

## Jak należy uregulować odpowiedzialność za treść w Internecie? Wybrane aspekty

Choć już w temacie opracowania pojawia się pytanie sugerujące, iż w tekście można znaleźć na nie odpowiedź, sprawa nie jest tak prosta. Opracowanie to stanowi zaledwie zachętę do podjęcia takiej próby, stara się jednak przy tym przedłożyć dobre budulce. Dlaczego? Otóż, jakkolwiek opracowanie nie jest ani nazbyt nowatorskie, ani specjalnie odkrywczе (przynajmniej dla specjalistów z tej dziedziny; dodajmy też: nie taki był tego cel), to jednak stara się przedstawić problem nieco inaczej, w tym bardziej kompleksowo, niż robiono to do tej pory.

Przede wszystkim – nie mamy tutaj do czynienia z kolejnym tekstem typu: „zaczęło się dawno temu w Ameryce, a potem były orzeczenia we Francji, a potem w Wielkiej Brytanii, a jeszcze tak podchodzono do tematu gdzieś tam”. Innymi słowy, zamiast dokonywać przeglądu ustawodawstw różnych krajów i przywoływać różnorodne orzeczenia z różnych porządków prawnych, skupiliśmy się bardzo mocno na próbie interpretacji wyłącznie polskich przepisów oraz ich europejskich odpowiedników (czy raczej na odwrót). Nie znaczy to oczywiście, że brak jest odesłań do innych krajów. Takie zachowanie pozwoliłoby nam na napisanie maksymalnie trzech stron tekstu (zwłaszcza z uwagi na brak polskich orzeczeń w tego typu sprawach). Staramy się jednak, by odwołania do innych ustawodawstw, orzeczeń, poglądów doktryny itd. odbywało się nie na poziomie ogólnym, ale na poziomie poszczególnych haseł, szczegółowych problemów. Wierzmy bowiem, że tylko dzięki takiej metodzie uda się udzielić odpowiedzi na pytania takie, jak:

1. Czy hosting to przechowywanie, czy także udostępnianie treści, a więc – czy wyłączenia odpowiedzialności pośredników znajdują zastosowanie do współczesnych form świadczenia usług w sieci, takich jak np. Web 2.0 czy portale społecznościowe?
2. Jak należy interpretować wiarygodną wiadomość mającą zasadnicze znaczenie dla oceny działań pośrednika, który chce skorzystać z możliwości uniknięcia (ograniczenia) odpowiedzialności?
3. Czy należy tworzyć nowe kategorie podmiotów/czynności wchodzących w zakres opisywanej regulacji (np. *search engines*, *hiperlinking*), czy też niesie to jakieś zagrożenia?

Niezależnie od powyższego opracowanie duży nacisk kładzie też na dwie sfery, które – jak wspomnieliśmy – z pewnością nie są nowatorskie i odkrywczе, ale jednak są konsekwentnie pomijane przy tego typu rozważaniach albo wręcz które – przynajmniej w polskiej debacie prawniczej – nie istnieją lub prawie nie istnieją.

Pierwsza z kategorii spraw opisanych w poprzednim akapicie dotyczy głównie odwołania się do kwestii praw podstawowych. Niby jest to rzecz oczywista, nawet niektóre orzeczenia europejskich trybunałów coś wspominają o wolności słowa, ale wydaje się, że stanowi to listek figowy mający przykryć wstydlivość władzy (ustawodawczej i sądowniczej) przed oparciem się na własnych fundamentach. Wbrew tym praktykom i – powiedzmy – mimo wszystko staramy się, na ile pozwalają na to możliwości tego krótkiego opracowania, głośno przypomnieć, że istnieją takie prawa, jak wolność słowa czy prawo do sądu, i muszą one nieco „bardziej dociskać wagę”, porównującą dziś nieco bezrefleksyjnie i automatycznie różne sprzeczne interesy i prawa.

Wreszcie, prawie na sam koniec, w pracy znajdziemy krótki rozdział poświęcony alternatywnym próbom rozwiązania drażliwej kwestii regulacji odpowiedzialności pośredników. Rozdział o tyle ciekawy, że niektóre z pomysłów (w tym nie tylko akademickie, ale funkcjonujące w praktyce!), chyba po raz pierwszy w ogóle zostały przedstawione w szerszym dyskursie na gruncie polskiej publicystyki, w tym publicystyki prawniczej.

## 1. Wprowadzenie

Nie ma masowego wykorzystania Internetu bez pośredników. To może nieco uproszczone stwierdzenie, ale dość dobrze oddające specyfikę aktualnego stanu rzeczy. Szybki rozwój tego medium stał się możliwy dzięki usługodawcom umożliwiającym podłączenie się do globalnej sieci, przesyłanie informacji czy też ich przechowywanie<sup>1</sup>. Szybki, bo dokonywany bezpośrednio przez użytkowników. Nie jest jednak żadnym odkryciem, że prócz korzyści, jakie to rozwiązanie niesie, Internet może też przynosić straty. Tak materialne, jak i czysto osobiste.

Odkąd jednak Internet stał się dostępny dla praktycznie każdego, pojawiły się kłopoty ze skutecznym określeniem sposobów dochodzenia odpowiedzialności za treści, które – zdaniem zgłaszających zastrzeżenia – udostępniono z naruszeniem cudzych praw autorskich lub których treść naruszała inne prawnie chronione dobra i interesy. Z jednej strony oczywiste jest, że odpowiedzialność za takie naruszenie powinien ponosić bezpośredni sprawca, który treść tę udostępnił. Jak jednak postępować, gdy treść ta jest dostępna za pomocą środków technicznych należących do pośredniczącego w jej rozpowszechnianiu usługodawcy? Czy w takim przypadku pośrednik powinien ponosić odpowiedzialność, czy nie?

Obecnie istniejące systemy prawne, ale także zbudowane na nich interpretacje doktryny i orzecznictwa nie udzielają na powyższe pytanie jednoznacznej odpowiedzi. Z jednej bowiem strony dość powszechnie w wielu ustawodawstwach dopuszczalne są różne formy odpowiedzialności pośredniej (np. za pomocnictwo), które – przynajmniej teoretycznie – mogły stanowić podstawę odpowiedzialności pośredników dostarczających usługi elektroniczne. Z drugiej zaś – dąży się do wprowadzenia różnego rodzaju szczególnych procedur, które w zamierzeniu mają bądź to zapewnić poszkodowanym lepszą ochronę (np. poprzez zmuszenie usługodawców do szybkiego usuwania bezprawnych treści), bądź to usługodawcom szczególne immunitety (zabezpieczające ich przed np. uznaniem za pomocników w popełnieniu czynu zabronionego). Względnie – najlepiej do osiągnięcia obu celów jednocześnie, a przy tym przy poszanowaniu praw podstawowych.

Efekty tych działań są jednak częstokroć odwrotne do zamierzonych. Prawa podstawowe zdają się bowiem schodzić na dalszy plan, a pierwotne zamierzenie wprowadzenia barier ochronnych dla pośredników skutkują w praktyce tym, że niespełnienie wymagań dodatkowego immunitetu nie jest przesłanką do badania odpowiedzialności na zasadach ogólnych, ale przesłanką odpowiedzialności jako takiej.

Taki stan rzeczy może budzić poważne wątpliwości i daje asumpt do podjęcia próby dokonania możliwie szerokiej analizy funkcjonujących rozwiązań.

---

<sup>1</sup> Zob. raport OECD: *The Role of Internet Intermediaries in Advancing Public Policy Objectives. Forging Partnerships for Advancing Policy Objectives for the Internet Economy*, Paryż, 2010, <http://www.oecd.org/dataoecd/18/44/46013181.pdf>.

## 2. Grupy interesów

Wprowadzenie do opracowania ujawniło nam dwie podstawowe grupy zainteresowane prawidłowym uregulowaniem odpowiedzialności za treści w Internecie: a więc przede wszystkim ISP (pośredników/usługodawców) oraz *content providers* (dostawców treści / użytkowników). Z drugiej strony mamy podmioty, które tej odpowiedzialności poszukują. Są to głównie osoby, których dobra osobiste zostały naruszone, ale też uprawnieni z tytułu praw autorskich czy praw własności przemysłowej. Niejako między nimi można ułokować szeroko pojętych wydawców prasy, którzy sami mogą pozywać, ale często też i są pozywani w procesach sądowych (albo inaczej: sami mogą być pośrednikami i jednocześnie dostawcami treści). Prócz tego istotną zainteresowaną grupę stanowią różnorakie serwisy Web 2.0, portale społecznościowe, usługodawcy świadczący usługi typu *cloud computing*<sup>2</sup>, których pozycja nie jest do końca jasna. Warto jednak pamiętać, że nie tylko krąg wydawców prasy może kwalifikować się do różnych ról. Praktycznie każdy uczestnik rynku usług społeczeństwa informacyjnego może zostać zakwalifikowany do więcej niż jednej grupy. Nie można więc dokonać jednoznacznego, wyczerpującego, a przede wszystkim w pełni wyodrębniającego podziału grup/podmiotów zainteresowanych przedmiotową problematyką.

Co więcej, wydaje się także, że w tej sferze mieszczą się też instytucje państwowe, które z jednej strony bardzo często są dostawcą treści, z drugiej – działają jako pośrednicy. W ich jednak przypadku pojawia się tutaj dodatkowa, ale nieodłączna rola regulatora, która czasem może prowadzić do uzurpowania sobie wręcz nienależnej i całkowicie nadrzędnej roli (por *casus* propozycji poddania nadzorowi Krajowej Rady Radiofonii i Telewizji tzw. nielinearnych usług audiowizualnych świadczonych przez Internet)<sup>3</sup>.

Można spróbować założyć, iż pewne podmioty – mimo możliwości zaliczenia ich do kilku grup – mają w pewnym zakresie wyraźnie odmienne cele. Tak na przykład nie powinno zasadniczo ulegać wątpliwości, że uprawnieni z tytułu praw autorskich będą dążyli do możliwie najszerzego obciążania usługodawców odpowiedzialnością za treści (materiały) dostarczane przez usługobiorców, podczas gdy zarządzający np. portalami społecznościowymi (mimo że sami korzystają i chronią swoje prawa własności intelektualnej) mają zgoła odmienne cele.

Tak czy inaczej, dla pewnego jednak – minimalnego choćby – zobrazowania podmiotów objętych problematyką dokumentu można powiedzieć, że grupy interesów (przyjęte na potrzeby niniejszego opracowania) prezentują się następująco:

- 1) pośrednicy/ISP,
- 2) portale społecznościowe/podobne,
- 3) wydawcy/prasa,
- 4) uprawnieni z tytułu praw autorskich / własności przemysłowej / IP,
- 5) konsumenci/usługobiorcy (użytkownicy),
- 6) organy państwa / organy administracji państwowej.

## 3. Problem badawczy

Jeśli wychodzimy z założenia (raczej niekwestionowanego, a wyrażonego we wprowadzeniu do dokumentu), że Internet zawdzięcza swój rozwój pośrednikom, oznacza to, że zmiana zasad funkcjonowania tychże pośredników (zmiana wynikająca z niekorzystnego dla nich stanowienia

---

<sup>2</sup> Zauważmy przy tym, że o ile odnośnie Web 2.0 czy portali społecznościowych powstają istotne problemy z zakwalifikowaniem ich do tzw. host providerów, o tyle w przypadku cloud computingu większym problemem może być kwestia właściwej jurysdykcji, co jednak zasadniczo pozostaje poza zakresem rozważań opracowania.

<sup>3</sup> <http://www.rp.pl/artukul/600415.html>

i stosowania prawa) będzie skutkowała zmianą Internetu. Nie znaczy to wszakże, że Internet przestanie istnieć. Najprawdopodobniej nie będzie mógł jednak funkcjonować w kształcie, w jakim go znamy. To z kolei rodzi pytania natury prawnej.

Niniejszy dokument musi więc zanalizować tak istniejący stan prawny, jak i tendencje jego zmian, uwzględniając przy tym techniczne aspekty funkcjonowania sieci. Całościowa analiza winna wyjaśnić, czy obowiązujące prawo oraz jego dokonane i planowane zmiany są właściwym rozwiązaniem, uwzględniającym zasady ochrony praw podstawowych, a jednocześnie pozwalającym na korzystny rozwój Internetu, czy też należy dokonać mniej lub bardziej radykalnych transformacji, np. w kierunku pełniejszego wyłączenia odpowiedzialności pośredników, czy przeciwnie – w celu obciążenia ich dodatkowymi obowiązkami.

#### 4. Kluczowe pytania

Aby odpowiedzieć na tak postawione pytanie, należy wyjaśnić, kilka kwestii szczegółowych, z których najważniejsze dotyczą:

- 1) oceny funkcjonowania (skuteczności) obecnych rozwiązań, pod kątem zarówno ISP, jak i tych podmiotów, których prawa są naruszane;
- 2) wskazania podstawowych problemów interpretacyjnych uregulowań prawnych;
- 3) wskazania podstawowych praw i wolności, które mogą być naruszane przy takim czy innym rozwiązaniu przyjętym w systemie prawnym;
- 4) zaprezentowania alternatywnych rozwiązań, które istnieją w innych niż polskie/europejskie systemach prawnych bądź które są zgłaszane przez poszczególne grupy interesów.

Jednocześnie w tym miejscu należy wyjaśnić, że zasadnicza część rozważań opracowania dotyczy wyłącznie odpowiedzialności usługodawców przechowujących dane, przy praktycznie całkowitym pominięciu *access providers*. Wynika to z faktu, że zasady odpowiedzialności tych ostatnich, tak w zakresie zwykłego przesyłu (*mere conduit*), jak i *cachingu* nie budzą teoretycznie większych wątpliwości i nie podnosi się w tym zakresie poważniejszych zastrzeżeń<sup>4</sup>. Niewykluczone jednak, że w przyszłości także ten obszar będzie wymagał głębszego rozeznania, z uwagi na coraz większe i częstsze ingerencje *access providers* w treść informacji przesyłanych przez usługobiorców, wywołane – jednocześnie – przez rozwój technologii to umożliwiający oraz mniej lub bardziej sformalizowane próby nakłonienia do tego tychże usługodawców.

#### 5. Metodologia

Dokument ma mieć charakter prawniczy, co oznacza, że jego trzon będą stanowiły interpretacje i rekonstrukcja norm, obowiązujących przede wszystkim na terenie RP oraz UE. Aby jednak opracowanie to miało jak najbardziej praktyczny i pomocniczy charakter, wiele argumentów będzie się odwoływało do badań i opracowań – własnych oraz przygotowanych przez osoby trzecie, w tym także dysponentów praw autorskich, organizacje pozarządowe, jak i wykonanych na zlecenie rządów czy organizacji międzynarodowych.

---

<sup>4</sup> V. Thibault, G. Spindler, G. M. Riccio, A. Van der Perre, *Study on the Liability of Internet Intermediaries*, listopad 2007.

## 6. Analiza

### 6.1. Definicje

Czytając poniższe definicje, należy mieć na uwadze, iż mają one stanowić wyłącznie pewną wskazówkę i wstępną (ogólną) pomoc podczas lektury dalszych rozdziałów opracowania. Niektóre z haseł mają swoje legalne wyjaśnienia, inne są tylko mniej lub bardziej technicznymi terminami. Praktycznie żadne jednak z nich nie ma jednego, ustalonego i powszechnie akceptowanego znaczenia. Dotyczy to tak terminów prawnych (gdzie na gruncie różnych ustaw rozumienie ich może być odmienne), jak i terminów technicznych (gdzie rzadko kiedy spotykamy się z jakimikolwiek skodyfikowanymi wyjaśnieniami). Dodatkowo, należy pamiętać, że niektóre definicje zostaną w ramach niniejszej ekspertyzy w dalszych rozdziałach pogłębione, co może wpływać na ich nieco odmienne (zazwyczaj szersze) rozumienie.

Definicje nie obejmują wszystkich haseł, które pojawiają się w opracowaniu, ani tych, które mogłyby się tutaj pojawić z uwagi na tematykę, a stanowią jedynie wybór najczęściej występujących przypadków – bądź też przypadków, które z uwagi na ich charakterystykę zdają się być najlepszymi przykładami zarysowanych w kolejnych rozdziałach problemów (tak np. portale społecznościowe).

**Pośrednik/ISP** – pojęcie usługodawcy będącego pośrednikiem w dostarczaniu treści (tzw. *intermediary service provider*, stąd ISP) pojawia się w wielu dokumentach, w tym w oficjalnych aktach prawnych. Na potrzeby niniejszego dokumentu przyjmuję jednak jego najogólniejsze rozumienie, przez co termin ten odnosił się będzie przede wszystkim do podmiotów pośredniczących w dostarczaniu informacji w Internecie, pośród których można wyodrębnić podmioty, które umożliwiają dostęp do sieci innym podmiotom, tj. *access providers*, i podmioty, które przekazują, przechowują i udostępniają informacje w Internecie, tj. przede wszystkim *host providers* (por. też definicje poniżej)<sup>5</sup>.

**Usługodawca** – osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową, świadczy usługi drogą elektroniczną w rozumieniu ustawy o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz.U. Nr 144 poz. 1204).

**Usługobiorca** – osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która korzysta z usługi świadczonej drogą elektroniczną (bardzo często jest nim, choć nie musi zawsze być, konsument).

**Access provider** – pośrednik, dostawca dostępu do Internetu za pośrednictwem urządzeń technicznych, poprzez sieć (infrastrukturę) telekomunikacyjną. Oprócz zapewnienia dostępu do sieci *access provider* może świadczyć także inne usługi w zakresie transmisji danych, takie jak m.in. *mere conduit* czy *caching*.

**Host provider** – pośrednik, udostępnia pamięć serwerów w celu przechowywania i udostępniania różnego rodzaju danych osób trzecich.

**Web 2.0** – potoczne określenie serwisów internetowych, w których działaniu podstawową rolę odgrywa treść generowana przez użytkowników danego serwisu (*user generated content*).

---

<sup>5</sup> Zob. też jednak np. Konwencja o cyberprzestępczości, Budapeszt, 23 listopada 2001 roku, gdzie „dostawca usług” oznacza: 1) dowolny podmiot prywatny lub publiczny, który umożliwia użytkownikom jego usług komunikowanie się za pomocą systemu informatycznego, oraz 2) dowolny inny podmiot, który przetwarza lub przechowuje dane informatyczne w imieniu takich usług komunikacyjnych lub użytkowników takich usług.

**Portale społecznościowe** – rodzaj interaktywnych stron WWW, które są współtworzone przez sieci społeczne osób dzielących wspólne zainteresowania lub chcących poznać zainteresowania innych (np. Nk.pl, Facebook, GoldenLine). Większość portali społecznościowych dostarcza użytkownikom wielu sposobów komunikacji, np. czaty, komunikatory, listy dyskusyjne, blogi, fora dyskusyjne.

**NTD** – procedury „powiadomienia i usuwania” (*notice and take down*), przewidujące sposób zachowania się pośrednika, umożliwiające mu wyłączenie odpowiedzialności (przede wszystkim polegają na tym, że pośrednik po uzyskaniu właściwego zawiadomienia o bezprawnym zachowaniu zobowiązany jest do uniemożliwienia dostępu do takich danych).

**Ustawa** – ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 9 września 2002 r.).

**Dyrektywa** – dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (2000/31/WE) (Dz.U. UE L z dnia 17 lipca 2000 r.).

## **6.2. Założenia, cele i perspektywy istniejących rozwiązań (ocena pod kątem zarówno ISP, jak i tych podmiotów, których prawa są naruszane)**

Mniej więcej w połowie lat 90. zarówno w USA<sup>6</sup>, jak i w Europie<sup>7</sup> rozpoczęła się poważna dyskusja na temat prawnych uregulowań umieszczania treści w Internecie. Zauważono bowiem, że rozwój Internetu może być zagrożony, jeśli pośrednicy byłiby (nadmiernie) narażeni na roszczenia za dane umieszczane przez użytkowników (usługobiorców, konsumentów), zwłaszcza pod kątem potencjalnego naruszania prawa własności intelektualnej, w tym przede wszystkim praw autorskich. Z drugiej jednak strony zainteresowane grupy interesu starały się lobbować za korzystnymi dla nich rozwiązaniami, przedstawiając przy tym swoje racje. W pierwszej więc kolejności podkreślano (jest to zresztą argument zasadniczo aktualny), iż w ogromnej ilości przypadków potencjalnych naruszcycieli praw (zwłaszcza wspomnianych prawa autorskich) jest zbyt wielu, są oni do pewnego stopnia anonimowi i nie sposób ich odnaleźć<sup>8</sup>. Dlatego też odpowiednie zdefiniowanie i egzekwowanie odpowiedzialności pośredniej jest niezbędne. Zresztą nie sposób nie dostrzec, że argument ten jest uzupełniany i popierany przez dane dotyczące np. nielegalnego rozpowszechniania muzyki w sieci. Przykładowo – Międzynarodowa Federacja Przemysłu Fonograficznego podała, że około 95% muzyki ściągniętej w sieci (*downloaded*) odbywało się bez jakichkolwiek licencji<sup>9</sup>. Także stosunkowo niezależne organizacje, jak np. Organizacja Współpracy Gospodarczej i Rozwoju (OECD), przyznawały, że korzystanie z „pirackich” dóbr cyfrowych jest „powszechne”<sup>10</sup>. Przy czym nie sposób nie zauważyć, że niektórzy twierdzą, iż poza ułatwieniem takiego rozwiązania niewątpliwie pozywanie setek czy tysięcy konsumentów nie byłoby pożądane od strony marketingowej<sup>11</sup>.

---

<sup>6</sup> J. R. Fichtner, T. J. Strader, *Automated takedown notices and their potential to generate liability under section 512(f) of the Digital Millennium Copyright Act*, „Journal of Intellectual Property Law & Practice”, 2010, 1 of 9.

<sup>7</sup> M. Marzouki, *European Internet Policies Between Regulation and Governance: Issues with Content Regulation*, Graz 2008

<sup>8</sup> E. Rosati, *On secondary infringement and beyond: the future of online copyright law*, „Journal of Intellectual Property Law & Practice” (2010) 5 (4): 282-284.doi.

<sup>9</sup> [www.ifpi.org/content/library/dmr2009.pdf](http://www.ifpi.org/content/library/dmr2009.pdf)

<sup>10</sup> OECD, *Economic Impact of Counterfeiting and Piracy 2007*, [www.oecd.org/dataoecd/13/12/38707619.pdf](http://www.oecd.org/dataoecd/13/12/38707619.pdf).

<sup>11</sup> „Suing end users for online infringements is usually not economically viable—and, in any event, may not be good PR”, D. Osborne, *User generated content (UGC): trade mark and copyright infringement issues*, „Journal of Intellectual Property Law & Practice” (2008) 3 (9): 555-562.

W każdym razie na bazie takich założeń i faktów zarówno w Stanach Zjednoczonych, jak i w Europie wprowadzono pewne rozwiązania, które w zamierzeniu miały z jednej strony zapewnić bezpieczeństwo i ochronę podmiotom narażonym na naruszanie ich praw i interesów, a z drugiej – nie utrudniać rozwoju Internetu. Po obu stronach oceanu przyjęto jednak inne uregulowania. Amerykańskie przepisy zostaną w pewnym zakresie omówione w rozdziale 6.5, zaś europejskie i polskie ustawodawstwa, w zakresie niezbędnym dla niniejszego opracowania, najlepiej prezentuje poniższa tabela.

Dyrektywa	Ustawa
<p style="text-align: center;"><b>Art. 14. Hosting</b></p> <p>1. Państwa Członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwu informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę, usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem że:</p> <p>a) usługodawca nie ma wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji, a w odniesieniu do roszczeń odszkodowawczych, nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności; lub</p> <p>b) usługodawca podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony.</p> <p>2. Ustęp 1 nie ma zastosowania, jeżeli usługobiorca działa z upoważnienia albo pod kontrolą usługodawcy.</p> <p>3. Niniejszy artykuł nie ma wpływu na możliwość wymagania od usługodawcy przez sądy lub organy administracyjne, zgodnie z systemem prawnym Państw Członkowskich, żeby przerwał on naruszenia prawa lub im zapobiegł oraz nie ma wpływu na możliwość ustanowienia procedur regulujących usuwanie lub uniemożliwianie dostępu do tych informacji przez Państwa Członkowskie.</p>	<p style="text-align: center;"><b>Art. 14.</b></p> <p>1. 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 zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych.</p> <p>2. Usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych.</p> <p>3. Usługodawca, który uzyskał wiarygodną wiadomość o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych, jeżeli niezwłocznie zawiadomił usługobiorcę o zamiarze uniemożliwienia do nich dostępu.</p>

Jak wynika z wcześniejszych uwag, zacytowane przepisy obowiązują już nieco ponad lub niemal 10 lat. Jest to więc dostatecznie długi okres, by spróbować dokonać oceny funkcjonowania dyrektywy i polskiej ustawy. Szczegółowe w tym zakresie rozwiązania, z rozróżnieniem na poszczególne aspekty, znajdują się w dalszych rozdziałach. W tym miejscu warto jednak wspomnieć, że istniejące przepisy ulegają stałej interpretacji, tak przez sądy krajowe, jak i wspólnotowe, w związku z czym nawet ich jednoznaczna na pozór wykładnia może przynieść odmienne rozstrzygnięcia w praktyce<sup>12</sup>, nie mówiąc o niepewności, jaka może się wiązać z najbardziej znaczącymi orzeczeniami Trybunału (d. ETS)<sup>13</sup>. Po drugie, postanowienia art. 14 ustawy i dyrektywy o uniemożliwianiu dostępu do

<sup>12</sup> Najbardziej charakterystyczne i znane chyba w tym zakresie są trzy orzeczenia wydane przez paryski *Tribunal de Grande Instance* w sprawach *Lafesse vs. MySpace*, *Nord Quest Production vs. Dailymotion* i *SARL Zadig Production et al. V. Google Inc. et AFA*, gdzie przy stosunkowo podobnych stanach faktycznych wydano zupełnie odmienne wyroki.

<sup>13</sup> Por. zwłaszcza opinię rzecznika generalnego N. Jääskinen przedstawioną w dniu 9 grudnia 2010 r. w sprawie C-324/09 *L'Oréal SA przeciwko eBay International AG* w zestawieniu z odmiennymi motywami wyroku Trybunału (wielka izba) z 23 marca 2010 r. w sprawach połączonych od C-236/08 do C-238/08, *Google przeciwko Louis Vuitton*.

danych bezprawnych są w jakimś stopniu uzupełniane przez krajowe ustawodawstwa, które wprowadzają dodatkowe rozwiązania umożliwiające przede wszystkim specjalnym organom administracyjnym blokowanie dostępu do danych w sieci (por. ostatni francuski projekt LOPPSI 2<sup>14</sup>). Jednocześnie organy państwowe, a zwłaszcza wspólnotowe, dążą nie tylko do próby wprowadzenia obowiązku blokowania niektórych stron na poziomie ustawodawstwa europejskiego<sup>15</sup>, ale – co wydaje się szczególnie niebezpieczne z uwagi na brak jakiegokolwiek monitoringu stanowienia prawa i nadzoru nad stanowieniem prawa – próbuje się nakłaniać pośredników w sposób nieformalny do blokowania dostępu do stron uznanych za nielegalne/bezprawne<sup>16</sup>. Wskazane perspektywy nie wchodzą bezpośrednio w rozważania niniejszego opracowania, jednak jak się wydaje, nie sposób ich pominąć przy całościowej ocenie problemu.

### 6.3. Wskazanie podstawowych problemów interpretacyjnych uregulowań prawnych

#### 6.3.1. Wyłączenie, ograniczenie, odrębne zasady odpowiedzialności czy doprecyzowanie istniejących zasad?

Rozdział 3 polskiej ustawy o świadczeniu usług drogą elektroniczną, w którym zawarty jest art. 14, nosi tytuł *Wyłączenie odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną* i zasadniczo nie powinien budzić wątpliwości. Dzieje się tak jednak, kiedy porównamy go z tytułem odpowiedniego działu przedmiotowej dyrektywy, który nosi nazwę *Odpowiedzialność usługodawców będących pośrednikami*. Nawet dla laika ta różnica powinna być znacząca, albowiem o ile pierwszy sugeruje, że w razie niespełnienia warunków przewidzianych w art. 12–14 pośrednik odpowiada na zasadach ogólnych, o tyle drugi stwarza wrażenie, że w rzeczywistości ustawodawca sformułował tutaj autonomiczne zasady odpowiedzialności (czyli że niespełnienie tych warunków jest równoznaczne z odpowiedzialnością).

Wątpliwości te ulegają jeszcze pogłębieniu, kiedy przyjrzymy się treści preambuły do dyrektywy. Otóż w pkt 42 ustawodawca wspólnotowy posłużył się terminem *exemption from liability* oznaczającym całkowite wyłączenie odpowiedzialności usługodawcy, zaś w pkt 45 – operuje terminem *limitations of the liability*, który powinien być tłumaczony jako ‘ograniczenia odpowiedzialności’. I choć komentatorzy zdają się uznawać, iż prawidłowa interpretacja powinna zmierzać do opowiedzenia się za poglądem, według którego dyrektywa odnosi się do całkowitego wyłączenia odpowiedzialności usługodawców<sup>17</sup>, to jednak ta różnorodność terminologiczna może rodzić zasadne pytania o rzeczywisty zakres odpowiedzialności usługodawców.

W tym kontekście jeszcze większą niepewność wywołuje jedna z ostatnich opinii rzecznika generalnego, który wskazał, iż „można by argumentować, że przepisy dotyczące odpowiedzialności zawarte w art. 12, 13 i 14 dyrektywy 2000/31 należy rozumieć jako odstępstwa od odpowiedzialności, które powinny w związku z tym podlegać ścisłej wykładni. W mojej opinii niekoniecznie jest tak w istocie, ponieważ w wielu państwach członkowskich odpowiedzialność usługodawcy w sytuacjach określonych w tych artykułach jest wyłączona ze względu na brak

---

<sup>14</sup> <http://prawo.vagla.pl/node/9357>. Odnosnie blokowania dostępu zob. też

<http://www.panoptykon.org/content/relacje-z-debaty-blokowanie-stron-internetowych-rok-po-pocz-tek-cenzury-czy-odpowied-na-real>.

<sup>15</sup> Choć wydaje się, że w pewnym zakresie dostrzeżono ten problem i powoli przebijają się do opinii publicznej głosy przeciwko takim rozwiązaniom, także w Parlamencie Europejskim – <http://www.panoptykon.org/content/europosowie-przeciwko-cenzurze-internetu-kilka-s-w-komentarza-do-g-osowania-w-libe>.

<sup>16</sup> <http://www.edri.org/edriagram/number8.15/edri-euroispa-notice-takedown-comission>

<sup>17</sup> G. Rączka, *Prawne zagadnienia hostingu*, PPH.2009.4.31

subiektywnej winy. Tak więc przepisy te można bardziej trafnie zakwalifikować jako potwierdzenia lub wyjaśnienia istniejącego prawa aniżeli jako odstępstwa od niego<sup>18</sup>.

### 6.3.2. Co to jest hosting, co to jest przechowywanie danych?

Jak widać z zestawienia w powyższej tabeli, jedynie europejski ustawodawca obok terminu „przechowywanie informacji” (w polskiej ustawie „przechowywanie danych”) posługuje się pojęciem hostingu. Żadne z nich nie jest jednak nigdzie wyjaśnione, co prowadzi do bardzo różnorodnych interpretacji.

Zacznijmy od tego, że w definicjach wyjaśniliśmy, iż *host provider* to pośrednik, który udostępnia pamięć serwerów w celu przechowywania i udostępniania różnego rodzaju danych osób trzecich. Nie jest to jednak ani pełna, ani ścisła definicja. Po pierwsze wynika to z tego, że rodzajów hostingu jest tak naprawdę bardzo wiele, a wśród nich istnieją dodatkowe podziały, np. w zakresie web hostingu. Po drugie, i to zresztą rodzi największe problemy, zasadniczo istotą hostingu (przynajmniej z założenia) jest samo tylko oddanie do dyspozycji zasobów serwera, a już niekoniecznie umożliwienie udostępniania danych usługobiorców.

Tak czy inaczej, nawet jeśli udałoby się ustalić techniczną, sformalizowaną definicję hostingu jako takiego, nie jest pewne, czy ustawodawca europejski właśnie do niej się odnosił. Ta niewiadoma jest jeszcze bardziej widoczna na gruncie naszego porządku prawnego, gdzie – jak zaznaczono – w ogóle pominięto termin „hosting”, a ograniczono się tylko do samego „przechowywania”.

Takie rozwiązanie przyniosło skutek w postaci (naszym zdaniem zbyt radykalnych, ale trudnych do pominięcia) interpretacji, zgodnie z którymi „należy stwierdzić, 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”<sup>19</sup>.

Przyjęcie tego ostatniego stanowiska oznaczałoby, że praktycznie żaden z obecnie funkcjonujących pośredników, uważanych potocznie (powszechnie?) za host providera, nie mógłby korzystać z wprowadzonych wyłączeń. W rzeczywistości bowiem każda współczesna działalność pośredników (z pominięciem *access providers*) polega nie tylko na oddawaniu do dyspozycji swoich serwerów w celu przechowywania danych, ale też w celu ich ekspozycji, wymiany, współtworzenia etc. I nie dotyczy to wcale tylko serwisów typu Web 2.0 czy portali społecznościowych, choć dla nich ma zapewne największe znaczenie.

Dlatego też najprawdopodobniej, chcąc „chronić” Internet jako taki, większość komentatorów przyjmuje odmienne (można rzec zdroworozsądkowe) założenie, zgodnie z którym „należy koniecznie przyjąć”<sup>20</sup>, iż termin „hosting” obejmuje także udostępnianie tych materiałów w Internecie „w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym”. Czyli udostępnianie też. Dodajmy jednak, iż mimo tak kategorycznych wypowiedzi nadal część doktryny o uznanym dorobku wskazuje, że nie jest jasne, jakie podmioty zaliczyć do kręgu opisanego w art. 14, a „problem odpowiedzialności usługodawców usług społeczeństwa informacyjnego w dobie tzw. Web 2.0 (...) wymaga z pewnością przemyślanej reakcji

<sup>18</sup> K. Sorvari, *Vastuu tekijänoikeuden loukkauksesta erityisesti tietoverkkoympäristössä*, (Odpowiedzialność za naruszenie prawa autorskiego w Internecie), WSOY, Helsinki 2005, s. 513–526, za: opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 9 grudnia 2010 r., Sprawa C-324/09 L'Oréal SA przeciwko eBay International AG.

<sup>19</sup> P. Sadowski, *Wyłączenie odpowiedzialności przy świadczeniu usług hostingu – polemika*, MOP 2009 nr 16.

<sup>20</sup> J. Barta, R. Markiewicz, *Przechowywanie utworów na stronach internetowych*, ZNUJ 2009.3.5.

ustawodawcy<sup>21</sup>. Problem w tym zakresie może być jeszcze większy, jeśli ustawodawca zdecyduje się wprowadzić dodatkowe wyłączenia odpowiedzialności wyszukiwarek internetowych i zamieszczających w sieci linki. Im bowiem większa kazuistyka, tym węższa wykładnia istniejących wyłączeń.

### 6.3.3. Wydawca czy nie

Z powyższymi trudnościami ściśle łączy się kolejny problem. Otóż w piśmiennictwie zdaje się przeważać pogląd, wedle którego wyłączenie odpowiedzialności za hosting/przechowywanie zachodzi tylko wtedy, gdy działalność taka ma charakter neutralny, pasywny i transparentny. Ma na to wskazywać przede wszystkim pkt 42 preambuły dyrektywy, według którego „[w]yłączenia w dziedzinie odpowiedzialności ustanowione w niniejszej dyrektywie obejmują jedynie przypadki, w których działalność podmiotu świadczącego usługi społeczeństwu informacyjnego jest ograniczona do technicznego procesu obsługi i udzielania dostępu do sieci komunikacyjnej, (...) działanie takie przybiera charakter czysto techniczny, automatyczny i bierny<sup>22</sup>.

Taki pogląd znalazł istotne potwierdzenie w licznych orzeczeniach, zwłaszcza sądów francuskich, które przyjmowały, iż świadczenia usługi hostingowej nie można odseparować od dominujących (np. w ramach serwisu eBay) organizowania i prowadzenia aukcji internetowej i z tego powodu kwestionowano wyłączenie odpowiedzialności<sup>23</sup>.

Znaczące odstępstwo od tej zasady wyrażono w innym wyroku (zresztą *nota bene* także sądu francuskiego), w którym przyjęto, że działalność redakcyjna (pojęcie wydawcy) ma miejsce tylko wówczas, gdy dochodzi do wyboru materiałów udostępnianych online<sup>24</sup>. Nie mają takiego charakteru ograniczenia rozmiarów plików czy segregowanie tematyczne. Można też łączyć materiały ISP (jego własne) z materiałami przechowywanymi, pod warunkiem wyraźnego odseparowania, żeby nie wprowadzać w błąd. Uznano też, że sprzedaż miejsca reklamowego nie upoważnia do traktowania ich jako wydawców<sup>25</sup>. Bardzo podobnie wypowiedział się też stosunkowo niedawno sąd w Madrycie, w sprawie *Telecinco vs. YouTube*, **gdzie przyjęto jednoznacznie, że popularna platforma do dzielenia się (udostępniania) plików muzycznych i wideo nie może być uznana za redakcję (wydawcę), jest natomiast host providerem, który w pełni korzysta z wyłączenia przewidzianego w art. 14 dyrektywy<sup>26</sup>.**

Kwestia ta w dalszym ciągu nie jest jednak przesądzona na poziomie europejskim. Przypomnieć bowiem wypada, że w słynnym orzeczeniu w sprawie **Google vs. Louis Vuitton** Trybunał (ETS) stwierdził, że „w celu ustalenia, czy odpowiedzialność podmiotu świadczącego usługę odsyłania mogłaby zostać ograniczona na podstawie art. 14 dyrektywy 2000/31, należy zbadać, czy działanie tego podmiotu ma charakter »czysto techniczny, automatyczny i bierny«<sup>27</sup>.

<sup>21</sup> P. Polański, *Prawo Internetu. Wprowadzenie*, Warszawa 2008, s. XXX.

<sup>22</sup> J. Barta, R. Markiewicz, *Przechowywanie utworów...*, zob. także P. V. Ecke, M. Truyens, *Recent events in EU Internet Law*, „Journal of Internet Law” 2008/4, s. 28.

<sup>23</sup> W orzeczeniu z 30 czerwca 2008 r. w sprawie eBay (Tribunal de Commerce de Paris, jugement prononce le 30 Juin 2008, Premiere Chambre B, RG No. 2006077799), we wcześniejszym orzeczeniu z 7 czerwca 2006 r. *Tiscali Media vs. Dargaud Lombard, Lucky Comics* [Cour d’appel de Paris (4ème chambre, section A)] czy w sprawie *Jean Yves L. dit Lafesse vs. Myspace* (Tribunal de Grande Instance de Paris, Ordonnance de référé, 22 June 2007).

<sup>24</sup> Orzeczenie z 15 kwietnia 2008 r. (*Lafesse vs. Dailymotion*, Sąd Rejonowy w Paryżu).

<sup>25</sup> Zob. też B. Allgrove, P. Balboni, A. Haines, N. Heckh, L. Mosna, N. Quoy, *Liability of Web 2.0 Service Providers – A Comparative Look*, „Computer Law Review International” 2008/3, s. 66.

<sup>26</sup> E. Bonadio, D. Mula, *Madrid court confirms YouTube’s host status*, „Journal of Intellectual Property Law & Practice”, (2011) 6 (2): 82–84.

<sup>27</sup> Wyrok Trybunału (wielka izba) z 23 marca 2010 r. w sprawach połączonych od C-236/08 do C-238/08, *Google przeciwko Louis Vuitton*, pkt 114.

Odmienne jednak nieco podejście zaprezentował niedawno rzecznik generalny, który podniósł, iż ma „pewne trudności z tą interpretacją”. Uznał bowiem (wydaje się, że w sposób logiczny i przekonujący), że pkt 42 preambuły do dyrektywy wspominający o automatycznym i biernym charakterze usług odnosi się tylko do „zwykłego przekazu” (*mere conduit*) oraz cachingu. Do hostingu miałyby się odnosić zaś tylko pkt 46 preambuły, który brzmi następująco: „W celu skorzystania z ograniczenia odpowiedzialności podmiot świadczący usługi społeczeństwa informacyjnego polegające na przechowywaniu informacji od chwili faktycznego zapoznania się z informacją lub powzięcia wiadomości o bezprawnej działalności musi niezwłocznie podjąć działania w celu usunięcia lub uniemożliwienia dostępu do przedmiotowych informacji; usuwanie lub uniemożliwianie dostępu musi być przeprowadzane w poszanowaniu zasady wolności wyrażania opinii oraz procedur ustanowionych w tym celu na poziomie krajowym”.

#### 6.3.4. Wiedza o bezprawności

Zarówno w polskiej ustawie, jak i w dyrektywie znajduje się odwołanie do wiedzy pośrednika, która może mieć wpływ na jego odpowiedzialność, niemniej jednak w obu przypadkach to odwołanie jest nieco inne. Mimo tych różnic spróbujemy jednak dokonać możliwie najbardziej właściwego odczytania polskiej normy w świetle przepisów dyrektywy. Wydaje się, że szczególnie tutaj pomocne (w braku wyjaśnień na poziomie europejskim) będzie odwołanie się do innych krajowych implementacji prawa wspólnotowego.

W pierwszej kolejności wypada jednak zauważyć (co widać z tekstu zamieszczonego w tabeli), iż dyrektywa niejako oddziela wiedzę (odnosząc ją do roszczeń odszkodowawczych) od posiadania wiarygodnych wiadomości (w stosunku do wszelkich innych roszczeń). Tymczasem polska ustawa nie tylko nie wyróżnia specjalnie roszczeń odszkodowawczych, ale niejako zrównuje oba te pojęcia. Jak w takim razie należy oceniać stan „wiedzy” w zestawieniu z wiarygodną wiadomością (czy urzędowym zawiadomieniem, które obok wiarygodnej wiadomości pojawia się w przepisach)?

Wydaje się, że możliwe do obrony są tutaj dwa stanowiska. Pierwsze z nich zakładałoby, że wiedza powstaje tylko wówczas, gdy pośrednik otrzyma wiarygodną wiadomość. Do oceny takiego stanu rzeczy niezbędne jest jednak dokonanie wyjaśnienia, czym ta wiarygodna wiadomość (urzędowe zawiadomienie) jest, co zostanie dokonane w kolejnych punktach.

Drugie podejście opierałoby się na założeniu, że wiedza może być niezależna od otrzymania wiarygodnej wiadomości. Innymi słowy, można uznać, że pośrednik wiedział o naruszeniu prawa mimo braku otrzymania wiarygodnej wiadomości (np. z uwagi na sposób funkcjonowania usługodawcy czy choćby jego kontakty osobiste z naruszcycielem<sup>28</sup>).

Przeprowadzone badania prowadzą do wniosku, że w poszczególnych krajach problem ten został rozwiązany w bardzo różny sposób. Jedne z nich przyjęły zasadę, że stan wiedzy powstaje tylko po powiadomieniu przez stosowne władze, inne przyjęły sformalizowane procedury NTD, wreszcie ostatnia grupa uznała, że należy opierać się tutaj na krajowych standardach odnośnie posiadania wiedzy jako takiej<sup>29</sup>.

W zakresie tych ostatnich właśnie założeń (oparcie na standardach posiadania wiedzy jako takiej) warto przywołać orzeczenia niektórych sądów krajowych. I tak np. sądy w Niemczech uznały, że niedbalstwo (zaniedbanie) czy działanie, które można określić jako zamiar ewentualny (*dolus*

<sup>28</sup> Zob. też G. Pacek, *Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych*, [http://cbke.prawo.uni.wroc.pl/files/ebiuletyn/Wybrane\\_zagadnienia\\_zwiazane\\_z\\_odpowiedzialnoscia.pdf](http://cbke.prawo.uni.wroc.pl/files/ebiuletyn/Wybrane_zagadnienia_zwiazane_z_odpowiedzialnoscia.pdf).

<sup>29</sup> T. Verbiest, G. Spindler, G. M. Riccio, A. Van der Perr, *Study on the...*

*eventualis*) nie powodują powstania wiedzy w rozumieniu niemieckiej ustawy, implementującej dyrektywę<sup>30</sup>. W odniesieniu do roszczeń odszkodowawczych, dostawcy usług hostingowych mogą cieszyć się przywilejem zwolnienia z odpowiedzialności, gdy nie są świadomi faktów lub okoliczności, które świadczą o bezprawności w sposób oczywisty (interpretowane w doktrynie niemieckiej jako brak rażącego niedbalstwa<sup>31</sup>).

Trzeba jednak przy tym pamiętać, że wiedza odnosić się musi nie tylko do samej informacji o konkretnych danych bezprawnie zamieszczonych na serwerach usługodawcy, ale również do świadomości, że są one udostępniane bezprawnie<sup>32</sup>. Przy czym także w tym zakresie poziom wiedzy jest podniesiony. Przykładowo w prawie austriackim wprowadzono zapis, zgodnie z którym naruszenie prawa musi być oczywiste dla „nieprawnika”, bez jakichkolwiek dalszych poszukiwań i badań<sup>33</sup>.

W świetle tych wyjaśnień na koniec wypada zauważyć, że polska ustawa, w przeciwieństwie do postanowień dyrektywy i w odróżnieniu od przywołanych uregulowań innych krajów członkowskich UE, nie wprowadza wymogu braku świadomości faktów lub okoliczności, z których wynika bezprawny charakter hostingowanych treści. Teoretycznie więc można uznać, iż zasady wyłączenia odpowiedzialności uległy tutaj jeszcze większemu złagodzeniu, co sprowadzałoby się do przyjęcia, iż irrelevantne pozostają wszelkie formy pośredniego wskazywania na naruszenie. Niemniej w literaturze prezentowany jest pogląd, zgodnie z którym konieczne jest przeprowadzanie wykładni „prounijnej”, w efekcie czego należałoby przyjąć, że wiedza o bezprawności może przybrać charakter pośredni (tzn. może np. wynikać z okoliczności towarzyszących udostępnianiu utworu<sup>34</sup>).

### 6.3.5. Wiarygodna wiadomość

Pojęcie wiarygodnej wiadomości nie jest, jak wspomniano, wyjaśnione w ustawie. W związku z tym można przyjąć tutaj różne jego interpretacje. Pierwsza z nich będzie się ściśle łączyła z poprzednim punktem – w tym sensie, że za wiarygodną wiadomość uznamy jakąkolwiek wiadomość, która skutkować będzie powstaniem stanu wiedzy o danych bezprawnie zamieszczonych na serwerach usługodawcy, jak również stworzy świadomość, że są one udostępniane bezprawnie.

Drugie podejście prowadziłoby do uznania, że wiarygodna wiadomość to ta tylko, która została dostarczona w ściśle określonej procedurze powiadamiania (NTD). Na dzień dzisiejszy takiej procedury jednak nie ma w krajowym porządku prawnym, niemniej z uwagi na proponowane zmiany w ustawie oraz podobne podejście niektórych państw członkowskich UE wymaga to wspomnienia (zob. też podrozdział 6.5.2.).

Rozwiązanie trzecie jest swoistym kompromisem między wspomnianymi koncepcjami i – jak się wydaje – to właśnie ono obowiązuje na gruncie polskiej ustawy. Mianowicie, jakkolwiek brak jest dotychczas precyzyjnego wyjaśnienia warunków formalnych takiej wiadomości (co ma miejsce przy

<sup>30</sup> BGH, 23.9.2003, VI ZR 335/02, NJW 2003, 3764; OLG Brandenburg, 16.12.2003, 6 U 161/02, MMR 2004, 330 (331); OLG Düsseldorf, 26.2.2004, I-20 U 204/02, MMR 2004, 315 (316); LG Düsseldorf, 29.10.2002, 4a O 464/01, MMR 2003, 120 (124).

<sup>31</sup> *Härting*, CR 2001, 271 (276); *Spindler*, CR 2001, 325 (332 f.); *Eck/Ruess*, MMR 2003, 363 (364); *Spindler*, in: *Spindler/Wiebe, Internet-Aktionen und Elektronische Marktplätze*, 2nd ed. 2004, Kap. 6 Rn. 25. ...

<sup>32</sup> T. Verbiest, G. Spindler, G. M. Riccio, A. Van der Perre, *Study on the...*, podobnie J. Barta, R. Markiewicz, *Przechowywanie utworów...*

<sup>33</sup> W praktyce jednak sądy ustalony standard oceniają dość dowolnie, przyjmując np. obraźliwe wypowiedzi i zniesławienie reputacji przedsiębiorstwa jest możliwe do uznania za bezprawne przez każdego, także przez nieprawnika (AU8 OLG Innsbruck, 24/5/2005, 2 R 114/05i, [http://www.internet4jurists.at/entscheidungen/olgi\\_114\\_05i.htm](http://www.internet4jurists.at/entscheidungen/olgi_114_05i.htm)).

<sup>34</sup> J. Barta, R. Markiewicz, *Przechowywanie utworów...*

procedurze NTD), to jednak wykładnia językowa i celowościowa zdają się przemawiać za nieco podobnymi, acz nie tak sformalizowanymi wymogami.

Skoro bowiem słowo „wiarygodny” rozumiemy jako: ‘godny wiary, zasługujący na zaufanie, nieulegający wątpliwości, prawdziwy’, a także ‘pewny, autentyczny’, a dodatkowo o doniosłym i poważnym znaczeniu takiej wiadomości świadczy zestawienie z pojęciem urzędowego zawiadomienia, to wiadomość będzie musiała pochodzić od podmiotu, któremu powyżej wymienione cechy możemy przypisać<sup>35</sup>.

Pożądane byłoby także, aby oprócz „źródła pochodzenia” (osoby bądź jednostki poważnej, posiadającej autorytet i odpowiednie doświadczenie czy kwalifikacje w danej materii) wiarygodna wiadomość posiadała też dużo bardziej rozbudowaną treść. Zauważmy bowiem, że w przypadku urzędowego zawiadomienia (por. uwagi poniżej) *de facto* nie jest istotne, jakie dowody czy uprawdopodobnienia ono zawiera, gdyż i tak nad całością „przeważa” strona podmiotowa. Inaczej jest jednak przy wiarygodnej wiadomości. Należy więc przyjąć, że wiarygodna wiadomość powinna przynajmniej podawać, które konkretnie fragmenty treści naruszają prawa i na jakiej podstawie oparty jest taki wniosek. Innymi słowy, do uznania wiadomości za wiarygodną nie wystarcza samo podanie adresu strony internetowej i wyrażenie obawy co do prawnego charakteru treści — niezbędne jest bowiem szczegółowe uzasadnienie takiego zawiadomienia<sup>36</sup>.

Warto przy tym w tym miejscu podnieść, że jedyne chyba szerzej znane polskie orzeczenie, które zajmowało się także wiarygodną wiadomością wskazuje, iż wewnętrzne regulaminy host providerów (np. przewidujące i ustalające elementy wiarygodnej wiadomości) są niewiążące dla poszukującego ochrony. Sama zaś wiarygodna wiadomość, zwłaszcza w przypadku zaniedbań odnośnie podania prawidłowego adresu korespondencyjnego czy braku upowszechnienia wiedzy o zmianie sposobu kontaktu, może być przesłana zasadniczo dowolną drogą, która umożliwi pośrednikowi zapoznanie się z nią („każda forma zawiadomienia pozwanego przez powoda o naruszeniu jego dóbr powinna być uznana za dopuszczalną”<sup>37</sup>).

### 6.3.6. Urzędowe zawiadomienie

Krótko wypada wspomnieć o urzędowym zawiadomieniu. Rozumienie tego pojęcia nie rodzi aż takich kontrowersji, jak interpretacja wiarygodnej wiadomości. Dość powszechnie przyjmuje się bowiem, że z urzędowym zawiadomieniem będziemy mieli do czynienia np. „w razie otrzymania odpisu postanowienia zabezpieczającego w sprawie o naruszenie praw autorskich”<sup>38</sup>, także nieprawomocnego. Taka sama ocena powinna istnieć zasadniczo w zakresie wszelkich orzeczeń sądów powszechnych, ale też i organów administracji.

Nie jest jednak pewne, czy można przyjąć, że urzędowym zawiadomieniem będzie także jakakolwiek inna informacja pozbawiona określonych nakazów, o ile pochodzić będzie ona od podmiotu, który możemy zakwalifikować jako urzędowy (w raczej szerokim tego słowa znaczeniu). Gdyby przyjąć takie założenie, należałoby stwierdzić, że z urzędową wiadomością będziemy mieli do czynienia

<sup>35</sup> G. Pacek, *Wybrane zagadnienia...*

<sup>36</sup> Zob. też G. Rączka, *Prawne zagadnienia...*, która – powołując się na dorobek prawa karnego – postuluje, by wiarygodna wiadomość obejmowała dwa elementy: subiektywny i obiektywny: „dla przyjęcia, że wiadomość jest wiarygodna, nie wystarcza więc jedynie subiektywne odczucie osoby zobowiązanej do zawiadomienia o tym, że informacja jest wiarygodna. Konieczne jest również zaostrożenie kryteriów oceny odnośnie do źródła informacji oraz spojrzenie na wiadomość z punktu widzenia każdego rozsądnego człowieka (...) konieczne jest istnienie faktu wskazującego na popełnienie przestępstwa, który powinien wzbudzić przekonanie, że do jego popełnienia rzeczywiście doszło”.

<sup>37</sup> Wyrok Sądu Apelacyjnego we Wrocławiu z 15 stycznia 2010 r., I ACa 1202/09, Opubl: Orzecznictwo Sądu Apelacyjnego we Wrocławiu rok 2010, Nr 2, poz. 167.

<sup>38</sup> X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 141.

w przypadku każdego zawiadomienia przez sądy, prokuratury, a także przez organy administracji rządowej, samorządowej, Policji etc.

#### 6.4. Uregulowania dotyczące host providerów a ochrona podstawowych praw i wolności

Jak zostało to już wskazane wcześniej, jedną z przesłanek wprowadzenia odnośnych uregulowań wyłączających (ograniczających) odpowiedzialność ISP było zapewnienie podmiotom poszukującym ochrony prawnej (głównie uprawnionym z tytułu praw własności intelektualnej) efektywnej drogi do egzekwowania swych praw. Pośrednik w przypadku otrzymania wiarygodnej wiadomości powinien bowiem działać niezwłocznie, uniemożliwiając dostęp do bezprawnych treści.

Pojawia się tu od razu na wstępie pytanie o podstawy takiego uprzywilejowania. Zauważmy bowiem, że np. właściciel galerii handlowej nie ma szczególnego prawnego obowiązku zamykania butiku w tejże galerii się znajdującego, jeśli dowie się, że właściciel sprzedaje tam podrobione ubrania. Można mieć więc wątpliwości co do zasadności takiego rozwiązania w świetle równości wobec prawa<sup>39</sup>.

Poważniejsze jednak wątpliwości rodzi dalsza tego konsekwencja. Otóż jeśli pośrednik zastosuje się do określonej przepisami procedury i uniemożliwi dostęp do danych umieszczonych na serwerze (na stronie WWW), to *de facto* zachowa się jak arbiter, który rozstrzyga spór między poszukującym ochrony a domniemanym naruszcycielem. To ten efekt może budzić najpoważniejsze obawy.

Nie sposób się w tym miejscu nie odnieść do zasad rządzących wymiarem sprawiedliwości i leżących u jego podstaw. Odwołać się można wręcz do przedstawionej w *Drugim traktacie o rządzie* J. Locke'a wizji przechodzenia przez ludzkość od stanu natury do stanu władzy sprawowanej przez rząd obywatelski. Główną niedogodnością tego pierwszego było uprawnienie każdego do karania przestępcy występującego przeciwko wskazaniom prawa naturalnego i brak gwarancji przed nadużywaniem tego prawa. Panaceum na powyższy stan rzeczy było zdaniem Locke'a stworzenie rządu obywatelskiego, którego jednym z najważniejszych atrybutów był monopol na wymierzanie sprawiedliwości<sup>40</sup>.

To nastawienie – przynajmniej teoretycznie – nie uległo zmianie na gruncie aktualnej konstytucji RP. Jak podkreśla się bowiem w literaturze, „wolności i prawa obywatelskie w demokratycznym państwie prawa gwarantowane są przez liczne instytucje, z których najważniejszą grupę stanowią organy ochrony prawnej. Spośród tych organów na pierwszym miejscu plasują się sądy – jako niezawisłe i niezależne instytucje sprawujące wymiar sprawiedliwości – kształtujące właściwe postawy i zachowania podlegających im podmiotów. Władza sądownicza, jako »trzecia« władza – po ustawodawczej i wykonawczej ma uzupełniać, równoważyć i wzajemnie z poprzednimi troszczyć się o harmonijny rozwój społeczności”<sup>41</sup>.

Właściwie osadzony i zabezpieczony w systemie prawnym sąd zapewnia prawo do bezstronnego rozstrzygnięcia sporu (prawo do sądu), przy czym na ową bezstronność składa się m.in. jawność

<sup>39</sup> Ciekawe w tym miejscu jest jednak spostrzeżenie, że istnieje wiele przykładów, zwłaszcza w europejskich porządkach prawnych, które wskazują na inne (surowsze) traktowanie identycznych zachowań w sieci i poza nią. Najlepszym przykładem jest tutaj walka z pornografią dziecięcą, za którą w elektronicznym środowisku uważane są rysunki i obrazy – zob. M. Marzouki, *European Internet Policies Between Regulation and Governance: Issues with Content Regulation*. Odnośnie przykładów z galerią handlową zob. też bardzo podobne porównanie: K. Szczepanowska-Kozłowska, *Operator rynku elektronicznego a prawo własności intelektualnej*, „Rzeczpospolita” z 12 marca 2011 r. (<http://www.rp.pl/artukul/406510.625449-Operator-ryнку-elektronicznego—a-prawo-własności-intelektualnej.html?p=2>).

<sup>40</sup> J. Locke, *Dwa traktaty o rządzie*, przeł. Z. Rau, Warszawa 1992, s. 171–172, [za:] W. Jasiński, *Bezstronność sądu i jej gwarancje w polskim procesie karny*, Oficyna 2009.

<sup>41</sup> W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Kraków 1998, s. 183.

postępowania<sup>42</sup>, ustne i pisemne uzasadnianie wydawanych orzeczeń<sup>43</sup>, kontrydiktoryjność<sup>44</sup>. Dodajmy jeszcze, że owe zasady odnoszą się nie tylko do postępowań rozpoznawczych, ale także egzekucyjnych (wykonawczych). Jak podkreśla doktryna, „[w] postępowaniu egzekucyjnym mamy do czynienia zarówno z prawem do sądu wierzyciela, którego częścią jest dostęp do egzekucji sądowej, jak i z prawem do sądu dłużnika, który ma prawo do kwestionowania słuszności lub zgodności z prawem egzekucji. Dlatego zadaniem ustawodawcy jest stworzenie w tej kwestii regulacji, które z jednej strony zapewnią dłużnikowi ochronę przed bezprawną lub niesłuszną egzekucją, a z drugiej strony zapewnią wierzycielowi możliwość skutecznego dochodzenia swoich roszczeń (realizuje się to np. przez postępowanie klauzulowe, powództwa przeciwegzekucyjne)”<sup>45</sup>.

Tymczasem, w ramach usług hostingowych rola pośrednika może być sprowadzona nie tylko do roli niemal nieograniczonego arbitra, ale także egzekutora roszczeń, który bez żadnej właściwie kontroli, w sposób niejawni, bez udziału zainteresowanych stron może zapewnić zgłaszającemu ten sam dokładnie efekt, który musiałby on osiągnąć po skierowaniu sprawy najpierw do sądu, a później do komornika (w przypadku spraw cywilnych). Pominięte jest więc nie tylko konstytucyjne prawo do sądu, ale nie ma również kształtowania właściwych postaw społeczeństwa, modelowanych przez poddające się kontroli aparaty władzy państwowej.

Wydaje się więc dość oczywiste, że skutek istniejących uregulowań odnośnie wyłączenia odpowiedzialności pośredników za treść w Internecie co najmniej w znacznym stopniu koliduje z gwarantowanym prawem do sądu. Trudno jednak spotkać jasne i przekonujące wyjaśnienia takiego stanu rzeczy ze strony polskich czy unijnych prawodawców. Takie podejście dziwi tym bardziej, że w świetle np. wyroków Europejskiego Trybunału Praw Człowieka, jakkolwiek prawo do sądu nie jest uznawane za prawo absolutne, to jednak ograniczenia w tym zakresie powinny być wprowadzane niezwykle ostrożnie i z ogromnym wyczuciem. Muszą być uzasadnione i proporcjonalne w stosunku do celu, jaki się chce osiągnąć<sup>46</sup>.

Uznanie pośredników za niemal niczym nieskrępowanych arbitrów jest bardzo bliskie też uznaniu ich za cenzorów. Naruszenie prawa do wolności słowa, do wyrażania opinii, do swobody komunikowania się jest zresztą stosunkowo najczęściej wymieniane obok prawa do sądu jako to prawo, które najbardziej jest zagrożone przy obecnym kształcie art. 14 polskiej ustawy i dyrektywy. Przy czym pamiętajmy, że wolność słowa nie obejmuje tylko sformułowań politycznych czy opinii o innych osobach (a więc wolności słowa w wąskim, tradycyjnym rozumieniu), ale także wypowiedzi komercyjne. W cytowanej już wielokrotnie opinii rzecznika generalnego w sprawie L'Oréal SA vs. eBay wyraźnie przypomniano, że np. „aukcje zamieszczane przez użytkowników rynku elektronicznego są informacjami handlowymi i jako takie są chronione przez prawo podstawowe wolności wypowiedzi i informacji określone w art. 11 ust. 1 karty praw podstawowych UE. Prawo to

---

<sup>42</sup> H. Gajewska-Kraczkowska, *Prawo do publicznego procesu jako element praw jednostki*, [w:] *Prawa jednostki a prawo karne*, (red.) M. Wędrychowski, Warszawa 1995, s. 53–56; B. Wójcicka, *Podstawy wyłączenia jawności rozprawy*, Acta UL Folia Iuridica 1988, nr 35, s. 41.

<sup>43</sup> J. Wojciech, *Bezstronność sądu i jej gwarancje w polskim procesie karny*, Oficyna 2009, rozdz. X, pkt 1.

<sup>44</sup> A. Sanders, *A Fair Trial for the Suspect?*, [w:] A. Eser, C. Rabenstein, im Spannungsfeld von *Effizienz und Fairness; Criminal Justice between Crime Control and Due Process*, s. 193–194.

<sup>45</sup> P. Pogonowski, *Realizacja prawa do sądu w postępowaniu cywilnym*, 2005. Tamże: „egzekucja orzeczeń sądowych i innych tytułów wykonawczych jest niezbędną częścią każdego systemu prawnego. Jest elementem koniecznym do skutecznej realizacji norm prawnych. Niesie ze sobą daleko idące konsekwencje, które dla egzekwowanego dłużnika mogą stanowić problem życiowy i społeczny”.

<sup>46</sup> Wyrok ETPC z 8 lipca 1986 r., 9006/80, Lithgow i inni vs. Wielka Brytania, § 194, cytujące wyrok ETPC z 28 maja 1985 r., 8225/78, Ashingdane vs. Wielka Brytania, § 57; tak samo wyrok z 21 września 1994 r., 17101/90, Fayed vs. Wielka Brytania, § 65; z nowszych orzeczeń zob. z dnia 18 lutego 1999 r., 26083/94, Waite i Kennedy vs. Niemcy, § 59.

obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe”<sup>47</sup>.

Zauważmy też, że istniejące, kontynentalne regulacje (nawet przy dopuszczeniu pośrednika do działania w roli cenzora) mają w swym zakresie istotną lukę. Otóż, zasadniczo, jeśli *host provider* uzyskał wiadomość o naruszeniu, której nie można traktować jako wiarygodnej (w rozumieniu jednej ze wskazanych powyżej interpretacji), a mimo to usunął dane usługobiorcy, to nie ponosi on żadnej odpowiedzialności wobec usługobiorcy (przy czym na gruncie polskiej ustawy jest tu jeszcze wymagane dochowanie aktu staranności w postaci powiadomienia o zamiarze uniemożliwienia dostępu). Wynika z tego wprost, że hostingodawca jest (może nie wprost, ale *implicite*) niemal zachęcany do usuwania treści, gdyż w tym przypadku ryzykuje niewiele (lub wcale nie ryzykuje).

Oczywiście wydaje się, że usługobiorca w przypadku zablokowania dostępu do jego danych na skutek otrzymania przez pośrednika „niewiarygodnej” wiadomości miałby roszczenie odszkodowawcze wobec żądającego uniemożliwienia dostępu do danych (gdyby np. wysłał „niewiarygodną” wiadomość, wiedząc o braku bezprawności).

Jednak podjęcie takiego działania raczej jest bardzo mało prawdopodobne. Po pierwsze usługobiorca jest zazwyczaj zbyt słaby, aby popierać samodzielnie tego typu roszczenia. Nie ma ani wiedzy, ani zaplecza finansowego na prowadzenie sporu z doświadczonymi podmiotami. Z tego zresztą powodu, jak pokazują badania, w ogromnej większości przypadków ISP nie badają nawet przesyłanych do nich zgłoszeń pod kątem ich prawdziwości (wiarygodności), tylko od razu usuwają dane<sup>48</sup>. Po drugie jednak, i to wydaje się decydujące, przy braku jasnej definicji wiarygodnej wiadomości udowodnienie jej nieistnienia (czyli wykazania niewiarygodności) jest praktycznie niemożliwe. W tym punkcie widać więc dodatkowo, jak istotne jest precyzyjne określenie przesłanek uznania wiadomości za wiarygodną.

Trzeba tu dodać jeszcze jedną uwagę. Otóż coraz częściej komercyjni właściciele praw autorskich wykorzystują w swojej działalności narzędzia skanujące w celu usprawnienia procesu wykrywania naruszeń. Tego typu programy przeszukują Internet w poszukiwaniu potencjalnie naruszających treści. Jeśli odpowiednie warunki zostaną spełnione, programy generują i wysyłają automatyczną informację o naruszeniu praw do dostawcy usług hostingowych. Wszystko to odbywa się prawie bez kontroli człowieka, dzięki czemu liczba wysłanych zawiadomień o naruszeniu jest oszałamiająca. Jedna z instytucji zajmujących się cyfrową ochroną praw autorskich twierdzi, że w ten sposób wysłała ponad milion zgłoszeń w każdym miesiącu<sup>49</sup>.

Wspomniane okoliczności prowadzą więc do tego, że z jednej strony pośrednikowi bardziej opłaca się uniemożliwić dostęp do danych, niż tego nie czynić, a z drugiej – powoduje to usuwanie treści, która w żaden sposób nie jest bezprawna<sup>50</sup>. W efekcie, jak podają amerykańskie studia, nawet jedna trzecia zawiadomień kierowanych do pośredników jest wadliwa lub oczywiście nieuzasadniona<sup>51</sup>.

---

<sup>47</sup> Opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 9 grudnia 2010 r., Sprawa C-324/09 L'Oréal SA przeciwko eBay International AG, pkt 157.

<sup>48</sup> Jakkolwiek w literaturze raczej się jednak nie kwestionuje tego, że taka jest w istocie powszechna praktyka – por. J. R. Fichtner, T. J. Strader, *Automated takedown notices and their potential to generate liability under section 512(f) of the Digital Millennium Copyright Act*, „Journal of Intellectual Property Law & Practice”, 2010, 1 of 9.

<sup>49</sup> Tamże.

<sup>50</sup> Przy tej okazji warto jeszcze wspomnieć że na tle np. prawa amerykańskiego wymaga się, aby wysyłający zawiadomienie o naruszeniu jego praw brał pod uwagę okoliczności umożliwiające usługobiorcy korzystanie z danych, np. na zasadzie dozwolonego użytku – zob. J. T. Brown, *Fair use and a takedown notice under the Digital Millennium Copyright Act*, „Journal of Intellectual Property Law & Practice”, 2009, 4 (4): 243-244.

<sup>51</sup> J. Urban, L. Quilter, *Efficient Process or „Chilling Effects”? Take-down Notices Under Section 512 of the Digital Millennium Copyright Act: Summary Report*, [http://mylaw.usc.edu/documents/512Rep-ExecSum\\_out.pdf](http://mylaw.usc.edu/documents/512Rep-ExecSum_out.pdf).

Na koniec zwróćmy uwagę na jeszcze jedną rzecz. Pośrednicy są dziś pod dużą presją, gdyż – jak wspomnieliśmy wcześniej – częstokroć prawo w sieci jest dużo bardziej restrykcyjne niż prawo poza nią. Cele polityczne, związane głównie, ale nie wyłącznie z pornografią dziecięcą, bezpieczeństwem Internetu, szczególną ochroną własności intelektualnej, prowadzą do budowania różnych sposobów nadzoru i dodatkowych obowiązków. Skutkuje to powstaniem efektu „schłodzenia” (*chilling effect*), w którym wolność słowa nie jest wprost naruszana i ograniczana, ale nie ma warunków do swej naturalnej ekspresji.

W szczególności pośrednicy na skutek niejasnych i bardzo szerokich uregulowań prawnych decydują się na wprowadzanie restrykcyjnych zapisów własnych regulaminów, dzięki czemu mają możliwość uniemożliwienia dostępu do danych – niezależnie od tego, czy otrzymają wiarygodną wiadomość w rozumieniu dyrektywy czy ustawy; czy wiadomość tę wyśle automat czy pokrzywdzony działający w dobrej wierze; niezależnie od tego, czy usługobiorca jest „piratem”, czy też działa w granicach dozwolonego użytku. Wobec tego, myśląc o prawidłowym rozpisaniu odpowiedzialności pośredników w sieci, rządy powinny mieć na uwadze nie pojedyncze regulacje (osobno świadczenie usług drogą elektroniczną, osobno ochrona dzieci, osobno hazard itd.), ale całościowy system prawny i wzajemne powiązania odrębnych decyzji skupiające się na medium, jakim jest Internet<sup>52</sup>.

## 6.5. Alternatywne sposoby regulacji odpowiedzialności pośredników

Niniejsze opracowanie ma na celu przede wszystkim scharakteryzowanie istniejących w polskim porządku prawnym rozwiązań. Taka analiza nie byłaby jednak pełna, gdyby nie zawierała porównania, czy też zestawienia, z innymi modelami wyłączenia/ograniczenia odpowiedzialności ISP. Poniższe punkty mają więc na celu ogólne przybliżenie innych możliwych lub funkcjonujących rozwiązań.

### 6.5.1. Generalne wyłączenie odpowiedzialności

Istniejący w Europie (a za nim w Polsce) system związany z odpowiedzialnością pośredników ma charakter horyzontalny<sup>53</sup>, tak więc niezależnie od reżimu odpowiedzialności (prawo karne, cywilne, administracyjne) oraz od rodzaju dokonanego naruszenia (naruszenie praw autorskich, dóbr osobistych, reguł konkurencji) w razie spełnienia określonych w ustawie przesłanek usługodawca zwolniony jest od odpowiedzialności<sup>54</sup>. W tym sensie jest to więc wyłączenie generalne. Dodajmy jednak zastrzeżenie, że jest to perspektywa wyrażana dość powszechnie na gruncie prawa polskiego. W innych ustawodawstwach nie zawsze panuje tutaj taka zgodność. Przykładowo nauka prawa czeskiego, odnosząc się do dokonanej tam implementacji dyrektywy, podnosi, że wyłączenia z art. 12–14 mają znaczenie tylko dla stosunków prywatnoprawnych. Nie obejmują więc ewentualnej odpowiedzialności karnej czy administracyjnej<sup>55</sup>.

Przyjmując jednak ową „generalność” (w tym horyzontalność) wyłączeń, trzeba pamiętać, że po pierwsze, dla różnych pośredników są różne wymogi i zastrzeżenia (odrębnie dla zwykłego przesyłu, dla cachingu, dla *host providers*), po drugie – zważywszy na problemy z interpretacją pojęć:

---

<sup>52</sup> W podobny sposób konkluduje tę sprawę także m.in. cytowany już raport OECD, *The Role of Internet Intermediaries...*, parts II and III, pkt 114.

<sup>53</sup> B. Sołtys, M. Podleś, w: W. Dubis, J. Gołaczyński, J. Jacyszyn, M. Leśniak, M. Podleś, M. Skory, B. Sołtys, *Umowy elektroniczne w obrocie gospodarczym*, red. J. Gołaczyński, Warszawa 2005, s. 166.

<sup>54</sup> P. Podrecki, P. Litwiński, Z. Okoń, M. Smycz, T. Targosz, D. Kasprzycki, M. Świerczyński, *Prawo Internetu*, 2007, rozdział 5.5.11.

<sup>55</sup> R. Polčák, *The Legal Classification of ISPs. The Czech Perspective*, JIPITEC, 2010 (1), s. 173.

hosting/przechowywanie – nie wiadomo tak do końca, do jakich konkretnie usług się to odnosi. W tym sensie owa „generalność” nie jest spełniona.

Z odmiennym rozwiązaniem spotykamy się na gruncie prawa amerykańskiego. Tam, w § 230 ustawy Communications Decency Act z 1996 r., znajdujemy wzmiankę przewidującą, iż „żaden operator lub użytkownik usług interaktywnych nie może być traktowany jako wydawca czy źródło informacji dostarczonej przez innego dostawcę treści”<sup>56</sup>.

Powyższe uregulowanie zostało uchwalone w części w reakcji na orzeczenie z 1995 r. w sprawie *Stratton Oakmont, Inc vs. Prodigy Services Co*<sup>57</sup>, które sugerowało, że dostawca usług, który zakładał jakąś formę redagowania treści w odniesieniu do zawartości dostarczonej przez usługobiorcę, stawał się wydawcą i w konsekwencji był prawnie odpowiedzialny za zniesławienie i inne czyny popełnione przez użytkowników.

Jakkolwiek zacytowane przepisy posiadają pewien wyjątek – nie dotyczą odpowiedzialności z tytułu naruszenia praw własności intelektualnej i odpowiedzialności karnej (na poziomie ustawodawstwa federalnego), stąd brak tu wspomnianego aspektu wyłączenia horyzontalnego – to jednak w praktyce są oceniane bardzo pozytywnie.

Najważniejsza konstatacja sprawdza się bowiem do tego, że brak wyszczególnienia odrębnych usług świadczonych drogą elektroniczną powoduje możliwość zastosowania wyłączenia niezależnie od charakteru aktywności pośrednika, a więc niezależnie od tego, czy będzie on access providerem, czy będzie świadczył usługi systemów wyszukiwawczych, czy też będzie prowadził serwis społecznościowy albo serwis z aukcjami internetowymi, a nawet – czy będzie zwykłym użytkownikiem przesyłającym treści, których nie jest autorem<sup>58</sup>.

To z kolei łączy się ściśle z szeroką i niemal pełną ochroną wolności słowa. Zresztą podkreślano to nie tylko w doktrynie<sup>59</sup>, ale także w orzecznictwie. Słynny wyrok w sprawie *Zeran vs. America Online*<sup>60</sup> zważył, że „ilość informacji przekazywanych za pośrednictwem usług interaktywnych komputer jest (...) oszałamiająca. Widmo odpowiedzialności deliktowej w zakresie tak mnogiego obszaru wymiany komunikacji miałyby oczywiście negatywne konsekwencje (*chilling effect*). (...) Kongres uznał wagę interesów związanych z wolnością wypowiedzi i zdecydował się na wprowadzenie dla dostawców usług immunitetu, w celu uniknięcia takich negatywnych konsekwencji”<sup>61</sup>. Z tych przyczyn ta właśnie regulacja jest przez wielu postrzegana jako ta, która w największym stopniu przyczyniła się do znacznego rozwoju innowacyjnych usług i stron internetowych (w tym *user generated content sites*) w ciągu ostatnich 15 lat<sup>62</sup>.

---

<sup>56</sup> Tłumaczenie własne, por. „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” (<http://www.law.cornell.edu/uscode/47/230.html>).

<sup>57</sup> *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 31063/94, 1995 WL 323710, 1995 N.Y. Misc. LEXIS 712 (N.Y. Sup. Ct. 1995).

<sup>58</sup> *The Role of Internet Intermediaries...*, parts II and III, pkt 33.

<sup>59</sup> L. Edwards, *From Casual Censorship to Cartelisation? ISP Control of Illegal and Harmful Content*, 3rd IDP Conference on Internet, Law, and Politics, Barcelona, 2007.

<sup>60</sup> *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), [1] cert. denied, 524 U.S. 937 (1998).

<sup>61</sup> Tłumaczenie własne, por. „The amount of information communicated via interactive computer services is...staggering. The specter of tort liability in an area of such prolific speech would have an obviously chilling effect. (...) Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect”.

<sup>62</sup> *The Role of Internet Intermediaries in Advancing...*, parts II and III, pkt 17.

### 6.5.2. Notice and takedown

Uzupełnieniem uregulowań CDA jest procedura *notice and takedown*, zaproponowana w innej amerykańskiej ustawie Digital Millennium Copyright Act<sup>63</sup> (DMCA). Ustawa ta odnosi się tylko do ochrony praw autorskich, jednak z uwagi na najpełniejsze (najbardziej konkretne i precyzyjne) uregulowanie procedury powiadomiania pośredników o domniemanych naruszeniach stanowi ona nie tylko doskonały przykład do analizy, ale też była źródłem inspiracji (przynajmniej w teorii) dla postanowień dyrektywy i polskiej ustawy.

I tak, z chwilą otrzymania przez ISP powiadomienia o naruszeniu prawa, należy ocenić i sprawdzić, czy powiadomienie posiada wszystkie przewidziane prawem elementy, tj.:

- 1) własnoręczny lub cyfrowy podpis właściciela wyłącznych praw autorskich;
- 2) opis utworu, którego ma dotyczyć naruszenie;
- 3) opis materiału (strony WWW), który przypuszczalnie narusza prawa do utworu, w sposób umożliwiający jego odnalezienie;
- 4) odpowiednie informacje umożliwiające kontakt z dokonującym zgłoszenia;
- 5) oświadczenie zgłaszającego, że pozostając w dobrej wierze, uważa on, że opisany materiał nie został umieszczony przez uprawnionego – ani za jego zgodą, ani w zgodzie z obowiązującym prawem;
- 6) oświadczenie, że składana informacja jest dokładna oraz – pod groźbą kary za krzywoprzysięstwo – oświadczenie, że zgłaszający jest uprawnionym bądź też jest umocowany do działania w imieniu uprawnionego.

Jeśli zgłaszający nie spełni ww. wymagań to zgłoszenie można zignorować, gdy zaś zgłoszenie spełnia wymagania, należy zawiadomić dysponenta strony internetowej o otrzymaniu zawiadomienia i o uniedostępnieniu danych na stronie. Po prawidłowym spełnieniu powyższych czynności ISP zwolniony jest z odpowiedzialności wobec poszkodowanego. Dysponent strony może wnieść jednak swoiste zarzuty (tzw. *counter-notice*), które – aby przyniosły odpowiedni skutek – muszą także spełniać pewne wymogi formalne (dość podobne do samego zgłoszenia).

Jeśli dostawca usług prawidłowo i niezwłocznie poinformował dysponenta strony (do której uniemożliwiono dostęp) o otrzymanym zawiadomieniu, a jednocześnie nie otrzymał od niego zarzutów, to jest tym samym zwolniony z odpowiedzialności także wobec tej osoby. W razie natomiast otrzymania prawidłowo sformułowanych zarzutów ISP powinien przesłać ich kopię do zgłaszającego – z zastrzeżeniem, że strona zostanie ponownie aktywowana po upływie 10 dni roboczych. Po upływie 10 dni od otrzymania zarzutów (nie później jednak niż 14 dni) usługodawca reaktywuje stronę, chyba że otrzyma on zawiadomienie, że zgłaszający wszczął odpowiednie postępowanie, mające na celu wydanie przez sąd nakazu uniemożliwienia dostępu do strony przez ISP.

Oczywiście cała regulacja wynikająca z DMCA jest nieco bardziej rozbudowana, ale powyżej przytoczono najważniejsze elementy, które mogą być pomocne w konstruowaniu podobnych rozwiązań na gruncie prawa polskiego. W istocie bowiem w chwili obecnej trwają prace legislacyjne nad nowelizacją ustawy o świadczeniu usług drogą elektroniczną. Jedną z propozycji MSWiA jest uszczegółowienie wymagań (elementów), jakie musi w sobie zawierać wiarygodna wiadomość<sup>64</sup>. W dużej mierze propozycje, które zostały dotychczas udostępnione, uwzględniają analogiczne rozwiązania zaatlantyckie. W porównaniu jednak do DMCA brak im co najmniej dwóch istotnych elementów. Po pierwsze, nie sprecyzowano, że zgłaszający wiarygodną wiadomość w sytuacji przesłania przez dysponenta strony WWW *counter notice* musi złożyć odpowiedni wniosek do sądu

<sup>63</sup> Title II of the Digital Millennium Copyright Act (Pub. L. 105-304, 112 Stat. 2860).

<sup>64</sup> <http://bip.mswia.gov.pl/portal/bip/218/19383/>

(np. pozew czy wniosek o zabezpieczenie), poprzestając na niejasnym sformułowaniu zobowiązującym zgłaszającego do „podjęcia czynności prawnych mających na celu ochronę naruszonych praw”<sup>65</sup>.

Po drugie, propozycja ministerstwa nie zawiera wymogu składania zgłoszenia w dobrej wierze. Takie rozwiązanie zaś mogłoby chronić przed nadużywaniem procedury NTD, w tym przed zautomatyzowaniem żądania uniemożliwiania dostępu do niepożądanych usług elektronicznych.

### 6.5.3. *Notice and stay down*

Procedura *notice and stay down* opiera się na stosunkowo podobnym założeniu, co *notice and take down*, z tym że idzie niejako krok dalej. Otóż, o ile co do zasady przy procedurze *notice and take down* w czystej postaci wiarygodna wiadomość może dotyczyć tylko zdarzenia przeszłego lub teraźniejszego, o tyle *notice and stay down* przyjmuje, że wystarczy jedno zawiadomienie, które automatycznie obliguje do sprawdzania, czy nie dochodzi do dalszych naruszeń w zakresie pierwotnego zgłoszenia (albo przez tę samą osobę, albo wobec tego samego dobra).

Zasadniczo większość komentatorów przyjmuje, że taki proceder byłby sprzeczny z zakazem wprowadzania obowiązku monitorowania usług przez pośredników (art. 15 dyrektywy)<sup>66</sup>. W rzeczywistości jednak ustawodawstwa niektórych państw (czy ich interpretacja) zmierzają ku uznaniu istniejącej tam procedury (nawet jeśli przypomina NTD) *de facto* za *notice and stay down*. Tak jest zwłaszcza we Francji<sup>67</sup>, gdzie zresztą wydano kontrowersyjne orzeczenie uznające odpowiedzialność spółki Google, która czekała na kolejne wiarygodne wiadomości, a powinna była – zdaniem sądu – usunąć wszystkie filmy wideo, które odpowiadały pierwotnemu zgłoszeniu, skoro wiedziała już, że stanowi to naruszenie praw autorskich<sup>68</sup>.

Trzeba też jednak wskazać, że w nieco podobnym kierunku wypowiedział się ostatnio rzecznik generalny, pisząc w swej opinii, że jeżeli „wykryto naruszenie przez A znaku towarowego X w formie zamieszczenia oferty na rynku elektronicznym we wrześniu, to nie wykluczam, że operator rynku mógłby zostać uznany za posiadającego wiarygodne wiadomości o informacjach, działalności, stanie faktycznym lub okolicznościach, jeśli A w październiku zamieści nową ofertę dotyczącą tych samych lub podobnych towarów oznaczonych znakiem towarowym X. W takich okolicznościach należałoby raczej mówić o tym samym ciągłym naruszeniu, aniżeli o dwóch odrębnych naruszeniach”<sup>69</sup>.

### 6.5.4. *The notice and notice*

Jeszcze inny system przyjęto w Kanadzie. Otóż w tamtejszym systemie prawnym uznano, że najlepszym rozwiązaniem może być procedura, w której wprawdzie poszkodowany/uprawniony składa zawiadomienie (wiarygodną wiadomość), ale jedynym obowiązkiem pośrednika jest jej

<sup>65</sup> Por. też G. Pacek, *Nowe paragrafy dla Internetu*, <http://www.rp.pl/artukul/4.613549.html>.

<sup>66</sup> Zob. m.in. opinie wyrażone w ramach konsultacji dla Komisji Unii Europejskiej: [http://www.edri.org/files/EDRI\\_ecommerceresponse\\_101105.pdf](http://www.edri.org/files/EDRI_ecommerceresponse_101105.pdf), [http://brussels.ebaymainstreet.com/files/eBay%20Main%20Contribution%20To%20EC%20E-Commerce%20Consultation%20-%205Nov2010\\_FINAL.pdf](http://brussels.ebaymainstreet.com/files/eBay%20Main%20Contribution%20To%20EC%20E-Commerce%20Consultation%20-%205Nov2010_FINAL.pdf), [http://www.euroispa.org/files/1011\\_euroispa\\_consultation\\_ecommerce.pdf](http://www.euroispa.org/files/1011_euroispa_consultation_ecommerce.pdf), <http://www.ja.net/development/legal-and-regulatory/regulated-activities/related-regulatory-documents/2010.10-EC-eCommerceDirective.html>.

<sup>67</sup> <http://www.gesac.org/fr/prisesdeposition/contenudownload/072VDH10.pdf>

<sup>68</sup> *Zadig Productions i inni vs. Google Inc. Afa*; (TGI Paris 19 octobre 2007).

<sup>69</sup> Opinia rzecznika generalnego N. Jääskinena przedstawiona w dniu 9 grudnia 2010 r., Sprawa C-324/09 L'Oréal SA przeciwko eBay International AG.

przekazanie do usługobiorcy. Usługodawca nic więcej nie czyni: nie podaje danych osobowych, nie uniemożliwia dostępu do treści, nie usuwa danych etc.<sup>70</sup>

Wiele organizacji broniących praw autorskich krytykuje takie rozwiązanie jako niedające pełnych gwarancji porzywdzonym<sup>71</sup>, ale – jak podają z kolei inni komentatorzy – w rzeczywistości system ten przynosi niespodziewane efekty. Otóż wedle jednego z udostępnionych badań aż 71% usługobiorców po trzymaniu zawiadomień od swojego usługodawcy usunęło dobrowolnie treści, których dotyczyło zgłoszenie<sup>72</sup>.

### 6.5.5. Notice and „disconnection”

Ta procedura zwana jest też jako *graduated response* albo – najbardziej chyba popularnie – *three strikes*. Zasadniczo jest to nie tyle odrębna procedura, ile uzupełnienie już istniejących o dalej idące skutki. Polega bowiem ona na tym, że usługodawca jest zobowiązany do odcięcia użytkowników od usług (od sieci) w razie powtarzającego się naruszenia prawa autorskich („*tri-strike and you’re out*”).

Próby wprowadzenia takiego prawa były podejmowane w wielu krajach, w tym w Europie, m.in. we Francji, gdzie ostatecznie się to nie udało i w Wielkiej Brytanii, gdzie powiodło się to częściowo<sup>73</sup>. Wydaje się, że wprowadzenie takich rozwiązań będzie stosunkowo trudna na gruncie europejskim<sup>74</sup>, jednak w wielu krajach, np. w Irlandii, przyjęto je dobrowolnie przez samych pośredników.

### 6.5.6. Rozwiązania dodatkowe

Poza wspomnianymi powyżej systemami uregulowania odpowiedzialności ISP i ich zachowań zasadniczo nie ma żadnych, które byłyby szerzej stosowane lub rozważane. Niemniej warto wspomnieć o dwóch niezbyt szeroko rozpropagowanych głosach.

Pierwszy z nich zmierza do częściowego tylko wprowadzenia zagrożenia odpowiedzialnością za treść dla pośredników, przy generalnym dla nich immunitacie. Byłoby to rozwiązanie podobne do funkcjonującego w USA, gdzie obok wyłączenia z CDA mamy całą procedurę z DMCA. Różnica polegałaby jednak na tym, że wyjątki od zasady nie byłyby wprowadzane na zasadzie dowolności i lobbingu, jak to ma miejsce np. odnośnie ochrony praw autorskich, ale po przeanalizowaniu przesłanek ekonomicznych i zabezpieczeniu się przed możliwością działania pośrednika w roli cenzora i arbitra.

---

<sup>70</sup> Bill-61:

<http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3570473&Language=e&Mode=1&File=63#13>.

<sup>71</sup> <http://www.iipa.com/rbc/2010/2010SPEC301CANADA.pdf>

<sup>72</sup> M. Geist, *ACTA Internet Chapter Leaks: Renegotiates WIPO, Sets 3 Strikes as Model*, <http://www.michaelgeist.ca/content/view/4808/125/>, tenże: *The Effectiveness of Notice and Notice*, <http://www.michaelgeist.ca/content/view/1705/125/>.

<sup>73</sup> [http://en.wikipedia.org/wiki/Digital\\_Economy\\_Bill](http://en.wikipedia.org/wiki/Digital_Economy_Bill)

<sup>74</sup> Zob. Komunikat prasowy w sprawie porozumienia zawartego między Parlamentem Europejskim i Radą UE w sprawie zasad ograniczania dostępu do sieci ([http://www.piit.org.pl/piit2/index.jsp?place=Lead07&news\\_cat\\_id=116&news\\_id=4871&layout=2&page=text](http://www.piit.org.pl/piit2/index.jsp?place=Lead07&news_cat_id=116&news_id=4871&layout=2&page=text)), gdzie podano m.in., iż „Restrictions on a user’s internet access »may only be imposed if they are appropriate, proportionate and necessary within a democratic society«, agreed MEPs and Council representatives. Such measures may be taken only »with due respect for the principle of presumption of innocence and the right to privacy« and as a result of »a prior, fair and impartial procedure« guaranteeing »the right to be heard (...) and the right to an effective and timely judicial review«”.

Regulacja taka wymagałaby dokładnego rozważenia i badań, jednak jako przykład podaje się obowiązek uniemożliwiania dostępu do danych, zawierających wirusy i inne złośliwe oprogramowanie<sup>75</sup>. Z jednej bowiem strony tego typu dane mogą powodować znaczące szkody (od uszkodzenia sprzętu po kradzież pieniędzy), wobec czego kalkuluje się obciążyć usługodawcę kosztami dodatkowego działania, bo ogólny efekt jest opłacalny dla wszystkich. Z drugiej strony, wykrycie i ocena oprogramowania jako wirusa zdaje się być dużo prostsza i niemal automatyczna, w porównaniu np. do badania istnienia naruszenia dóbr osobistych, co częstokroć nawet dla sądów nie jest łatwą sprawą.

Drugie rozwiązanie, które jest warte przywołania, zakłada połączenie wielu istniejących rozwiązań przy dodaniu kilku nowych szczegółów. W wielkim skrócie – odpowiedzialność ISP mogłaby być co do zasady wyłączona, za wyjątkiem pozostawienia możliwości kierowania wniosków o zabezpieczenie, dzięki czemu pośrednicy nadal mieliby swoistą zachętę do uniemożliwiania dostępu do najbardziej szkodzących treści. Żeby jednak i ten (złagodzony już jakkolwiek) przymus psychologiczny (w postaci strachu przed postępowaniem o zabezpieczenie) nie był nadużywany przez przesyłających wiarygodne wiadomości, a jednocześnie aby zapewnić szybkość postępowań, należałoby wprowadzić jakąś formę sądu arbitrażowego, podobnego np. do sądów domenowych, który rozstrzygałby tego rodzaju spory<sup>76</sup>.

---

<sup>75</sup> D. Lichtman, *Holding Internet Service Providers Accountable*, Regulation Winter 2004–2005, <http://www.cato.org/pubs/regulation/regv27n4/v27n4-7.pdf>. Zob. też szerzej: D. Lichtman, E. Posner, *Holding Internet Service Providers Accountable*, July 2004 Chicago Law & Economics, Olin Working Paper No. 217, [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=573502](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=573502).

<sup>76</sup> M. A. Lemley, *Rationalizing Internet Safe Harbors*, „Journal of Telecommunications and High Technology Law”, Vol. 6, p. 101, 2007 Stanford Public Law Working Paper No. 979836 [[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=979836&](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=979836&)], a także M. A. Lemley, R. A. Reese, *A Quick and Inexpensive System for Resolving Digital Copyright Disputes*, 23, „Cardozo Arts & Entertainment L.J.” 1 (2005).