CBKE
e-BIULETYN

Wybrane zagadnienia związane z odpowiedzialnością dostawców usług *hostingowych*.

mgr Grzegorz Jarosław Pacek

absolwent Uniwersytetu Jagiellońskiego, pracownik Kancelarii Radcowskiej Marka Płonki w Bielsku-Białej

W pierwszej połowie XX wieku, na jednej ze ścian klubu golfowego, anonimowa osoba umieściła obelżywy wierszyk, zniesławiający jednego z członków owego klubu. Ponieważ autora inkryminujących wypowiedzi nie udało się znaleźć, pozwany został właściciel klubu golfowego. W wyroku kończącym sprawę, sąd przyznał rację powodowi, uznając wierszyk za szkalujący i przypisując odpowiedzialność administratorowi klubu, który „miał całkowitą kontrolę nad ścianami", mógł więc usunąć obraźliwe słowa. Zdaniem sądu, nie miał znaczenia fakt, że właściciele klubu nie podjęli żadnej aktywnej czynności, mającej na celu czy to napisanie wierszyka, czy też jego umieszczenie na murach[1].

Powyższa historia pokazuje, że prawdopodobnie zawsze, istniały sytuacje, w których konieczne było pociągnięcie do odpowiedzialności osób, które nie tylko nie dopuściły się zakazanego czynu, ale też nie można im było przypisać działania w ramach np. pomocnictwa, czy też w ramach szczególnego reżimu odpowiedzialności (chociażby redaktora naczelnego gazety). Problem ten nabrał jednak niewątpliwie odrębnej mocy z momentem powstania Internetu, który – poza ogromnym spektrum pozytywnych aspektów jego istnienia – niesie ze sobą m.in. niebezpieczeństwo łamania porządku prawnego, w tym głównie poprzez anonimowe umieszczanie bezprawnych treści. Z racji funkcjonowania sieci www, okazało się, że najprostszym rozwiązaniem prowadzącym do blokowania zakazanych treści przez osoby niemożliwe do zidentyfikowania, jest pociągnięcie do odpowiedzialności dostawców usług internetowych, zarówno tym, którzy jedynie umożliwiają dostęp do sieci innym podmiotom (tzw. *acces providers*), jak i tym, które

[1] *Byrne v. Dean* [1937] 1 KB 818

przekazują, przechowują i udostępniają informacje w Internecie (*service providers*)[2]. Niniejsza praca ma za zadanie opisać sposób unormowania w prawie polskim i europejskim możliwości pociągnięcia do odpowiedzialności tej drugiej grupy usługodawców i tylko w zakresie jakim to dotyczy usług *hostingowych*. Niemniej jednak pewne wnioski być może będą mogły znaleźć zastosowanie co do innych rodzajów usług świadczonych drogą elektroniczną.

Hosting najogólniej można określić jako przechowywanie przez usługodawcę (*internet service provider* – dalej ISP) danych osób trzecich (usługobiorców). Dane przechowywane są zazwyczaj poprzez udostępnienie zasobów własnych serwerów (czy też np. wirtualnych platform cyfrowych). Oprócz tego, najczęściej, w ramach usługi klient może otrzymywać dostęp do środowiska systemu operacyjnego o określonych umową parametrach, dostęp do sieci, zasilanie i wsparcie administratorów[3]. Niektórzy spośród autorów rozróżniają dwie formy *hostingu*, tj. utrzymywanie materiałów dostarczonych przez konkretnego usługobiorcę (np. utrzymywanie witryny danej firmy) oraz *hosting* polegający na utrzymywaniu materiałów dostarczonych przez wielu usługodawców (np. zamieszczanych w ramach grup dyskusyjnych)[4]. Ponadto, podkreśla się, że przechowywanie danych i udostępnianie ich innym podmiotom jest z założenia nieograniczone w czasie[5], co odróżnia tę usługę przede wszystkim od *cachingu*, definiowanego jako automatyczne i czasowe pośrednie przechowywanie danych[6].

Z powodu tak określonych działań i zakresu czynności, jakie podejmują ISP, są oni najczęściej pierwszymi podmiotami, pod adresem których domniemani, czy rzeczywiście poszkodowani będą kierowali swoje roszczenia. Przyczyna – jak podkreśla się w piśmiennictwie – jest prozaiczna: „do dostawcy usług internetowych znacznie łatwiej dotrzeć niż do mniej lub bardziej anonimowego użytkownika[7]”. Zresztą w rzeczywistości niejednokrotnie nie jest to nawet nie tyle „łatwość” dotarcia, co wręcz faktyczna niemożliwość. Nie tak dawno w Polsce rozgorzała dyskusja na temat tego, czy i jak można uzyskać dane użytkowników sieci WWW, zwłaszcza gdy nie jest prowadzone postępowanie karne[8]. Skoro więc, osoby czynnie i aktywnie naruszającej określone dobra nie da się, bądź nie jest łatwo ustalić, poszkodowani zaczęli podejmować kroki mające na celu pociągnięcie do odpowiedzialności ISP, jako tych, którzy wprawdzie bezpośrednio

[2] J. Barta, R. Markiewicz, *Ja tu tylko przesyłam*, "Rzeczpospolita" z 31 sierpnia 1999 r.
[3] Http://pl.wikipedia.org/wiki/Hosting
[4] Tak dokładnie X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 139
[5] D. Kot, *Dyrektywa Unii Europejskiej o handlu elektronicznym i jej implikacje dla prawa cywilnego*, KPP 2001, nr 1, s. 93
[6] Ibidem, s. 92
[7] Z. Okoń, *Oskarżony: ISP odpowiedzialność dostawcy usług internetowych*, IDG, 1 grudnia 2000r. (http://www.internetstandard.pl/artykuly/7661.html)
[8] Zob. m.in. S. Wikariak, *Bez prokuratora sprawca anonimowy*, „Rzeczpospolita” z dnia 25 marca 2006r. oraz polemizujący z nim P. Hajdys, *I bez prokuratora sprawcę można zidentyfikować*, „Rzeczpospolita” z dnia 29 marca 2006r.

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

nie zamieszczali na serwerach bezprawnych treści, jednak – zgodnie z logiką przedstawioną w orzeczeniu prezentowanym we wstępie tej pracy – mieli nad nimi kontrolę i mogli je usunąć[9].

Początkowo jednak sądy sprzeciwiały się takiej praktyce. Tak było np. w jednej z pierwszych głośnych spraw, mianowicie *Cubby v. CompuServe*[10], gdzie uznano, że pozwany dostawca usług, nie ma takiej kontroli na rozpowszechnianymi publikacjami, jak np. wydawca prasy tradycyjnej i w efekcie odmówiono pociągnięcia go do odpowiedzialności[11]. Jednak kolejne orzeczenia zmieniły kierunek przyjętej wykładni. Znamienna jest tu zwłaszcza sprawa *Playboy Enterprises v. Frena* z 1993r., w której sąd uznał, że ISP naruszył prawa autorskie powoda, mimo iż nie był świadomy tego, że jego użytkownicy udostępniali w sieci zdjęcia zamieszczane w magazynie „Playboy", a które chronione były prawem autorskim[12] oraz sprawa *Stratton Oakmont, Inc. v. Prodigy Services Co.*[13], w której pozwany został uznany za wydawcę, gdyż według sądu, miał możliwość usunięcia wiadomości przesyłanych przez swoich użytkowników.

Ostatnie z wymienionych orzeczeń postawiło ostatecznie dostawców usług internetowych w bardzo trudnej sytacji, której rozwiązanie mogłoby własciwie polegać tylko na stosowaniu arbitralnej cenzury prewencyjnej, która nie dość, że byłaby uciążliwa dla samych usługodawców, co na ogromną skalę wkraczałaby w konstytucyjnie przyznany zakres wolności słowa. Dlatego też w Stanach Zjednoczonych zdecydowano się przyjąć dwa akty prawne, które miały zapobiegać nieograiczonemu wytaczaniu procesów sądowych przeciwko ISP, tj. Communications Decency Act[14] oraz Digital Millennium Copyright Act[15]. Pierwszy wprowadził ważne zastrzeżenie, zgodnie z którym „[ż]aden dostawca interaktywnych usług komputerowych nie może być traktowany jako wydawca informacji dostarczonych przez *content providers*[16]". Jednocześnie jednak postanowiono,

---

[9] Dodać jeszcze trzeba, że istnieją też wcale liczne poglądy, krytykujące zwolnienie, bądź „rozluźnienie" odpowiedzialności ISP, np. dlatego, że „dotychczas postęp techniczny (np. upowszechnienie pojazdów mechanicznych, wykorzystywanie energii atomowej itp.) niósł z sobą zazwyczaj raczej zaostrzenie, a nie złagodzenie odpowiedzialności korzystających z niego" – taką opinię m.in. przywołują J. Barta, R. Markiewicz, *op. cit.*). Istnieją też opinie, które sprzeciwiają się wprowadzaniu ochrony dla ISP ze względów słusznościowych – tak ja się wydaje należy interpretować stanowisko przedstawione w *Informacji na temat działań społeczności międzynarodowej na rzecz objęcia Internetu systemem prawa przy jednoczesnej ochronie swobody wypowiedzi i informacji*, przygotowanej przez Departament Strategii i Analiz Krajowej Rada Radiofonii i Telewizji w grudniu 2005r., w którym wskazano, iż „[j]edną z barier przestrzegania prawa w Internecie jest komercyjne nastawienie dostawców usług internetowych. Stoją oni przed dylematem polegającym z jednej strony na byciu traktowanym jako podmioty ponoszące odpowiedzialność społeczną za dostarczane usługi, z drugiej - na konieczności pomnażania zysków" (opracowanie dostępne jest na stronach www.krrit.gov.pl)

[10] *Cubby, Inc. vs. CompuServe Inc.*, 776 F. Supp. 135(SDNY 1991)

[11] Por. stanowisko M. Wojtasika, *Naruszanie dóbr osobistych w Internecie,* „Radca Prawny" nr 6/57 (dostępne także w formie elektronicznej na stronie http://www.redakcja.radca.prawny.lex.pl/01_6/zawartosc.html), który opowiada się za traktowaniem ISP „jako dostawców technicznych środków służących do przekazywania informacji, nie decydujących o ich merytorycznym kształcie (tak, jak np. drukarnia drukująca gazetę, w której znajdują się materiały naruszające czyjeś dobra osobiste)".

[12] *Playboy Enterprises, Inc. v. Frena*. 839 F. Supp. 1552 (MD Fla. 1993.)

[13] Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995)

[14] Communications Decency Act (CDA) z 1996 roku, stanowiący Tytuł V ustawy Telecommunications Act z 1996

[15] Digital Millennium Copyright Act (DMCA) z 1998 roku, Pub. L. 105-304

[16] *Content provider*, czyli pierwotny dostawca zawartości, podmiot wprowadzający do sieci "własne" materiały

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

że cytowany przepis, „nie może być interpretowany w celu ograniczenia lub rozszerzenia praw związanych z własnością intelektualną[17]”. To ostatnie zastrzeżenie spowodowało, że sądy w sprawach, w których chodziło o naruszenie praw autorskich, czy praw do znaku towarowego, pomijały to ograniczenie, przyjmując ostatecznie odpowiedzialność ISP[18]. Tym samym wyłączenie przewidziane w CDA mogło znaleźć zastosowanie tylko i wyłącznie w sprawach, w których dochodziło do naruszenia dóbr osobistych[19].

Odnośnie zaś DMCA, trzeba z kolei zastrzec, że przedstawiona tam procedura, związana z wyłączeniem odpowiedzialności ISP, odnosi się jedynie do utworów chronionych prawem autorskim. Niemniej jednak, z uwagi na ciekawe rozwiązania, które mogą się okazać przydatne w dalszej części pracy, warto poświęcić jej nieco więcej uwagi. Otóż wychodząc ostatecznie z założenia, że odpowiedzialność ISP nie może być nieograniczona, a przede wszystkim niezależna od chociażby świadomości usługodawcy, wprowadzono odpowiednie zapisy regulujące proces zawiadamiania o dokonanych naruszeniach, który – w razie prawidłowego przeprowadzenia – zwalnia dostawcę usług z odpowiedzialności[20]. I tak z chwilą otrzymania wiadomości, należy ją ocenić, sprawdzając, czy spełnia ona wszystkie z poniższych wymagań, tj. sprawdzić, czy zawiera:

1. własnoręczny lub cyfrowy podpis właściciela wyłącznych praw autorskich
2. opis utwory, którego ma dotyczyć naruszenie
3. opis materiału (strony www), który przypuszczalnie narusza prawa do utworu opisanego w pkt 2, w sposób umożliwiający jego odnalezienie
4. odpowiednie informacje umożliwiające kontakt z dokonującym zgłoszenia („skarżącym” - *complainer*)
5. oświadczenie „skarżącego”, 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

[17] Zob. § 230
[18] Ford Motor Co. v. Greatdomains.com, Inc., 2001 WL 1176319, 1 (E.D.Mich. 2001), a wcześniej także Gucci America, Inc. v. Hall & Associates, 135 F. Supp. 2d 409 (S.D.N.Y. 2001).
[19] Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997). Odnośnie omówienia niektórych amerykańskich orzeczeń dotyczących odpowiedzialności ISP w świetle CDA i zasady wolności słowa zob. też G. C. Walsh, *Internet Service Provider Liability for Contributory Trademark Infringement After >>Gucci<<*, „Duke Law & Technology Review” 2002 nr 0025
[20] DMCA Tytuł II, Sekcja 202, § 512

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

6. oświadczenie, że składana informacja jest dokładna oraz – pod groźbą kary za krzywoprzysięstwo – oświadczenie, że „skarżący" jest uprawnionym, bądź też jest umocowany do działania w imieniu uprawnionego[21]

Jeśli „skarżący" nie spełni pkt 2, 3 lub 4, wówczas zgłoszenie można zignorować. Jeśli natomiast problemy wystąpią w odniesieniu do pkt 1, 5 lub 6, to należy spróbować skontaktować się ze „skarżącym" w celu otrzymania pozostałych informacji. Wreszcie, w sytuacji gdy zgłoszenie spełnia wszystkie wymagania, należy zawiadomić właściciela strony internetowej o otrzymaniu zawiadomienia i o uniedostępnieniu danych na stronie[22].

Po prawidłowym spełnieniu powyższych czynności ISP zwolniony jest z odpowiedzialności wobec poszkodowanego. Właściciel strony może wnieść jednak swoiste zarzuty (tzw. *counter-notice*), które – aby przyniosły odpowiedni skutek – muszą także spełniać pewne wymogi formalne. Przede wszystkim więc, muszą zawierać:

1. własnoręczny lub cyfrowy podpis właściciela usuniętej lub zablokowanej strony
2. opis materiałów (strony) usuniętych lub zablokowanych
3. oświadczenie, że właściciel pozostając w dobrej wierze, uważa, iż dane zostały uniedostępnione na skutek pomyłki (np. że była zgoda, albo dokonano tego w ramach dozwolonego użytku), albo też, że „skarżący" błędnie zidentyfikował kwestionowany materiał
4. nazwisko i dane teleadresowe umożliwiające kontakt z właścicielem przedmiotowej strony, a także jego zgoda na objęcie jurysdykcją odpowiedniego sądu (zależnie od miejsca zamieszkania).

Jeśli dostawca usług prawidłowo i niezwłocznie poinformował właściciela strony (do której uniemożliwiono dostępu) 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 „skarżącego", z zastrzeżeniem, że strona zostanie ponownie aktywowana po upływie 10 dni roboczych. Po upływie 10 dni od otrzymania zarzutów (nie później jednak niż dni 14),

[21] Pomijam tu część uregulowań, które oczywiście cytowane DMCA zawiera, ale która jest zbyt szczegółowa dla niniejszego opracowania, bądź moim zdaniem nieprzydatna (np. ustanawianie specjalnych „Agentów") – w tym zakresie odsyłam do treści aktu.

[22] Niektórzy autorzy, przygotowywujący np. proceduty dla poszczególnych ISP, zalecają, aby przed samym zablkowaniem strony, umożliwić usługobiorcy dobrowolne wykoananie tej czynności – por. np. „Complying with the Digital Millennium Copyright Act. Responding to Notices of Alleged Infringement", przygotowane dla Uniwersytetu Teksańskiego (http://www.utsystem.edu/OGC/IntellectualProperty/dmcaisp.htm)

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

usługodawca reaktywuje stronę, chyba że otrzyma on zawiadomienie, że „skarżący" wszczął odpowiednie postępowanie, mające na celu wydanie przez sąd nakazu uniemożliwienia dostępu do strony przez ISP.

W ślad za rozwiązaniami przyjętymi w Stanach Zjednoczonych, odpowiednie uregulowania, ograniczające odpowiedzialność pośredników internetowych, starały się przyjąć także inne państwa[23]. Dla naszych rozważań najważniejsze będą jednak jedynie postanowienia Dyrektywy 2000/31/WE[24] (dalej: Dyrektywa) oraz ustawy o świadczeniu usług drogą elektroniczną[25] (dalej: usude lub ustawa). Ponieważ jednak, jak dotychczas oba ww. akty prawne były już wielokrotnie omawiane[26], pragnę w ramach niniejszego – wszak fragmentarycznego przecież – omówienia skupić się na wybranych problemach usude, korespondującymi z przedstawionymi wcześniej zagadnieniami[27].

Przyjrzyjmy się więc dokładnie art. 14 usude, który w ust. 1, mówi, że „[n]ie ponosi odpowiedzialności za przechowywane dane ten, kto (...) **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". Próbując sprecyzować sytuacje, w których mogłoby dojść do zwolnienia ISP z odpowiedzialności, należy, jak widać, rozpocząć od przesłanki braku pozytywnej wiedzy o bezprawnym charakterze danych. I tak, w pierwszej kolejności, należy zauważyć, że z dosłownego brzmienia cytowanego artykułu, mogłoby się wydawać, iż to na usługodawcy ciąży ciężar wykazania niewiedzy, gdyż z takiego faktu to on wywodziłby skutki prawne – tzn. nie ponosiłby odpowiedzialność. Taka konstatacja jest jednak nieprawidłowa, gdyż udowadnianie czegoś czego nie ma, prowadziłoby praktycznie do absurdu, ponadto jednak nie zapominajmy, że wyłączenie odpowiedzialności dotyczy także odpowiedzialności karnej, w której istnieje zasada domniemania niewinności. Nie wydaje się zasadne, aby w tym zakresie inaczej traktować roszczenia oparte na prawie karnym, a inaczej na prawie cywilnym. Tak więc, należy

[23] Trzeba jednak zauważyć, że nie wszystkie, nawet wysoko rozwinięte państwa mają odpowiednie akty prawny. Przykładem braku takich uregulowań jest Kanada, która jednak wypracowała odpowiednie procedury poprzez orzecznictwo – por. m.in. SOCAN v. CAIP, 2002 FCA 166 (May 1, 2002), a także A. Gahtan, *ISPs protected from liability*, July 15, 2002 (http://www.gahtan.com/alan/articles/200207%20ISP%20Liability.htm)

[24] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) z dnia 8 czerwca 2000 r., *Dziennik Urzędowy L 178*

[25] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. z roku 2002, Nr 144, poz. 1204

[26] Zob. m. in. K. Kosmala, *Dyrektywa o handlu elektronicznym i projekt jej implementacji*, dostępne w serwisie prawo.vagla.pl. Por. też P. Podrecki (redakcja), Z. Okoń, P. Litwiński, M. Świerczyński, T. Targosz, M. Smycz, D. Kasprzycki, *Prawo Internetu*, Warszawa 2004, wydanie elektroniczne [w:] LexPolonica Maxima, a także R. Cisek, J. Jezioro, A. Wiebe, *Dobra i usługi informacyjne w obrocie gospodarczym*, Warszawa 2005, wydanie elektroniczne [w:] LexPolonica Maxima, oraz cytowane już prace D. Kota i X. Konarskiego

[27] Pomijam więc zarówno zagadnienie ogólne, jak np. – odmiennie niż w USA – horyzontalny charakter regulacji, tj. zwalniający z odpowiedzialności niezależnie od reżimu odpowiedzialności i niezależnie od rodzaju dokonanego naruszenia, jak też pewne kwestie poboczne, a więc m.in. brak obowiązku stałego monitorowania sieci, co *expressis verbis* zarówno w usude, jak i w Dyrektywie zostało stwierdzone.

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

przyjąć, to osoba kierujące wobec ISP odpowiednie roszczenia, będzie musiała wykazać, iż ten ostatni wiedział o istniejących naruszeniach. Trzeba w tym miejscu podkreślić, że ustawa ogranicza się wyraźnie tylko do braku wiedzy, a więc prawnie irrelewantne, w odniesieniu do ewentualnej odpowiedzialności usługodawcy, pozostaną możliwości zdobycia takiej wiedzy, nawet gdyby mogło to być dokonane przy dołożeniu najmniejszego wysiłku, jak tez nie będzie istotne, czy ISP mógł przewidywać umieszczenie bezprawnych danych na swoim serwerze. Co więcej, ustawa, w przeciwieństwie do Dyrektywy (w zakresie odpowiedzialności cywilnej), oddziela wiedzę od świadomości. Świadomość istnienia naruszeń nie pozwala na gruncie polskiego praw na obciążenie odpowiedzialnością ISP. Jednocześnie usude wskazuje, że pozytywna wiedza zaistnieć musi z chwilą otrzymania urzędowego zawiadomienia lub wiarygodnej informacji. Te dwie sytuacje niewątpliwie wyłączają możliwość zasłaniania się „niewiedzą", jakkolwiek wydaje się, że możliwe jest, iż poszkodowany udowodni w inny sposób, wiedzę ISP o naruszeniach (np. na skutek związków towarzyskich z właścicielem kwestionowanej strony internetowej). Owe inne możliwości powinny być jednak badane bardzo rygorystycznie, a ich moc dowodowa powinna być oceniana przez pryzmat definicji urzędowego zawiadomienia oraz wiarygodnych wiadomości.

Ustawodawca polski, przy jednoczesnym milczeniu na ten temat Dyrektywy, wprowadził pojęcie urzędowego zawiadomienia, co należy ocenić zdecydowanie pozytywnie. Bo choć nie ma definicji legalnej tego pojęcia, to jego rozumienie wydaje się – na pierwszy rzut oka – dość oczywiste, a z pewnością łatwiejsze niż zrozumienie terminu „wiarygodnych wiadomości[28]". Mimo to, warto jednak przyjrzeć się mu bliżej. Zauważmy na wstępie, że w piśmiennictwie, przykładowo podaje się, iż z urzędowym zawiadomieniem będziemy mieli do czynienia „w razie otrzymania odpisu postanowienia zabezpieczającego w sprawie o naruszenie praw autorskich", także nieprawomocnego[29]. Można się domyślać, że zarówno redakcja zastosowana przez ustawodawcę, jak i przyjęte przez komentatorów stanowisko, wynika z brzmienia pkt 45 Preambuły, poprzedzającej Dyrektywę, który brzmi następująco: „[o]graniczenia odpowiedzialności usługodawców będących pośrednikami przewidziane w niniejszej dyrektywie nie mają wpływu na możliwości zakazów sądowych różnych typów; zakazy takie mogą przede wszystkim przybierać formę orzeczeń sądów lub innych organów administracyjnych wymagających, aby usunąć lub zapobiec każdemu naruszeniu prawa, łącznie z usunięciem bezprawnych informacji lub uniemożliwieniem dostępu do nich". Można więc przyjąć, że orzeczenia sądów i innych organów administracji są przykładem urzędowych zawiadomień,

[28] Patrz wyjaśnienia niżej
[29] X. Konarski, *op. cit.,* s. 141

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

jednak takie zachowania nie muszą wcale ograniczać się do formułowania konkretnych zakazów. Mając na uwadze, że urzędowe zawiadomienia zestawione zostały z pojęciem wiarygodnych wiadomości, należy przyjąć, że urzędowym zawiadomieniem będzie oczywiście także informacja pozbawiona określonych nakazów, o ile pochodzić będzie od podmiotu, który możemy zakwalifikować jak urzędowy w raczej szerokim tego słowa znaczeniu. Jeśli chodzi o ten ostatni aspekt, to należy stwierdzić, że z urzędową wiadomością będziemy mieli do czynienia w przypadku zawiadomienia przez sądy, prokuratury, a także przez organy administracji rządowej, samorządowej, policji[30]. Pamiętając o wspomnianym na początku akapitu pozytywnym aspekcie takiego, odmiennego od wspólnotowego, zredagowania art. 14 usude, trzeba dodatkowo podkreślić, że ustawa przewiduje dodatkowe korzyści związane z otrzymaniem urzędowego zawiadomienia, poza samą możliwością jego prawidłowego zdefiniowania i odczytania przez ISP. Otóż w sytuacji, gdy usługodawca otrzyma takie zawiadomienie, nie jest on już zobligowany do powiadamiania usługobiorcy o zamiarze uniemożliwienia dostępu. Takiej możliwości brak , gdy usługodawca otrzyma „tylko" wiarygodną wiadomość.

Tym sposobem przejść trzeba do wyjaśnień dotyczących wiarygodnej wiadomości. Także to pojęcie nie zawiera ustawowej definicji, jednak w odróżnieniu od urzędowego zawiadomienie, rozumienie tego pojecie jest daleko bardziej skomplikowane. X. Konarski przyznaje wprost, że wykładnia tej przesłanki „powodować będzie z pewnością istotne problemy interpretacyjne", dlatego też sam powstrzymuje się niejako od tego zadania, uznając, że „dopiero praktyka sądowa, wypracuje wzorzec prawidłowego postępowania usługodawcy[31]". Otóż wydaje się, że pewne doprecyzowanie omawianego zagadnienia jest jednak nawet nie tyle możliwe, co w braku jakichkolwiek działań ze strony ustawodawcy – konieczne. Spróbujmy więc rozpocząć od wykładni językowej, dzięki czemu zobaczymy, iż słowo wiarygodny, należy rozumieć jako: „godny wiary, zasługujący na zaufanie, nie ulegający wątpliwości, prawdziwy", a także „pewny, autentyczny[32]". O doniosłym i poważnym znaczeniu takiej wiadomości świadczy także zestawienie z pojęciem urzędowego zawiadomienia, dlatego też wiadomość będzie musiała pochodzić od podmiotu, któremu powyżej wymienione cechy możemy przypisać. Niewątpliwie będzie to sam poszkodowany lub osoba działająca w jego imieniu. Wydaje się, że można dopuścić także możliwość uznania za wiarygodną, informacji dostarczonej przez osobę trzecią. Trzeba to jednak

[30] Podobne stanowisko na gruncie art. 818 kodeksu cywilnego przedstawia H. Ciepła [w:] G. Bieniek, H. Ciepła, S. Dmowski, J. Gudowski, K. Kołakowski, M. Sychowicz, T. Wiśniewski, C. Żuławska, *Komentarz do kodeksu cywilnego. Księga trzecia. Zobowiązania. Tom II,* Warszawa 2002, s. 532
[31] X. Konarski*, op. cit.*, s. 141
[32] E. Sobol (red.), *Mały słownik języka polskiego*, Warszawa 1997, s. 1013

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

rozbić z wielką ostrożnością, uwzględniając leksykalne znaczenia słowa wiarygodny[33]. Moim zdaniem za prawidłowy należy uznać też tylko taki przekaz, który będzie skierowany bezpośrednio od osoby uznanej za wiarygodną do usługodawcy. Nie będzie spełniało więc tego kryterium, zaprezentowanie problemu za pomocą środków masowego przekazu.

Warto też podkreślić, że pożądane byłoby, 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, *de facto* nie jest istotne jakie dowody, czy uprawdopodobnienia zawiera w swej treści, gdyż i tak nad całością „przeważa" strona podmiotowa. W szczególności więc, trzeba 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[34]. Warto jeszcze w tym miejscu wskazać na fragment art. 14 ust. 1 lit. a) Dyrektywy, który wspomina o wiedzy „o stanie faktycznym lub okolicznościach, które w sposób **oczywisty** świadczą o tej bezprawności", a także na stanowiska przedstawione na gruncie prawa karnego, gdzie przyjmuje się, iż wiadomość jest wiarygodna „jeśli istnieje **obiektywny dowód** czynu zabronionego, jak też treść wiadomości wzbudza przekonanie, że czyn zabroniony został istotnie popełniony[35]".

Podsumowując, wiadomość, aby została uznana za wiarygodną musi pochodzić od osoby zasługującej na zaufanie (najlepiej samego poszkodowanego), a jednocześnie musi przedstawiać fakt dokonania określonego naruszenia w sposób precyzyjny, czy wręcz pewny. Z pewnością musi to być coś więcej niż uprawdopodobnienie. Należy także przyjąć, że zgłoszenie można badać pod względem wiarygodności także co do jego części, np. uznając, że wskazanie bezprawnego użycia zdjęcia poszkodowanego jest oczywistym naruszeniem prawa do wizerunku, natomiast jednoczesne, ogólne zgłoszenie naruszenia dóbr osobistych już tego wymogu spełniać nie będzie. W tym ostatnim więc wypadku ISP nie będzie zobligowany do zablokowania całej strony, a jedynie usunąć będzie musiał kwestionowane zdjęcie.

---

[33] Będą się tu więc kwalifikowały moim zdaniem wiadomości przekazane przez osoby sprawujące funkcje publiczne, ale przesłane drogą prywatną, a nie urzędową, a także informacje od organizacji, o uznanej renomie, zajmujących się badaniem i monitorowaniem określonego zjawiska (np. odnośnie stron propagujących faszyzm – Stowarzyszenia „Nigdy Więcej").

[34] W szczególności za niewiarygodne należy uznać zawiadomienie o treści typu: „Moje dobra osobiste zostały naruszone na stronie x".

[35] B. Kunicka – Michalska, *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego*, *Komentarz*, Warszawa 2000, s. 154. Opinia ta zaprezentowana została odnośnie art. 240 kodeksu karnego, który również wspomina o wiarygodnej wiadomości

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

Kolejnym problemem pojawiającym się przed *serice provider'em*, jest odpowiedź na pytanie, czy polski ustawodawca uregulował faktycznie procedurę powiadamiania, a jeśli tak, czy zrobił to wyczerpująco i właściwie. Jak to zostało przedstawione w pierwszej części pracy, taka procedura – zwana *notice and take down*[36] - funkcjonuje w USA. Taka procedura została pominięta w ramach prac nad Dyrektywą, a także w późniejszym czasie nie znaleziono powodów, by regulować ją ustawowo, pozostawiając dookreślenie formalności Państwom Członkowskim, z których jedynie Finlandia podjęła się tego zadania[37]. Zamiast tego, Dyrektywa zachęca do ustanawiania właściwych procedur w kodeksach postępowania, opracowywanych przez „stowarzyszenia i organizacje handlowe, zawodowe[38]". Pozostawienie tego poszczególnym krajom, a w efekcie brak istnienia właściwych rozwiązań, wydaje się być w tym wypadku jednak posunięciem niewłaściwym. W szczególności, jak za chwilę będę starał się wykazać, brak takich procedur w polskiej ustawie, stawia ISP w dosyć skomplikowanej sytuacji.

Zaznaczyłem bowiem wcześniej, że usude rozróżnia wyraźnie dwie okoliczności: otrzymania urzędowego zawiadomienia lub otrzymania wiarygodnej wiadomości. W tym pierwszym przypadku, zadanie usługodawcy ogranicza się tylko i wyłącznie do niezwłocznego zablokowania danej strony, dzięki czemu nie ponosi odpowiedzialności ani wobec poszkodowanego, ani wobec właściciela strony. W drugim natomiast wypadku, aby nie odpowiadać wobec usługobiorcy, ISP powinien jeszcze dopełnić aktu staranności, jakim jest zawiadomienie właściciela strony o zamiarze uniemożliwienia do niej dostępu. Pytanie: po co ustawodawca wprowadził takie rozróżnienie? Z pewnością nie po to, aby usługobiorca mógł zabezpieczyć w jakiś sposób swoje dane, czy też uprzedzić swoich „czytelników", że strona będzie niedostępna, gdyż gdyby tak miało być, to nie istnieje przekonywujący argument, żeby nie dawać takiej samej możliwości usługobiorcy, również w przypadku blokowania danych na skutek urzędowego zawiadomienia. Należy więc przyjąć, że ustawodawca nakazał ISP powiadamiać o zamiarze zablokowania strony, aby usługobiorca miał możliwość zakwestionowania, czy też dokładniej podważenia wiarygodności otrzymanego (nieurzędowego) zawiadomienia. Wydaje się to rozwiązaniem sensownym[39], na dodatek zgodnym z procedurą stosowaną na gruncie DMCA. Problem w tym, że usude, nie zawiera, analogicznego do ustawy amerykańskiej, ograniczenia swoistej wymiany zdań pomiędzy poszkodowanym, a usługobiorcą. Innymi słowy, na gruncie aktualnie obowiązującego prawa, praktycznie w nieskończoność może być wymieniana

[36] J. Barta, R. Markiewicz, *op. cit.*
[37] A i tak tylko w zakresie ochrony prawa autorskiego – zob. *First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*, Bruksela 2003, COM(2003) 702 final, s. 14 i n
[38] Art. 16 Dyrektywy oraz pkt 40 jej Preambuły
[39] *Audiatur et altera pars*

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

korespondencja, która z jednej strony będzie wskazywała istnienie naruszenia, a z drugiej je kwestionowała[40]. Taka sytuacja staje się szczególnie niebezpieczna, kiedy powodem zgłoszenia nie będzie naruszenie skonkretyzowanego dobra niematerialnego, dzięki czemu dość łatwo i w sposób pewny można uznać, że doszło do naruszenia prawa wyłącznego, ale gdy poszkodowany będzie zarzucał naruszenie dóbr osobistych, np. poprzez wypowiedź wykraczającą poza dozwoloną krytykę. Wówczas bowiem, argumenty żadnej ze stron prawdopodobnie nie będą na tyle silne, by mogły przeważyć na korzyść wiarygodności popełnienia deliktu lub jej przeczyć, natomiast ISP zostanie postawiony w roli arbitralnego cenzora, który musiałby orzekać o tak drażliwej i trudnej do rozstrzygnięcia kwestii, z którą nawet sądy powszechne niejednokrotnie mają poważny kłopot. Z tych względów należy postulować jednak przyjęcie odpowiednich, powszechnie obowiązujących regulacji, które bądź to wyłączą możliwość usługobiorcy do podważania wiarygodności zawiadomienia (co byłoby rozwiązaniem niezalecanym), bądź, które podobnie jak to czyni DMCA, ograniczą ilość możliwej wymiany poglądów pomiędzy poszkodowanym i właścicielem strony, a usługodawcą (co byłoby najwłaściwsze).

Powszechnie zostało uznane, że polska ustawa o świadczeniu usług drogą elektroniczną pełna jest błędów[41], jednak uczciwie trzeba też przyznać, że w zakresie omawianej w niniejszej pracy problematyki, niejednokrotnie przynosi lepsze rozwiązania, niż jej unijny pierwowzór[42]. Pozytywna ocena, nie jest jednak oceną wzorową. Jak starałem się wykazać, art. 14 usude posiada na tyle istotne luki, że w konsekwencji ISP może znaleźć się w bardzo niebezpiecznej sytuacji, której rozwiązania nie bardzo widać. Niezależnie jednak od postulatu wprowadzenia precyzyjnej procedury notyfikacyjnej odnośnie problemów z *hostingowanymi* stronami, trzeba także podnieść inne uwagi *de lege feredna*. Wśród nich, bardzo ważnym wydaje się konieczność uchwalenia takich uregulowań prawnych, które będą ułatwiały poszkodowanym możliwość zidentyfikowania usługobiorców, naruszających ich prawa. W obecnej sytuacji, poszkodowani często zdecydowani są wszcząć „z góry przegrany" proces przeciwko ISP, byle tylko uzyskać dane anonimowego właściciela strony www, umieszczającego bezprawne treści i dane. Z drugiej strony brak pewności

[40] Należy bowiem przyjąć, że z momentem uzyskania odpowiedzi usługobiorcy, skutecznie podważającej wiarygodność zgłoszenia poszkodowanego, nie można przyjąć, że ISP miał w ogóle do czynienia z zaistnieniem przesłanki zezwalającej na zablokowanie strony. W takim stanie rzeczy wiarygodna wiadomość przecież obiektywnie nie istniała.

[41] Por. m.in. W. Iszkowski, X. Konarski, *Usługi elektroniczne*, „Rzeczpospolita" z dnia 4 marca 2003r. oraz X. Konarski, *op. cit.*, s. 16 i n.

[42] Ta uwaga w szczególności odnosi się do wprowadzenia pojęcia urzędowego zawiadomienia i osiągnięcia tym sposobem większej pewności po stronie ISP. Można się zastanawiać, czy w przyszłości nie należałoby w ogóle odejść od pojęć typu „wiarygodna wiadomość". Por. deklarację wydaną przez OBWE wspólnie z organizacją Reporterzy bez Granic w czerwcu 2005 r., zawierającą 6 zaleceń w celu zagwarantowania swobody wypowiedzi w Internecie. Deklaracja ta powstała jako przyczynek do dyskusji na Światowy Szczyt Społeczeństwa Informacyjnego (Tunis, 16-18 listopada 2005 r.). Jeden z jej punktów brzmi następująco: „techniczny dostawca Internetu nie może być uznawany za odpowiedzialnego za zwykłą transmisję (*conduit*) lub hosting zawartości, **chyba, że odmawia on podporządkowania się decyzji sądu**" (podkr. – moje; podaję za Informacją KRRiTv, o której wspominam w przypisie 9).

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone

co do swojej sytuacji oraz wiedzy o wybraniu prawidłowego rozwiązania sporu po stronie usługodawców, umożliwia niejednokrotnie prowadzenie swoistej polityki perswazyjnej[43], mającej na celu zablokowanie kwestionowanej strony, bez możliwości całościowego i należytego oglądu problemu (a więc *de facto* pozbawiającej domniemanego naruszyciela prawa do swojej obrony). Obecnie, mając na uwadze takie zagrożenia i niejasności, możliwe jest tylko stosowanie w praktyce raczej rygorystycznego rozumienia „wiarygodności" zawiadomienia. Można też sugerować, że oprócz zaprezentowanej wykładni tego słowa, nie jest wykluczone (a zatem powinno zostać uznane za prawidłowe) żądanie przez ISP od zgłaszającego konkretnych informacji, analogicznych do tych, które nakazuje stosować DMCA[44]. Natomiast ustalenie samej procedury zgłaszania musi koniecznie zostać ustalone jak najszybciej, jeśli nie przez ustawodawcę, to chociaż w postaci jakiegoś kodeksu przyjętego powszechnie przez największych polskich administratorów, udostępniających serwery w ramach usług *hostingowych*.

[43] Zob. P. Waglowski, *Treści antysemickie na serwerze neostrady*, http://prawo.vagla.pl/node/6212 z dnia 25 kwietnia 2006r. O wywieraniu presji przez (prawdziwie lub domniemanie) poszkodowanych, także tego samego autora, *Presja biznesu na ISP*, http://prawo.vagla.pl/node/1922 z dnia 20 grudnia 2002r.
[44] Patrz powyżej, s. 4 i przytoczone tam pkt 1 do 6

Prawa autorskie © :: CBKE :: Wszystkie prawa zastrzeżone