CBKE
e-BIULETYN

Odpowiedzialności dostawcy usług internetowych

mgr Aleksandra Kuczerawy

absolwentka Uniwersytetu Wrocławskiego

Odpowiedzialność dostawców usług internetowych jest problemem, wzbudzającym co raz większe zainteresowanie. Używanie sieci w sposób naruszający porządek prawny rodzi pytanie o podmiot odpowiedzialny. Trzeba mieć bowiem na uwadze fakt, iż kontrola treści umieszczanych w Internecie jest utrudniona, co spowodowane jest jej ogromną ilością. Nie napotykając na ograniczenia w postaci granic państwowych, użytkownicy Internetu mogą cieszyć się niemalże nieograniczoną swobodą, jako że ich działania nie są, w większości przypadków, krępowane prawami określonych państw. Wynika to z braku unifikacji prawa, czego efektem jest możliwość znalezienia państwa, którego prawo nie będzie klasyfikowało danych treści jako bezprawne. Prowadzi to do wybierania przez użytkowników serwerów umieszczonych w krajach, w których ich działania będą akceptowane. Oczywiście, równie często miejsce ma umieszczanie treści o charakterze bezprawnym na serwerach w krajach, gdzie ewidentnie uznawane są one za naruszające porządek prawny. W obu tych sytuacjach istotnym zagadnieniem jest kwestia, w jakim stopniu za zapewnienie dostępu do takich informacji odpowiedzialny powinien być dostawca usługi internetowej. Przed ustaleniem pewnych ogólnych zasad oraz stworzeniem konkretnych regulacji do zagadnienia tego często stosowano przepisy prawa prasowego, dostawcę usług stawiając na równi z wydawcą. Rozwój nauki dotyczącej prawnych aspektów komunikacji elektronicznej pozwolił na stworzenie odpowiednich norm prawnych, które powinny ułatwić rozwiązanie tego problemu.

Dostawca usług internetowych (*Internet Service Provider, ISP*), jest jednym z podmiotów pośredniczących w dostępie do treści (*intermediary service providers*). Zauważyć należy, iż pojęcie podmiotów pośredniczących w dostępie do treści jest szersze od terminu dostawcy usług internetowych. Do kręgu dostawców pośredniczących w dostępie do treści zalicza się trzy grupy

usługodawców, to znaczy: dostawców sieci (*network providers*), dostawców dostępu do sieci (*access providers*) oraz dostawców usług (*service providers*). Świadczą oni odmienne od siebie usługi, a także odróżnia ich techniczna możliwość reagowania na informacje o naruszeniach praw osób trzecich, a co za tym idzie, różny jest zakres ich odpowiedzialności. W niniejszej pracy omówiona zostanie specyfika odpowiedzialności dostawców usług internetowych. Do świadczonych przez nich usług zalicza się na przykład: *hosting*, usługę dostępu do serwera ftp, czy usługę poczty elektronicznej. Usługa *hostingu*, polega na samoistnym, nieograniczonym w czasie przechowywaniu danych dostarczanych przez dostawców treści (*content providerów*), poprzez udostępnianie im miejsca na dysku na potrzeby na przykład: stron WWW, BBS, lub grup dyskusyjnych. Usługodawcy świadczący tę usługę są najbardziej narażeni na odpowiedzialność za naruszenie praw osób trzecich, jako że, zajmują się oni „prezentowaniem" światu treści, których dobór zależy od korzystających z ich usług dostawców treści. Mogą oni przechowywać materiały dostarczone przez jednego usługodawcę, co ma miejsce, gdy utrzymuje na swoim serwerze jego stronę WWW, lub materiały dostarczane przez wielu usługodawców, na przykład w ramach grup dyskusyjnych.[1] To do nich zwracać będą się osoby trzecie, których prawa zostały naruszone, po pierwsze, dlatego, że łatwiej będzie ich zidentyfikować, a po drugie, będzie to wynikało z większej możliwości uzyskania odszkodowania, co w literaturze nazywane jest „sięganiem do głębszej kieszeni".[2]

Warto zwrócić uwagę, iż zasady dotyczące odpowiedzialności, nie tylko dostawców usługi *hostingu*, ale wszystkich podmiotów pośredniczących w dostępie do treści, zostały uregulowane w dyrektywie o handlu elektronicznym[3] (dalej d.h.e.) oraz w ustawie z 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (dalej u.s.u.d.e.) według modelu horyzontalnego. Oznacza to, że wyłączenie odpowiedzialności dotyczy zarówno odpowiedzialności cywilnej, karnej, jak i administracyjnej.[4] Gdyby więc, przepisy określonego prawa materialnego stanowiły o odpowiedzialności usługodawcy, to jest on od niej zwolniony na podstawie przepisów dotyczących świadczonej przez niego usługi, oczywiście przy spełnieniu warunków wymienionych przez dany przepis.[5] Taki sposób regulacji jest korzystny dla pośredniczących dostawców usług, ponieważ daje im pewność prawną, której nie gwarantowałby wertykalny model regulacji. Przeciwnicy horyzontalnego modelu zarzucali mu, że ustanawia poziom odpowiedzialności zbyt

[1] J. Gołaczyński (red.), [w:] W. Dubis, J. Jacyszyn, M. Leśniak, M. Podleś, M. Skory, B. Sołtys, Umowy elektroniczne w obrocie gospodarczym, Warszawa 2005, s.19
[2] R. Julia – Barcelo, Liability for on-line intermediaries: A European Persepctive, http://www.droit.fundp.ac.be/Textes/online.pdf (odwiedzana ostatnio 1.4.2006 r.), s. 4
[3] dyrektywa nr 2000/31/WE w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, w szczególności handlu elektronicznego
[4] K. Kosmala, Dyrektywa o handlu elektronicznym i projekt jej implementacji, artykuł dostępny na stronie www.vagla.pl (odwiedzana ostatnio 1.4.2006 r.), s. 6
[5] X. Konarski, Komentarz do ustawy o świadczeniu usług droga elektroniczną, Warszawa 2004, s. 126

nisko.[6] Model wertykalny natomiast, przyjęty został, w pewnym zakresie, w USA w ustawie z 1998r. *Digital Millenium Copyright Act* (*DMCA*) dotyczącej odpowiedzialności usługodawców za naruszenia praw autorskich w związku z rozpowszechnianiem utworów w sieciach.[7]

Usługa *hostingu* i wyłączenia od odpowiedzialności przy jej świadczeniu uregulowana została w art. 14 w dyrektywie o handlu elektronicznym oraz w ustawie o świadczeniu usług drogą elektroniczną. Regulacje zawarte w tych przepisach są do siebie bardzo podobne, jednak występują w nich również dość znaczące różnice, o czym dalej.

W ty miejscu chciałabym zwrócić uwagę na fakt, iż przedstawione wyłączenia od odpowiedzialności, nie mają zastosowania w przypadku określonym w ust. 4 art. 14 u.s.u.d.e., to znaczy, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów ustawy z 15 grudnia 2000r. o ochronie konkurencji i konsumentów. Uznaje się, iż w przepisie tym chodzi o kontrolę nad czynnościami podejmowanymi przez dostawcę treści, nie zaś o kontrolę nad transmitowaną lub przechowywaną informacją. Nie chodzi również, jak mogłoby sugerować odwołanie do ustawy o ochronie konkurencji i konsumentów, o kontrolę kapitałową.[8]

Odpowiedzialność dostawcy usług wobec osób trzecich

Według art. 14 ust. 1 ustawy o świadczeniu usług drogą elektroniczną nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi do nich dostęp. Przepis ten ma na celu wyłączenie odpowiedzialności dostawcy usługi *hostingu*, który nie mając obowiązku monitorowania przechowywanych danych (art. 15 u.s.u.d.e.), może nieświadomie udostępniać treści o charakterze bezprawnym. Może to być zarówno dziecięca pornografia, propagowanie faszystowskiego lub innego totalitarnego ustroju lub nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych bądź wyznaniowych, jak i informacje naruszające prawa osób trzecich, w szczególności prawa autorskie i dobra osobiste. Jak to już zostało zauważone,

[6] R. Julia – Barcelo, *op. cit*., s.14
[7] X. Konarski, *op. cit*., s. 125
[8] *Ibidem*, s.145

horyzontalny sposób uregulowania odpowiedzialności pozwala na skorzystanie z wyłączenia przewidzianego w tym przepisie zarówno w przypadku odpowiedzialności karnej, jak i cywilnej[9].

Odpowiedzialność wobec osoby trzeciej, której prawa mogły zostać naruszone poprzez treść danych przechowywanych przez usługodawcę, a umieszczonych w sieci przez usługobiorcę, uznać należy za odpowiedzialność deliktową i oceniać na podstawie art. 415 i nast. KC. Według ogólnej zasady odpowiedzialności wyrażonej w art. 415 KC, niezbędnymi przesłankami koniecznymi dla powstania odpowiedzialności odszkodowawczej są: szkoda – którą w tym wypadku jest naruszenie praw osoby trzeciej, zdarzenie, z którym ustawa łączy obowiązek odszkodowawczy oraz zachodzący między nimi związek przyczynowy. Jak jest przyjęte, podstawową zasadą odpowiedzialności z tytułu czynów niedozwolonych jest zasada winy. Należy mieć na uwadze, iż „z punktu widzenia odpowiedzialności cywilnej każdy stopień winy uzasadnia nałożenie na sprawcę szkody obowiązku jej naprawienia".[10] Dokonując oceny, czy w konkretnym stanie faktycznym, dostawcy usługi *hostingu* można przypisać winę, trzeba pamiętać o treści art. 15 u.s.u.d.e., zwalniającego usługodawców z obowiązku monitorowania przechowywanych danych. Dzięki tej regulacji wyłączona została możliwość uznania działania usługodawcy za zawinione, jednak tylko do momentu uzyskania przez niego informacji o bezprawnym charakterze przechowywanych danych.[11] Natomiast po otrzymaniu takiej informacji, w formie urzędowego zawiadomienia lub wiarygodnej wiadomości, i zignorowaniu jej, spełniona zostaje przesłanka odpowiedzialności, jaką jest wina, która najczęściej przyjmowałaby postać niedbalstwa, choć nie można wykluczyć wystąpienia winy umyślnej. Prowadziłoby to do sytuacji, gdy nie można stwierdzić braku wiedzy usługodawcy o bezprawności przechowywanej informacji lub działalności z nimi związanej, co z kolei jest przesłanką pozwalającą na skuteczne wyłączenie odpowiedzialności. Odrębną kwestią jest forma powiadomienia usługodawcy o bezprawnym charakterze przechowywanych przez niego informacji. W zasadzie, nie budzi wątpliwości informacja będąca urzędowym zawiadomieniem. Za przykład takowego podawany jest odpis postanowienia zabezpieczającego w sprawie o naruszenie praw autorskich. Ewentualne pytanie brzmieć może, czy usługodawca powinien czekać, z zablokowaniem dostępu do informacji, na uprawomocnienie się orzeczeń lub decyzji. Uznawane jest, że może on uniemożliwić dostęp jeszcze przed ich uprawomocnieniem się.[12] Więcej problemów powstaje w związku z przesłanką uzyskania wiarygodnej wiadomości. Czy wystarczy wiadomość stwierdzająca, iż naruszone zostały czyjeś prawa, czy raczej powiadomienie takie powinno zawierać więcej informacji dotyczących

[9] P. Lindholm, F. A. Maennel, Directive on Electronic Commerce (2000/31/EC), Computer und Recht International, Nr 3/2000, s. 69
[10] Z. Banaszczyk [w:] K. Pietrzykowski (red.) Kodeks cywilny. Tom 1.Komentarz, Warszawa 1998, s.991
[11] X. Konarski, *op. cit*., s. 140
[12] *Ibidem*, s. 141

naruszonych praw, określając konkretnie ich rodzaj i podając dokładny adres strony, na której bezprawne dane się znajdują. Niewątpliwie pomocna byłaby regulacja procedury notyfikacji o bezprawności *hostowanych* informacji, precyzująca formę, w jakiej dostawca usługi powinien być powiadamiany o bezprawności przechowywanych danych. Zapewne znacznie poprawiłoby to sytuacje usługodawcy, który nie musiałby sam dokonywać oceny, czy dane powiadomienie jest informacją wiarygodną, co może sprawić trudności, zwłaszcza w przypadku, gdy umieszczający dane w sieci przedstawi wiarygodne dowody na to, że informacje te nie mają charakteru bezprawnego. Zaznaczyć trzeba, iż dyrektywa o handlu elektronicznym, również nie zawiera uregulowania tej kwestii, jest ona natomiast ujęta we wspomnianej już amerykańskiej ustawie DMCA. Procedura ta nazwana jest „*notice and take down*" i dokładnie określa, jakie czynności mają być wykonane, aby doprowadzić do zablokowania dostępu do informacji naruszających prawo. Przyjmuje się, iż uregulowanie tej kwestii znacznie upraszcza cały proces czynności koniecznych do wykonania, gdy w grę wchodzi ewentualne naruszenie prawa przy świadczeniu usługi *hostingu*. Na pewno pozwala to na skrócenie czasu koniecznego do podjęcia przez usługodawcę stosownych działań, co jest ważne, ponieważ osobom, których prawa zostały naruszone, zależeć będzie, na ogół, na niezwłocznym usunięciu do nich dostępu.[13]

Uregulowanie zawarte w art. 14 ust. 1 u.s.u.d.e. na pierwszy rzut oka wydawać się może takie samo jak zawarte w dyrektywie o handlu elektronicznym, jednak polska wersja tego przepisu zawiera pewne, dość istotne różnice. W d.h.e. przewidziano odrębne przesłanki odpowiedzialności karnej i cywilnej. Elementem, od którego zależy rodzaj ponoszonej odpowiedzialności jest wiedza o bezprawnej działalności usługobiorcy. W przypadku posiadania faktycznej wiedzy na ten temat istnieje możliwość poniesienia przez usługodawcę odpowiedzialności karnej. Natomiast pociągnięcie go do odpowiedzialności cywilnej możliwe jest, gdy był on świadomy faktów i okoliczności, które w oczywisty sposób świadczą o bezprawności działania. W u.s.u.d.e. art. 14 odnosi się do wszystkich rodzajów odpowiedzialności, co znaczy, że ustanowione zostały takie same zasady wyłączenia odpowiedzialności karnej i cywilnej. Oznacza to, że złagodzone zostały zasady wyłączenia odpowiedzialności cywilnej, ponieważ, według ustawy, wymagane jest do tego posiadanie przez usługodawcę takiej samej pozytywnej wiedzy, jak w przypadku odpowiedzialności karnej. Różnica ta nie budzi jednak zastrzeżeń, jako że poziom ochrony ustanowiony przez dyrektywę jest maksymalny, co znaczy, że wprowadzenie surowszych kryteriów odpowiedzialności nie jest dopuszczalne, natomiast nie ma przeciwwskazań do ich złagodzenia.[14]

[13] P. Podrecki (red.),[w:] Z. Okoń, P. Litwiński, M. Świerczyński, T. Targosz, M. Smycz, D. Kasprzycki, Prawo Internetu, Warszawa 2004, s. 212
[14] *Ibidem*, s. 212 i nast.

Podsumowując rozważania na temat odpowiedzialności dostawcy usługi *hostingu* wobec osób trzecich, która uregulowana została w art. 14 ust. 1 u.s.u.d.e., należy zauważyć, iż dotyczące tej kwestii przepisy ustawy o świadczeniu usług drogą elektroniczną i dyrektywy o handlu elektronicznym różnią się od siebie, jednak w sposób nie budzący większych sprzeciwów. Istotniejszym problemem, który da się zaobserwować, jest nieprecyzyjne określenie sposobu powzięcia informacji przez usługodawcę o bezprawnym charakterze przechowywanych danych, a właściwie forma nazwana „wiarygodną wiadomością". Pojęcie takie nie występuje w dyrektywie, która mówi tylko o powzięciu przez usługodawcę wiedzy lub świadomości, nie precyzując również, jak miałoby się to odbyć. W związku z brakiem odpowiedniej procedury, podobnej do tej, jaką wprowadzono do porządku prawnego w USA, uznać należy, że wzorzec prawidłowego postępowania usługodawcy w takiej sytuacji wypracowany zostanie dopiero w praktyce sądowej, na którą trzeba będzie jeszcze poczekać, ponieważ jak do tej pory, sądy polskie nie orzekały w takich sprawach.

Odpowiedzialność usługodawcy wobec usługobiorcy.

Odpowiedzialność dostawcy usługi wobec jej odbiorcy uregulowana została w ust. 2 i 3 art. 14 u.s.u.d.e. Według pierwszego z nich, usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił do nich dostęp, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych. W ust. 3 uregulowano natomiast odpowiedzialność usługodawcy w przypadku otrzymania przez niego wiarygodnej wiadomości o bezprawności przechowywanych danych dostarczonych przez usługobiorcę. Po uniemożliwieniu dostępu do takich informacji, nie odpowiada on względem usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych, pod warunkiem, że niezwłocznie powiadomił usługobiorcę o zamiarze uniemożliwienia do nich dostępu. Warto zaznaczyć, że regulacji dotyczącej tej kwestii nie ma w dyrektywie o handlu elektronicznym, co było przedmiotem zarzutów stawianych jej twórcom. Prawdopodobnie, pod wpływem tej krytyki polski ustawodawca zdecydował się na wprowadzenie do u.s.u.d.e. wyłączenia odpowiedzialności usługodawcy względem usługobiorcy.[15] Potrzeba istnienia takiej regulacji wynika z możliwości poniesienia szkody przez usługobiorcę w związku z usunięciem zamieszczonych przez niego

[15] X. Konarski, *op. cit*., s. 142

danych. Oczywiście odpowiedzialność usługodawcy dopuszczalna jest tylko w przypadku, gdy usunięte przez niego informacje okazały się nie mieć charakteru bezprawnego. Nie można przecież wykluczyć sytuacji, w której osoba trzecia działając na szkodę usługobiorcy składa nieprawdziwe zawiadomienie o naruszeniu przez informacje swoich praw, doprowadzając w ten sposób do ich zablokowania przez usługodawcę, który chcąc uniknąć odpowiedzialności względem osoby trzeciej uniemożliwiłby dostęp do takich informacji. Gdyby więc, okazało się, że powiadomienie o bezprawności nie było prawdziwe, a usługobiorca poniósł szkodę w związku z usunięciem jego danych, mógłby domagać się od usługodawcy odszkodowania z tytułu niewykonania lub nienależytego wykonania łączącej ich umowy. Odpowiedzialność taka jest odpowiedzialnością kontraktową, jako że usługodawcę i usługobiorcę łączy zawarta umowa o przechowywanie danych.[16] Do jej przesłanek, zgodnie z art. 471 i nast. KC, należą: szkoda – w znaczeniu uszczerbku majątkowego, fakt niewykonania lub nienależytego wykonania zobowiązania przez dłużnika oraz łączący te dwie okoliczności związek przyczynowy. Zgodnie z art. 361 §1 i 2 K.C. dłużnik odpowiada wobec wierzyciela za szkodę, która jest normalnym następstwem niewykonania lub nienależytego wykonania zobowiązania. Ponadto, niewykonanie lub nienależyte wykonanie zobowiązania musi być następstwem okoliczności, za które dłużnik odpowiada.[17] W omawianym przypadku uznać należy, iż usługodawca odpowiada za swoje świadome działanie, jakim jest usunięcie dostępu do informacji. Również w przypadku tej odpowiedzialności jej zasadą naczelną jest zasada winy. W przepisie art. 14 ust. 2 i 3 u.s.u.d.e. o winie można mówić tylko w przypadku ust. 3, od momentu niespełnienia przez usługodawcę warunku niezwłocznego zawiadomienia usługobiorcy o zamiarze uniemożliwienia do nich dostępu. W ust. 2 tego artykułu, gdy usługodawca otrzymuje urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych, jego odpowiedzialność jest wyłączona bezwarunkowo. Oznacza to, że zasady wyłączenia odpowiedzialności zostały odmiennie określone dla przypadków, gdy dostęp do informacji został uniemożliwiony na skutek uzyskania przez usługodawcę urzędowego zawiadomienia o jej bezprawnym charakterze (art. 14 ust. 2) oraz gdy stało się to na skutek otrzymania przez usługodawcę wiarygodnej wiadomości (art. 14 ust.3).[18]

W sytuacji otrzymania przez usługodawcę urzędowego zawiadomienia o bezprawności przechowywanych danych i po ich zablokowaniu, dostawca usługi *hostingu* zwolniony jest z odpowiedzialności względem odbiorcy tej usługi, mimo, że strony te wiąże umowa

[16] B. Sołtys, M. Podleś, [w:] J. Gołaczyński (red.), W. Dubis, J. Jacyszyn, M. Leśniak, M. Podleś, M. Skory, B. Sołtys, Umowy elektroniczne w obrocie gospodarczym, Warszawa 2005., s. 166 - 175
[17] W. Czachórski, Zobowiązania, Warszawa 2003, s. 324 i nast.
[18] X. Konarski, *op. cit*., s. 143

o przechowywaniu informacjo dostarczanych przez usługobiorcę. Przepis ten nie wymaga, aby usługodawca powiadamiał usługobiorcę o zamiarze zablokowania jego danych.

Mniej jasna regulacja dotyczy otrzymania przez usługodawcę wiarygodnej wiadomości o bezprawnym charakterze danych. W celu wyłączenia odpowiedzialności konieczne jest niezwłoczne poinformowanie usługobiorcy o zamiarze zablokowania jego danych, co, jak można wnioskować z treści tego przepisu, powinno nastąpić przed uniemożliwieniem dostępu do danych. Wątpliwości może budzić kwestia, czy dostawca ma obowiązek czekać w takim przypadku na reakcję ze strony usługobiorcy, a jeśli tak, to jak długo. Nie wydaje się to konieczne, chociaż odpowiedź otrzymana od usługobiorcy nie może pozostać bez znaczenia, nie można mu bowiem odmówić prawa do ustosunkowania się do zarzutów umieszczenia w sieci informacji naruszającej porządek prawny. Słusznie uważa się, iż w powiadomieniu o zamiarze usunięcia danych powinna zostać podana tego przyczyna, co znaczyć może podanie treści wiarygodnej informacji. Nie wydaje się natomiast wystarczające samo poinformowanie o uniemożliwieniu dostępu do danych. Usługobiorca, którego dane mają zostać zablokowane powinien mieć możliwość obrony i wykazania, iż informacje umieszczane przez niego w sieci nie mają charakteru bezprawnych. Może on przecież przedstawić dowody świadczące o tym, że treści te są całkowicie legalne i równocześnie zażądać odblokowania dostępu do danych. W sytuacji takiej, usługodawca znalazłby się w niewątpliwie kłopotliwej sytuacji, w której musiałby dokonać oceny, która z informacji, pochodząca od powiadamiającej osoby trzeciej lub od usługobiorcy, jest bardziej wiarygodna. Osądzając to, usługodawca musi przecież pamiętać, że może być narażony na odpowiedzialność zarówno ze strony osoby trzeciej – deliktową, jak i ze strony usługobiorcy – kontraktową. W uzasadnieniu do projektu ustawy stwierdzone w tej kwestii zostało, iż „ usługodawca mając świadomość potencjalnej bezprawności udostępnianej informacji, powinien starannie rozważyć zasadność tego żądania”[19]. Prowadzi to do zarzucenia przedstawionej regulacji charakteru iluzoryczności.

Zaprezentowane argumenty wydają się wzmacniać przedstawione już stanowiska, na temat potrzeby uregulowania procedury, której wykonanie znacznie uprościłoby sytuacje usługodawców zwalniając ich z roli sędziego w tych, niejasnych przecież, przypadkach. Jeszcze raz przywołam w tym miejscu rozwiązanie przyjęte przez amerykańską ustawę DMCA. Procedura „*notice and take down*”, o której już była mowa, ma swoją odpowiedniczkę dotyczącą czynności ponownego umożliwiania lub odblokowywania dostępu do danych. Stosowanie uzupełniającej procedury „*put back*” nie tylko dokładnie wskazuje dostawcom usług *hostingu* jak mają się zachować w danej sytuacji, znacznie ułatwiając im pracę, ale przede wszystkim pozwala

[19] *Ibidem*, s.144

na zwolnienie usługodawcy z odpowiedzialności względem obu stron. Mając na uwadze, iż zarówno polski, jak i wspólnotowy ustawodawca często czerpie pomysły z amerykańskich uregulowań dotyczących elektronicznej wymiany danych, warto zwrócić uwagę na rozwiązanie zastosowane w kwestii zwolnienia dostawcy usługi *hostingu* od odpowiedzialności, mając nadzieje, że sytuacja usługodawców europejskich spotka się z podobnym udogodnieniem.[20]

Wnioski

Na zakończenie chciałam przedstawić pewne zagadnienia związane z omówionym tematem.

W literaturze światowej podkreślane są często zalety procedury „zawiadomienia i usuwania informacji" uregulowanej dokładnie w § 512(c)(3) *Digital Millenium Copyright Act*. Wprawdzie ustawa ta dotyczy tylko praw autorskich, jednak nie ma wątpliwości, iż procedura zawiadamiania może mieć zastosowanie niezależnie od rodzaju naruszanych praw. Przeważa pogląd, iż obowiązek usunięcia lub zablokowania dostępu do informacji może skutecznie powstać jedynie w przypadku spełnienia przez zawiadomienie określonych wymogów formalnych oraz dotyczących zawartości. Od dostawcy usługi internetowej, świadczącego usługę *hostingu*, wymaga się, aby określił on osobę wyznaczoną do odbierania zawiadomień o danych naruszających porządek prawny. Do podstawowych informacji, które muszą zostać zawarte w takim zawiadomieniu, aby wywarło ono pożądany skutek należy, po pierwsze podpisanie zawiadomienia przez osobę je składającą. Musi ono podawać dokładnie, do jakiego utworu prawa zostały naruszone, stosując procedurę do innych sytuacji, można to zastąpić wymaganiem sprecyzowania, jakiego rodzaju prawo zostało naruszone. Konieczne jest również podanie dokładnej lokalizacji informacji bezprawnej, co ma pozwolić na bezproblemowe odnalezienie jej w systemie usługodawcy. Powinno także zawierać dane osoby zawiadamiającej, w celu umożliwienia kontaktu z nią. Ciekawym wymaganiem jest to, aby w powiadomieniu zawarte zostało oświadczenie, stwierdzające, iż osoba zawiadamiająca czyni to w dobrej wierze. Jeśli powyższe wymagania nie zostaną spełnione, uważa się, że usługodawca nie posiada pozytywnej wiedzy o bezprawności przechowywanych przez siebie informacji, ani nie jest świadomy faktów lub okoliczności, z których widoczna jest bezprawna działalność lub informacja. Stanowisko to zostało złagodzone w taki sposób, iż jeśli nie spełnione zostały wymagania formalne, ale treść naruszonego prawa jest znana oraz możliwy jest kontakt z osoba zawiadamiającą, uznawane jest, iż usługodawca nie

[20] *Ibidem*, s.138 - 146

posiadał pozytywnej wiedzy, pod warunkiem, że będzie działał odpowiednio w celu nawiązania kontaktu z osobą zawiadamiającą lub podejmie inne stosowne środki w celu uzupełnienia braków formalnych. Ustawa DMCA stanowi również, że umyślne powiadomienie niezgodne z prawdą skutkuje odpowiedzialnością odszkodowawczą nałożona na zawiadamiającego.[21] Jest regulacja jak najbardziej pożądana, a brak takowej uważany jest za niedociągnięcie polskiej ustawy. Może przecież dość do sytuacji, gdy osoba zawiadamiająca będzie świadomie dążyła do narażenia usługobiorcy na szkodę wywołaną usunięciem z sieci treści, do czego dojdzie na skutek świadomego nieprawdziwego powiadomienia. Uznaje się, iż w takim przypadku odpowiedzialność rozpatrywać trzeba na zasadach ogólnych, ze szczególnym uwzględnieniem art. 415 i nast. KC.[22]

Drugą procedurą zawartą w amerykańskiej ustawie DMCA, na którą warto zwrócić uwagę, jest ta, dotycząca przywracania lub odblokowywania dostępu do informacji, które okazały się nie być bezprawnymi. Procedura „*put back*" przewiduje, iż przede wszystkim dostawca usługi musi poinformować dostawcę treści o usunięciu lub zablokowaniu jego danych. Norma zawarta w § 512 (g)(3) daje usługobiorcy możliwość przeciwdziałania przez złożenie powiadomienia o tym, że jego dane nie są bezprawne. Powiadomienie takie musi spełnić takie same warunki, jak to opisane wcześniej. Następnie dostawca usługi musi poinformować nadawcę pierwszego powiadomienia o złożonym „przeciw-powiadomieniu". Po dokonaniu tego powinien z powrotem udostępnić lub odblokować dostęp do spornej treści w terminie nie krótszym niż 10 dni urzędowych, i nie dłuższym niż 14 dni urzędowych liczonych od otrzymania drugiego powiadomienia, chyba że wyznaczona do odbierania tych informacji osoba wcześniej zostanie zawiadomiona o wystąpieniu osoby powiadamiającej o bezprawności informacji do sądu o nakaz powstrzymania się od bezprawnego działania. W momencie spełnienia tych warunków przez usługodawcę, uwalnia się on od odpowiedzialności względem obu stron.[23]

Procedura taka, oprócz niewątpliwej zalety, jaką jest zwolnienie usługodawcy od odpowiedzialności, jest korzystna również dla osób, które posiadają informacje na temat bezprawnych treści umieszczonych w sieci i pragną doprowadzić do ich usunięcia lub zablokowania. Mając tak sprecyzowane informacje na temat sposobu, w jaki ma odbywać się powiadamianie, w zasadzie, nie powinno dość do zaistnienia sytuacji, gdy osoba, która natrafiła w sieci na bezprawne informacje, nie wie co zrobić. Oczywiście, należy zakładać, iż w krajach, w których procedura taka nie została opisana, powiadomienie powinno wyglądać w podobny sposób. Mając jednak na uwadze liczbę użytkowników Internetu, myślę że nie jest korzystne

[21] U. Sieber, Law, Information and Information Technology, (red.) E. Lederman, R. Shapira, The Hague/ London/ New York 2001., s. 258
[22] X. Konarski, *op. cit.*, s. 145
[23] U. Sieber, *op. cit.*, s. 258

pozostawianie ich w niepewności dotyczącej działań koniecznych do podjęcia w celu usunięcia lub zablokowania treści o charakterze bezprawnym. Zaznaczyć trzeba, że w pewnych kategoriach treści bezprawnych procedura usuwania ich z sieci jest bardzo uproszczona i polega tylko na zawiadomieniu odpowiedniego organu, który niezwłocznie blokuje taką informację. Dotyczy to w szczególności dziecięcej pornografii, w walce, z którą dostrzec można wyjątkowo dobrze zintegrowane działania na szczeblu międzynarodowym, co oczywiście jest jak najbardziej pożądane. Aby jak najsprawniej odbywało się blokowanie dostępu do treści o takim charakterze w wielu państwach tworzone są specjalne „gorące linie", których działalność polega na przyjmowaniu zawiadomień, na które reaguje się niezwłocznie.[24] Bardzo często organizowane są one przez zrzeszenia dostawców usług, ale również istnieją linie o charakterze prywatnym, jednak niezależnie od statusu, większość z nich współpracuje z policją. Na gruncie europejskim powstała idea zharmonizowania i skoordynowania działań owych „gorących linii", czego podjęła się Gorąca Linia Zrzeszonych Europejskich Dostawców Usług Internetowych[25] (INHOPE).[26]

W przypadku naruszeń innych praw, determinacja w walce z nimi w sposób skoordynowany na szczeblu międzynarodowym nie jest już tak silna. Prowadzi to do sytuacji spotykanej obecnie dość często, która polega na tym, że dostawcy zawartości mając świadomość, że ich działalność nie jest zgodna z prawem, korzystają z usług dostawców mających siedziby poza Unią Europejską, zamieszczając swoje strony WWW na serwerach spoza Europy. Prowadzi to do sytuacji, gdy ogólnie wiadomo jest o stronach naruszających, na przykład, czyjeś dobra osobiste poprzez podawanie danych osobowych i wizerunków tych osób, jednak z uwagi na fakt, iż są one umieszczane na serwerach w USA, zablokowanie ich nie jest już takie proste.[27] Oczywiście możliwe jest podejmowanie działań w celu usunięcia takich stron z sieci, jednak w większości przypadków będzie to wymagało bardziej skomplikowanych czynności, co sprawi, iż nie będzie to proste do wykonania przez „zwykłych" użytkowników sieci.

Mając na uwadze zaprezentowane w pracy zagadnienia, należy stwierdzić, iż ustawodawstwo polskie, a także zharmonizowane ustawodawstwo unijne zapewniające współpracę krajów Wspólnoty zasługują na uznanie, jednak nie są regulacjami wystarczającymi do zapewnienia funkcjonowania „czystego" Internetu. Rzucająca się w oczy jest prostota, z jaką dostawcy treści, pragnący umieścić w sieci informacje naruszające czyjeś prawa, mogą ominąć skonstruowane przepisy. W tym momencie brak granic w Internecie, co przecież jest ogromną jego

[24] „Meldepunkt Kinderporno ob Internet" w Holandii, „Netz gegen Kinderporno" w Niemczech, The Internet Watch Foundation w Wielkiej Brytanii, the National Center of Missing and Exploited Children w USA.
[25] Internet Hotline Providers In Europe Association, http://www.europa.eu.int/ISPO/iap/projects/inhope.html
[26] U. Sieber, *op. cit.*, s. 280 i nast.
[27] Pewne utrudnienia sprawia również częste „zasłanianie się" Pierwszą Poprawką do Konstytucji USA mówiąca o wolności słowa, której szerokie stosowanie pozwala na swobodne funkcjonowanie na serwerach amerykańskich stron np.: KuKluxKlanu.

zaletą, może być postrzegane jako główne utrudnienie. Pamiętać należy także, iż w tym temacie nie jest trudno zbliżyć się do granicy między zapewnianiem zgodności z prawem a cenzurowaniem. Brać pod uwagę trzeba jednocześnie zagadnienia takie jak: wolność słowa, prawo do prywatności czy tajemnica korespondencji.

Moim zdaniem, konkluzją nasuwającą się po przestudiowaniu zagadnienia, jest to, że dla prawidłowego i, co istotne, skutecznego uregulowania potrzebna jest bardziej rozbudowana współpraca między jak największą liczbą państw. Najbardziej dopracowane przepisy, jednak ograniczone tylko do terytoriów jednego lub kilku krajów, nie są w stanie poradzić sobie z przeszkodą, jaką, w tym momencie, jest ponadgraniczność Internetu. Dlatego dla zapewnienia „czystego" Internetu konieczne jest stworzenie reguł obowiązujących we wszystkich krajach, niestety nie wydaje się aby miało to nastąpić w najbliższym czasie.