

## **Opinia nt. projektu nowelizacji ustawy o świadczeniu usług drogą elektroniczną** **dr Krzysztof Siewicz**

Przedmiotem niniejszej opinii jest analiza oraz krytyka projektu nowelizacji ustawy o świadczeniu usług drogą elektroniczną, dostępnego pod adresem: <http://bip.mswia.gov.pl/portal/bip/218/20209/>. Zakres opinii obejmuje wyłącznie tę część projektu, w którym proponuje się wprowadzenie nowego rozdziału 3a.

### **1 Uwagi ogólne**

Rozdział 3a ma uregulować „procedurę powiadamiania i blokowania dostępu do bezprawnych informacji”. Z uzasadnienia projektu wynika, że procedura ta jest wzorowana na amerykańskiej ustawie „Digital Millenium Copyright Act”, DMCA i zawartej w niej procedurze „notice and takedown”.

Pojawia się zatem pytanie natury ogólnej, a mianowicie dlaczego to właśnie DMCA stało się wzorem dla projektodawców. W uzasadnieniu projektu nie ma niestety odpowiedzi na to pytanie. Jest ona jednak niezbędna, zwłaszcza wobec funkcjonowania w innych krajach innych procedur. Na uwagę zasługuje np. kanadyjska procedura „notice and notice”. Nie pozwala ona usługodawcy na samodzielne blokowanie informacji, a mimo to istnieją badania pokazujące jej skuteczność w walce z naruszeniami (zob. np. <http://www.michaelgeist.ca/content/view/5703/125/>). Uzasadnienie dla implementowania w Polsce regulacji amerykańskich jest wymagane tym bardziej, że Dyrektywa 2000/31 nie przesądza co do konieczności stosowania procedury „notice and takedown”. Art. 14 ust. 1 pkt b Dyrektywy stanowi bowiem: „usługodawca podejmuje niezwłocznie **odpowiednie działania w celu usunięcia lub uniemożliwienia** dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony” (wytłuszczenie własne) Konieczne jest co najmniej wyjaśnienie, dlaczego projektodawcy uznają amerykańską procedurę za odpowiednią.

W uzasadnieniu analizowanego projektu brak jest w szczególności wyjaśnienia dlaczego projektodawcy uważają, że procedura DMCA mająca w USA zastosowanie tylko do naruszeń praw autorskich może sprawdzić się w odniesieniu do wszelkiego rodzaju „bezprawnych informacji”. Informacje te cechuje przecież duża różnorodność – mogą one zawierać nie tylko bezprawnie rozpowszechniane utwory, ale także np. treści naruszające prywatność i inne dobra osobiste. Jeszcze inną grupę stanowią materiały propagujące rozmaite totalitarne reżimy lub treści pedofilskie. Różnice pomiędzy tymi informacjami powodują różne problemy, które powinny być z kolei rozwiązywane za pomocą różnych narzędzi. Chodzi tu zwłaszcza o to, że punkty równowagi interesów i praw wszystkich zainteresowanych stron mogą znajdować się w innych miejscach w zależności od tego, z jakiego rodzaju treścią mamy do czynienia. Dla przykładu, inna jest waga naruszenia prawa autorskiego, zwłaszcza gdy dotyczy profesjonalnego podmiotu, dysponującego istotnymi środkami, w porównaniu do wagi naruszenia prywatności osoby fizycznej. Tymczasem, jednolita procedura dla wszystkich rodzajów „bezprawnych informacji” oznacza, że punkt równowagi zostanie wyznaczony tak samo, bez uwzględnienia specyfiki określonego przedmiotu.

### **2 Brak powiązania z art. 14**

W proponowanym brzmieniu Rozdział 3a stanowi regulację autonomiczną, niepowiązaną z innymi

przepisami ustawy. Brak jest w nim w szczególności powiązania z obecnym art. 14 ustawy. Prowadzi to do bardzo istotnej sprzeczności. Np. według projektowanego art. 15c pkt 2 lub 3 usługodawca mógłby odrzucić wiarygodną wiadomość. Z kolei zgodnie z art. 15e pkt 1 usługodawca mógłby odblokować dostęp do treści w wyniku sprzeciwu usługobiorcy. Nie proponuje się natomiast żadnej zmiany w art. 14. Będzie on wobec tego nadal stanowił, że usługodawca nie ponosi odpowiedzialności jeżeli zablokuje dostęp po uzyskaniu wiarygodnej wiadomości. Zawarte w nim wyłączenie odpowiedzialności nie będzie miało zatem zastosowania w przypadku, gdy usługodawca odrzuci wiadomość lub uwzględni sprzeciw zgodnie z art. 15c pkt 2 lub 3 oraz art. 15e pkt 1 (odpowiednio).

Taki stan rzeczy może prowadzić do niskiej praktycznej przydatności Rozdziału 3a. Usługodawcy nie będą przecież mieli zbyt dużej motywacji do stosowania jego przepisów inaczej niż poprzez blokowanie dostępu i odrzucanie sprzeciwów usługobiorców. Tylko w ten sposób będą się bowiem mieścili w „przyjaznej przystani” art. 14. W celu zapewnienia spójności i przydatności nowej regulacji konieczne jest zatem wskazanie w art. 14, że wyłączenie odpowiedzialności stosuje się w przypadku działania zgodnego z całą procedurą określoną w Rozdziale 3a, a nie tylko z jednym z jej wariantów.

Na marginesie warto zauważyć, że art. 14 posługuje się pojęciem „danych” i odnosi się do „bezprawnego charakteru danych lub związanej z nimi działalności”. Z kolei projektowany Rozdział 3a posługuje się pojęciami „informacje” oraz „treści”. Ponadto, traktuje on wprost o „bezpprawnych informacjach” oraz „bezpprawnych treściach”. Brakuje nie tylko wyjaśnienia wzajemnych relacji zakresów tych pojęć, ale też wyjaśnienia w jaki sposób bezprawność mogłaby się do nich odnosić bezpośrednio. Zgodnie bowiem z podstawowymi zasadami prawa, bezprawne mogą być działania lub zaniechania, a nie same przedmioty, do których się one odnoszą. Konieczne jest co najmniej ujednoczenie terminologii z istniejącym art. 14.

### **3 Problematiczna definicja „uprawnionego”**

Proponowany Art. 15a zawiera swoistą definicję legalną „uprawnionego”. W skrócie, miałyby to być posiadacz informacji o bezprawnych treściach zamieszczonych w sieci Internet. Oznacza to, że „uprawnionym” może być w zasadzie każdy. Fakt posiadania informacji o bezprawnych treściach nie jest tu szczególnie wyróżniający, gdyż osoby nie mające takich informacji i tak nie podejmowałyby działań. Trudno zatem zrozumieć po co ustawodawca miałby wprowadzać taką definicję legalną, zamiast po prostu wskazać, że „uprawnionym” może być każdy.

Nie ma jednak powodu, aby istniał wyraźny przepis definiujący uprawnionego. Po pierwsze, fakt przysługiwania uprawnień związanych z określonymi danymi publikowanymi w Internecie będzie i tak wynikał z odrębnych przepisów (np. prawa autorskiego). Po drugie, nie ma potrzeby wyróżnienia specjalnej kategorii podmiotów, które mogłyby składać wiarygodne wiadomości i nadanie im do tego ustawowych uprawnień (zwłaszcza, że zaproponowana definicja obejmuje w zasadzie każdego). Istotą przesłania „wiarygodnej wiadomości” jest bowiem doprowadzenia do określonego stanu świadomości (wiedzy) usługodawcy. To, od kogo taka wiadomość zostanie przesłana jest kwestią wtórną, o ile doprowadzi ona do uświadomienia usługodawcy, że przechowuje dane o bezprawnym charakterze lub, że z danymi związana jest określona bezprawna działalność.

Ścisłe rzecz ujmując, „wiarygodna wiadomość” w rozumieniu art. 14 polskiej ustawy oraz dyrektywy 2000/31 może przecież w ogóle nie mieć nadawcy. Widać to wyraźnie zwłaszcza po angielskim tekście art. 14 dyrektywy 2000/31, który „wiarygodną wiadomość” wiąże ze stanem świadomości usługodawcy („does not have actual knowledge” i „is not aware of”). Ten stan może być wynikiem otrzymania wiadomości od kogoś, ale może też być wynikiem samodzielnego poznania lub powiadomienia przez system teleinformatyczny.

Niewątpliwie jednak to, kto jest nadawcą wiadomości ma znaczenie, gdyż wpływa na poziom jej wiarygodności. Często, choć nie zawsze, bardziej wiarygodne wiadomości pochodzą od osób, które są w stanie wykazać określony tytuł prawny do przedmiotowych danych. Można zatem zastanowić się nad ujęciem kwestii nadawcy wiadomości przy ustalaniu poziomu jej wiarygodności (w ramach ustawowych wskazówek co do kryteriów, jakie należy brać pod uwagę przy ocenie wiarygodności, o czym dalej w niniejszym dokumencie).

W związku z powyższym zasadne jest zrezygnowanie z tej części art. 15a, który zawiera definicję legalną uprawnionego. W tym zakresie wystarczająca jest aktualna treść art. 14, który określa całą sytuację od strony usługodawcy. Wskazuje on w szczególności, że usługodawca korzysta z wyłączenia odpowiedzialności w przypadku określonej reakcji na wiarygodną wiadomość.

#### **4 Nieuzasadnione wymaganie identyfikacji**

Wskazanie elementów wiarygodnej wiadomości określone w art. 15a, a także treść art. 15c pkt 3 powodują konieczność identyfikacji nadawcy wiarygodnej wiadomości. Istnieje ryzyko, że w praktyce spowoduje to wymaganie przez usługodawców jak najpełniejszej identyfikacji. Działania takie tylko w części mogą być mitygowane przepisami o ochronie danych osobowych zawierającymi zasadą adekwatności oraz zasadą związania celem. Jest tak chociażby dlatego, że egzekwowanie tych zasad będzie czasochłonne, a uchwalenie projektu w obecnym brzmieniu pozwoli argumentować, że zasady te zostały ograniczone przepisami ustawy.

Wymaganie identyfikacji nadawcy wiarygodnej wiadomości może stanowić naruszenie prawa podmiotowego jednostki w przypadku, gdy nadawcą tym będzie twórca w rozumieniu prawa autorskiego. Do autorskich praw osobistych zalicza się bowiem prawo do udostępniania utworu anonimowo. Twórca ma zatem prawo do nieujawniania swojej tożsamości także wobec usługodawcy. Tym bardziej, że chodzi tu o usługodawcę, którego usługi osoba trzecia wykorzystuje do naruszania praw twórcy. Aktualna treść projektu zmusza twórcę do zrezygnowania z prawa do anonimowości po to, aby skorzystać z procedury uregulowanej w Rozdziale 3a.

Obowiązek identyfikacji nałożony na nadawcę wiarygodnej wiadomości jest problemem nie tylko w przypadku twórców. Zwiększa on bowiem ryzyko naruszenia prawa do prywatności lub nawet innych dóbr osobistych nadawców, takich jak życie lub zdrowie. Przepisy Rozdziału 3a mają mieć przecież zastosowanie nie tylko do naruszeń praw autorskich, ale także w odniesieniu do innych treści – w tym różnego rodzaju pomówień, pogroźek itd. Nie można zakładać, że wszyscy usługodawcy będą w stanie zabezpieczyć dane identyfikujące nadawców wiarygodnych wiadomości przed dostępem osób trzecich (w tym pomawiających lub grożących usługobiorców). Nie ma też gwarancji, że sami usługodawcy nie uczynią z otrzymanych

danych identyfikujących niewłaściwego użytku.

Przede wszystkim jednak, identyfikacja nadawcy jest po prostu niepotrzebna do sprawnego działania procedury uregulowanej w Rozdziale 3a, przynajmniej nie w każdym przypadku. Istnieją bowiem sytuacje, w których wiarygodność wiadomości zupełnie nie zależy od osoby jej nadawcy lub przypadku, w których wystarczy ujawnienie tylko pewnych danych kontaktowych (np. samego adresu e-mail, nawet bez imienia i nazwiska nadawcy). Nie ma zatem uzasadnienia dla wprowadzania powszechnego obowiązku identyfikacji nadawców wiarygodnych wiadomości. Takiego wymagania nie zawiera nawet DMCA, który wymaga podpisu oraz „informacji w rozsądnym zakresie wystarczającej do umożliwienia usługodawcy skontaktowania się z nadawcą, takich jak adres, numer telefonu lub e-mail” (tłumaczenie własne). Warto tu przypomnieć, że podpis osoby może ją identyfikować w sposób nie pozwalający na ujawnienie jej danych osobowych w szerszym zakresie (wystarczającą identyfikację może zapewnić też podpis całkowicie nieczytelny, jak też np. podpis inicjałami itd.). Co istotne, wymóg „podpisu” w DMCA nie oznacza konieczności zachowania formy pisemnej, ani korzystania z „bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem”.

Zakres danych osobowych zawartych w wiadomości może oczywiście wpływać na jej wiarygodność. Zatem, brak ustawowego obowiązku identyfikacji nie oznacza, że usługodawcy nie powinni móc wymagać podania określonych danych nadawców. Powinny to być jednak tylko takie dane, które są rzeczywiście potrzebne (powodują, że wiadomość może być uznana za wiarygodną). Wskazane jest wobec tego ustawowe ograniczenie zakresu danych, jakich może domagać się usługodawca i ograniczenie tej możliwości tylko do przypadków, w których brak danych powoduje niewiarygodność wiadomości. Należy też zrezygnować z art. 15c pkt 3, który pozwala usługodawcy odrzucić wiarygodną wiadomość złożoną na formularzu bez wskazania danych umożliwiających identyfikację jej autora.

Powyższe uwagi dotyczą także identyfikacji usługobiorcy, który zgodnie z proponowanym art. 15d może złożyć sprzeciw. Także i w tym wypadku nie jest uzasadnione, aby wymagać identyfikacji usługobiorcy w każdym przypadku. Podanie danych identyfikujących powinno natomiast mieć znaczenie dla oceny, czy sprzeciw zasługuje na uwzględnienie (gdy zależy to od konkretnych przymiotów usługobiorcy).

Na marginesie, projektowane przepisy nie zawierają wystarczających gwarancji, że dane identyfikujące i kontaktowe „uprawnionego” oraz usługobiorcy nie zostaną im przekazane przez usługodawcę w trakcie realizacji procedury uregulowanej w Rozdziale 3a. Przekazanie tych danych może grozić daleko idącymi konsekwencjami, nie tylko dla prywatności, ale nawet dla życia lub zdrowia tych osób. Wobec tego, poza usunięciem obowiązku identyfikacji należy zadbać o wprowadzenie przepisów, które w wyraźny sposób zakazują usługodawcy przekazywania tych danych. Ich udostępnienie może być dozwolone jedynie na podstawie innych przepisów, z zachowaniem stosownych procedur (w tym kontroli sądowej).

## **5 Niejasne i nieuzasadnione elementy „wiarygodnej wiadomości”**

Art. 15a zawiera listę elementów jakie będą musiały się znaleźć w „wiarygodnej wiadomości”. Poniższa tabela porównuje tę listę z analogiczną listą zawartą w DMCA – polskim punktem przyporządkowano ich amerykańskie odpowiedniki tam, gdzie było to możliwe.

Projektowany art. 15a	DMCA
1) dane określające uprawnionego, składającego zawiadomienie o umieszczeniu w sieci Internet bezprawnych informacji,	
2) dane kontaktowe uprawnionego,	(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
3) podpis uprawnionego albo osoby go reprezentującej,	(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
4) jednoznaczne wskazanie informacji, które naruszają prawa lub przedmiot działalności uprawnionego, do których dostęp powinien zostać zablokowany,	(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
6) dane umożliwiające usługodawcy zlokalizowanie bezprawnej treści,	
5) uzasadnienie,	(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site
7) kopia pełnomocnictwa,	
8) oświadczenie uprawnionego o: - braku autoryzacji treści zamieszczonych w sieci Internet, - zgodności z prawdą przedstawionych informacji.	(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.  (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Niektóre różnice widoczne w tej tabeli wynikają oczywiście z kwestii podstawowej. Mianowicie, procedura uregulowana w DMCA dotyczy tylko i wyłącznie naruszeń praw autorskich, podczas gdy

projektodawcy art. 15a mieli na celu skodyfikowanie „wiarygodnych wiadomości” dotyczących wszystkich możliwych „bezprawnych informacji”. Uzasadnia to bardziej ogólnikowe sformułowania art. 15a, choć nie tłumaczy wszystkich uproszczeń. Pokazuje to jednocześnie, że taka powszechna regulacja jest trudna, a być może wręcz niemożliwa. W szczególności, im bardziej ogólnikowe sformułowania, tym łatwiej będzie uznawać określone wiadomości za wiarygodne. Przechyli to punkt równowagi na korzyść podmiotów przesyłających zawiadomienia o – w ich opinii – bezprawnych informacjach, co nie zawsze jest uzasadnione.

Zasadne jest przede wszystkim zrezygnowanie z elementów, których w DMCA nie ma, czyli danych identyfikujących uprawnionego oraz kopii pełnomocnictwa. Kwestia identyfikacji została już omówiona powyżej. Natomiast wymaganie kopii pełnomocnictwa utrudni w praktyce wysyłanie wiarygodnych wiadomości drogą elektroniczną. Znacznie bardziej rozsądne jest wymaganie – wzorem DMCA – aby nadawca składał oświadczenie o występowaniu w imieniu uprawnionego (jeżeli działa w ten sposób) i ewentualne nałożenie dodatkowych sankcji w przypadku, gdyby oświadczenie to okazało się nieprawdziwe.

Z kolei w odniesieniu do elementów, które mają swoje odpowiedniki w DMCA warto zastanowić się nad ich doprecyzowaniem. I tak, opis „danych kontaktowych” powinien zawierać wyżej sygnalizowane gwarancje co do wymagania tylko takich danych, które są konieczne dla wiarygodności wiadomości. W odniesieniu do „podpisu” należy doprecyzować, że wiadomość nie musi mieć formy pisemnej, ani też nie musi być opatrzona „bezpiecznym podpisem elektronicznym weryfikowanym kwalifikowanym certyfikatem”.

Znamienne jest, że art. 15a pkt 8 wymaga od nadawcy oświadczenia o braku autoryzacji. W tym kontekście powinno tu zostać użyte raczej słowo „zezwoleństwo” lub „licencja” („autoryzacja” dotyczy raczej określonej praktyki związanej z publikacjami prasowymi, a w projekcie wydaje się być raczej niepoprawnym tłumaczeniem „authorization” użytym w DMCA). Ponadto, analogiczny punkt DMCA wymaga oświadczenia nie tylko co do braku zezwolenia uprawnionego („is not authorized by the copyright owner”), ale też co do braku zgodności z prawem („is not authorized ... by the law”). Z uwagi bowiem na przepisy o dozwolonym użytku, brak zezwolenia uprawnionego może nie być wymagany dla legalnego rozpowszechnienia określonych utworów (np. cytat, przedruk, wyjątki na rzecz instytucji naukowych, edukacyjnych). Należy wobec tego doprecyzować sformułowanie art. 15a pkt 8.

## **6 Formalizm nie rozwiązuje problemu oceny wiarygodności**

Proponowany art. 15c pozwala usługodawcy odrzucić wiarygodną wiadomość. Redakcja tego przepisu nie ogranicza powodów odrzucenia do kwestii formalnych, co oznacza, że usługodawca może w szczególności dokonać własnej oceny „wiarygodności” wiadomości. Jednak w całym projekcie nowelizacji brak jest jakichkolwiek wskazówek co do kryteriów, jakie usługodawca powinien brać pod uwagę przy tej ocenie. Innymi słowy, projektowana regulacja utrzymuje w tym zakresie aktualny stan prawny. Co istotne, to właśnie trudności w ocenie wiarygodności wiadomości są jednym z podstawowych zarzutów polskiej doktryny w odniesieniu do obecnej treści art. 14 ustawy (por. np. A. Kuczerawy, Odpowiedzialność dostawcy usług internetowych, Prawo Mediów Elektronicznych 6/2007 i przywołana tam literatura).

Kryteria oceny wiarygodności wiadomości mogą być oczywiście wypracowane przez praktykę i orzecznictwo. Jednak w wyniku dotychczasowej praktyki stosowania ustawy nie doszło do zbyt wielu

rozstrzygnięć w tym zakresie. Tym bardziej zatem warto sformułować pewne wytyczne już na poziomie ustawy. W przeciwnym razie usługodawcy będą motywowani do reagowania na jakiegokolwiek wiadomości, jeżeli tylko spełnią one wymogi formalne art. 15a pkt 1-8. Spowoduje to nieuzasadnione wzmocnienie pozycji nadawców wiadomości i w skrajnych przypadkach może ułatwić „cenzurowanie” treści całkowicie legalnych, a po prostu niewygodnych dla określonych podmiotów.

Przy formułowaniu takich wytycznych warto odwołać się do pojęcia „uprawdopodobnienia” obecnego w wielu przepisach KPC, wokół którego powstało już stosowne orzecznictwo. Orzecznictwo to skupia się jednak na negatywnej definicji „uprawdopodobnienia” wskazując różnice pomiędzy tym pojęciem, a pojęciem „udowodnienia”. W związku z tym, samo tylko wykorzystanie tego pojęcia w przepisach ustawy nie będzie wystarczającą wskazówką dla usługodawców. Zasadne jest poza tym wprowadzenie do ustawy przykładów elementów uwiarygadniających wiadomości, jednakże bez wymagania, aby były one obecne w każdej z nich.

Niezależnie jednak od ewentualnych ułatwień dla usługodawców w zakresie oceniania wiarygodności wiadomości, nie sposób nie zauważyć, że nie są to podmioty uprawnione ani kompetentne do dokonywania tej oceny. To, czy faktycznie doszło do naruszenia prawa w związku z umieszczeniem określonych danych „w Internecie” może prawidłowo ocenić jedynie sąd (nawet jeżeli chodzi o samo uprawdopodobnienie, a nie udowodnienie tego naruszenia). W obecnie proponowanym kształcie, procedura w zasadzie wyłącza udział sądu na etapie oceny wiadomości i sprzeciwu. Nie daje to gwarancji, że stan powstały w jej wyniku (zablokowanie lub odblokowanie dostępu do danych) będzie zgodny z ewentualnym przyszłym orzeczeniem sądu. Z tego punktu widzenia warto rozważyć zalety kanadyjskiej procedury „notice and notice”, która w swej istocie jest odpowiednikiem znanych i powszechnie stosowanych w Polsce „wezwań przedsądowych”.

## **7 Kwestie nieporuszone w projekcie ustawy**

Dotychczasowa praktyka stosowania art. 14 ustawy pokazała, że istnieje szereg problemów, do których jednak projekt nowelizacji w ogóle się nie odnosi. Poniżej skrótowo omówiono najważniejsze z tych problemów i wskazano na sposoby ich rozwiązania.

### **7.1 Zakres wyłączenia odpowiedzialności z art. 14**

Art. 14 dyrektywy 2000/31 dotyczy wyłączenia zarówno odpowiedzialności cywilnej, jak i karnej. Jest to tzw. model horyzontalny (zob. A. Kuczerawy, *Odpowiedzialność dostawcy usług internetowych*, *Prawo Mediów Elektronicznych* 6/2007 i przywołana tam literatura). W art. 14 ustawy brakuje jednak wyraźnego sformułowania pozwalającego twierdzić, że przepis ten rozciąga się zarówno na odpowiedzialność karną i cywilną.

Osobną kwestią jest ew. wyłączenie odpowiedzialności administracyjnej usługodawcy. P. Litwiński sformułował pogląd, że pomimo art. 14 usługodawca odpowiada za zabezpieczenie przechowywanych danych osobowych zgodnie z ustawą o ochronie danych osobowych (P. Litwiński, *Hosting danych osobowych*. Zagadnienia podstawowe, MOP rok 2008 numer 23). Jest to pogląd oparty na twierdzeniu, że usługodawca (dostawca hostingu) jest podmiotem, któremu powierzono przechowywanie danych

osobowych. Niewątpliwie jednak, w treści art. 14 brak jest wyraźnych sformułowań, że przepis ten nie obejmuje odpowiedzialności administracyjnej.

Należy zatem doprecyzować zakres wyłączenia odpowiedzialności wynikający z art. 14. Niewątpliwie powinien on wyraźnie obejmować odpowiedzialność cywilną i karną, chociażby dlatego, że tak wynika z dyrektywy 2000/31. Bez szerszej analizy trudno natomiast przesądzić, czy ograniczanie administracyjno-prawnej ochrony za pomocą art. 14 ustawy byłoby dobrym rozwiązaniem. Analiza ta nie powinna ograniczać się tylko do danych osobowych. Należy w szczególności określić dokładną relację między art. 14 a przepisami prawa prasowego.

## **7.2 „Posiadanie wiedzy”**

Jedną z przesłanek wyłączenia odpowiedzialności usługodawcy określonej w art. 14 ustawy jest brak wiedzy o bezprawnym charakterze przechowywanych danych lub związanej z nimi działalności. Otrzymanie wiarygodnej wiadomości jest tylko jednym z przypadków, w których usługodawca może taką wiedzę osiąść.

Istnieje wątpliwość, czy do „posiadania wiedzy” dochodzi w sytuacji moderowania serwisu przez usługodawcę. Sam fakt zapoznania się z określoną informacją i dopuszczenie jej do publikacji nie oznacza przecież, że osoba zapoznająca była w stanie ocenić wszystkie elementy konieczne do ustalenia statusu prawnego tej informacji. Dla przykładu, przeciętna osoba czytająca utwór nie jest w stanie ocenić, czy został on opublikowany legalnie w ramach licencji uprawnionego lub któregoś z przepisów o dozwolonym użytku. Podobne wątpliwości mogą dotyczyć treści naruszających prywatność i innych „bezprawnych informacji”. Należy wobec tego doprecyzować pojęcie „posiadania wiedzy” użyte w art. 14 tak, aby nie pozwalało ono na pociągnięcie do odpowiedzialności usługodawcy tylko z tego powodu, że prowadzi on moderowane forum lub serwis.

Potrzeba takiej nowelizacji jest tym pilniejsza, że zapadają już orzeczenia, w których moderacja utożsamiana jest z posiadaniem wiedzy o bezprawności (por. sprawa opisana pod: [http://www.obserwatorium.org/index.php?option=com\\_content&view=article&id=3717:sprawa-forum-akademickiego-stworzy-niebezpieczny-precedens-dotyczy-odpowiedzialnoci-za-komentarze-w-internecie&catid=40:zkraju&Itemid=34](http://www.obserwatorium.org/index.php?option=com_content&view=article&id=3717:sprawa-forum-akademickiego-stworzy-niebezpieczny-precedens-dotyczy-odpowiedzialnoci-za-komentarze-w-internecie&catid=40:zkraju&Itemid=34))