu" dostarcza także preambuła do dyrektywy o handlu elektronicznym. Podobnie jak w przypadku usług zwykłego przekazu oraz buforowania przypomnieć należy o wymogu technicznego procesu obsługi, co sprowadza się do działania usługodawcy „hostingu" o charakterze czysto technicznym, automatycznym i biernym, co z kolei oznacza, że podmiot świadczący usługi społeczeństwa informacyjnego nie ma wiedzy o informacjach przekazywanych lub przechowywanych ani kontroli nad nimi.[65] Jednakże powyższa charakterystyka jest zdecydowanie bardziej użyteczna do analizy przesłanek wyłączenia odpowiedzialności niż do zrozumienia istoty „hostingu" Powrócimy więc do niej w dalszej części wywodu.[66]

Również polska implementacja dyrektywy nie zawiera definicji „hostingu". W ustawie o świadczeniu usług drogą elektroniczną w ogóle

---

[63] Zgodnie z art. 2 pkt d dyrektywy „usługobiorca" to „każda osoba fizyczna lub prawna, która do celów zawodowych lub innych korzysta z usług społeczeństwa informacyjnego, w szczególności w celu poszukiwania informacji lub uzyskania do niej dostępu".

[64] Trudności, jakie wywołuje już samo rozumienie tego pojęcia, ma wiele powodów: anglojęzyczna etymologia, techniczny charakter, unijna proweniencja. Niestety, jeżeli znaczenie jakiegoś pojęcia nie jest powszechnie zrozumiałe, ustawodawca powinien – w świetle § 146 zasad techniki prawodawczej – w takiej sytuacji stworzyć definicję legalną w ustawie. Zamiast tego mamy w UsługiElektrU defnicje dużo jaśniejszych pojęć, jak adres elektroniczny czy siedziba.

[65] Por. pkt 42 preambuły.

[66] Także pkt 46 i 48 preambuły nie pozwalają na pogłębienie analizy istoty „hostingu" w dyrektywie o handlu elektronicznym.

nawet nie pojawia się termin *hosting*. Artykuł 14 ustawy o świadczeniu usług drogą elektroniczną mówi jedynie o udostępnianiu zasobów systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę. Polska implementacja dyrektywy uwypukla fakt, że dane usługobiorcy mają być przechowywane w systemie teleinformatycznym usługodawcy.[67] Pojęcie systemu teleinformatycznego jest zdefiniowane w art. 2 pkt 3 UsługiElektrU,[68] ale definicja ta nie przybliża nas do rozwiązania pierwszej fundamentalnej kwestii, mianowicie tego, czy usługa „hostingu" polega jedynie na przechowywaniu danych, czy też jej immanentnym elementem jest obowiązek ich udostępnienia użytkownikom Internetu w sytuacji, gdy zażyczy sobie tego usługobiorca usługi „hostingu".

Ujęcie „hostingu" w dyrektywie, jak i w naszej ustawie jest mało precyzyjne i nie oddaje bogactwa tej usługi. Istota „hostingu" sprowadza się do udostępnienia usługobiorcom pewnej infrastruktury komputerowej w celu przeniesienia tam danych, które z założenia mają być udostępnione użytkownikom serwisu do przeglądania. Istotą „hostingu" jest więc nie tyle samo przechowywanie, co właśnie udostępnienie przechowywanych danych użytkownikom Internetu, chyba że operator serwisu,o albo sam użytkownik ukryje lub zablokuje dostęp do kontrolowanych przez siebie danych.

Często akcentuje się element udostępnienia pamięci serwera w celu przechowywania danych, jako kluczowy w zrozumieniu istoty

---

[67] Por. J. BARTA, R. MARKIEWICZ, *op. cit.*, s. 314.

[68] System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. Prawo telekomunikacyjne (Dz. U. nr 73, poz. 852, z 2001 r. nr 122, poz. 1321 i nr 154, poz. 1800 i 1802 oraz z 2002 r. nr 25, poz. 253 i nr 74, poz. 676). Definicja ta stanowi przykład niedoskonałości tworzenia prawa, w której ustawodawca odsyła do ustawy, która utraciła już moc obowiązującą.

„hostingu".[69] Jest to jednak pewien skrót myślowy. Po pierwsze, zdalna przestrzeń dyskowa na nic się zda bez wydajnych procesorów, trwałych zasilaczy czy dużej i szybkiej pamięci podręcznej. Po drugie, oprócz wydajnej infrastruktury komputerowej istotne jest także bogactwo oferowanych usług, w tym m.in. obsługa języków skryptowych (np. PHP, czy ASP.NET), dostęp do baz danych (zarówno typu *open source*, jak i tych droższych, opartych na zamkniętym kodzie np. *MS SQL Server* czy *Oracle*). Chodzi więc nie tyle o przestrzeń dyskową, co infrastrukturę techniczną, która nasza ustawa określa mianem systemu teleinformatycznego.[70] Co więcej, w tego typu usługach bardzo istotną rolę odgrywa szybkość i wydajność nie tylko infrastruktury przechowującej dane, a w jeszcze większym stopniu narzędzi służących udostępnieniu tych danych internautom, czyli szybkości dostępu do Internetu, oferowanej przez usługodawcę „hostingu".

I nie chodzi tu o szybkość pobierania danych przez usługodawcę hostingu, a o przepustowość łącza w kierunku użytkowników serwisu (*upload capability*). W „hostingu" chodzi więc o uzyskanie dostępu do infrastruktury informatycznej umożliwiającej szybkie udostępnienie przechowywanych danych użytkownikom serwisu 24 godziny na dobę. Im lepsze parametry oferuje dostawca usługi, tym z reguły droższa usługa.

---

[69] Tak np. X. KONARSKI, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 139, który sprowadza *hosting* do przechowywania przez usługodawcę danych osób trzecich (usługobiorców); M. ŚWIERCZYŃSKI pojęcie „hostingu" odnosi do udostępniania pamięci podłączonych do sieci serwerów – M. ŚWIERCZYŃSKI, [w:] J. GOŁACZYŃSKI (red.), *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009, s. 133; Szerzej na kwestie te patrzy P. LITWIŃSKI, który pojęcie „hostingu" odnosi do udostępnienia pamięci podłączonych do sieci serwerów w celu przechowywania i udostępniania różnego rodzaju danych – P. LITWIŃSKI, [w:] P. PODRECKI, *Prawo Internetu*, Warszawa 2007, s. 219. Najszersze ujęcie, zbieżne z moim, wydaje się prezentować G. PACEK, *Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych*, Prawo Mediów Elektronicznych, 6/2007.

[70] Tak ujmuje kwestie „hostingu" również Wikipedia. Pod jej wpływem zapewne pozostają najbardziej zbieżne z moimi poglądy G. PACKA, *Ibidem*.

W praktyce gospodarczej spotykamy wiele odmian odpłatnej usługi „hostingu", które można jednak sprowadzić do trzech podstawowych modeli.

Po pierwsze, możemy wykupić usługę „hostingu", w ramach której usługodawca oddaje do pełnej lub częściowej dyspozycji usługobiorcy serwer, rozumiany tu dosłownie jako maszyna. Przy oddaniu serwera do pełnej dyspozycji usługobiorcy obowiązki usługodawcy sprowadzają się do monitoringu pracy serwera, sporządzania kopii zapasowych, instalacji poprawek do systemu operacyjnego oraz innych elementów wsparcia technicznego. Bardzo popularną odmianą tego typu „hostingu" jest usługa, w ramach której usługodawca nie oddaje pełnej kontroli usługobiorcy, biorąc na siebie odpowiedzialność za sprawne funkcjonowanie całego systemu teleinformatycznego (ang. *managed hosting service*). Nowszą odmianą tej technologii są coraz bardziej popularne usługi „hostingu w chmurze" (ang. *cloud hosting*), który opiera się na transparentnym dla usługobiorcy udostępnieniu wielu powiązanych ze sobą fizycznie serwerów (tzw. *clusters of servers*). *Cloud computing* pozwala usługobiorcy płacić jedynie za to, co realnie wykorzystał, w przeciwieństwie do wcześniej omówionych modeli „hostingu" opartych na zasadzie subskrypcji.

Po drugie, usługodawca może zaoferować usługę wirtualizacji serwera, która jest tańsza niż usługa „hostingu", bowiem usługobiorca nie otrzymuje do swojej dyspozycji maszyny, ale wirtualny dostęp do przestrzeni serwerowej. Wirtualizacja serwera występuje także w licznych odmianach. Najtańszym rozwiązaniem jest z reguły usługa współdzielenia przestrzeni dyskowej (ang. *shared hosting service*), w ramach której setki usługodawców otrzymują wirtualny dostęp do przestrzeni dyskowej tej samej maszyny. Zasoby przesyłane są za pomocą usługi FTP. W droższej odmianie tej usługi usługobiorca na jednej maszynie instaluje wiele wirtualnych serwerów (ang. *virtual private server*). W tej odmianie klient uruchamia własną wersję systemu operacyjnego i uzyskuje z reguły pełną kontrolę nad wirtualnym serwerem, który niezależnie od innych

wirtualnych maszyn ma wyłączny dostęp do własnej przestrzeni dyskowej oraz wszystkich elementów systemu operacyjnego.

Trzecim, najdroższym rozwiązaniem jest tzw. kolokacja serwera, czyli usługa polegająca na najmie fizycznej powierzchni u dostawcy „hostingu", w celu zamontowania tam serwera należącego do usługobiorcy hostingu. Usługobiorca sam zarządza swoimi komputerami ulokowanymi w siedzibie usługodawcy. Obowiązki dostawcy usługi sprowadzają się w tym przypadku do zapewnienia dostępu do Internetu oraz stałego dopływu prądu.[71]

W Internecie znajdziemy także wiele ofert nieodpłatnych usług „hostingu". Tego typu usługi są znacząco ograniczone, co polega na konieczności zamieszczenia reklam usługodawcy na stronie czy też tolerowania otrzymywania niechcianych wiadomości e-mail (co każe się zastanowić, czy nie mamy w istocie do czynienia z zamianą usług). Tak zwane darmowe usługi „hostingu" są ograniczone także miejscem oferowanym na przechowywanie plików usługobiorcy, szybkością dostępnych łączy, brakiem dostępu do komercyjnych, a często także niekomercyjnych baz danych oraz (często) brakiem obsługi języków skryptowych,[72] co w praktyce umożliwia przechowywanie jedynie bardzo prostych witryn internetowych.

Kolejną kwestią wymagającą głębszej analizy jest czas przechowywania danych. Eksperci zgodnie twierdzą, że tym, co odróżnia usługę „cachingu" od usługi „hostingu", jest czas przechowywania danych, który w pierwszym przypadku jest bardzo krótki, a w drugim niczym nieograniczony w czasie.[73] I znowu mamy tu do czynienia z pewnym skrótem myślowym. W przypadku klasycznego „hostingu" witryn internetowych praktycznie w każdym przypadku umowa o *hosting* danych

[71] Por. Wikipedia, >>http://en.wikipedia.org/wiki/Web_hosting_service<<, ostatni dostęp: 2.1.2011.

[72] Por. >>http://pl.wikipedia.org/wiki/Hosting<<, ostatni dostęp: 2.1.2011.

[73] Tak, np. X. KONARSKI, *Komentarz…*, s. 139.

będzie zawierana na czas określony, z reguły na rok. Oczywiście w praktyce takie umowy będą przedłużane na kolejne lata, jednakże nie można powiedzieć, że usługa „hostingu" jest świadczona nieskończenie długo. Przeświadczenie o nieokreślonym czasie trwania umowy „hostingu" wynika zapewne ze stosowania art. 14 ustawy o świadczeniu usług drogą elektroniczną do przechowywania danych użytkowników w ramach portali internetowych czy też przechowywania poczty elektronicznej na zdalnych serwerach pocztowych. Jest to jednak zagadnienie dość kontrowersyjne i zostanie omówione w dalszej części artykułu.

*Hosting* odnosi się przede wszystkim do usługi polegającej na przechowywaniu i udostępnianiu stron WWW, ale równie dobrze można mówić o „hostingu" w odniesieniu do innych zasobów umieszczanych w sieci, np. poczty elektronicznej czy danych udostępnianych w ramach sieci wymiany plików (ang. P2P). W tych modelach usługobiorca „hostingu" będzie najczęściej równocześnie występował w charakterze usługodawcy innych usług świadczonych drogą elektroniczną, np. operatora stron internetowych.

### *6.1.1. „Hosting" właściwy a „hosting" wirtualny*

Usługa „hostingu" jest wykorzystywana przede wszystkim dla przechowywania na zdalnym serwerze stron internetowych w celu ich udostępnienia użytkownikom Internetu. Tego rodzaju *hosting* jest z reguły odpłatny i ograniczony czasowo do jednego roku (*hosting* właściwy albo klasyczny). Można się spotkać także z nieodpłatnym udostępnieniem zdalnego serwera w zamian za np. obowiązek umieszczenia na stronach usługobiorcy reklamy podmiotu oferującego tego typu usługi, o czym była już mowa.

Przy „hostingu" stron WWW usługobiorca występuje równocześnie w roli dostawcy usługi społeczeństwa informacyjnego polegającej na oferowaniu dostępu do określonej witryny internetowej, np. sklepu

internetowego, portalu aukcyjnego, portalu społecznościowego czy wyszukiwarki. Tylko w wyjątkowych przypadkach, gdy witryna WWW nie będzie nawet pośrednio źródłem obrotu gospodarczego nie będzie można uznać usługobiorcy za równocześnie świadczącego usługi drogą elektroniczną, ze względu na niespełnienie przesłanki odpłatności oferowanej usługi.

Należy raz jeszcze podkreślić, że w praktyce gospodarczej istotą „hostingu" jest nie tylko przechowywanie, ale także udostępnianie stron internetowych osobom trzecim. Usługobiorca może ograniczyć dostęp pewnym kategoriom osób czy też umożliwić dostęp do pewnych danych wszystkim użytkownikom. Jednakże usługodawca musi umożliwić stały dostęp do wszystkich plików umieszczonych w publicznie dostępnym katalogu serwera zarówno usługobiorcy, jak i użytkownikom Internetu.

W sytuacji gdy usługobiorca „hostingu" właściwego korzystający z infrastruktury technicznej usługodawcy „hostingu" właściwego odpłatnie lub nieodpłatnie udostępnia część infrastruktury użytkownikom jego witryny internetowej, mamy do czynienia z przykładem „hostingu" wirtualnego. Przez *hosting* wirtualny należy rozumieć usługę polegającą na udostępnieniu użytkownikom danego serwisu infrastruktury technicznej podmiotu świadczącego usługę „hostingu" właściwego (klasycznego). Jest to swoiste użyczenie przestrzeni dyskowej oraz ograniczonej funkcjonalności serwisu, np. narzędzi do tworzenia i przesyłania komentarzy lub zasobów danego użytkownika.

Oprócz stron www wyróżnić należy *hosting* poczty elektronicznej. Sprowadza się on do przechowywania korespondencji pocztowej użytkowników serwisu usługobiorcy i jej udostępniania tylko konkretnemu użytkownikowi, który musi znać odpowiednie hasło. Z dostawcą usługi „hostingu" wiązać go jednak będzie podobna umowa jak w przypadku hostingu stron www. W sytuacji gdy operator skrzynki pocztowej korzysta z infrastruktury technicznej usługodawcy „hostingu", występuje

on równocześnie w roli usługodawcy usługi poczty elektronicznej, jak i dostawcy „hostingu" wirtualnego. Z perspektywy użytkownika operator kont pocztowych będzie oferował dostęp do korespondencji i innych plików użytkownika w zamian za „znoszenie" reklam danego usługodawcy i podmiotów z nim powiązanych. W przeciwieństwie do „hostingu" stron www, tego rodzaju *hosting* jest z reguły nieodpłatny i nieograniczony czasowo. Można się także spotkać z odpłatnym udostępnieniem tej usługi w zamian za, na przykład, pojemniejsze konto pocztowe.

Wreszcie wspomnieć należy o specyfice „hostingu" plików w ramach sieci P2P. *Hosting* w ramach sieci wymiany plików oznacza w istocie przechowywanie i udostępnianie danych na komputerach użytkowników, a nie na serwerze usługodawcy. Serwer usługodawcy przechowuje i udostępnia jedynie informacje o lokalizacji poszukiwanych plików (i tylko w najbardziej popularnym modelu sieci P2P, opartym na tzw. serwerach indeksujących). W tym modelu mamy do czynienia z interesującym odwróceniem ról, bowiem usługobiorca usług wymiany plików jest równocześnie usługodawcą usługi „hostingu". Natomiast dostawca usługi wymiany plików będzie równocześnie dostawcą usługi „hostingu" polegającej na przechowywaniu i udostępnianiu informacji o lokalizacji poszukiwanych plików. Przy czym należy zauważyć, że w tego rodzaju systemach należy mówić o wielu usługodawcach „hostingu", bowiem wymieniane pliki są przechowywane na wielu komputerach. *Hosting* plików w sieciach P2P ze względu na swą specyfikę jest z reguły nieodpłatny i nieograniczony czasowo.

### *6.1.2. Spór o zakres przedmiotowy wyłączenia odpowiedzialności z art. 14*

Doktryna jest raczej zgodna, że wyłączenie odpowiedzialności usługodawcy „hostingu" obejmuje zarówno przechowywane, jak i udostępniane dane. Ostatnio jednak ten pogląd został zakwestionowany.

P. Sadowski uznał, że „(…) zakresem wyłączenia odpowiedzialności z art. 14 UsługiElektrU jest wyłącznie przechowywanie danych – przepis ten nie obejmuje natomiast jakichkolwiek innych operacji na danych takich jak choćby udostępnienie tych danych w sieci Internet."[74]

Autor uzasadnił swoją interpretację brzmieniem art. 14 ustawy, które, jego zdaniem, nie wymaga odstąpienia od wykładni językowej. Skoro przepis mówi wyraźnie, że dostawca usługi „hostingu" 'nie ponosi odpowiedzialności za przechowywane dane', to nie zachodzi potrzeba odejścia od zasady *clara non sunt interpretanda*, bowiem jest jasne, że wyłączenie odpowiedzialności dotyczy tylko przechowywania danych, a nie ich udostępniania. Autor nie widzi także możliwości zakwestionowania powyższej interpretacji na podstawie brzmienia art. 14 dyrektywy 2000/31/WE, bowiem także w tym przypadku państwa członkowskie mają jedynie zapewnić, aby 'usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy'.

Także użyte przez ustawodawcę sformułowanie 'niezwłocznie uniemożliwi dostęp do tych danych' nie jest podstawą do przyjęcia rozszerzającej interpretacji, bowiem: po pierwsze, 'mogą istnieć stany faktyczne, w których dane są wyłącznie przechowywane bez ich udostępnianie komukolwiek' i po drugie, 'w typowym modelu dane są przechowywane przez usługodawcę, ale udostępniane osobom trzecim przez usługobiorcę'.

Za powyższą interpretacją przemawia literalna wykładania przepisów ustawy i dyrektywy. Jednakże takiemu ujęciu można także postawić pewne zarzuty:

Po pierwsze, takie ujęcie praktycznie unicestwia wyłączenie odpowiedzialności wobec usługodawców „hostingu", i to nie tylko „hostingu" wirtualnego, ale także „hostingu" właściwego. Jak to zostało już wyżej

---

[74] P. SADOWSKI, *Wyłączenie odpowiedzialności przy świadczeniu usług „hostingu" – polemika*, MOP 2009, nr 16.

przedstawione hosting właściwy polega nie tylko na przechowywaniu danych, ale także na ich udostępnianiu i trudno jest te funkcje rozdzielić. Nie jest bowiem celem samym w sobie umożliwienie przechowywania danych, ale przede wszystkim ich udostępnianie użytkownikom Internetu. W procesie wykładni należy więc wziąć pod uwagę fakt, że mamy do czynienia z pojęciami technicznymi, których interpretacji można dokonywać tylko w ich „naturalnym" kontekście.

Po drugie, takie ograniczenie rozumienia art. 14 byłoby najprawdopodobniej sprzeczne z intencją prawodawcy europejskiego oraz krajowego, bowiem od początku chodziło o wyłączenie odpowiedzialności podmiotów świadczących usługi „hostingu" w pełnym zakresie, a nie tylko w odniesieniu do jednej funkcji. Co więcej, w procesie wykładni art. 14 UsługiElektrU należy wziąć pod uwagę tytuł art. 14 dyrektywy, który – jak to zostało już zasygnalizowane we wstępie – brzmi *hosting*. Stanowi to realizację obowiązku prowspólnotowej wykładni prawa krajowego. A *hosting*, jak to zostało już wykazane wyżej, zakłada nie tylko przechowywanie danych, ale także ich udostępnianie.

Po trzecie, zarówno w dyrektywie, jak i w ustawie pojawia się nakaz uniemożliwienia dostępu do danych w sytuacji, gdy usługodawca dowie się o bezprawnym charakterze przechowywanych danych. Oznacza to niemożność zastosowania zasady *clara non sunt interpretanda*, bowiem istnieje tu wyraźne sprzężenie przechowywania i udostępniania danych. Co więcej, trudno będzie bez dokonania wykładni funkcjonalnej zrozumieć, wobec kogo mają być przechowywane dane zablokowane: usługobiorcy usługi „hostingu" czy też wszystkich użytkowników Internetu.

Wobec powyższego należy uznać, że wyłączenie odpowiedzialności usługodawcy „hostingu" w dyrektywie 2000/31/WE oraz w ustawie o świadczeniu usług drogą elektroniczną obejmuje zarówno przechowywanie, jak i udostępnianie tych danych użytkownikom Internetu.

### *6.1.3. Definicja „hostingu"*

Na podstawie analizy serwisów oferujących tego typu usługi można sformułować następującą roboczą definicję „hostingu":
„*Hosting* oznacza z reguły odpłatną usługę polegającą na zdalnym udostępnieniu usługobiorcy przez czas określony umową lub czas nieokreślony zasobów systemu teleinformatycznego usługodawcy w celu przechowywania i udostępniania użytkownikom Internetu danych tam umieszczonych przez samego usługobiorcę lub użytkowników jego serwisu".

W polskim prawie umowa „hostingu" należy do kategorii umów nienazwanych. Użycie zwrotu 'przechowanie' skłoniło niektórych autorów do rozważenia możliwości zastosowania do oceny obowiązków stron umowy „hostingu" *per analogiam* przepisów kodeksu cywilnego dotyczących umowy przechowania. To dość oczywiste nieporozumienie. W umowie „hostingu" chodzi nie o samo przechowywanie, ale o udostępnianie przechowywanych danych.[75] Kłóci się to z możliwością zastosowania art. 835 kc i nast. w drodze analogii również ze względu na fakt, że przepis ten zobowiązuje przechowującego do zachowania w stanie niepogorszonym rzeczy ruchomej oddanej mu na przechowanie. Nie dość, że nie mamy w przypadku „hostingu" do czynienia z rzeczami ruchomymi, to dane wprowadzane przez usługobiorcę, mogą i czasami będą, przedmiotem edycji przez dostawcę usługi.

Należy przy tym odróżniać *hosting* właściwy od „hostingu" wirtualnego. W „hostingu" właściwym, usługodawcą będzie operator infrastruktury komputerowej umożliwiającej przechowywanie i udostępnianie danych, natomiast usługobiorcą podmiot przechowujący dane, z reguły operator witryny internetowej, operator poczty

[75] Podobnie, J. BARTA, R. MARKIEWICZ, *op. cit.*, s. 314. Na temat charakteru prawnego umowy „hostingu" zob. G. RĄCZKA, *Prawne zagadnienia hostingu*, PPH 2007, s. 379.

elektronicznej, operator sieci P2P. W „hostingu" wirtualnym usługodawcą będzie z reguły usługobiorca „hostingu" właściwego, a usługobiorcą „hostingu" wirtualnego użytkownik serwisu usługodawcy (czyli użytkownik portalu internetowego, serwisu aukcyjnego, poczty elektronicznej itd).

## *6.2. Zakres podmiotowy wyłączenia odpowiedzialności z art. 14*

Jeżeli chodzi o wyznaczenie zakresu podmiotowego wyłączenia, nie budzi wątpliwości, że ochroną art. 14 objęci są „klasyczni" usługodawcy „hostingu", np. Netart.pl czy Home.pl. Natomiast pewne wątpliwości powstają w odniesieniu do „hostingu" wirtualnego, rozumianego jako udostępnienie nie tyle własnej infrastruktury komputerowej, co użyczenie systemu teleinformatycznego pierwotnego hostingodawcy użytkownikom serwisu. Zagadnieniem, które wymaga analizy, jest odpowiedź na pytanie, jakie podmioty obejmuje wyłączenie odpowiedzialności w ramach usługi „hostingu" w rozumieniu art. 14 ustawy i dyrektywy. Do tej analizy przydatne okaże się wprowadzone wyżej rozróżnienie „hostingu" właściwego i „hostingu" wirtualnego.

### *6.2.1. Odpowiedzialność dostawcy usługi „hostingu" właściwego*

W klasycznym modelu usługa „hostingu" jest oferowana przez *data centers*, czyli podmioty specjalizujące się w utrzymywaniu infrastruktury informatycznej dostępnej przez 24 godziny na dobę (*hosting* właściwy). Nie powinno budzić wątpliwości, że wyłączenie odpowiedzialności z art. 14 znajduje zastosowanie do takich podmiotów, bowiem ich model biznesowy opiera się na przechowywaniu i udostępnianiu danych bardzo wielu usługodawców (operatorów stron www czy operatorów skrzynek pocztowych). Trudno też oczekiwać od właścicieli

takich infrastruktur, by monitorowali treści umieszczane na serwisach podmiotów, których dane przechowują, bowiem z reguły nie będą one mieć nawet dostępu do oprogramowania czy baz danych generujących te treści.

Usługa „hostingu" w tym ujęciu jest świadczona na podstawie umowy zawieranej na czas określony, z reguły rok z możliwością przedłużenia, w zamian za świadczenie pieniężne płatne często za rok z góry. Właśnie gwarancja owej stałej i jednocześnie szybkiej dostępności zdalnie przechowywanych plików jest dla wielu operatorów witryn internetowych głównym powodem zainteresowania odpłatnym hostingiem. Ponadto usługodawcy „hostingu", w celu uatrakcyjnienia swojej oferty, poza przestrzenią dyskową umożliwiają także dostęp do systemów umożliwiających archiwizację danych, zabezpieczanie transakcji, usługi bazodanowe, możliwości gromadzenia i analizowania statystyk, operacje na domenach, zarządzanie kontami poczty elektronicznej itd. Zakres świadczonych usług zależy oczywiście od wysokości opłat.

W praktyce spotkać się można z modelem, w którym operator portalu internetowego sam sobie zapewnia *hosting* danych, eksploatując własną infrastrukturę informatyczną. Wiele, zwłaszcza mniejszych, ale także bardzo dużych podmiotów tak czyni, bowiem teoretycznie jedynym wymogiem, poza szybkim łączem internetowym i odpowiednim oprogramowaniem, jest dysponowanie podłączonym do sieci Internetu komputerem ze stałym adresem IP (choć nawet ten wymóg daje się obejść). Jednakże awaria własnej sieci informatycznej uniemożliwi dostęp do własnej witryny internetowej, zatem tylko bardzo duże podmioty mogą sobie pozwolić na utrzymywanie rozbudowanej infrastruktury informatycznej. Co więcej, w takim przypadku wyłączenie odpowiedzialności „hostingu" nie znajdzie zastosowania, bowiem operator witryny internetowej oraz usługodawca „hostingu" będą podmiotami tożsamymi, względnie pozostającymi pod wzajemną kontrolą, co

wyklucza zastosowanie wyłączenia odpowiedzialności w świetle art. 14 ust. 4 UsługiElektrU.[76]

Nie budzi wątpliwości możliwość powołania się na art. 14 ust. 1 ustawy o świadczeniu usług drogą elektroniczną przez dostawcę usługi „hostingu" właściwego, w stosunku do danych zamieszczonych przez usługobiorcę, jak i osoby trzecie korzystające z serwisu usługobiorcy. Innymi słowy, usługodawca „hostingu" właściwego nie będzie odpowiadał nie tylko za dane umieszczone przez usługobiorcę, ale także przez odbiorców usług jego usługobiorcy. Przykładowo, dostawca „hostingu" właściwego nie będzie odpowiadała nie tylko za dane umieszczone przez operatorów witryn internetowych, których dane przechowuje, ale także za informacje umieszczone na tych witrynach przez ich użytkowników. Uwzględnienie danych pochodzących od osób trzecich nie powoduje konieczności wyodrębnienia nowego modelu, ale odmianę modelu klasycznego zaprezentowanego wyżej, w którym przechowywane i udostępniane dane pochodzą jedynie od operatora portalu, występującego w podwójnej roli usługobiorcy „hostingu" i usługodawcy usług stron www.

### *6.2.2. Odpowiedzialność dostawcy usługi „hostingu" wirtualnego*

Jednakże w literaturze można się spotkać z powszechnym przekonaniem, że pojęcie przechowywania danych z art. 14 UsługiElektrU oraz dyrektywy 2000/31/WE znajduje zastosowanie w sytuacji, w której operator stron internetowych (bądź świadczący inne usługi społeczeństwa informacyjnego) umożliwia usługobiorcom tych usług przechowywanie

[76] Zgodnie z art. 14 ust. 4 ustawy: Przepisów ust. 1–3 nie stosuje się, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów o ochronie konkurencji i konsumentów. Redakcja tego wyjątku wywołuje kontrowersje, które będą pominięte w tym artykule. Zob. np. X. KONARSKI, *Komentarz…*, s. 145–146. Por. z M. ŚWIERCZYŃSKI, *Ustawa…*, s. 134.

danych w ramach serwisu takiego operatora (*hosting* wirtualny). W praktyce dotyczy to np. przechowywania komentarzy użytkowników na serwisach aukcyjnych czy blogach.

Przyjęcie tak szerokiej wykładni „hostingu", prowadzić będzie do tego, że od odpowiedzialności za bezprawne treści opublikowane przez użytkownika odpowiadać będzie sam użytkownik. Natomiast od odpowiedzialności zwolniony będzie zarówno dostawca infrastruktury informatycznej służącej przechowywaniu i udostępnianiu danych (*hosting* klasyczny), jak i operator witryny internetowej umożliwiającej przechowywanie i udostępnianie danych przesłanych przez użytkowników serwisu. Podkreślenia wymaga jednak fakt, że operator witryny www będzie zwolniony od odpowiedzialności tylko za dane przesłane przez użytkowników serwisu, a nie za własne dane. Natomiast usługodawca klasycznego „hostingu" będzie zwolniony w każdym przypadku, pod warunkiem spełnienia przesłanek określonych w art. 14 ustawy.

Literalna wykładnia omawianego artykułu może prowadzić do wniosku, że zakresem ochrony z art. 14 są objęci także operatorzy serwisów internetowych umożliwiających przechowywanie i udostępnianie danych przekazanych przez użytkowników serwisu. Może o tym świadczyć brzmienie art. 14 UsługiElektrU, który mówi wyraźnie o usłudze polegającej na udostępnianiu zasobów systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę. Ilekroć więc serwis internetowy będzie oferował taką funkcjonalność, to w tym zakresie operator takiego serwisu będzie występował w roli usługodawcy „hostingu". Co więcej, duże serwisy internetowe w znacznej mierze polegają na danych wprowadzanych przez użytkowników, a nie generowanych przez nie same, co czyni zadanie monitorowania wprowadzanych treści podobne do problemów klasycznego „hostingu".

Można jednak mieć poważne wątpliwości dotyczące możliwości zwolnienia od odpowiedzialności usługodawcy wirtualnego „hostingu".

– Po pierwsze, „klasyczny" hostingodawca nie sprawuje kontroli merytorycznej nad danymi wprowadzanymi do konkretnego serwisu przez jego użytkowników. Dba tylko o to, by funkcjonował nieprzerwany dostęp do danych na wszystkich „hostowanych" przez niego witrynach. Natomiast operator witryny internetowej umożliwiającej przesyłanie danych przez użytkowników ma dostęp do wszystkich narzędzi umożliwiających kontrolę przekazywanych danych.

– Po drugie, przyjęcie wykładni rozszerzającej może doprowadzić do ograniczenia zasady odpowiedzialności twórcy za publikowane treści w kontekście lawinowego wzrostu popularności tworzenia stron na podstawie programów *open source* oferujących wbudowane grupy dyskusyjne czy blogi. Należy bowiem mieć świadomość, że niedługo zdecydowana większość witryn www będzie oparta na rozbudowanych narzędziach umożliwiających przechowywanie i udostępnianie treści generowanych przez użytkowników. Nie stawia to jednak w gorszym położeniu administratorów serwisów „pasywnych", bowiem, jak już zostało to wyżej podkreślone, przyjęcie szerszej wykładni zakresu podmiotowego zwolni z odpowiedzialności administratorów serwisów drugiej generacji jedynie w odniesieniu do treści generowanych przez użytkowników, a nie treści publikowanych przez administratora portalu.

– Po trzecie, konieczne staje się wówczas udzielenie odpowiedzi na pytanie, czy administratorzy serwisów oferujących wirtualny *hosting* są także zwolnieni z obowiązku monitorowania treści przesyłanych przez użytkowników. Z pewności art. 15 nie zwalnia ich z obowiązku monitorowania „własnych" treści, natomiast spójność systemowa nakazywałaby objąć tym zwolnieniem operatorów witryn w odniesieniu do obowiązku monitoringu treści generowanych przez użytkowników.

– Po czwarte, usługa „hostingu" wirtualnego będzie z reguły usługą bezpłatną, w przeciwieństwie do klasycznej usługi „hostingu". Praktycznie nie występuje model biznesowy, w którym operator portalu internetowego pobiera opłatę za możliwość przechowania komentarzy

użytkownika z racji uczestniczenia w grupach dyskusyjnych czy przesyłania komentarzy. Podobnie rzecz wygląda z przechowywaniem poczty elektronicznej, choć w tym przypadku spotykamy się już dużo częściej z modelem subskrypcyjnym, w którym użytkownik za dodatkową opłatą może przechowywać e-maile na większej przestrzeni dyskowej niż w przypadku usług darmowej poczty elektronicznej.

– Po piąte, różnice dają się także zauważyć w odniesieniu do czasu przechowywania danych. W przypadku „hostingu" wirtualnego, jak i „hostingu" poczty elektronicznej czy „hostingu" w ramach sieci P2P będzie to, co do zasady, usługa nieograniczona w czasie. Natomiast w przypadku usługi „hostingu" klasycznego regułą będzie przechowywanie danych przez czas określony umową.

Obecnie trudno odpowiedzieć, w którą stronę pójdzie praktyka sądowa w Polsce i w Unii Europejskiej. W doktrynie zdaje się panować zgoda co do szerokiego interpretowania zakresu podmiotowego art. 14. Z drugiej strony, w swojej ostatniej opinii w sprawie *Google* rzecznik generalny Maduro zasugerował, że wyłączenie odpowiedzialności z art. 14 dotyczyć może tylko podmiotów, które pozostają neutralne wobec przechowywanych danych.[77] W tym świetle odmówił Google ochrony wynikającej z art. 14 dyrektywy w kontekście usługi linków sponsorowanych, bowiem uznał, że operator największej wyszukiwarki internetowej nie jest neutralny w generowaniu wyników w ramach tej usługi. W tym kontekście należy mieć wątpliwości, czy operator jakiejkolwiek witryny www pozostaje rzeczywiście neutralny wobec treści przekazywanych przez użytkowników.

---

[77] Opinia Rzecznika Generalnego w języku angielskim dostępna pod adresem >>http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-236/08<<. Szerzej: P.P. POLAŃSKI, *Liability of Search engines for sponsored and natural results – the case of Google*, [w:] S. KIERKEGAARD, *Legal Discourse in Cyberlaw and Trade*, Malta 2009, s. 273–285.

## *6.3. Przesłanki wyłączenia odpowiedzialności za „hosting"*

### *6.3.1. Przesłanki wyłączenia odpowiedzialności w prawie amerykańskim*

Podobnie jak w przypadku zwykłego przekazu oraz buforowania, postanowienia dyrektywy stanowią w znacznej mierze przetworzenie art. 512 (c) *Digital Millennium Copyright Act*. Zgodnie z nim usługa hostingu ujmowana jest jako przechowanie na żądanie użytkownika treści w systemie teleinformatycznym lub sieci kontrolowanej, lub obsługiwanej przez dostawcę usługi (ang. *the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider*). Warto przy tym wskazać na fakt, że DMCA – w przeciwieństwie do dyrektywy o handlu elektronicznym – nie posługuje się terminem *hosting*.[78]

DMCA wymienia trzy grupy przesłanek, które muszą być spełnione kumulatywnie, aby dostawca usługi „hostingu" mógł się uwolnić od odpowiedzialności za naruszenie prawa autorskiego.

– Po pierwsze, nie może on mieć wiedzy (ang. *actual knowledge*) o bezprawnym charakterze przechowywanych danych lub o nielegalnym charakterze działalności związanej z przechowywanymi informacjami. Wiedza rozumiana jest szeroko i obejmuje także świadomość okoliczności, które oczywiście świadczą o nielegalnej działalności. W przypadku

[78] DMCA, Section 512(C): „Information Residing on Systems or Networks At Direction of Users. – (1) In general. – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider (…)".

uzyskania tak pojmowanej wiedzy pośrednik musi natychmiast zablokować dostęp do kwestionowanych treści.[79]

– Po drugie, pośrednik nie może uzyskiwać żadnych finansowych korzyści w związku z nielegalną działalnością, pod warunkiem jednak że jest uprawniony i ma faktyczną możliwość kontrolowania tego typu działalności.[80]

– Po trzecie, po otrzymaniu zawiadomienia zgodnie ze specjalną procedurą określoną w DMCA natychmiast (ang. *expeditiously*) usunie lub zablokuje dostęp do treści, które mają rzekomo bezprawny charakter, lub treści, z którymi związana jest nielegalna działalność.[81]

### *6.3.2. Przesłanki wyłączenia odpowiedzialności w dyrektywie o handlu elektronicznym*

Zgodnie z art. 14 ust. 1 dyrektywy zatytułowanym *hosting*: „1. Państwa Członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem że:

a) usługodawca nie ma wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji, a w odniesieniu do roszczeń

---

[79] „(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; „(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or „(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to the material.

[80] „(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity."

[81] „(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."

odszkodowawczych – nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności; lub

b) usługodawca podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony."

Zgodnie z art. 14 ust. 2 dyrektywy, wyłączenie odpowiedzialności nie obejmuje przypadku, gdy usługobiorca działa z upoważnienia albo pod kontrolą usługodawcy. Natomiast ust. 3 omawianego artykułu daje możliwość wymagania od usługodawcy przez sądy lub organy administracyjne, by przerwał on naruszenia prawa lub im zapobiegł i otwiera drogę do ustanowienia procedur przez państwa członkowskie regulujących usuwanie lub uniemożliwianie dostępu do bezprawnych danych.

Porównanie obu wersji wskazuje na daleko idące podobieństwa. Obie regulacje zwalniają od odpowiedzialności podmioty przechowujące dane na żądanie usługobiorców. W obu przypadkach opis „chronionej" usługi jest podobny i sprowadza się do przechowywania danych. W obu ujęciach usługodawca nie może mieć wiedzy ani o bezprawnych danych, ani o nielegalnej działalności związanej z materiałami, które przechowuje. Zarówno w DMCA, jak i w dyrektywie wiedza jest interpretowana szeroko i obejmuje nie tylko konkretne przypadki naruszeń, ale także ogólną świadomość nielegalności prowadzonych działań. Wreszcie w obu instrumentach usługodawca musi natychmiast zablokować dostęp do kwestionowanych treści po uzyskaniu wiedzy o naruszeniach związanych z przechowywanymi danymi.

Są jednak i pewne istotne różnice. Po pierwsze, tak jak w przypadku pozostałych wyłączeń odpowiedzialności – rozwiązanie europejskie chroni usługodawców od roszczeń wysuwanych nie tylko na podstawie prawa autorskiego, ale także innych dziedzin prawa. Dostawca usługi „hostingu" uwolniony jest zarówno od odpowiedzialności karnej, jak i cywilnej. Po drugie, rozwiązanie europejskie różnicuje przesłanki

odpowiedzialności karnej i cywilnej. Do przypisania odpowiedzialności cywilnej wystarczy wykazanie świadomości okoliczności wskazujących na nielegalną działalność, natomiast odpowiedzialność karno-prawna wymaga udowodnienia wiedzy o konkretnym naruszeniu prawa. Do zastosowania sankcji karnych konieczne jest wykazanie świadomego przechowywania nielegalnych treści (np. chronionych utworów muzycznych bez zgody podmiotu praw wyłącznych), bądź świadomego godzenia się na nielegalną działalność związaną z przechowywanymi danymi, które same w sobie mogą być legalne (np. przechowywanie serwisów hazardowych w krajach, które zakazują hazardu). Po trzecie, uwolnienie się od odpowiedzialności za przechowywane dane DMCA wymaga wykazania się brakiem korzyści finansowych związanych z kwestionowaną działalnością lub przechowywanymi danymi, pod warunkiem jednak posiadania możliwości realnego wpływu na prowadzoną działalność. Takiego wymogu nie zawiera dyrektywa. Natomiast prawodawca europejski wyłącza możliwość powołania się na przepisy dyrektywy w sytuacji, gdy usługobiorca, czyli przechowujący dane działa pod kontrolą lub z upoważnienia usługodawcy. Uzasadnienie różnic w tym zakresie nie jest proste. Prawdopodobnie intencją prawodawcy europejskiego było stworzenie podobnych, lecz lakoniczniej ujętych oaz bezpieczeństwa w stosunku do DMCA. Być może rozumowanie było takie, że działalnie pod kontrolą powinno być zawsze traktowane jak działanie usługobiorcy, nawet jeśli usługodawca nie czerpie z tego tytułu bezpośrednich korzyści finansowych.

Należy jednak zwrócić uwagę na pewne niebezpieczeństwo związane z takim ujęciem wyjątku od zasady wyłączenia odpowiedzialności dostawcy „hostingu". Otóż, jak zostało to już wykazane wcześniej, 'w praktyce gospodarczej funkcjonuje wiele odmian usługi „hostingu" i zdecydowana większość z nich przewiduje pełną lub większą kontrolę nad przechowywanymi danymi po stronie dostawcy usługi'. Rodzi to – choćby tylko teoretycznie – niebezpieczeństwo przesuwania

odpowiedzialności na usługodawcę hostingu, nawet jeśli naprawdę nie wie on ani nie ma świadomości nielegalnej działalności usługobiorcy. Stąd też bardzo ważne będzie ustalenie wykładni pojęcia kontroli w orzecznictwie Trybunału Sprawiedliwości. Niestety, ani rzecznik generalny w swojej opinii, ani Trybunał Sprawiedliwości w wyroku w sprawie *Google* – choć często się odwoływał do przesłanki kontroli w kontekście usługi „hostingu" – nie wskazali jednoznacznie, jak należy interpretować to pojęcie. Rzecznik Maduro wykluczył możliwość powołania się przez dostawcę usługi AdWords na ochronę z art. 14 dyrektywy, ze względu na „bezpośredni interes" (ang. *direct interest*), jaki Google ma w klikaniu na jego reklamy kontekstowe przez użytkowników Internetu. Ten bezpośredni interes wydaje się przypominać amerykański wymóg braku czerpania korzyści, jednakże Trybunał Sprawiedliwości nie zastosował „testu neutralności" w wersji zaproponowanej przez rzecznika generalnego. Stwierdził jedynie, że ani odpłatny charakter usługi odsyłania, ani ustalanie warunków odpłatności przez Google nie mogą zostać uznane za sprawowanie kontroli czy też za dowód posiadania wiedzy o bezprawnych treściach umieszczanych przez reklamodawców w sponsorowanych linkach. Kwestia ta wymaga dalszych badań.[82]

### *6.3.3. Przesłanki wyłączenia odpowiedzialności w prawie polskim*

Zgodnie z art. 14 ust. 1 ustawy o świadczeniu usług drogą elektroniczną „nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego

[82] Zobacz punkt 6.3 poniżej.

zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych."

W polskim prawie podmiot świadczący usługi „hostingu" będzie zwolniony od odpowiedzialności cywilnej, jak i karnej w sytuacji, gdy nie będzie można mu przypisać jakiejkolwiek wiedzy o bezprawnie umieszczonych treściach (np. zdjęciach pornograficznych z działem małoletnich) lub związanych z nimi działaniach (np. informacji o tym, gdzie znaleźć takie zdjęcia) na jego serwerze.[83] Natomiast w przypadku gdy taką wiedzę posiądzie, czy to w wyniku otrzymania urzędowego zawiadomienia, czy też w wyniku powzięcia innej „wiarygodnej wiadomości", jego odpowiedzialność odnawia się i może skutecznie uzyskać ochronę tylko w sytuacji, gdy zablokuje dostęp do danych, których legalność jest kwestionowana.

Polska implementacja wychodzi nieco poza model zawarty w dyrektywie o handlu elektronicznym i wyłącza także odpowiedzialność usługodawcy wobec usługobiorcy z tytułu zablokowania dostępu do przechowywanych treści. Co więcej, tylko w przypadku gdy usługodawca dowiedział się o bezprawnych treściach w wyniku otrzymania wiarygodnej informacji, będzie on musiał poinformować o fakcie zablokowania treści usługobiorcę. W przypadku otrzymania informacji o bezprawnych treściach w urzędowym zawiadomieniu (przykładowo w wyroku sądowym) nie będzie konieczne nawet poinformowanie usługobiorcy o podjętych działaniach.

---

[83] Dyrektywa o handlu elektronicznym umożliwiła także wyłączenie odpowiedzialności cywilnej w sytuacji, gdy usługodawca nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności. Zob. A.R. LODDER, [w:] A.R. LODDER, H.W.K. KASPERSEN, *eDirectives: Gudie to European Union Law on E-commerce. Commentary on the Directives on Distance Selling*, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, Haga 2002, s. 88–89.

## *6.4. Znaczenie wyroku w sprawie „Google"*[84]

Bardzo istotne dla pogłębienia analizy wyłączenia odpowiedzialności za „hosting" jest powoływane już wielokrotnie orzeczenie Trybunału Sprawiedliwości w sprawie Google. Jedynym zagadnieniem, które zostało poruszone przez *Cour de Cassation* we wszystkich wnioskach, było pytanie o możliwość powołania się przez Google na wyłączenie odpowiedzialności z tytułu przechowywania danych w rozumieniu art. 14 ust. 1 dyrektywy o handlu elektronicznym. Pytanie to można streścić w następujący sposób: czy operator wyszukiwarki może być uznany za świadczącego usługi społeczeństwa informacyjnego polegające na przechowywaniu informacji w rozumieniu dyrektywy 2000/31/WE? Rozciągnięcie sfery zastosowania art. 14 dyrektywy do kwestii odpowiedzialności podmiotów oferujących usługi wyszukiwania miałoby ten skutek, że odpowiedzialność podmiotu świadczącego usługę odsyłania rodziłaby się dopiero z chwilą poinformowania go o bezprawności działania reklamodawcy, i to pod warunkiem że nie zablokowałby on bezzwłocznie dostępu do kwestionowanych treści.

Aby odpowiedzieć na to pytanie, Trybunał w pierwszej kolejności zbadał, czy usługi typu *AdWords* świadczone przez operatora są usługami społeczeństwa informacyjnego w świetle dyrektywy o handlu elektronicznym, a następnie rozważył, czy usługa ta polega na przechowywaniu informacji. Po przeprowadzonej analizie przepisów dyrektywy Trybunał stwierdził, że Google *AdWords* można przypisać status podmiotu świadczącego usługi społeczeństwa informacyjnego.[85] Powyższe stwierdzenie

---

[84] Niniejszy punkt opracowania stanowi zmodyfikowaną wersję fragmentu artykułu: I. KOWALCZUK, P. POLAŃSKI, *Prawne aspekty reklamy w Internecie z wykorzystaniem usługi linków sponsorowanych*, Monitor Prawniczy 2011, nr 1, s. 30–32.

[85] Pkt 110 Wyroku *Google*. Dopełnieniem argumentacji Trybunału było przedstawienie i zbadanie historii legislacyjnej przez rzecznika w opinii, pkt 138.

zgodne jest z celem dyrektywy o handlu elektronicznym, a także z opinią rzecznika generalnego, stanowiskiem Komisji i jako takie nie wymaga szerszego komentarza.

Na wstępie Trybunał zauważył, że opierając się na dosłownym brzmieniu przepisu, dostawca usługi odpłatnego odsyłania (np. Google) może być uznany za podmiot świadczący usługi społeczeństwa informacyjnego polegające na przechowywaniu informacji dostarczonej przez użytkownika tej usługi (reklamodawcę) w świetle art. 14 dyrektywy 2000/31/WE, ponieważ „zachowuje na swoim serwerze niektóre informacje, takie jak wybrane przez reklamodawcę słowa kluczowe, link reklamowy i towarzyszący mu przekaz reklamowy, jak również adres strony tego reklamodawcy."[86] Tym samym Trybunał 'zasugerował możliwość objęcia pojęciem *hosting* także usług, w ramach których usługodawca oferuje jedynie przestrzeń wirtualną użytkownikom swojego serwisu internetowego (tzw. *hosting* wirtualny)'.[87] W tym ujęciu usługodawcą „hostingu" byłby także podmiot oferujący możliwość zgłaszania uwag na stronie w ramach tzw. blogu, przechowywałby on bowiem informacje na żądanie usługobiorcy.

Z drugiej jednak strony, Trybunał wskazał, że celem art. 14, jak i całej sekcji 4 dyrektywy o handlu elektronicznym było objęcie ochroną jedynie pośredników w przekazie informacji. Co za tym idzie, usługodawca będący pośrednikiem nie może mieć wiedzy o przekazywanych lub przechowywanych informacjach, ani sprawować nad nimi kontroli, a jego działanie musi mieć charakter „czysto techniczny, automatyczny i bierny".[88] Wymogi te Trybunał wyprowadził z literalnego brzmienia

---

[86] Pkt 111 wyroku *Google*.

[87] Rozróżnienie pojęcia „hostingu" właściwego i „hostingu" wirtualnego zostało wprowadzone powyżej.

[88] Pkt 113 i 114 *in fine* Wyroku Google. Szerzej na ten temat: P. POLAŃSKI, *Technical, automatic and passive: liability of search engines for hosting infringing content in the light of the Google ruling*, Private Law: Rights, Duties & Conflicts, (ed. S. KIERKEGAARD), ISBN: 978-87-991385-8-6, Barcelona 2010, s. 399–409.

motywu 42 dyrektywy 2000/31/WE.[89] Zastosowanie tych wymogów do oceny usługi typu AdWords Trybunał Sprawiedliwości pozostawił już sądowi krajowemu,[90] który – jak pokazuje stosowne orzecznictwo – miał z tym zagadnieniem sporo problemów i w efekcie nie dodał wiele do orzeczenia Trybunału.[91]

Tym samym „Trybunał uchylił się od udzielenia jednoznacznej odpowiedzi na pytanie czy usługa AdWords korzysta z ochrony gwarantowanej przez art. 14 dyrektywy". Po pierwsze, nie jest jasne, czy Google jako dostawca usług linków sponsorowanych działa w charakterze pośrednika w rozumieniu dyrektywy o handlu elektronicznym. Zgodnie z powoływanym już wielokrotnie motywem 42 dyrektywy o handlu elektronicznym, „wyłączenia w dziedzinie odpowiedzialności ustanowione w niniejszej dyrektywie obejmują jedynie przypadki, w których działalność podmiotu świadczącego usługi społeczeństwa informacyjnego jest ograniczona do technicznego procesu obsługi i udzielania dostępu do sieci komunikacyjnej, w której informacje udostępniane przez osoby trzecie są przekazywane lub przechowywane czasowo, w celu poprawienia skuteczności przekazu". Czy usługa typu *AdWords* jest ograniczona do technicznego procesu obsługi mającego na celu jedynie poprawienie skuteczności przekazu?

Można argumentować, że w przeciwieństwie do usług klasycznych pośredników w przekazie internetowym (zwykłego przekazu danych, „cachingu", „hostingu" właściwego) czy działalności klasycznych wyszukiwarek stron internetowych oferujących tzw. usługi naturalnego wyszukiwania, działalność wyszukiwarek linków sponsorowanych nie jest

---

[89] Porównaj analizę motywu 42 dyrektywy 2000/31/WE w odniesieniu do usług zwykłego przekazu, „cachingu" i „hostingu" powyżej.

[90] Pkt 119 wyroku *Google*.

[91] Zobacz wyroki: Cour de cassation, civile, Chambre commerciale, 13 juillet 2010, 08-13.944, Publié au bulletin; Cour de cassation, civile, Chambre commerciale, 13 juillet 2010, 06-20.230, Publié au bulletin; Cour de cassation, civile, Chambre commerciale, 13 juillet 2010, 06-15.136, Publié au bulletin.

konieczna do przekazania czy udostępnienia informacji w Internecie. Co więcej, nie jest jasne, czy usługa ta ma jedynie charakter techniczny, automatyczny i bierny. Choć bez wątpienia proces automatyzacji musi być nadzwyczaj rozwinięty w siedzibie amerykańskiego giganta, trzeba pamiętać, że jest on równocześnie wspierany pracą ogromnej rzeszy ludzi.

Po drugie, nie wiemy także, czy Google „ma wiedzę" lub „sprawuje kontrolę" nad usługą linków sponsorowanych. TSUE sformułował wiele zaleceń sądowi krajowemu, które ten powinien wziąć pod uwagę przy rozstrzyganiu tego zagadnienia. Zauważył między innymi, iż reklamy w ramach usługi AdWords wyświetlane są „na warunkach kontrolowanych przez spółkę", np. poprzez określanie porządku wyświetlania odesłań na podstawie, między innymi, płaconego przez reklamodawców wynagrodzenia.[92] Fakt pobierania wynagrodzenia od reklamodawców mógłby sugerować, co uczynił rzecznik generalny w swojej opinii, że Google „sprawuje kontrolę" nad przechowywanymi danymi, a tym samym że nie przysługuje mu ochrona na mocy analizowanego artykułu. Jednakże, jak wskazał Trybunał, ani odpłatny charakter usługi odsyłania, ani ustalanie warunków odpłatności przez Google nie może zostać uznane za sprawowanie kontroli czy też za dowód na posiadanie wiedzy o bezprawnych treściach umieszczanych przez reklamodawców.[93] Tym samym Trybunał nie zaakceptował zasady neutralności technologicznej sformułowanej przez rzecznika Maduro, który w fakcie zarabiania na pozycjonowaniu reklam naruszających prawo znaków towarowych upatrywał podstawę do odmówienia Google ograniczenia odpowiedzialności z art. 14 dyrektywy o handlu elektronicznym.

Z drugiej strony, jak stwierdził Trybunał „zgodność między wybranym słowem kluczowym a wyszukiwanym hasłem wpisanym przez internautę nie wystarczy sama w sobie, by uznać, że Google ma wiedzę

[92] Pkt 115 wyroku *Google*.

[93] Pkt 116 wyroku *Google*.

o informacjach wprowadzanych do jego systemu przez reklamodawców i zapisanych na jego serwerze lub że ma nad nimi kontrolę."[94] Dodać tylko można, że zgodność między słowem kluczowym odpowiadającym znakowi towarowemu a pojęciem wpisanym przez użytkownika wyszukiwarki jest o wiele mniej istotne niż możność ustalenia przez Google powiązania między reklamowanym słowem lub słowami a znakiem towarowym. Wobec braku bazy danych oferujących dostęp do wszystkich znaków towarowych w UE z podziałem na kraje możliwość sprawdzenia takiej zależności wydaje się praktycznie niemożliwe.

Trybunał natomiast położył nacisk na konieczność zbadania przez sądy krajowe kwestii roli Google przy sporządzaniu przekazu reklamowego, w szczególności przy tworzeniu linku reklamowego oraz doborze słów kluczowych.[95] Wydaje się, że poprzez to stwierdzenie Trybunał wskazał sądom krajowym przeanalizowanie pod kątem neutralności narzędzi sugerujących wybierane przez reklamodawcę słowa kluczowe będące imitacją lub kopią cudzych znaków towarowych oraz procesu sporządzania i prezentowania reklamy. Pomocna przy interpretacji „neutralności" zachowania Google może być także Opinia rzecznika Maduro, który wskazał, iż usługa ta nie jest czysto techniczną czynnością, a tym samym nie może być uznana za usługę „hostingu".[96]

Odpowiedź Trybunału jest wyważona, poprawna, lecz nie pozwala jednoznacznie odpowiedzieć na postawione pytanie. Bezsprzecznie usługa linków sponsorowanych stanowi usługę społeczeństwa informacyjnego w świetle dyrektywy o handlu elektronicznym. Bardziej kontrowersyjny jest poziom klarowności odpowiedzi Trybunału na drugie, dużo istotniejsze pytanie. Trybunał zdaje się, z jednej strony, przyjmować szerszą interpretację zakresu podmiotowego art. 14 dyrektywy, z drugiej

[94] Pkt 117 wyroku *Google*.

[95] Pkt 118 wyroku *Google*.

[96] Pkt 130 opinii *Google*.

zaś wymaga wykazania, że Google jest neutralnym technologicznie pośrednikiem w przekazie informacji, który z racji pełnienia tej funkcji nie sprawuje kontroli nad przechowywanymi danymi, ani nie wie o naruszeniach. Wobec tego nie wiadomo, czy podmioty oferujące usługi płatnego wyszukiwania mogą faktycznie skorzystać z ochrony na podstawie art. 14 dyrektywy. Pozostaje mieć nadzieję, że może sprawa *Interflora Inc v Marks & Spencer* (C-323/09) doprecyzuje warunki, na których – jeśli w ogóle – podmioty świadczące usługi odpłatnego odsyłania mogą się uwolnić od odpowiedzialności za przechowywane dane.

## *7. Odpowiedzialność dostawców narzędzi odsyłania (wyszukiwawczych)*

W prawie amerykańskim została uregulowana odpowiedzialność dostawców narzędzi odsyłania w sposób podobny do odpowiedzialności usługodawców „hostingu". Zgodnie z DMCA, usługodawca narzędzi odsyłania to dostawca usług umożliwiających odnalezienie treści, takich jak katalogi (ang. *directories*), indeksy, odesłania lub linki (ang. *hypertext links*).

Usługodawca będzie zwolniony od odpowiedzialności za odesłanie do treści naruszających prawo autorskie, jeżeli nie wie, że o tym, iż treści, do których odsyła, są bezprawne, lub też o tym, że wykorzystywane są one do nielegalnych celów.[97] By się uwolnić od odpowiedzialności, nie może

[97] „(d) Information Location Tools. – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if (…)".

być także świadomy okoliczności, z których wynika naruszanie prawa autorskiego – to właśnie ta przesłanka uniemożliwiła usługodawcom narzędzi wyszukiwawczych w ramach sieci P2P na skorzystanie z tej „oazy bezpieczeństwa". Podobnie jak w przypadku usługi „hostingu" w prawie amerykańskim drugim warunkiem do wyłączenia odpowiedzialności jest brak korzyści finansowej z tytułu naruszania prawa autorskiego w sytuacji, gdy dostawca usługi ma prawo i możliwość kontrolowania naruszeń. Wreszcie, w przypadku dowiedzenia się o bezprawności treści, do których odsyła, dostawca usługi musi natychmiast zablokować dostęp do bezprawnych treści, co sprowadza się do usunięcia odesłania albo z indeksu wyszukiwarki, albo z treści strony internetowej.

W przeciwieństwie do rozwiązań amerykańskich prawodawca europejski nie zdecydował się na wprowadzenie specjalnego wyłączenia od odpowiedzialności dostawców usług odesłań. Szybko jednak się okazało, że bez jasnego ustalenia zasad odpowiedzialności tego typu podmiotów na szwank narażona jest pewność obrotu w handlu elektronicznym. Doskonałym przykładem jest omówiony już wcześniej wyrok Trybunału Sprawiedliwości w sprawie Google, który nie dał jasnej odpowiedzi na pytanie, czy dostawca usługi AdWords może się powołać na art. 14 dyrektywy o handlu elektronicznym, w celu uniknięcia odpowiedzialności za naruszenie prawa własności przemysłowej. Poniżej zajmiemy kolejnymi problemami, które rodzą się na tle usług tzw. naturalnego wyszukiwania.

Z uwagi na fakt, iż pytania *Cour de Cassation* dotyczyły tylko usługi *AdWords*, Trybunał nie zajął się problematyką statusu prawnego usługi naturalnego wyszukiwania w świetle dyrektywy.[98] Jednakże rzecznik Maduro rozważył tę kwestię w swojej opinii. Stwierdził on mianowicie, że odpowiedzialność Google w ramach świadczenia powyższej usługi

[98] Por. P.P. POLAŃSKI, *Liability of Seach engines for sponsored and natural results – the case of Google*, (red. S. KIERKEGAARD), *Legal Discourse in Cyberlaw and Trade*, Malta 2009, s. 273 i n.

powinna być wyłączona ze względu jej neutralny charakter.[99] Chociaż Google ma interes w tym, aby wyświetlać odesłania do jak największej liczby stron internetowych, to zarazem nie ma żadnego interesu, aby kierować użytkowników na konkretne strony internetowe.[100] Powstaje jednak pytanie co do zastosowania podstawy prawnej wyłączenia odpowiedzialności Google. Rzecznik generalny Google udzielił niejednoznacznej odpowiedzi na to pytanie. Sformułował jednakże trzy tezy: (1) Google nie świadczy usług „hostingowych", (2) usługa Google może być zakwalifikowana jako podlegająca ograniczeniu odpowiedzialności z art. 13 dyrektywy (*caching*), (3) artykuły 12–14 mogą być stosowane przez analogię. Powyższe twierdzenie, ze względu na obszerność artykułu, prezentowane jest skrótowo, bowiem szersze omówienie tematu wymagałoby oddzielnego opracowania.

Uzasadnienie rozciągnięcia ochrony z art. 14 dyrektywy na usługi naturalnego wyszukiwania, zdaniem rzecznika, byłoby trudne ze względu na fakt, iż Google nie przechowuje informacji na żądanie użytkowników. Jednakże jeśli przez użytkowników rozumiemy administratorów stron internetowych, a nie użytkowników wyszukiwarki, wtedy można byłoby argumentować, że Google przechowuje jednak informacje. Między innymi dlatego, że jedno z narzędzi proponowanych przez Google daje możliwość dodawania przez administratorów dopiero co powstałych stron do indeksu Google. Zatem w takim wypadku można by zastosować ochronę wyłącznie ze względu na przechowywanie informacji.[101]

---

[99] Pkt 144 opinii *Google*.

[100] Na opinię rzecznika mogło mieć wpływ brytyjskie orzeczenie *Metropolita International Ltd v Designtechnica Corporation and Others*, w którym Google uznany został za świadczącego usługę *mere conduit*, a nie za wydawcę w świetle *common law*. Tym samym Google nie jest odpowiedzialny za zniesławiające treści zamieszczone na stronach internetowych. Za: P.P. POLAŃSKI, *Liability of Seach engines for sponsored and natural results – the case of Google*, (red. S. KIERKEGAARD), *Legal Discourse in Cyberlaw and Trade*, Malta 2009, s. 281.

[101] *Ibid.*, s. 281–283.

Inną bardzo ciekawą propozycją rzecznika jest próba zastosowania do usługi wyszukiwania Google art. 13 dyrektywy. Artykuł ten ogranicza odpowiedzialność usługodawców „cachingu" z „tytułu automatycznego, pośredniego i krótkotrwałego przechowywania tej informacji dokonywanego w celu usprawnienia późniejszej transmisji informacji na żądanie innych usługobiorców". Artykuł ten miał na celu chronić pośredników, którzy czasowo przechowują informacje użytkowników, jednakże warunki wyłączenia odpowiedzialności z art. 13 trudno będzie zastosować w stosunku do operatorów wyszukiwarek. Na przykład dostawca usług „cachingu" nie może modyfikować transmitowanych informacji, podczas gdy wyszukiwarki internetowe indeksują strony internetowe i modyfikują dane prezentowane na liście wyników wyszukiwania.

Podsumowując, rzecznik generalny doszedł do wniosku, iż operatorzy wyszukiwarek internetowych zasługują na ochronę na podstawie dyrektywy 2000/31/WE,[102] jednakże nie wskazał konkretnej podstawy wyłączenia odpowiedzialności tego typu podmiotów za usługi tzw. naturalnego wyszukiwania. Co więcej, w wyniku zastosowania zaproponowanego w swojej opinii „testu neutralności" w stosunku do Google uznał on, iż ani usługi naturalnego wyszukiwania, ani usługi typu AdWords nie podlegają zakresowi zastosowania art. 14. Biorąc pod uwagę fakt, iż Trybunał Sprawiedliwości nie odniósł się do kwestii odpowiedzialności dostawców usług wyszukiwawczych w sposób jednoznaczny, a także uwzględniając, iż test neutralności w wersji promowanej przez P. Maduro został odrzucony przez Trybunał,[103] należy postulować przyjęcie klarownych reguł odpowiedzialności dostawców narzędzi wyszukiwawczych. Jest to tym bardziej istotne, że praktycznie każdy większy

---

[102] Szerzej *Ibid.*, s. 284.

[103] Por. P.P. POLANSKI, (2010) *Technical, automatic and passive: liability of search engines for hosting infringing content in the light of the Google ruling*, [w:] S.M. KIERKEGAARD (red.), Private Law: Rights, Duties & Conflicts, Barcelona: IAITL, s. 399–409.

dostawca treści oferuje w ramach swojej usługi narzędzia wyszukiwawcze, które często przeszukują nie tylko własne zasoby usługodawcy, ale całą sieć www.

## *8. Procedura blokowania dostępu do bezprawnych treści*

Zgodnie z motywem 40 dyrektywy o handlu elektronicznym, „(…) usługodawcy mają w niektórych przypadkach obowiązek działania w celu zapobieżenia bezprawnej działalności lub wstrzymania jej; niniejsza dyrektywa powinna stworzyć podstawę odpowiednią do opracowania szybkich i niezawodnych procedur pozwalających na usuwanie lub uniemożliwianie dostępu do bezprawnych informacji; należy opracować takie mechanizmy na podstawie umowy dobrowolnej, negocjowanej między wszystkimi zainteresowanymi stronami, które byłyby wspierane przez Państwa Członkowskie; przyjęcie oraz zastosowanie takich mechanizmów leży w interesie wszystkich stron, które uczestniczą w świadczeniu usług społeczeństwa informacyjnego; przepisy niniejszej dyrektywy odnoszące się do odpowiedzialności nie powinny stanowić przeszkody w rozwoju i w skutecznym wykorzystywaniu, przez różne strony, systemów technicznych ochrony i identyfikacji, jak też instrumentów technicznych nadzoru możliwych dzięki technologiom cyfrowym w ramach ograniczeń ustanowionych przez dyrektywy 95/46/WE oraz 97/66/WE (…)".

Jak to już jednak było wielokrotnie podkreślane, Unia Europejska nie wprowadziła, ani nie opracowała do tej pory procedur blokowania dostępu do treści na wzór amerykański. Procedurę taką dopuszcza jednak dyrektywa o handlu elektronicznym i niektóre państwa członkowskie, np. Finlandia, wprowadziły własną wersję procedury blokowania

dostępu do treści. Na poziomie unijnym dotychczas nie udało się opracować takiej procedury, choć obecnie trwają prace nad analizą odpowiedzi zebranych w trakcie publicznych konsultacji nad przyszłością dyrektywy o handlu elektronicznym,[104] które mogą być przydatne przy tworzeniu stosownej procedury blokowania treści w przyszłości. Oprócz modelu *Notice-and-Takedown* przyjętego w DMCA rozważa się alternatywne modele, takie jak *Notice-and-Stay* czy *Stay-and-Stay*. W ramach modelu *Notice-and-Stay*[105] kwestionowane dane byłyby blokowane zgodnie z ustaloną procedurą, a ich przywrócenie na żądanie osoby, która je przesłała, nie byłoby możliwe. Z kolei w ramach modelu *Stay-and-Stay*[106] pośrednik byłby zobligowany do poinformowania osoby, który przesłała materiały naruszające prawo, o fakcie zablokowania treści. Ten ostatni model – w pewnym zakresie – wprowadziła Polska w ustawie o świadczeniu usług drogą elektroniczną.

## *9. Podsumowanie*

Ostatnie dziesięć lat funkcjonowania dyrektywy o handlu elektronicznym w odniesieniu do kwestii odpowiedzialności pośredników pokazuje, że w swych generalnych założeniach model ten się sprawdza. Konstatacja ta wymaga jednak kwalifikacji w odniesieniu do pięciu

---

[104] Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC), dostępne pod adresem: >>http://ec.europa.eu/yourvoice/ ipm/forms/dispatch?form=electroniccommerce&lang=fr<<, ostatni dostęp: 3.1.2011.

[105] Zgodnie z wyjaśnieniem zawartym w kwestionariuszu dostępnym powyżej, model ten został opisany jako „Regime of notification, take down and making sure that the content will not be reposted".

[106] *Ibidem*, „Regime in which ISP must on request inform the person who uploaded content violating the law".

kwestii, które wymagają – moim zdaniem – interwencji prawodawcy europejskiego.

– Po pierwsze, doprecyzowania wymaga ujęcie istoty „hostingu" z art. 14 dyrektywy o handlu elektronicznym. Dobrze byłoby wskazać, że usługa ta polega nie tylko na przechowywaniu informacji, ale także na ich udostępnianiu. Istotne staje się także doprecyzowanie „testu neutralności" zaproponowanego w wyroku w sprawie *Google*, a w szczególności ustalenia pojęcia „kontroli nad usługobiorcą" oraz problematyki czerpania finansowych korzyści z naruszeń prawa. Należałoby także jasno określić, czy i w jakim zakresie wyłączenie odpowiedzialności z art. 14 dyrektywy można stosować do usługodawców wirtualnego „hostingu", w ramach którego zwykli użytkownicy przechowują własne treści w serwisach Web 2.0 (ang. *user-generated content*). Być może należałoby stworzyć specjalne wyłączenie odpowiedzialności dla podmiotów oferujących usługi typu Web 2.0.

– Po drugie, konieczne wydaje się wprowadzenie procedury blokowania bezprawnych treści na poziomie wspólnotowym. Na przykład ze względu na nieostrość sformułowań wiele sporów budzi interpretacja pojęcia „niezwłocznego" zablokowania dostępu do treści bezprawnych. Brak tego precyzyjnego określenia procedury blokowania treści już dzisiaj skutkuje ograniczaniem wolności słowa na terenie Unii Europejskiej, bowiem dostawcy treści z założenia blokują dostęp do treści wskazanych przez innego użytkownika jako potencjalnie naruszających prawo właściwe. Model przyjęty w DMCA oraz wprowadzony w krajach, jak np. Finlandia, powinien służyć za punkt wyjścia. Jednakże poważnych analiz wymagają także alternatywne modele, takie jak *Notice-and-Stay* czy *Stay-and-Stay*.

– Po trzecie, ostatnie spory wokół korzystania z usług wyszukiwarek pokazują, że konieczne jest wprowadzenie przesłanek wyłączenia odpowiedzialności dla dostawców tego typu usług. Opinia rzecznika generalnego P. Maduro oraz orzeczenie Trybunału Sprawiedliwości w sprawie

*Google* poszukiwały ochrony dla dostawców tych technologii w dyrektywie o handlu elektronicznym, ale bez większych rezultatów. Wyłączenie odpowiedzialności jest konieczne nie tylko w celu zapewnienia większej pewności prawnej globalnym liderom, takim jak Google, ale także wszystkim dostawcom usług społeczeństwa informacyjnego, którzy udostępniają na swoich stronach narzędzia wyszukiwawcze.

– Po czwarte, doprecyzowania wymaga utrzymanie braku ogólnego obowiązku filtrowania treści w świetle rozwoju pornografii dziecięcej oraz innych naruszeń prawa. W szczególności konieczne wydaje się wskazanie przypadków, w których usługodawcy muszą podjąć obowiązek aktywnego filtrowania treści. Raz jeszcze w tym miejscu pojawia się problem stosowania art. 14 do serwisów internetowych oferujących możliwość zamieszczania treści przez ich użytkowników.

– Po piąte, wskazane jest wyznaczenie bardziej klarownej granicy między obszarem oddziaływania dozwolonego użytku publicznego w dyrektywie o harmonizacji prawa autorskiego i wyłączeń odpowiedzialności w dyrektywie o handlu elektronicznym. Chodzi przede wszystkim o jasne określenie, czy usługodawcy „cachingu" podlegają zakresowi zastosowania art. 5 dyrektywy o prawie autorskim, czy też regulacja ta – w odniesieniu do pośredników w dostępie do informacji – odnosi się wyłącznie do dostawców usług zwykłego przekazu. ■

## *O Autorze*

Dr Przemysław Polański. Z wykształcenia prawnik i informatyk, absolwent Uniwersytetu im. Adama Mickiewicza w Poznaniu oraz Monash University w Australii. Doktoryzował się na Melbourne University w Australii; wydał książkę „Customary law of the Internet" dystrybuowaną przez Cambridge University Press. Autor ponad 70 artykułów naukowych poświęconych prawu nowych technologii. Obecnie dyrektor Strategii Produktów Elektronicznych Wydawnictwa C.H. Beck oraz adiunkt Katedrze Metod Ilościowych i Zastosowań Informatyki Akademii Leona Koźmińskiego, a także wykładowca na Uniwersytecie Warszawskim.

PRZEMYSŁAW POLAŃSKI

# Legal liability for content disseminated over the Internet*

# Odpowiedzialność prawna za treści rozpowszechniane w Internecie

* The paper has been based on research conducted by the Author in the European University Institute in Florence in 2010 within the framework of the Summer Fellowship Program and sponsored by the Natolin European Centre.

# *1. Introduction*

In June 2010 ten years had passed from the adoption of Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market,[1] which established the legal framework for development of Internet economy in the European Union. The Directive was implemented into Polish legal order via the Act on the provision of services by electronic means[2] and into the Polish civil code.

The recent decade has witnessed not only a dramatic growth in the number of Internet users, which has just exceeded two thirds of the Union population in Europe, but also the accompanying massive-scale development of services offered on the World Wide Web, which are defined by the Directive as information society services. Consequently, over 330 million[3] Internet users in the EU can daily shop on the Web, find information, compare prices or get education, but also make themselves heard on blogs, share own photos or videos, develop jointly such encyclopaedias as Wikipedia, or attend remote "e-learning" courses. Within this period the world of The Internet has developed in the EU on a massive scale, transforming

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8th June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (directive on electronic commerce), O. J. EC L 178 of 17.07.2000.

[2] The Act of 18th July 2002 on the provision of services by electronic means (Journal of Laws No. 144, item 1204 as amended.). Hereinafter referred to as the Electronic Services Act or the act on the provision of services by electronic means.

[3] Precisely 337,779,055 users in June 2010. Source: >>http://www.internetworldstats.com/ europa.htm<<, last accessed on: 19.11.2010.

from a huge set of static websites served to users into a gigantic web of interactive pages, where users may upload their own content.

In the era of so-called Web 2.0 the users of interactive services have at the same time become authors of the content published therein, massively transforming the mindsets about development of Internet services and posing a challenge to Internet market regulators, who were creating the original legal solutions a decade ago in different realities. The directive on electronic commerce constituted legal foundations for the development of electronic economy, focusing on creation of liberal rules for establishment in the web, at the same time guaranteeing to Internet entrepreneurs application of the country of origin rule, which was intended to have the entrepreneur's operation governed by a single legal system in the EU. Besides those guarantees, the directive on electronic commerce created several important mechanisms harmonizing the legislations of Member States[4] in the area of on-line information obligations and on-line advertising, on-line contracting, and it transposed from the USA the mechanism of limitation of legal liability for transmission or storage of content for some categories of service providers distributing content over the Internet.

One of the goals of the directive was to remove problems arising in connection with emerging disparities between legislation and case-law of Member States concerning liability of service providers acting as intermediaries. European law-maker acknowledged that those disparities prevent smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition.[5] Therefore the supreme goal was to strike a balance between the different interests at stake and establish principles upon which industry agreements and standards can be based.[6]

---

[4] For a broader discussion of the topic see: P. POLAŃSKI, *Usługi…*

[5] Recital 40 of directive on electronic commerce.

[6] Recital 41 of directive on electronic commerce.

Introduction of the rules governing exemptions from liability of intermediaries for content distributed over the Internet aimed to enable to them freedom of operations on the web. This concerns providers of the following services: mere conduit, caching, and hosting. When releasing them from the burden of active search for illegal data, and at the same time excluding or limiting their liability for provided information, the EU law-maker failed to cover with this regime explicitly the service providers of information location tools in the Internet or establish a special regime for non-profit educational institutions, as did American law-maker in the *Digital Millennium Copyright Act*.[7] Moreover the European law-maker failed to define a procedure to be used by an entrepreneur notified about storage of illegal content, aimed to disable or enable access to the allegedly infringing content. The aforementioned shortcomings give rise to serious problems in the application of the provisions of the directive and of the national regulations that implement them; those issues are clearly visible in the ECJ judgments in the combined cases C-236/08, 237/08 and 238/08 concerning Google browser.

This paper aims to analyse in a greater detail the adequacy of the solutions in force against the background of the current state of Internet development in the EU. Part one briefly discusses the American act, which was a model for EU solutions. This is followed by an analysis of the solutions currently adopted in the directive and in the act on the provision of services by electronic means, as regards absence of obligation to monitor the content and exemption from liability for mere conduit, caching and hosting of data. In the summary the paper will draw up conclusions and put forward postulates concerning a reform of the regime governing the liability of Internet service providers in the EU.

[7] See: section 512, *Digital Millennium Copyright Act*.

## *2. Liability of intermediaries in the USA*

Solutions concerning limitation of liability of intermediaries on the Internet were worded for the first time and adopted in the American *Digital Millennium Copyright Act* of 1998, which excludes or limits the liability of intermediaries on the Internet only as regards copyright infringements. Exemption from liability of intermediaries for infringement of personal right is worded differently in the *Communications Decency Act*. Both solutions require at least a brief discussion.

### *2.1. Digital Millennium Copyright Act (DMCA)*

The main intention of the originator of the DMCA was not to introduce a new regime of liability for infringements of copyrights on the web, but to limit the liability of intermediaries distributing content on the web arising out of the existing American law. This limitation concerns both direct liability, contributory liability and vicarious liability. However providers of data transmission, caching, hosting or information location services may invoke relevant legal provisions only of they are able to prove they are service providers, with DMCA containing two definitions of a service provider. According to the first one, a service provider is an entity offering services of the transmission of material of user's choosing.[8] According to the second one, a service provider is an entity providing (1) online services or (2) network access, or (3) the operator of network facilities.[9] The second definition is a much broader

[8] On European soil this definition is reflected in the definition of the provider of services of mere conduit.

[9] Section 512(k)(l)(B): "a provider of online services or network access, or the operator of facilities therefore, and includes an entity described in subparagraph (A)."

one and its scope covers all categories of entities indicated above, including subcontractors acting for the benefit of the indicated categories of intermediaries.

Limitation of liability of intermediaries in the DMCA covers five categories of intermediaries:

1. Providers of services of data transmission over telecommunication networks, i.e. Transitory Communications,[10] which may be briefly defined as services of access to the Internet data transmission over telecommunication networks. In the European Union and Poland such services are defined as mere conduit.
2. Providers of the system caching services,[11] i.e. data buffering to enable their swifter downloading. DMCA requires the server to be configured in accordance with general practices of IT industry. The reference to standards generally used in the industry may be construed as a reference to Internet practices, which are in the making, with major institutions, such as IETF W3C, expected to develop relevant standards.[12]
3. Providers of services of the storage of information on systems or networks at direction of users.[13] The directive on electronic commerce calls this service "hosting", while Polish law defines it as data storage at direction of service recipients. The aforementioned types of services will be analysed further in the paper.
4. Providers of the services of Information location tools,[14] including in particular access to content on the web via hyperlinks provided to the user in search results, site catalogues or online directories. It is worthwhile stressing here that the European Union did

[10] DMCA, Section 512(a).

[11] DMCA, Section 512(b).

[12] HR2281, p. 73.

[13] DMCA, Section 512(c).

[14] DMCA, Section 512(d).

not introduce this exemption to the directive on electronic commerce; this gives rise to many interpretation doubts, which is best evidenced by the judgment of the Court of Justice (discussed later on) in the cases C-236-238/08, with Google search engine being the defendant.

5. Non-for-profit institutions of higher learning. DMCA contains a special clause allowing for application of the aforementioned limitations of liability to universities acting as intermediaries in the access to material online.[15] The special position of universities is related to the exceptional role they play in dissemination of knowledge and support for unrestrained exchange of thought in the society. One general condition and three detailed ones have to be met to enable reliance on limitation of liability. As concerns the general condition, the fundamental criterion is the function played by the faculty member when infringing the law. Institutions of higher learning are not liable like an ordinary employer for law infringements made by faculty members when performing a teaching or research function; however law infringements made by the same faculty member when exercising managerial or operational responsibilities will be fully attributed to the institution. However, even exercise of teaching or research functions will not protect an institution of higher learning if the infringing activities involve providing online access to instructional materials that have been 'required or recommended' for a course taught by the infringing faculty member and/or the infringing graduate student within the last three years. Second, the institution must not have received more than two notifications of claimed infringement with respect to the particular faculty member or particular graduate student within the last three years. Third, the institution must provide to the users of its system or network

[15] HR2281, p. 74.

> – whether they are administrative employees, faculty members, or students – materials that accurately describe and promote compliance with copyright law. The aforementioned premises shall be taken into account only when and if the institution were to be liable under the law in force, as it was not law-makers intention to introduce via DMCA a new or different kind of liability for institutions of higher learning.[16]

American legislation was the first to introduce exemptions of the aforementioned categories of service providers from obligation to actively monitor its service or affirmatively seek facts indicating infringing activity.[17] This does not mean, however, it was American law-makers intention to discourage the intermediaries from content monitoring. On the contrary, according to the rationale in draft HR2281, courts should not conclude that the service provider loses eligibility for limitations on liability solely because it engaged in a monitoring program.[18] The idea was adopted in Article 15 of the directive on electronic commerce in relation to all type of infringements, not just to copyright violations. Under DMCA a copyright owners may request identification of the personal data of persons infringing their monopoly from entities covered with liability restriction or exemption.[19]

The concept to restrict liability under copyrights for acting as an intermediary in the data transfer, storage or search, translates into full exclusion of monetary relief (including also court costs and attorneys' fees)[20] and far-reaching restriction of securing damages through injunctive relief. If a service provider is unable to invoke any of the discussed

---

[16] HR2281, p. 75.

[17] Section 512 (m) DMCA.

[18] HR2281, p. 73.

[19] Section 512 (h) DMCA.

[20] "Monetary relief is defined in subsection (k)(2) as encompassing damages, costs, attorneys' fees, and any other form of monetary payment," HR2281, p. 73.

restrictions, he can still be protected using other legal bases, including the concept of fair use. Against this background it is worthwhile adding that under the Polish copyright doctrine a view has emerged of admissibility of making a claim requesting holding content back from distribution against the discussed categories of Internet service providers.[21]

## *2.2. Communications Decency Act (CDA)*

Just as DMCA is central in defining the rules for exclusion of liability for copyright infringements online, similarly important role is played by the *Communications Decency Act* for defamation in the Internet. The regulations adopted in the CDA enabled intermediaries to interfere in the content generated by service users without being accused of publishing illegal content. The Act was adopted in response to a much publicised court ruling of 1995 in the case of *Stratton Oakmont, Inc. v. Prodigy Services Co*,[22] where the New York Supreme Court decided that a provider of services enabling access to a discussion forum where it acted as an active moderator, may be held liable for contents of postings generated by the users of the said forum.

According to Article 230 CDA, "(…) no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[23] American courts have developed a three-stage test aimed to facilitate the application of the said regulation of telecommunication law, where a defendant to effectively invoke immunity under Article 230 CDA, needs to prove that:

---

[21] J. BARTA, R. MARKIEWICZ, *Prawo autorskie*, Warszawa 2010, p. 311.

[22] 1995 WL 323710 (N.Y. Sup. Ct. 1995).

[23] *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider* (p. 230 CDA).

1) he is the provider of user of an interactive computer system;
2) does not act in the capacity of the publisher or speaker of defamatory content, and
3) is not the source of defamatory content.

The discussed regulation definitely strengthened the position of intermediaries in the access to content online, including in particular the operators of sites displaying content uploaded there by the users, who presently may freely interfere in the content of postings to eliminate obviously illegal content. However, Article 230 has become the source of controversies owing to practices of American courts, which apply this regulation in a very liberal manner; as a consequence in many cases victims of defamation have no chance to obtain any compensation from anyone, particularly when information on the source of illegal content is missing. A frequently quoted example is afforded by the case of *Zeran v. AOL*,[24] whereby defamed Zeran failed to receive a relief from the discussion forum service provider, despite the fact that AOL was greatly in delay with removal of defamatory content. The discussed regulation is particularly significant in the context of regulating the liability for hosted content.

## *3. Absence of the obligation to monitor content in the European Union*

Similarly to DMCA, directive on electronic commerce does not impose on providers of the services of mere conduit, caching and hosting a general obligation actively to seek facts or circumstances indicating

[24] 129 F.3d 327 (4th Cir. 1997).

illegal activity. However, Member States may establish obligations for information society service providers:

- promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service, or
- to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

The above position of the European law-makers is motivated by a quite common conviction that those entities would be hardly able to perform their basic functions if they were charged with the obligation of prior checking the content being distributed or stored. The volume of data they process is so large that this would result in imposition of excessive and disproportionate obligations on service providers, consequently leading to increased prices of access to Internet and online services.[25] And finally, such actions would lead to introduction of censorship in the Internet, paradoxically and significantly weakening the legal position of online service providers, because any interference in the transmitted data could be recognised as interference in the content of the processed data, and consequently deprive them of protection under the 'safe havens' stipulated in the directive and in the act on the provision of services by electronic means.

Owing to absence of a general obligation to monitor the content, directive explicitly provides for monitoring of specifically indicated content. According to recital 47 of directive, "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect

[25] See: *First Report…*

orders by national authorities in accordance with national legislation." Moreover, service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities.[26] And this option causes a growing legal uncertainty in the World Wide Web. A good example is afforded by mutually contradictory rulings of German courts concerning *RapidShare* portal. The decision of the Dusseldorf District Court of 23rd December 2008 ruled that *RapidShare* was obliged to prevent piracy and use more effective means to prevent copyright infringements. However, the Dusseldorf Court of Appeals in its decision issued on 27th April 2010 ruled that *RapidShare* was not liable for copyright infringements either as a direct perpetrator or as an accessory.[27] Beyond any doubt the EU should bring some order into its rules of content monitoring, with introduction of the obligation to monitor the uploaded content being a good solution,[28] provided that the topical scope of the application of this obligation is more precisely phrased.

Poland implemented Article 15 of directive in an even more laconic form, namely by providing that a provider of the services of mere conduit, caching or hosting is not obliged to check the data he transmits, stores or makes available. Thus the act clearly determined that immunity from liability for those entities is not dependent on maintenance of due diligence on their part in the scope concerning the very monitoring of data being stored or transmitted.[29] On the other hand,

---

[26] Recital 40 of directive on electronic commerce.

[27] Quoted after: J. BARTA, R. MARKIEWICZ, *Prawo autorskie*, p. 333.

[28] Introduction of such obligation is advocated by J. BARTA i R. MARKIEWICZ, *op. cit.*, p. 333.

[29] See: A. FRAŃ, *A comment to Article 15 of the act of 18th July 2002 on the provision of services by electronic means* (Journal of Laws 02.144.1204), LEX/el. 2002. A very similar comment by: M. ŚWIERCZYŃSKI, [in:] J. GOŁACZYŃSKI, K. KOWALIK-BAŃCZYK, A. MAJCHROWSKA, M. ŚWIERCZYŃSKI, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Oficyna, 2009, *A comment to Article 15 of the act of 18th July 2002 on the provision of services by electronic means* (Journal of Laws 02.144.1204).

Polish implementation of the directive lacks any explicit exclusion of the obligation actively to seek facts and circumstances indicating illegal activity. A question arises whether exclusion of the obligation to monitor the processed data includes exclusion of active seeking for illegal content. If there is no obligation to check data, then even more so there is no obligation actively to seek for such content. Nevertheless – to obtain the fullest possible legal certainty – it would be better to introduce *de lege ferenda* a precise exclusion of the obligation in this regard also.

Relief from the obligation actively to monitor the content by intermediaries transmitting or storing data is of fundamental importance for understanding of the essence of the liability of those entities in the European Union and in Poland. As time passes, we can observe gradual transformation of the above model towards a gradual introduction of the obligation actively to monitor the transmitted and stored data. The most publicised example, which later found some followers in the European Union, is the obligation introduced by France to suspend Internet access to Internet users who were notified three times of infringing copyrights (so-called HADOPI law).[30]

Presently a heated discussion is raging in the European Parliament on the adoption of a new directive concerning children pornography in

[30] HADOPI is an abbreviation of "Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet" (literally: The High Authority for the distribution of works and protection of rights in the Internet). The law *Loi favorisant la diffusion et la protection de la création sur Internet* was passed on 13th May 2009 by the French National Assembly, but on 10th June 2009 the French Constitutional Council declared the main part of the bill unconstitutional. On 22nd October 2009 the Constitutional Council approved a revised version of HADOPI, requiring judicial review before revoking a person's internet access. See: E. PFANNER, *France Approves Wide Crackdown on Net Piracy* (22.11.2009) available at: >>http://www.nytimes.com/2009/10/23/ technology/23net.html<<, last accessed on: 12.12.2010.

the Internet.[31] Such Member States as France and Spain, which introduced into their legislation the obligation actively to monitor copyright infringements and gambling in the Internet, persistently lobby for mandatory disabling of access to websites containing pornographic materials with participation of children. On the other hand, the governments of Germany and Romania advocate leaving to Member States the discretion in this regard.[32] The final shape of the new directive is to be settled upon in early 2011.

## *4. Exemption from liability for mere conduit*

### *4.1. Essence of mere conduit*

Mere conduit denotes the service of data transmission initiated by users, but rendered by Internet infrastructure operators. To ordinary users this service is offered by Internet service providers, such as operators of fixed and mobile telephone networks, cable or satellite television networks. On the other hand, Internet service providers themselves need to use services of other Internet operators to be able to transmit any transmission sent from another place on Earth. Those are usually the biggest global telecommunication operators, who could be easily charged with

[31] See: COM(2010)94 final, containing Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, available at: >>http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282010%290094_/com_com%282010%290094_pl.pdf<<, last accessed on: 12.12.2010.

[32] It is worthwhile adding here that the eyes of the European public opinion are focused on Poland, which is urged by NGOs protecting civic freedoms to support the position of Germany and Romania. See: >>http://www.edri.org/files/angelilli_wd.pdf<<.

liability for illegal content, whose actual distributors they become. Under the US law, the provider of such services, called transitory communications, is "(…) an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[33] European law contains no definition of an entity offering data transmission services.

## *4.2. Grounds for exemption from liability for mere conduit*

The ground to restrict liability for mere conduit is modelled on exclusion of liability for carrier or courier service providers. Since it is difficult to charge such entities with liability for the content they carry during the transport of parcels or letters, the intermediaries in Internet data transmission quite fast decided to win for themselves similar guarantees in legal provisions. In this connection the legal systems of many states, including the US and European law, granted protection to technical intermediaries transmitting data in telecommunication networks and to Internet service providers.

The legal design of the exclusion of liability of mere conduit intermediaries is not uniform in EU law as it is contained both in the directive on electronic commerce and in the directive on the harmonisation of certain aspects of copyright and related rights in the information society. Both said directives establish the proper legal framework for liability of intermediaries in the Internet, which is corroborated in the preamble to the directive on electronic commerce. According to recital 50 of the said directive, for the authors of both instruments it was important that they come into force within a similar time scale with a view

[33] Section 512(k)(1)(A) DMCA.

to establishing a clear framework of rules relevant to the issue of liability of intermediaries for copyright and relating rights infringements at Community level.

The regulations contained in the directive on electronic commerce were definitely modelled on regulations included in Article 512 (a) DMCA, which were in main part taken over into directive's content. According to the US act, a service provider shall not be liable for the content of material transmitted over telecommunication networks, controlled by or operated for the service provider under five conditions:[34]

1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

[34] "(a) TRANSITORY DIGITAL NETWORK COMMUNICATIONS. – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if –

"(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

"(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

"(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

"(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

"(5) the material is transmitted through the system or network without modification of its content.

3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
5) the material is transmitted through the system or network without modification of its content.

Generally speaking, providers of online data access or transmission services are not liable if the services are provided through an automated technical process, without modification or selection of the material by the service provider and the intermediary does not initiate transmission or select the recipients of the material (except as an automatic response to the request of another person). Also the automated process has to lead to swift deletion of all copies of the transmitted data.

The aforementioned solution was fundamentally accepted in the European law. According to Article 12 (1) of the directive on electronic commerce, where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

a) does not initiate the transmission;
b) does not select the receiver of the transmission; and
c) does not select or modify the information contained in the transmission.

The exclusion of liability relates in particular to the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission (Article 12(2) of the directive). However the directive does not affect the possibility for a court or administrative authority of requiring the service provider to terminate or prevent an infringement (Article 12(3)).

It is easy to see a fundamental similarity of EU solutions with the American original and such conclusion is not challenged by the fact that the American law provides for more grounds for immunity. The modifications introduced in the directive are mainly editorial. Under both legal systems the basic ground for exemption from liability is the neutral character of the transmission activity. The above interpretation is reinforced by interpretation clues contained in the directive. The first of them clearly stresses the requirement that the activity of the information society service provider shall be "(…) of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored."[35] The other one determines that any collaboration with the recipient of the service in order to undertake illegal acts goes beyond the activities of mere conduit: "A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of 'mere conduit' or 'caching' and as a result cannot benefit from the liability exemptions established for these activities."[36]

---

[35] Recital 42 of the preamble to directive on electronic commerce. See also the ruling in case *Google*.

[36] Recital 44 of the preamble to directive on electronic commerce.

The differences in the wording of the exemptions from liability follow mainly from the fact that DMCA provides only for immunity against copyright infringements, whereas directive 2000/31/EC excludes liability of the providers of mere conduit services for any content they transmit. The only noticeable element that was not clearly detailed in Article 12 of the directive is the situation where a service provider selects the recipients of the material except as an automatic response to the request of another person ("autoresponder"), which is an admissible exception from the rule banning initiation of transmission. On the other hand the directive admits the possibility of refraining from the rule prohibiting modification of the transmitted data, when such modification concerns "(…) manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission,"[37] which is not clearly expressed in DMCA provisions. The aforementioned exception legitimizes the customary practice of modification of the headers of the received packets to enable a further transmission. However, significant doubts arise in connection with the possibility of invoking the aforementioned recital by the entities that include in the transmitted data some other content, such as e.g. advertising transmissions, which we will address later on in the paper.

### *4.3. Integrity of the transmitted data and the Deep Packet Inspection*

One of the most interesting – albeit, alas, completely omitted by legal analysis – threads concerning exemption from liability of mere conduit service providers is the assessment of their practices of modification of the transmitted packets in the light of the required prohibition to

[37] Recital 43 of the preamble to the directive on electronic commerce.

modify the content of the transmitted transmissions. It has to be borne in mind that probably a decisive majority of Internet service providers use assistance of technological companies offering tools analysing the content transmitted via infrastructure of a given intermediary. This is an aftermath of a specific warrant requiring readiness to undertake an analysis of the transmitted data, something directly required under the directive on electronic commerce. According to Article 12 paragraph 3 of the directive, a court or administrative authority may require the service provider to terminate or prevent an infringement, which as a result means that the service provider concerned shall disable access to a specific IP number or apply less invasive technologies enabling the filtering of the transmitted data.

*Deep Packet Inspection* is a technology enabling a real-time analysis of the complete content of the transmitted packets. The analysis concerns not only the header of the intercepted packet, but also the part of the transmitted data which is the fundamental purpose of the transmission, i.e. so-called payload. As a result, a service provider applying such technology may learn the content of the transmitted transmission or assemble from parts a more extensive transmission and then analyse it. A simpler form of packet analysis (so-called shallow packet inspection) has been used for a long time to protect electronic communication (e.g. in firewall devices) through inspection of packet headers in order to disable or enable traffic depending on the IP address and port. It was, however, limited by inability to analyse the content itself, mainly due to the volume of data. The present technical progress has allowed for real-time data filtering.

Moreover, the currently offered hardware solutions are capable of inferring the type of transmitted information even when data are encrypted. As a consequence DPI has currently many applications, from the issue of transmission security, through traffic monitoring, copyright protection, censorship, customised advertising to consumer

profiling. Application of this type of technology to improve Internet security rather does not give rise to any legal doubts, unlike the use of DPI, e.g. for advertising purposes.

The use by service providers of mere conduit of DPI technologies for marketing purposes may provide grounds to repeal exemption from liability under Article 12 of the Electronic Services Act and under Directive 2000/31/EC. In such situation ISPs interfere with the choice made by the data recipient and alter the integrity of the transmitted transmissions, because in order to able to attach advertising content to the content downloaded by s service recipient, the intermediaries need to change temporarily the direction of data transmission, i.e. the recipient of the data, and consequently – to alter the integrity of the transmitted data. This phenomenon is related to development of online advertising networks, which monitor the behaviours of buyers on pages belonging to their system.

According to Directive 2000/31/EC, a service provider may benefit from the exemptions for 'mere conduit' provided he does not modify the information he transmits, except manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.[38] Profiling of users with the use of DPI technology can be hardly called a manipulation of a technical nature which does not alter the integrity of the information because the transmission is enriched with advertising content, which content provider did not place in his service. It is worthwhile quoting here once again Recital 42 of Directive 2000/31/EC, which clearly states that exemptions from liability cover only the cases, where "(…) the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by

[38] Recital 43, Directive 2000/31/EC.

third parties is transmitted (…)," and such activity is of a mere technical, automatic and passive nature, which implies the provider has neither knowledge of nor control over the information which is transmitted. The goal of advertising networks is exactly to have control over the largest possible volume of the data on behaviours of Internet users[39] stored in cookie files. In recapitulation, service providers of mere conduit will lose the protection guaranteed to them by directive on electronic commerce when they use content filtering systems for marketing purposes, thus altering the integrity of transmitted data by inserting relevant advertising messages.

## *4.4. Protection of service providers of mere conduit under copyright law*

### *4.4.1. Permitted public use under directive 2001/29/EC*

With regard to claims based on copyright law, service providers of mere conduit in the European Union have at their disposal a legal instrument ensuring to them an even greater protection than Directive 2000/31/EC on electronic commerce. Directive 2001/29/EC admits explicitly the possibility to transmit content beaching copyright and related rights in the frames of mere conduit service. In such context this solutions is going further than the model proposed under the US DMCA and adopted in the directive on electronic commerce.

Recital 33 of Directive 2001/29/EC states that: "The exclusive right of reproduction should be subject to an exception to allow certain acts of temporary reproduction, which are transient or incidental reproductions,

[39] For a broader discussion of advertising networks see e.g. K.C. LAUDON, C.G. TRAVER, *E-commerce 2010: Business, Technology, Society*, 6 edition, Boston 2010, pp. 8–15 and the following ones.

forming an integral and essential part of a technological process and (…)." Article 5 paragraph 1 of Directive 2001/29/EC words this aim as follows:

"Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary, or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2."

In view of the above provision, acts of reproduction are permitted only when five conditions are met cumulatively, namely:

- a given act is temporary;
- it is transient and incidental;
- it is an integral and essential part of a technological process;
- it is carried out for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made, and
- it has no independent economic significance (i.e. it has no economic value).

However, when interpreting Article 5 paragraph 1, one needs to refer once again to Recital 33 of the Directive: "(…) to the extent that they meet these conditions, this exception should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information. A use should be considered lawful where it is authorised by the rightholder or not restricted by law."

Bearing the aforementioned in mind, it has to be stated that Directive 2001/29/EC permitted acts of reproduction under copyright law in the frames of mere conduit service when two additional conditions are met:

1) the mere conduit service provider keeps the integrity of data, and
2) the service provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information.

The first of the above premises is present in the directive on electronic commerce and has been already discussed in a greater detail. One could also argue that this is not a separate premise, because the prohibition to alter the integrity of data can be inferred from the requirement that the process be carried out "(…) for the sole purpose of enabling either efficient transmission in a network between third parties by an intermediary (…)." If the sole purpose is transmission in a network, then any other elements, such as e.g. modification of packets, go beyond this purpose. The other premise appears in the directive on electronic commerce as one of the grounds exempting from liability of service providers of caching services (discussed in a greater detail further on in the paper). However, it seems that the other requirement has hardly any practical significance, because data transmission service providers rather do not interfere with the process of data acquisition, e.g. data about visits in a given service, although, as we have seen on the example of Deep Packet Inspection technology, sometimes intermediaries interfere with the data for marketing purposes. In such case they will also lose the protection guaranteed to them by European copyright law. In recapitulation, only when those two additional premises are met, one can speak of the admissibility of the reproduction of works in the frames of mere conduit services.

### *4.4.2. Significance of the ruling in the case of "InfoPaq"*

In its judgement in the case *C-5/08 of InfoPaq*, the Court of Justice made a further interpretation of the above provision and deemed that the aforementioned conditions – as exceptions to the rule of obtaining permission to reproduce works – must be interpreted strictly.[40] An additional argument in favour of accepting the thesis that a restrictive interpretation of this article shall be used, is comprised, on the one hand, by the requirement to ensure legal security to authors as regards protection of their works, and on the other hand, by the necessity to apply a so-called three-tier test (Article 5 paragraph 5), which assumes that the exceptions and limitations provided for in the directive shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.

As regards the requirement of transience in the case *C-5/08*, Infopaq, operating an Internet media monitoring business, claimed that the acts of reproduction at issue in the main proceedings fulfilled the condition relating to transient nature, since they were deleted at the end of the electronic search process. The Court of Justice found that: "(…) an act can be held to be 'transient' within the meaning of the second condition laid down in Article 5(1) of Directive 2001/29 only if its duration is limited to what is necessary for the proper completion of the technological process in question, it being understood that that process must be automated so that it deletes that act automatically, without human intervention, once its function of enabling the completion of such a process has come to an end."[41]

---

[40] Case *C-5/08 Infopaq*, Recital 56.

[41] Case C-5/08 *InfoPaq*, Recital 64.

Application of the above finding to the case of *InfoPaq* proved to be challenging. The Court of Justice of the European Union ordered the national court to determine whether the issue concerns a technological solution covered by exemption under Article 5 of the directive. It added two clues. First, that "(…) in the main proceedings, the possibility cannot be ruled out at the outset that in the first two acts of reproduction at issue in those proceedings, namely the creation of TIFF files and text files resulting from the conversion of TIFF files, may be held to be transient as long as they are deleted automatically from the computer memory." Second, "(…) regarding the third act of reproduction, namely the storing of a text extract of 11 words, the evidence submitted to the Court does not permit an assessment of whether the technological process is automated with the result that that file is deleted promptly and without human intervention from the computer memory. It is for the national court to ascertain whether the deletion of that file is dependent on the will of the user of the reproduction and whether there is a risk that the file might remain stored once the function of enabling completion of the technological process has come to an end."

When analysing the above rationale, one may conclude that at the present stage of the development of new technologies, a judge faces an issues so complex that his knowledge and experience are not sufficient to give a fair judgement. Unfortunately, the work of a judge is limited to phrasing of very general interpretation guidelines, which the Court subsequently is already unable to use to solve the issue at hand. For example: why does the Court suggest that scanning of a document into TIFF format followed by conversion of TIIF files into text files is automatic and results in automatic deletion of the reproduced content, while the storing of a text extract of 11 words or deletion of those extracts is not automatic? Certainly, one may argue that judges are extremely cautious in the wording of their judgements, practically delegating the application of general guidelines to national courts

and explicitly indicating that the aforementioned classifications cannot be ruled out.

### *4.4.3. Permissible use of protected works under Polish copyright law*

Article 5 paragraph 1 of Directive 2001/29/EC was implemented into Polish legislation via Article 231 of copyright law. According to this provision "No author's permission shall be required for transitory or incidental reproduction of works, such reproduction having no independent economic significance but constituting an integral and fundamental part of a manufacturing process the sole purpose of which is to enable: 1) transmission of work through the data transmission system between third parties by an intermediary, or 2) the use of work in compliance with law." The aforementioned comments shall be used to interpret the above provision.

The doctrine has identified the problem of mutual relation between Article 12 of the act on the provision of services by electronic means and Article 231 of the copyright law, which implements the discussed provision of Directive 2001/29/EC. As a consequence a view has surfaced that the aforementioned Article 231 of the copyright law is a special provision in relation to Article 12 of the act on the provision of services by electronic means, and therefore it is the only condition to exempt from liability a service provider of mere conduit under copyright law.[42] This position shall be agreed with.

### *4.4.4. Obligation to disclose the personal data of Internet users*

Article 15 (2) explicitly grants the possibility for a court or administrative authority to undertake actions or acquire information from

[42] J. BARTA, R. MARKIEWICZ, *Prawo autorskie*, Warsaw 2010, p. 312.

intermediaries of mere conduit, but this privilege does not concern private entities. One of the most interesting judgements of the Court of Justice in this context was the ruling in the case *C-275/06 Promusicae v Telefonica*. The Spanish collective rights management organisation requested the Internet service provider to disclose the identities and physical addresses of certain persons who on the dates it indicated downloaded files from the KaZaA file exchange program. *Telefonica* refused such disclosure arguing that transfer of the concerned data is possible only under criminal and not civil proceedings. In view of the above, many questions concerning not only the directives concerning new technologies, but also fundamental rights, were addressed to the Court of Justice.

After long deliberations, the Court of Justice came to the following conclusion: "(…) Directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require the Member States to lay down (…) an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings." Absence of the obligation to communicate personal data to collective rights management organisations was interpreted as a victory of file exchange networks. However, the judges included in the judgement's summary a suggestion that courts "(…) must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality." Even foregoing the ambiguity of such guidelines, one may conclude that national courts could as well order communication of such data if they deem that this does not breach the proportionality between the rights of privacy and personal data protection right on the one hand, and the property right and the right to make effective claims for own rights before courts on the other.

# *5. Exemption from liability for caching services*

## *5.1. Essence of caching*

Caching is a service consisting in temporary storage of data in an IT system located between the service recipient and content providers with a view to accelerating the access thereto (data caching). As a rule such service is available in the frames of Internet access services or within corporate networks. In the former case, the provider of access service temporarily stores on his computer websites and other data downloaded by his subscribers so that the next users reaching for those resources may download them directly from service provider's server. In the latter case the entity that caches data is the local network administrator, who stores them and makes accessible to users of his network from a so-called proxy server, whose functions – besides temporary data caching – also include content filtering and anonymous use of the Internet by people working within a local network.[43]

## *5.2. Grounds for exemption from liability for caching*

### *5.2.1. Caching under US law*

Limitation of liability for caching service providers was introduced for the first time in the US Digital Millennium Copyright Act. DMCA defines caching service as the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider.[44] The service is characterised under DMCA as follows:

---

[43] According to Recital 14 of the directive on electronic commerce, "(…) this Directive cannot prevent the anonymous use of open networks such as the Internet."

[44] DMCA, Section 512(b).

1) the material is made available online by a person other than the service provider, and
2) the material is transmitted from the content provider through the system or network to a user at the direction of that user, and
3) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted, request access to the material from content provider.[45]

DMCA excludes liability for copyright infringements by offering system caching, i.e. caching of illegal data in order to enable their faster downloading by service recipients, when several conditions are met:

1) the material is transmitted to the subsequent users without modification to its content (from the manner in which the material was received by the first user);[46]

---

[45] "(b) SYSTEM CACHING. – "(1) LIMITATION ON LIABILITY. – A service provider shall not be liable for monetary relief, or, except as provided In subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –
"(A) the material is made available online by a person other than the service provider;
"(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and
"(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

[46] "(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A).

2) the caching service provider complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, however except such rules adopted by the material provider that are used to prevent or unreasonably impair the intermediate storage;[47]
3) the caching service provider does not interfere with the ability of technology associated with the material to return to the material provider the information that would have been available to that person if the material had been obtained by the subsequent users directly from that person, except that this subparagraph applies only if that technology:
   a) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material,
   b) is consistent with generally accepted industry standard communications protocols, and
   c) does not extract information from the provider's system or network other than the information that would have been available

[47] "(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data Communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies.

to the material provider if the subsequent users had gained access to the material directly from that person;[48]

4) if the material provider has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the caching service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions;[49] and

   a) if the caching service provider removes, or disables access to, the material that is claimed to be infringing upon notification of claimed infringement),

   b) if the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered

---

[48] "(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology –

"(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

"(ii) is consistent with generally accepted industry standard communications protocols; and

"(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person.

[49] "(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and…

that the material be removed from the originating site or that access to the material on the originating site be disabled.[50]

### *5.2.2. Caching in the directive on electronic commerce*

According to Article 13 of the directive on electronic commerce, caching is defined as the information society service consisting in automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request.[51] The definition proposed in DMCA is more extensive and better describes the essence of caching, which consists in temporary storage of information transmitted from material provider to service user (service recipient) solely with a view to making more efficient the information onward transmission to subsequent users. It is worthwhile pointing out here the difference in the function of transient information storage under this service and under mere conduit service, referred to in Article 12 paragraph 2 of the directive, sometimes termed Internet routing. In the

[50] "(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if – "(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and "(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

[51] According to Article 13 paragraph 1 of the directive "Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request (…)".

case of mere conduit, the main goal is to enable transmission, and not to accelerate the access to data.

Similarly to mere conduit service, the legal design of exemption from liability for data caching quite faithfully replicates the solutions adopted under the *Digital Millennium Copyright Act*:

a) the provider does not modify the information;
b) the provider complies with conditions on access to the information;
c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. Similarly to the mere conduit service, court or administrative authorities may require the service provider to terminate or prevent an infringement.

A service provider can benefit from exemptions for caching when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits. This condition shall be interpreted in the same manner as for mere conduit service.[52] Firstly, the prohibition of modification of the stored information does not concern manipulations of a technical nature

[52] Quite interesting are the considerations of Advocate General P. Maduro, who in the opinion to the combined case of *Google* suggests exemptions for data caching may be applied to providers of web browser services, and specifically to providers of the services of so-called natural search results. See below.

which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission."[53] Secondly, the activity of the information society service provider shall be limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted. Thirdly, his activity shall be of a mere technical, automatic and passive nature, which implies the provider has neither knowledge of nor control over the information which is transmitted.[54] Fourthly, exemption from liability for a service provider does not cover a situation where the service provider deliberately collaborates with one of the recipients of his service in order to undertake illegal acts.[55]

Both the directive and DMCA demand that the information caching system be configured in accordance with industry standard communications protocols and technologies. The reference to industry standard communications and protocols may be interpreted as a reference to the customary laws in the Internet that are only now in the initial stages of development and deployment, with Internet industry standards setting organizations, such as the Internet Engineering Task Force and the World Wide Web Consortium, expected to act promptly and without delay to establish these protocols.[56] Such references are made for the condition to comply with the rules concerning information updating and undistorted permissible use of technologies to source data on information use. The differences between European and American versions, besides a more precise definition of the essence of caching and presence of the access disabling procedure, are limited to wording and better detailing of the exceptions to the grounds for exemption from liability.

---

[53] Recital 43 of the preamble to directive on electronic commerce.

[54] Recital 42 of the preamble to directive on electronic commerce.

[55] Recital 44 of the preamble to directive on electronic commerce.

[56] See: HR2281, p. 73. On customs in the Internet, see: P. POLAŃSKI, *Customary law of the Internet*, Hague 2007.

– Firstly, as regards the condition to respect the information updating rule, American law-maker explicitly stipulates that the rules can be ignored by the provider of caching service where their application would prevent or unreasonably impair provision of caching service. The directive shall prove that such rules are commonly ignored, which may greatly hamper the application of this exemption in practice.

– Secondly, as regards the condition to respect the rule of undistorted acquisition by the material provider of the data on the information use, DMCA introduces three requirements, out of which only one found way to the directive. Both instruments refer to industry standards in this respect. However DMCA admits the possibility of breaching this rule also in a situation when – similarly to the previous case – this would unreasonably impair provision of this service, and also when the material provider would obtain more data on the use of information than if the subsequent users had gained access to the material directly from that person. European service providers have to make do with good knowledge of industry-standard customs.

– Thirdly, as concerns the respect for the rules of access to information, the American law-maker included an instruction that if the material provider has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions. The European law-maker is more laconic, although one can hardly have any doubt in this case whether such type of data can be made available to persons other those authorised. It is worthwhile stressing here once again that despite lack of reference to industry standards, customary laws have been developed in this respect, such as prohibition for a service provider to cache encrypted data or prohibition to store pages available after logging on. A provider of caching services shall comply with those rules.

Polish transposition of Article 13 of the directive, although worded differently, as a rule is consistent with the purpose of Directive 2000/31/EC. Therefore all aforementioned comments shall be taken into account when applying this provision.

## *5.3. Caching and copyright*

Similarly to mere conduit services, when analysing exemptions from liability for caching one shall take into account the already discussed Article 5 paragraph 1 of the directive on the harmonisation of certain aspects of copyright and related rights in the information society. It is worthwhile recalling that temporary acts of reproduction, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable a transmission in a network between third parties by an intermediary, of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction rights.

Permissible use under Article 5 paragraph 1 of the directive and Article 231 of the copyright law concerns transient and incidental reproductions, i.e. ones that disappear when transmission process ends. In the Polish implementation of this provision, the absence of the condition of temporary character was noticed, but it can be inferred from the transient or incidental nature of the reproduction.[57]

---

[57] In the doctrine, one can encounter an attempt at defining transient reproduction, which is deemed short-term reproduction, deleted automatically after use or after a specified time, and of incidental reproduction as a reproduction that takes place only during a technical process. See: P. ŻERAŃSKI, *Zakres dozwolonego użytku dostawcy usług internetowych w świetle Article 23[1] Prawa autorskiego w kontekście ustawy o świadczeniu usług drogą elektroniczną*, MoP 2008, No. 20, invoking: M. WELSER, [in:] *Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, Ergänzungsband zum Urheberrecht*, (ed.) A.-A. WANDTKE, Winfried Bullinger, Monachium 2002, p. 44.

A question arises whether this provision may be applied also to providers of caching service. A positive answer in this respect would liberate service providers from the necessity to meet many conditions for exemption from liability under the directive on electronic commerce and the act on the provision of services by electronic means. Such interpretation may be supported by – already quoted several times – Recital 33 of the directive on the harmonisation of certain aspects of copyright and related rights in the information society, which states that the exception should cover acts of caching, including those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information. Loading of information into a cache in combination with the functioning of transmission systems may be interpreted as an order to cover caching service with this exception. Moreover the European law-maker explicitly requires respect for the rule of non-interference with information on the data use by service users, which is one of the conditions to exclude liability for caching under the US and European law.

However a question so asked must be answered negatively. Although the provision at hand allows for a temporary reproduction of files, but it does so for a particular case of loading data into the cache of the user's computer (or, more precisely, its operating system). However, with regard to temporary reproductions by intermediaries[58] it requires they involve solely the data transmission, i.e. mere conduit.[59] As a rule caching is not required for information transmission. However, opinions on that

[58] P. ŻERAŃSKI points out that within the meaning of the Electronic Services Act one must not identify the notion of an intermediary with a service provider. P. ŻERAŃSKI, *op. cit.*

[59] Rightly so: J. BARTA, R. MARKIEWICZ, *op. cit.*, pp. 312–313.

issue are still divided[60] and a competent EU institution shall intervene to remove the doubts in this regard. This also does not rule out adoption of such manner of applying the discussed provisions, where first it is checked whether the discussed case of permissible public can be used, and only as a second resort the possibility of applying Article 13 of the directive and the act on the provision of services by electronic means is checked.

## *6. Exemption from liability for hosting*[61]

The issue of liability of service providers of hosting is among the most hotly debated in the law doctrine and case-law. A rapid website development would be impossible without hosting services, because their creators or administrators need space where they can store their works and make them available to web users. Also other popular Internet services, such as electronic mail or file exchange in controversial *peer-to-peer* networks require hosting service for postings being received or files being made accessible. On the other hand, the very notion of hosting is not uniformly understood in the Polish doctrine, which is unfortunate as this is a legally central issue because the way it is defined will determine the scope of liability of the providers of such type of online services pursuant to provisions of the directive on electronic commerce and the act on the provision of services by electronic means.

---

[60] The possibility to invoke permissible use is supported by: P. ŻERAŃSKI, *op. cit.*, "(…) transient reproductions emerging during those processes may be covered with permissible use under Article 23[1] of the Copyright Law", and also by K. GIENAS, *Systemy Digital Rights Management…*, *op. cit.*, p. 21, P. PODRECKI, [in:] *Prawo Internetu*, *op. cit.*, p. 47.

[61] In a slightly modified form, sections 6.1 and 6.2 were previously published in an article titled: *Uwagi na temat odpowiedzialności usługodawcy hostingu w Internecie* (ed. J. GOŁACZYŃSKI), *Informatyzacja postępowania sądowego i administracji publicznej*, Warsaw 2010, pp. 299–312.

In the doctrine we encounter a problem with interpretation of the notion of hosting, because neither the directive on electronic commerce nor the act on the provision of services by electronic means define this term. At the same time both instruments characterise this service as data storage, which is too narrow a definition. As a rule hosting is a service provided against a charge and consisting in making remotely available to a service recipient, for a period defined by a contract or by an unidentified time, of the IT system resources of the service provider with a view to storing and making accessible to Internet users of the data stored there by the service recipient or the users of his service. Here one needs to differentiate between dedicated (classic) *hosting* and virtual hosting, an issue addressed in more detail below.

## *6.1. Essence of hosting*

The issue of hosting was regulated in Article 14 of Directive 2000/31/EC on electronic commerce and Article 14 of the act on the provision of services by electronic means, which implements directive provisions. The discussed directive exempts – under certain conditions to be discussed later – the service provider from criminal and civil legal liability for "information stored at the service recipient's request".[62] The regulation at hand provides for information storage only and not for making it available. Therefore doubts may arise – in particular – whether making the stored data accessible to other service recipient is at the core of this service.[63]

---

[62] The English version makes a similar stipulation, providing for an information society service, which "(…) is provided that consists of the storage of information provided by a recipient of the service".

[63] According to Article 2 bullet d of the directive, a 'recipient of the service' is "any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible."

The directive on electronic commerce does not contain a legal definition of hosting.[64] Moreover, in the directive on electronic commerce the very term of hosting is contained only in the title of an article, and not in its very tenor. The preamble to the directive on electronic commerce also provides hardly any material that might help deepen the analysis of the notion of hosting. Similarly to mere conduit and caching services, the preamble recalls the requirement that the activity shall be limited to the technical process of operating, which means that the activity of the provider of hosting service is of a mere technical, automatic and passive nature, which in turn implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.[65] However, the above characteristics are definitely much more useful for an analysis of conditions for exemption from liability than for understanding the essence of hosting. Hence we will address the issue again further on in the paper.[66]

Polish implementation of the directive also fails to include a definition of hosting. The act on the provision of services by electronic means does not contain the term of hosting at all. Article 14 of the act on the provision of services by electronic means provides only for making the resources of the information and communication technology (ICT) system available for the purpose of data storage by the service recipient. The Polish implementation of the directive stresses the fact that the data of the service recipient shall be stored in the service provider's ITC system.[67] The notion of ITC system is

---

[64] The difficulties raised by the very understanding of the term have many reasons: the English etymology, technical nature, EU provenience. Unfortunately, if a meaning of a certain term is not commonly comprehensible, in the light of § 146 of the principles of law-making technique, in such situation the law-maker should create a relevant legal definition in the act. Instead the Electronic Services Act contains definitions of much clearer terms, such as the electronic address or the seat.

[65] See Recital 42 of the preamble.

[66] Also Recitals 46 and 48 of the preamble do not allow for an in-depth analysis of the essence of hosting in the directive on electronic commerce.

[67] See: J. BARTA, R. MARKIEWICZ, *op. cit.*, p. 314.

defined in Article 2 bullet 3 of the Electronic Services Act,[68] but this definition does not bring us any closer to a resolution of the first, fundamental issue, namely whether the hosting service consists solely in data storage, or is the obligation to make them accessible to Internet users, upon request of the recipient of the hosting service, an immanent element thereof.

The notion of hosting both in the directive and in our act is hardly precise and does not do justice to the richness of this service. The essence of hosting lies in provision of access for service recipients to certain computer infrastructure with a view to transferring there the data that as a rule are to be made available for viewing to site users. Hence the core of hosting service is not storage by itself but making available of the data to Internet users, unless the service operator or the user himself hides or disables access to the data he controls.

The element of providing access to server's memory with a view to storing data is frequently stressed as a central one in the understanding of the essence of hosting.[69] This is a mental shortcut, though. Firstly,

---

[68] The information and communication technology system – a set of cooperating IT devices and software, ensuring data processing and storage, plus data sending and receiving by ICT networks via the end device proper for a given network within the meaning of the Act of 21st April 2000, the Telecommunication Law (the Journal of Laws No. 73, item 852, of 2001 No. 122, item 1321 and No. 154, items 1800 and 1802 and of 2002 No. 25, item 253 and No. 74, item 676). This definition is an example of imperfect law-making, where the law-maker refers to an Act that is no longer in force.

[69] For example: X. KONARSKI, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warsaw 2004, p. 139, who reduces the notion of hosting to storage by the service provider of the data of third persons (service recipients); M. ŚWIERCZYŃSKI referred the notion of hosting to provision of access to the memories of servers connected to a network – M. ŚWIERCZYŃSKI, [in:] J. GOŁACZYŃSKI (ed.), *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warsaw 2009, p. 133; A broader perspective on the issue is offered by P. LITWIŃSKI, who refers the notion of hosting to provision of access to the memories of servers connected to a network with a view to storing and making accessible various types of data – P. LITWIŃSKI, [in:] P. PODRECKI, *Prawo Internetu*, Warsaw 2007, p. 219. A broader interpretation, consistent with mine, seems to be presented by G. PACEK, *Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych*, Prawo Mediów Elektronicznych, 6/2007.

remote disc space would be of no use without powerful processors, durable power supplies or large and fast cache. Secondly, despite an efficient computer infrastructure of equal importance is wealth of offered services, including support for scripting languages (e.g. *PHP*, or *ASP.NET*), access to databases (both of open source type and the more expensive ones, closed-code ones, such as *MS SQL Server* or *Oracle*). So the notion concerns not so much the disc space, but rather the technical infrastructure, which our act calls the information and communication technology system.[70] Moreover, an extremely significant role in the services of this type is played by the speed and efficiency not only of the data capture infrastructure, but also – to an even greater extent – by the tools that enable making those data available to Internet users, i.e. the speed of access to the Internet offered by the provider of hosting service.

And this does not concern the speed of data download by the hosting service provider, but rather the upload capability. Therefore hosting is about gaining access to IT infrastructure enabling fast and 24/7 provision of access to the stored data for site users. As a rule, the better the performance offered by the service provider is, the more expensive the service gets.

In business practice we encounter many varieties of hosting service offered against a charge, which may be reduced to three basic models.

Firstly, we can purchase a hosting service where the service provider makes a server, understood here literally as a machine, partially or fully available to the service recipient. When the server is fully made available to the service recipient, the obligations of the service provider are limited to the monitoring of the server's operation, making backup copies, installations of operating system fixes and other elements of technical support. A very popular variety of this type of hosting is a service where

[70] This is also the interpretation of hosting in Wikipedia. Probably under its influence the views of G. PACK, *Ibidem* remain most convergent with mine.

the service provider does not give up full control to the service recipient, assuming responsibility for efficient operation of the entire ICT system – so called managed hosting service. A more recent variety of this technology is comprised by the increasingly popular cloud hosting services, which are based on providing – transparent for the service recipient – access to clusters of servers. Cloud computing enables the service recipients to pay only for what they actually used, in contrast to previously discussed hosting models based on subscription principle.

Secondly, the service provider may offer the service of server virtualization, which is cheaper than the hosting service, because what the service recipient gains is not access to a machine, but virtual access to server space. Server virtualization has also many varieties. As a rule the cheapest solution is the *shared hosting service*, where hundreds of service recipients gain virtual access to disc space on the same machine. Resources are sent via FTP service. In a more expensive variety of this service, the service recipient installs many virtual servers on a single machine – so-called virtual private server. In this variety, the client launches own version of the operating system and as a rule gains full control over the virtual private server, which – regardless of other virtual machines – has exclusive access to own disc space and all elements of the operating system.

The third, and the most expensive, solution is so-called server colocation, i.e. a service consisting in leasing physical space at the hosting provider's premises with a view to installing there a server owned by the service recipient. The service recipient manages own computers located at the service provider's premises on his own. The obligations of the service provider are limited in this case to provision of Internet access and uninterrupted power supply.[71]

---

[71] See: Wikipedia, >>http://en.wikipedia.org/wiki/Web_hosting_service<<, last accessed on: 2.1.2011.

In the Internet we will also find many offers of free hosting services. Such services are greatly limited, entailing the obligation to post service provider's ads on the page or the necessity to tolerate receiving unwanted e-mails (which makes one think whether in fact this does not make for a different type of service altogether). So-called free hosting services are also limited by space offered for storage of service recipient's files, the speed of available connections, lack of access to commercial, and frequently also non-commercial, databases and (often) lack of support for scripting languages,[72] which in practice enables storage of only very simple websites.

Another issue requiring a deeper analysis is the time of data storage. Experts are univocal in stating that the factor differentiating caching from hosting is the time of data storage, which is very short for the former service, and unlimited in time for the latter.[73] And this is just another mental shortcut. In the case of classic hosting of websites, the data hosting agreement will be virtually each time concluded for a definite time, as a rule for one year. Certainly in practice such contracts are extended for successive years, but hosting service cannot be said to be provided infinitely. The conviction of indefinite time duration of hosting agreements most likely follows from application of Article 14 of the act on the provision of services by electronic means to storage of users' data in the frames of Internet portals or storage of electronic mail on remote mail servers. However, this is a relatively controversial issue and it will be discussed further on in the paper.

Hosting refers first of all to a service consisting in storage and making available of websites, but one can speak as well of hosting with reference to other resources posted on the web, e.g. electronic mail or data made available under P2P file exchange networks. Under such models

---

[72] See: >>http://pl.wikipedia.org/wiki/Hosting<<, last accessed on: 2.1.2011.

[73] E.g. X. KONARSKI, *Komentarz…*, p. 139.

the recipient of hosting service will usually act also as the provider of other services provided by electronic means, e.g. as the operator of Internet pages.

### *6.1.1. Dedicated hosting versus virtual hosting*

Hosting service is used mainly to store websites on a remote server with a view to making them accessible for Internet users. Such type of hosting is usually provided against a charge and time-limited to one year (dedicated or classic hosting). One may also encounter provision of free access to a remote server in exchange for e.g. the obligation to post on the service recipient pages of the ads of the entity providing such type of service, something we have already addressed earlier in the paper.

When hosting Internet pages, the service recipient simultaneously acts as the information society service provider; the service consists in offering access to a specified website, e.g. an Internet store, auction portal, a social networking portal or a browser. Only in exceptional cases, when a website will not be even indirectly the source of economic circulation, the service recipient cannot be recognised simultaneously as an entity providing services by electronic means, due to failure to meet the conditions of providing the service against a charge.

It needs to be stressed again that in economic practice the essence of hosting consists not only in the storage but also in making Internet pages accessible to third parties. The service recipient may restrict the access for some categories of persons, or enable access to certain data to all users. However, the service provider must enable constant access to all files posted in a publicly accessible server folder to both the service recipient and the Internet users.

In a situation where the recipient of dedicated hosting service using the technical infrastructure of the provider of dedicated hosting service, provides a chargeable or free access to a part of the infrastructure for

his website users, we deal with an example of virtual hosting. By virtual hosting we shall understand a service consisting in provision of access for users of a given service to the technical infrastructure of the entity providing the dedicated (classic) hosting service. This is a kind of providing access to disc space and limited service functionality, e.g. to tools for comment creation and sending or to resources of a given user.

Besides websites, one should identify also electronic mail hosting. This consists in storage of postings of the users of service recipient's site and making them accessible only for a specific user, who needs to know the relevant password. However, he will be bound with the hosting service provider by contract similar to the one for the hosting of www pages. In a situation where the mailbox operator uses the technical infrastructure of the hosting service provider, he acts simultaneously as the electronic mail service provider and virtual hosting service provider. From the perspective of the user, the mail account operator will offer access to the postings and other files of the user in exchange for "tolerating" the ads of a given service provider and entities associated with him. In contrast to the hosting of Internet pages, this type of hosting as a rule is free and not time-limited. One may also encounter provision of such service against a charge, in exchange for e.g. a mail account with a greater capacity.

Finally, we need to mention the specifics of the hosting of files in P2P network. In practice hosting in the frames of file exchange networks means storage and providing access to data on the computers of the users, and not on the service provider's server. The service provider's server only stores and provides access to information about location of the searched files (and only in the most popular model of P2P networks, based on so-called indexing servers). Under that model we are dealing with an interesting reversal of roles, because the provider of file exchange services is simultaneously the provider of hosting service. On the other hand the provider of file exchange service will be simultaneously the

provider of hosting service consisting in the storage and provision of access to the information on locations of the searched files. One needs to point out here that in such systems one may speak of several providers of hosting service, because the exchanged files are stored on many computers. Due to its specifics, the file *hosting* in P2P networks is as a rule free and not time-limited.

### *6.1.2. Dispute concerning the objective scope of exemption from liability under Article 14*

The doctrine is rather univocal that the exemptions from liability for provider of hosting service covers both the stored data and the data made available. However, recently this view has been challenged. P. Sadowski deemed that "(…) the scope of exemption from liability under Article 14 of the Electronic Services Act covers exclusively data storage – this provision does not cover any other operations on the data concerned, such as for example making those data accessible in the Internet."[74]

The author justified his interpretation by the tenor of Article 14 of the Act, which – in his opinion – does not require any departure from literal linguistic interpretation. If the provision explicitly states that the provider of hosting service 'is not liable for the stored data', there is no need to depart from the *clara non sunt interpretanda* principle as it is clear that the exemption from liability concerns solely data storage, and not making them accessible. Moreover the author does not see any possibility of the above interpretation being challenged under Article 14 of directive 2000/31/EC, because also in this case Member States shall only ensure that 'service provider is not liable for the information stored at the request of a recipient of the service'.

---

[74] P. SADOWSKI, *Wyłączenie odpowiedzialności przy świadczeniu usług "hostingu" – polemika*, MOP 2009, No. 16.

Also the wording used by the law-maker 'the provider (…)' shall act '(…) expeditiously to remove or to disable access to the information' is not the basis for adoption of a broader interpretation, because: firstly, "there can be actual states when the data are only stored without being made available to anyone", and secondly, "in a typical model the data are stored by the service provider but made available to third parties by the service recipient."

The above interpretation is supported by literal understanding of the provisions of the act and of the directive. However, certain objections can be raised against such interpretation:

Firstly, such interpretation practically annihilates the exemption from liability for providers of both virtual and dedicated hosting services. As has been already detailed above, dedicated hosting consists not only in data storage but also in making them accessible and those two functions are hard to separate, because enabling data storage is not the goal in itself; the main goal is to make the data accessible to Internet users. The interpretation process has to take into account the fact that we deal with technical terms, which may be construed only in their "natural" context.

Secondly, such limitation of the understanding of Article 14 most likely would contradict the intention of both the European and national law-makers, because since the very start the issue at hand has been that of exclusion of liability of hosting service providers in full scope, and not just with regard to one function. Moreover, when interpreting Article 14 of the Electronic Services Act, one shall take into account the title of Article 14 of the said directive, which – as was already mentioned in the introduction – reads 'hosting'. This constitutes realisation of the obligation of pro-Community interpretation of national law, and as was indicated above, hosting assumes not only data storage but also making them accessible.

Thirdly, both the directive and the act contain an obligation to disable access to data when the service provider learns about illegal nature

of the stored information. This translates into impossibility to apply the *clara non sunt interpretanda* principle, because there is a clear feedback between data storage and making them accessible. Moreover, without making a functional interpretation it will be difficult to understand to whom the access to the stored data is to be disabled: to the recipient of hosting service or to all Internet users.

In view of the above, it needs to be deemed that exception from liability for a provider of hosting service in directive 2000/31/EC and in the act on the provision of services by electronic means covers both the storage and making the data accessible to Internet users.

### *6.1.3. Definition of hosting*

Basing on the analysis of sites offering this type of service, one may phrase the following working definition of:
"As a rule hosting is a service against a charge consisting in provision of access for a service recipient for a contractually limited time or for indefinite time to resources of service provider's ICT system with a view to storing, and making accessible for Internet users, the data stored there by the service recipient or by the users of his site."

In Polish law, the hosting contract belongs to the category of innominate contracts. The use of expression 'storage' urged some authors to consider the possibility to apply for the assessment of obligation of the parties to a hosting contract of the provisions of the civil code concerning a deposit agreement *per analogiam*. This is a quite obvious misunderstanding. A hosting contract is not about storage itself but about provision of access to the stored information.[75] This contradicts the possibility of application of Article 835 and the following ones of

[75] Similarly: J. BARTA, R. MARKIEWICZ, op. cit., p. 314. For legal nature of a hosting contract see: G. RĄCZKA, *Prawne zagadnienia hostingu*, PPH 2007, p. 379.

the civil code by analogy due to the fact that this provision obliges the entity storing the data to keep in a not worsened condition the movable entrusted to it for storage. In the case of hosting we do not deal with movable; additionally the data input by the service recipient may, and sometimes are, edited by the service provider.

Here one needs to differentiate between dedicated hosting and virtual hosting. In dedicated hosting, the service provider is the operator of computer infrastructure enabling the storage and provision of access to information, while the service recipient is the entity storing the information; as a rule this is a website operator, electronic mail operator, a P2P network operator. In virtual hosting, the service provider is usually the recipient of dedicated hosting service, while the recipient of virtual hosting service is a user of the service provider's site (i.e. a user of an Internet portal, auction service, electronic mail etc.).

## *6.2. Subjective scope of exemption from liability under Article 14*

As regards the definition of the subjective scope of exemptions, there are no doubts that protection under Article 14 covers the 'classic' providers of hosting service, e.g. NetArticlepl or Home.pl. However, certain doubts arise with regard to virtual hosting, understood not so much as provision of access to own computer infrastructure, but as granting the use of the ICT system of the primary hosting provider for site users. The issue that requires an analysis is an answer to the question what entities are covered with the exemption from liability under hosting service within the meaning of Article 14 of the act and directive. The differentiation between dedicated hosting and virtual hosting made above will be useful for this analysis.

### *6.2.1. Liability of service providers of dedicated hosting*

Under the classic model, hosting service is offered by data centres, i.e. entities specialising in maintenance of IT infrastructure 24/7 (dedicated hosting). There should be no doubt that exclusion of liability under Article 14 applies to such entities, because their business model is based on storage and provision of access to data of a great number of service providers (operators of www pages or operators of mailboxes). It can be hardly expected of the owners of such infrastructures to monitor the content uploaded to the sites of entities whose data they store, because as a rule they will not even have access to software or databases generating this content.

Hosting service so understood is rendered pursuant to a contract concluded for definite time, as a rule for a year with the option to be extended, in exchange for a pecuniary consideration, frequently paid for the whole year in advance. For many operators of websites the guarantee of the uninterrupted, and at the same time fast, accessibility of the stored files is the main reason to take interest in hosting against a charge. Moreover, to make their offer more attractive, providers of hosting services – besides disc space – give also access to systems enabling data archiving, transaction protection, database services, the possibility to collect and analyse statistics, operations on domains, electronic mail account management etc. Of course the scope of rendered services is proportionate to the amount of charges.

In practice, one can encounter a model where the operator of an Internet portal secures data hosting service for himself by using own IT infrastructure. Many, particularly smaller, but also very large entities do so, because theoretically the only requirement, besides a fast Internet connection and proper software, is the one to have an Internet-connected computer with a permanent IP address (although

even this requirement can be bypassed). However, a failure of own IT network will disable access to own website, so only very large entities can afford to maintain an expansive IT infrastructure. Moreover, in such case exclusion of liability for hosting does not apply, because the website operator and the hosting provider are the same entity, or entities under mutual control, which precludes application of exemption from liability under Article 14 paragraph 4 of the Electronic Services Act.[76]

There is no doubt that a service provider of dedicated hosting may invoke Article 14 paragraph 1 of the act on the provision of services by electronic means in relation to the data uploaded by the service recipient and by third persons using the service recipient's site. In other words, a service provider of dedicated hosting will not be liable not only for the data uploaded by a service recipient, but also for those uploaded by recipients of the services of his service recipient. As an example, a provider of dedicated hosting will not be liable not only for the data uploaded by operators of websites whose data he stores, but also for the information placed on those websites by their respective users. Taking into account the data coming from third persons does not result in a necessity to identify a new model; it suffices to establish a variety of the classic model presented above, where the data stored and made accessible come solely from the portal operator, acting in a double role of the recipient of hosting service and the provider of web page services.

[76] According to Article 14 para. 4 of the Act, The provisions of paragraphs 1–3 do not apply, if the service provider has taken control over the service recipient in the meaning of provisions of the Act on Competition and Consumer Protection. The editing of this exception gives rise to controversies, which will not be addressed in this paper. See e.g.: X. KONARSKI, *Komentarz…*, pp. 145–146. See: M. ŚWIERCZYŃSKI, *Ustawa…*, p. 134.

### *6.2.2. Liability of service providers of virtual hosting*

However there is a widespread belief in the literature that the notion of data storage under Article 14 of the Electronic Services Act and Directive 2000/31/EC applies in a situation where the operator of Internet pages (or one providing other information society services) enables to recipients of the services the storage of data in the frames of the site of such operator (virtual hosting). In practice this concerns e.g. storage of users' comments on auction services or blogs.

Adoption of such a broad interpretation of hosting is bound to lead to a situation where the user himself will be liable for illegal content published by such user. At the same time exemption from liability will extend to both the provider of IT infrastructure used for storage of and access to data (classic hosting), and the operator of a website enabling storage of and access to the data sent by site users. However, it needs to be stressed that the operator of a website will be exempted from liability only for the data sent by site users, and not for his own data. On the other hand, the provider of classic hosting will be exempted from liability in either case, provided the conditions defined in Article 14 of the act are fulfilled.

A literal interpretation of the discussed article may lead to a conclusion that protection under Article 14 covers also operators of Internet sites enabling storage of and access to data provided by site's users. Such interpretation may be supported by the tenor of Article 14 of the Electronic Services Act, which explicitly provides for a service consisting in making accessible resources of an ICT system with a view to storing data by the service recipient. Whenever such Internet site offers such functionality, then in this scope the operator of such site will appear in the role of a provider of hosting service. Moreover, big Internet sites largely depend on the data input by users, and not ones generated by

themselves, which makes the task of the monitoring of the input content similar to the problems arising in the case of classic hosting.

However, one may have serious doubts concerning the possibility to exempt from liability a provider of virtual hosting.

– Firstly, a classic hosting provider does not exercise any substantive control over the data input into a specific site by its users. He only ensures uninterrupted access to the data stored on all of the websites he hosts. On the other hand, the operator of a website enabling data transmission by users has access to all tolls enabling monitoring of the transmitted data.

– Secondly, adoption of a broader interpretation may lead to restriction of the principle of author's liability for the published content in the context of a landslide growth in the popularity of the creation of web pages on the basis of *open source* applications offering embedded discussion groups or blogs. We need to be aware of the fact that soon a decisive majority of websites will be based on extended tools enabling the storage of and access to content generated by users. However, this does not put at a disadvantage the administrators of "passive" sites, because – as has been already stressed before – adoption of a broader interpretation of the subjective scope will release from liability the administrators of second generations sites only with regard to content generated by users, and not the content published by the portal administrator.

– Thirdly, it becomes necessary then to provide an answer to the question whether the administrators of sites offering virtual hosting are also released from the obligation to monitor the content sent by users. Certainly Article 15 does not release them from the obligation to monitor "own" content, while systemic cohesion would command covering with this exemption website operators with regard to the obligation to monitor the content generated by users.

– Fourthly, as a rule the service of virtual hosting will be a free service in contrast to the classic hosting service. In practice there is no

business model where the operator of an Internet portal collects a fee for the possibility to store user's comments due to participation in discussion groups or posting comments. The situation is quite similar for storage of electronic mail, although in this case we encounter more frequently the subscription model, where upon payment of a fee the user may store e-mails on greater disc space than in the case of free electronic mail services.

– Fifthly, the differences can be found out as concerns the duration of data storage. In the case of virtual hosting, and hosting of electronic mail or hosting in the frames of P2P networks, as a rule this service will be time-unlimited. On the other hand, under classic hosting as a rule the data will stored for contractually defined time.

Currently it is difficult to tell which direction the judicial practice in Poland and in the European Union is going to take. There seems to be a widespread agreement in the doctrine that the subjective scope of Article 14 shall be interpreted broadly. On the other hand, in his most recent opinion in the case of *Google* the Advocate General Maduro suggested that service providers seeking to benefit from a liability exemption under Article 14 of the E-Commerce Directive should remain neutral as regards the information they carry or host.[77] In this context he refused to Google protection pursuant to Article 14 of the directive in the context of sponsored link service, considering that the operator of the biggest web browser is not neutral in generation of results under this service. In this context it is doubtful whether the operator of any website is truly neutral as regards the information provided by users.

---

[77] The opinion of the Advocate General in English is available at: >>http://curia.europa.eu/jurisp/ cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-236/08<<. Szerzej: P.P. POLAŃSKI, *Liability of Search engines for sponsored and natural results – the case of Google*, [in:] S. KIERKEGAARD, *Legal Discourse in Cyberlaw and Trade*, Malta 2009, pp. 273–285.

## *6.3. Grounds for exemption from liability for hosting*

### *6.3.1. Grounds for exemption from liability under US law*

Similarly to the case of mere conduit and caching, provisions of the directive are largely just a modification of Article 512 (c) of the *Digital Millennium Copyright Act*. According to the latter, hosting service is defined as the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider. It is worthwhile pointing out that in contrast to the directive on electronic commerce, DMCA does not use the term of hosting.[78]

DMCA lists three groups of conditions to be met cumulatively by a provider of hosting service to be eligible for exemption from liability for copyright infringements.

– Firstly, such service provider does not have actual knowledge that the material or an activity using the material on the system or network is infringing. The said knowledge is defined broadly and included also being aware of facts or circumstances from which infringing activity is apparent. Upon obtaining such knowledge or awareness, the intermediary shall act expeditiously to remove, or disable access to the material.[79]

---

[78] DMCA, Section 512(C): "Information Residing on Systems or Networks At Direction of Users. – (1) In general. – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider (…)".

[79] "(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; "(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or "(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to the material.

– Secondly, the intermediary does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.[80]

– Thirdly, upon notification of claimed infringement as described in a dedicated procedure defined in the DMCA, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[81]

### *6.3.2. Grounds for exemption from liability under the directive on electronic commerce*

According to Article 14 paragraph 1 of the directive titled 'Hosting': "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

According to Article 14 paragraph 2 of the directive, the exemption from liability shall not apply when the recipient of the service is acting under the authority or the control of the provider. Paragraph 3 of the

[80] "(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity."

[81] "(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."

said Article provides for the possibility for a court or administrative authority, in accordance with Member States legal systems, of requiring the service provider to terminate or prevent an infringement, and opens the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

When the two versions are compared, far-reaching similarities are visible. Both regulations exempt from liability entities that store information at the request of service recipients. In both cases the description of the 'protected' service is similar, being reduced to data storage. In both versions the service provider must not have knowledge neither of illegal material, nor of illegal activities connected with the material. Both under the DMCA and under the directive, the knowledge is interpreted very broadly and covers not only specific infringement cases, but also the general awareness of infringing nature of the pursued activities. And last but not least, under both instruments the service provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

However, there are also some significant differences. Firstly, just as was the case for other exemptions from liability – the European solution protects service providers against claims made not only under copyright law, but also other law fields. The provider of hosting service is exempted from both criminal and civil liability. Secondly, the European solutions differentiate between criminal and civil liability grounds. Proving awareness of circumstances indicating infringing activity suffices to impute civil liability; on the other hand imputation of criminal liability requires knowledge of a specific law infringement to be proven. To apply criminal sanctions it is necessary to prove that the service provider was aware of storing infringing content (e.g. protected musical works without consent of record labels), or consciously consented for infringing activity related to the stored material, which by itself may be non-infringing (e.g. storage of gambling sites in the countries which prohibit gambling). Thirdly,

to be exempted from liability for stored data under the DMCA, the intermediary is required to prove that he does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity. The directive does not contain such requirement. On the other hand, the European law-maker excludes the possibility to invoke the directive provision when the recipient of the service. i.e. the entity that stores data, is acting under the authority or the control of the provider. It is no easy to justify the differences in this regard. Probably it was the intention of the European law-maker to establish similar but more tersely worded safety havens compared to the DMCA. Perhaps the reasoning was that acting under control shall be always treated as an act of the service recipient, even if the service provider does not receive a financial benefit therefrom.

Attention shall be drawn, however, to certain danger pertaining to such wording of the exception from the rule of the exemption from liability for a provider of hosting service. As has been already demonstrated in the paper, 'in economic practice there are many functioning varieties of hosting service and a decisive majority of them provide for full or greater control of the stored material on the part of the service provider.' This – even if only theoretically – gives rise to risk of transferring liability onto hosting service provider, even if he has neither knowledge, nor awareness of the infringing activities of the service recipient. Therefore it will be extremely important to decide on an interpretation of the notion of control in the case-law of the Court of Justice. Unfortunately, neither the Advocate General in his opinion, nor the Court of Justice in its ruling in the case of *Google*, although both frequently referred to the condition of control in the context of hosting service, they did not indicate unambiguously how this notion shall be interpreted. Advocate Maduro excluded the possibility for the provider of AdWords service to invoke protection under Article 14 of the directive, owing to the direct pecuniary interest that Google has in Internet users clicking on the ads' links.

This direct interest seems to resemble the American requirement of not receiving a financial benefit, but the Court of Justice did not apply the 'neutrality test' in the version proposed by the Advocate General. It only stated that neither the chargeable nature of the referencing service, nor determination of the charging conditions by Google may be considered as exercise of control or proof of having knowledge about infringing material placed by advertisers in the sponsored links. This issue needs to be investigated further.[82]

### *6.3.3. Grounds for exemption from liability under Polish law*

According to Article 14 paragraph 1 of the act on the provision of services by electronic means "The responsibility for the stored data shall not be borne by the person, who, making the resources of an ICT system available for the purpose of the data storage by a service recipient, is not aware of unlawful nature of the data or the activity related to them, and in case of having been informed or having received a message on unlawful nature of the data or the activity related to them, makes immediately the access to the data impossible."

Under Polish law, a provider of hosting services will be exempted from both civil and criminal liability when no knowledge about illegally placed material can be imputed to him (e.g. pornographic photos with participation of minors) or about related activities (e.g. information of where such photos can be found) on his server.[83] In case when he

[82] See section 6.3 below.

[83] The directive on electronic commerce enabled also exemption from civil liability when the service provider does not know the actual state or circumstances which obviously point to infringing nature of material or activities related thereto. See: A.R. LODDER, [in:] A.R. LODDER, H.W.K. KASPERSEN, *eDirectives: Guide to European Union Law on E-commerce. Commentary on the Directives on Distance Selling*, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, Hague 2002, pp. 88–89.

obtains such knowledge, either via an official notification, or is acquiring other "reliable information", his liability is renewed and he can be granted effective protection only if he disables access to the data whose legality was challenged.

Polish implementation goes slightly beyond the model contained in the directive on electronic commerce and excludes also liability of a service provider towards a service recipient on account of disabling access to the stored material. Moreover, only when the service provider learns about infringing material by obtaining reliable information, he will have to inform the service recipient about the fact of disabling the access to data. If he receives the information about infringing material in an official notification (for example a court decision) he is not even obliged to inform the service recipient about the undertaken actions.

## *6.4. Significance of the judgement in the case of Google*[84]

With a view to enhancing the analysis of exemption from liability for hosting, it will be extremely important to quote yet again the judgement of the Court of Justice in the case of Google. The only issue addressed by *Cour de Cassation* in the conclusions was the question concerning the possibility for Google to invoke exemption from liability for data storage under Article 14 paragraph 1 of the directive on electronic commerce. The said question can be recapitulated as follows: may a browser operator be deemed as a provider of information society services consisting in storage of information within the meaning of Directive 2000/31/EC? Extension of the scope of application of Article 14 of the directive to the issue of liability of entities offering browsing services would yield an effect whereby the liability of the provider of the referencing service

[84] This section is a modified version of a fragment of the article: I. KOWALCZUK, P. POLAŃSKI, *Prawne aspekty reklamy w Internecie z wykorzystaniem usługi linków sponsorowanych*, Monitor Prawniczy 2011, No. 1, pp. 30–32.

would arise only at the moment when he is informed about illegal nature of the advertiser's actions, and only provided that he fails to expediently disable the access to the challenged material.

In order to answer this question, the Court investigated first whether the *AdWords* services provided by the operator are information society services in the light of the directive on electronic commerce, and then it considered whether this service consists in information storage. After the analysis of the directive provisions, the Court decided that Google *AdWords* features all of the elements of the definition of an information society service provider.[85] The above statement is accordant with the purpose of the directive on electronic commerce, with the opinion of the Advocate General, and with the position of the Commission, and as such it does not require any broader comment.

Initially the Court pointed out that, basing on the literal tenor of the provisions, a provider of chargeable referencing service (e.g. Google) can be recognised as an entity providing information society services consisting in storage of information supplied by the user of this service (advertiser) in the light of Article 14 of Directive 2000/31/EC, because he "holds in memory on its server, certain data, such as the keywords selected by the advertiser, the advertising link and the accompanying commercial message, as well as the address of the advertiser's site."[86] Thus the Court suggested that the notion of hosting may also cover the services whereby the service provider offers only virtual space to the users of his web service (so-called virtual hosting)'.[87] Under such interpretation, a provider of hosting service would be also an entity enabling submission of remarks

[85] Section 110 of the judgement in combined cases *Google*. The Court's argumentation was supplemented by presentation and investigation of the legislative history by the Advocate in his opinion, section 138.

[86] Section 111 of the judgment in combined case *Google*.

[87] The differentiation between the terms of dedicated hosting and virtual hosting was introduced above.

on the site in the frames of so-called blog, because then he would store information at the request of the service recipient.

On the other hand, however, the Court pointed out that the goal of Article 14 and of the entire section 4 of the directive on electronic commerce was to protect only intermediaries in information transmission. Consequently, a service provider being an intermediary needs to have neither knowledge of nor control over the information which is transmitted or stored and his activity shall be "(…) of a mere technical, automatic and passive nature."[88] The Court inferred those requirements from literal wording of Recital 42 of Directive 2000/31/EC.[89] Application of those requirements to assessment of the services of AdWords type service was left by the Court of Justice up to the decision of the national court,[90] which – as demonstrated by relevant case-law – had many problems with this issue and as a result hardly added anything of value to the judgment of the Court of Justice.[91]

Therefore "the Court avoided giving an unequivocal answer to the question whether AdWords service benefits from protection guaranteed under Article 14 of the directive". Firstly, it is not clear whether Google as a provider of sponsored links service acts in the capacity of an intermediary within the meaning of the directive on electronic commerce. According to – already quoted on many occasions – Recital 42 of the

---

[88] Sections 113 and 114 *in fine* of the judgment in the case of *Google*. For a broader discussion on the topic see: P. POLAŃSKI, *Technical, automatic and passive: liability of search engines for hosting infringing content in the light of the Google ruling*, Private Law: Rights, Duties & Conflicts, (ed. S. KIERKEGAARD), ISBN: 978-87-991385-8-6, Barcelona 2010, pp. 399–409.

[89] For the sake of comparison, see the analysis of Recital 42 of Directive 2000/31/EC with regard to services of mere conduit, caching and hosting above.

[90] Section 119 of the judgement in combined case *Google*.

[91] See the following judgements: Cour de cassation, civile, Chambre commerciale, 13 juillet 2010, 08-13.944, Publié au bulletin; Cour de cassation, civile, Chambre commerciale, 13 juillet 2010, 06-20.230, Publié au bulletin; Cour de cassation, civile, Chambre commerciale, 13 juillet 2010, 06-15.136, Publié au bulletin.

directive on electronic commerce, "the exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; (…)." Is a service of *AdWords* type limited to technical process of support aimed solely to making the transmission more efficient?

One may argue that in contrast to services of classic intermediaries in Internet transmission (mere conduit, caching, and dedicated hosting) or activities of classic website browsers offering so-called natural search services, the activities of sponsored link search engine services may be required to transmit or make accessible information in the Internet. What is more, it is not clear whether this service is only of technical, automatic and passive nature. Although most likely the process of automation is very well developed in the seat of the American giant, it must be borne in mind that it is simultaneously supported with work of an army of people.

Secondly, we do not know also whether Google "has knowledge" or "has control" over support for sponsored links. The Court of Justice of the European Union phrased several recommendations for the national court to be taken into account when resolving this issue. Among other things, it pointed out that advertisements in the frames of AdWords service are displayed "under conditions which Google controls", e.g. by determining the order of display according to, inter alia, the remuneration paid by the advertisers.[92] The fact of collection of remuneration from advertisers might suggest – which the Advocate General did in his opinion – that Google "has control" over the stored information, and hence that it is not eligible for protection under the analysed article. However,

[92] Section 115 of the judgement in the case of *Google*.

as was pointed out by the Court, neither the mere fact that the referencing service is subject to payment, nor the fact that Google sets the payment terms cannot be construed as proof that Google has control or has knowledge about infringing material input by advertisers.[93] Hence the Court did not accept the principle of technological neutrality worded by Advocate Maduro, who saw a ground to refuse to Google limitation of liability under Article 14 of the directive on electronic commerce in the fact that Google made money on positioning of ads infringing the trademark law.

On the other hand, the Court stated that "(…) concordance between the keyword selected and the search term entered by an Internet user is not sufficient of itself to justify the view that Google has knowledge of, or control over, the data entered into its system by advertisers and stored in memory on its server."[94] One can only add that concordance between the keyword corresponding to a trademark and the search term entered by an Internet user is much less important than Google's ability to establish the connections between the advertised word or words and a trademark. In view of lack of databases offering access to all trademarks in the EU with breakdown into countries, the probability of checking such dependence seems virtually unlikely.

The Court attached great stress to the necessity for the national court to examine the role played by Google in the drafting of the commercial message, including in particular the establishment or selection of keywords.[95] It seems that by stating so, the Court recommended that the national courts shall analyse – from the viewpoint of neutrality – the tools suggesting the keywords selected by advertisers being imitations or copies of somebody else's trademarks, and the process of ads' making

[93] Section 116 of the judgement in the case of *Google*.

[94] Section 117 of the judgement in the case of *Google*.

[95] Section 118 of the judgment in the case *Google*.

and presenting. When construing the neutrality of Google's behaviours, it will be helpful to refer to the opinion of the Advocate Maduro, who pointed out that this service is not a purely technical activity, so it cannot be recognized as hosting service.[96]

The Court's answer is balanced, correct, but fails to answer the asked question unequivocally. It is beyond any doubt that the service of sponsored links is an information society service in the light of the directive on electronic commerce. More controversial is the level of clarity of the Court's answer to the second, much more important question. On the one hand, the Court seems to adopt a broader interpretation of the subjective scope of Article 14 of the directive, while on the other it requires a proof that Google is a technologically neutral intermediary in information transmission, who – due to exercise of this role – neither controls the stored data, nor knows about infringements. Therefore it is not known whether entities offering search services against remuneration may indeed invoke protection under Article 14 of the directive. We may only hope that the case of *Interflora Inc. v Marks & Spencer* (C-323/09) will detail the conditions under which – if at all – the entities providing referencing services against remuneration may be exempted from liability for the stored data.

## *7. Liability of providers of information location tools*

The American law regulates the liability the providers of information locations tools similarly to the liability of the providers of hosting services. According to the DMCA, a provider referring or linking users

[96] Section 130 of the opinion in the case *Google*.

to an online location is a provider of information location tools, including a directory, index, reference, pointer, or hypertext link.

A service provider shall be exempted from liability for linking or referring to infringing material or activity if he does not have actual knowledge that the material or activity is infringing.[97] To be exempted from liability he may not be aware, either, of the fact or circumstances from which copyright infringement activity is apparent – which was exactly why providers of search tools within P2P networks were unable to take advantage of this 'safe haven'. Similarly to the case of hosting, the other condition to exclude liability under US law is that the service provider does not receive a financial benefit directly attributable to the infringing activity, in a case where the service provider has the right and ability to control such activity. And finally, upon notification of claimed infringement of the content the provider links to, he shall respond expeditiously to remove, or disable access to, the material that is claimed to be infringing, which means that link to such material is to be removed either from the index of the search engine or from the content of the website.

In contrast to American solutions, the European law-maker decided against introducing a dedicated exemption from liability for providers of referencing services. However, it turned out fast that when liability rules are not clearly defined for such entities, certainty of turnover in electronic commerce suffers. An excellent example is afforded by the previously discussed judgement of the Court of Justice in the case of *Google*, which failed to provide a clear answer to the question whether the provider of AdWords service may invoke Article 14 of the directive

[97] "(d) Information Location Tools. – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or referencing users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if (…)".

on electronic commerce to avoid liability of industrial property law infringements. We will address below other problems arising in connection with the so-called natural search services.

Owing to the fact that the questions asked by *Cour de Cassation* concerned only *AdWords* service, the Court did not address the issue of the legal status of natural search in view of the directive.[98] However, Advocate General Maduro considered this issue in his opinion. He stated that Google's liability for provision of this service shall be excluded because it is neutral as regards the information it carries.[99] Although, admittedly, Google has an interest – even a pecuniary interest – in displaying the more relevant sites to the internet user; however, it does not have an interest in bringing any specific site to the internet user's attention.[100] However, a question arises as to application of the legal ground for exemption from liability for Google. The Advocate General for Google provided an ambiguous answer to this question. He phrased three theses: (1) Google does not provide hosting services, (2) Google service may be qualified as one covered with limitation of liability under Article 13 of the directive (caching), (3) Articles 12–14 may be applied by way of analogy. Due to the volume constraints of this paper, the above statement is presented in brief, because a broader discussion of the topic would require a separate paper.

---

[98] See: P.P. POLAŃSKI, *Liability of search engines for sponsored and natural results – the case of Google*, (ed. S. KIERKEGAARD), *Legal Discourse in Cyberlaw and Trade*, Malta 2009, p. 273 and the following.

[99] Section 144 of the opinion in the case of *Google*.

[100] The Advocate's opinion might have been influenced by the UK judgement in the case of *Metropolita International Ltd v Designtechnica Corporation and Others*, where Google was pronounced a service provider of mere conduit, and not a publisher in the light of common law. Therefore Google is not liable for defamatory content placed on websites. Quoted after: P.P. POLAŃSKI, *Liability of Search engines for sponsored and natural results – the case of Google*, (ed. S. KIERKEGAARD), *Legal Discourse in Cyberlaw and Trade*, Malta 2009, p. 281.

According to the Advocate General, justification of the extension of protection under Article 14 of the directive onto natural search services would be difficult owing to the fact that Google does not store information upon users' request. However, if users are understood as website administrators instead of search engine users, then one might argue that Google does store information. This is so, among others, because one of the tools proposed by Google provides the possibility for administrators to add the just created pages to the Google index. Hence in such case protection might be applied solely on the account of information storage.[101]

Another interesting proposal of the Advocate General was an attempt to apply Article 13 of the directive to search services. This Article limits the liability of caching providers for "(…) automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request." The Article was intended to protect the intermediaries who temporarily store users' information, but it will be difficult to apply the grounds for exemption from liability under Article 13 to search operators. For example, to be eligible for exemption, a provider of caching services may not modify the transmitted information, while web search engines index websites and modify the data presented in search result lists.

In recapitulation, the Advocate General came to a conclusion that operators of Internet search engines deserve to be protected under Directive 2000/31/EC,[102] however he failed to point out a specific ground for exemption of liability of this type of entities for services of so-called natural search. What is more, as a result of application of the "neutrality test" proposed in his opinion to Google, he deemed that neither

[101] *Ibid.*, pp. 281–283.

[102] For a broader discussion see: *Ibid.*, p. 284.

neutral search services nor services of AdWords type are covered with application of Article 14. Taking into account the fact that the Court of Justice did not address the issue of the liability of search engine services in an unequivocal manner, and also considering that the neutrality test in the form promoted by P. Maduro was rejected by the Court,[103] one has to postulate adoption of clear rules governing the liability of information location tools. This is all the more important as virtually every bigger content provider offers information location tools, which frequently search not only through own resources of the service provider, but also the entire World Wide Web.

## *8. Procedure for disabling access to infringing material*

According to Recital 40 of the directive on electronic commerce, "(…) service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by

[103] See:. P.P. POLANSKI, (2010) *Technical, automatic and passive: liability of search engines for hosting infringing content in the light of the Google ruling*, [in:] S.M. KIERKEGAARD (ed.), Private Law: Rights, Duties & Conflicts, Barcelona: IAITL, pp. 399–409.

the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC."

As has been stressed on many occasions, the European Union has neither introduced nor developed so far the procedures for disabling access to content modelled on American solutions. However, such procedure is admitted under the directive on electronic commerce, with some member states, such as Finland, introducing their own versions of the procedures for disabling access to content. At the EU level, efforts to develop such procedure have failed so far, although works are under way on an analysis of answers collected during public consultations on the future of the directive on electronic commerce,[104] which may prove useful in the creation of a relevant content access disabling procedure in the future. Besides the *Notice-and-Takedown* model adopted in DMCA, alternative models are considered, such as *Notice-and-Stay* or *Stay-and-Stay*. Under the *Notice-and-Stay*[105] model, the challenged content would be taken down and it could not be reposted upon request of the person who posted it. On the other hand, under *Stay-and-Stay*[106] model the ISP must inform the person who uploaded content violating the law about the fact of disabling of the content. To a certain extent the latter model was introduced by Poland in the act on the provision of services by electronic means.

---

[104] Public consultations on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC), available at: >>http://ec.europa.eu/yourvoice/ ipm/forms/dispatch?form=electroniccommerce&lang=fr<<, last accessed on: 3.1.2011.

[105] According to the explanation contained in the questionnaire accessible above, the model was described as follows: "Regime of notification, take down and making sure that the content will not be reposted".

[106] *Ibidem*, "Regime in which ISP must on request inform the person who uploaded content violating the law".

## *9. Summary*

The recent decade of the functioning of the directive on electronic commerce with regard to the issue of the liability of intermediaries has demonstrated that the model generally works. However, this assertion needs to be qualified as regards five issues; ones requiring, in my opinion, an intervention of the European law-makers.

– Firstly, the notion of hosting under Article 14 of the directive on electronic commerce needs to be phrased more precisely. It would good to point out that the service consists not only in information storage, but also in making it accessible. It seems also important to detail the 'neutrality test' proposed in the judgement in the case of *Google*, including in particular a definition of the notion of "control over the recipient of the service" and the issue of receiving financial benefits from law infringement. It should be also clearly defined whether, and if yes, to what extent, exemption from liability under Article 14 of the directive may be applied to service providers of virtual hosting, whereby user-generated content is stored on Web 2.0 sites. Perhaps we should establish a special exemption from liability for entities offering Web 2.0 services.

– Secondly, it seems necessary to introduce the procedure for disabling infringing content at the Community level. For example, owing to fuzzy phrasing, many disputes are raised by the interpretation of the term of 'expedient' disabling of access to infringing content. Lack of precise definition of the procedures for disabling access to content already today results in restriction of the freedom of expression in the European Union, because content providers as a rule disable access to any content indicated by another user as potentially infringing the relevant law. The model adopted in the DMCA and introduced in such countries as e.g. Finland, should be the starting point. However, an in-depth analysis

is required also to consider alternative models, such as *Notice-and-Stay* or *Stay-and-Stay*.

– Thirdly, the recent disputes surrounding the use of search engine services demonstrate that it is necessary to introduce conditions for exemption from liability of the providers of such services. The opinion of the Advocate General P. Maduro and the judgement of the Court of Justice in the case of *Google* sought protection for providers of those technologies in the directive on electronic services, but with hardly any success. Exemption from liability is necessary not only to ensure greater legal certainty to global leaders, such as Google, but also to all providers of information society services, who provide access to information location tools on their websites.

– Fourthly, maintenance of the absence of a general obligation to monitor content needs to be defined precisely in view of widespread development of children pornography and other law infringements. It seems particularly necessary to identify the cases where service providers have to pursue the obligation of active content monitoring. This is where the issue of applying Article 14 to Internet sites offering to the users the facility to post their own content, comes again into play.

– Fifthly, it is advisable to define a clearer border between the area of interaction of permissible public use in the directive on the harmonization of copyright and exemptions from liability in the directive on electronic commerce. The issue at hand concerns first and foremost a clear stance on whether service providers of caching are covered with the scope of application of Article 5 of the copyright directive or – alternately – whether this regulation with regard to intermediaries in provision of access to information concerns solely service providers of mere conduit. ■

## *About the Author*

Przemysław Polański, Ph.D. Educational background in law and information technology; a graduate of the Adam Mickiewicz University in Poznań and of the Monash University of Australia. A Ph.D. degree at the Melbourne University of Australia; published a book "Customary law of the Internet" distributed by Cambridge University Press. The author of over 70 research papers dedicated to new technology law. Currently the Director of Electronic Product Strategy at C.H. Beck publishing house and a research associate at the Department of Quantitative Methods & Information Technology at the Kozminski University; a lecturer at the Warsaw University.