ODPOWIEDZIALNOŚĆ DOSTAWCÓW I UŻYTKOWNIKÓW INTERNETU ZA ZAWARTOŚĆ STRON INTERNETOWYCH W ŚWIETLE PRAWNYCH I SPOŁECZNYCH REGULACJI

Rozprawy Społeczne, Nr 1 (VI), 2012

Małgorzata Gruchoła

Katolicki Uniwersytet Lubelski Jana Pawła II

Streszczenie: Celem artykułu jest przedstawienie mapy zagrożeń w globalnej sieci oraz wskazanie podmiotów ponoszących odpowiedzialność za zawartość stron internetowych (dostawcy treści: Internet Content Providers, dostawcy usług internetowych: Internet Service Providers i użytkownicy globalnej sieci), analiza podstaw prawnych ich działalności i wynikająca z nich odpowiedzialność w tytułowym zakresie (Dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r., art. 12-15; Ustawa z dnia 18 lipca 2002 r., art. 14). Ponadto weryfikacja podejmowanych działań samoregulacyjnych (European Internet Service Providers Associations) oraz omówienie kodeksów dostawców treści i usług internetowych (m.in.: Spam code of conduct of ISPA - Austria, Evropská Asociace Státnich Loterii A Toto Spolecnosti - Czechy, Code of Conduct for search engines/Verhaltenssubkodex fur Suchmaschinenanbieter der FSM - Niemcy i inne). Artykuł zamyka analiza kodeksów internautów, czyli netykiety oraz podsumowujące wnioski i postulaty.

Odpowiedzialność za treści znajdujące się na stronach internetowych ponoszą trzy grupy podmiotów: dostawcy treści, dostawcy usług internetowych oraz użytkownicy internetu. Obowiązujące przepisy prawa nie zawsze są skuteczne. Po pierwsze, nie umożliwiają egzekwowania przepisów prawa krajowego w innych państwach. Jest to istotne przy transgranicznym charakterze internetu. Po drugie, zauważa się rozbieżności europejskich i amerykańskich regulacji prawnych. Po trzecie, wszelkie próby wprowadzenia blokowania szkodliwych czy nielegalnych treści spotykają sie z protestami w imię wolności słowa. Skuteczna odpowiedzialność wymaga łączenia doświadczeń z różnych państw na bazie wspólnego, ujednoliconego prawa globalnego.

Netykiety sieciowe będące rodzajem przewodników, drogowskazów służą standaryzacji praktyk internautów. W szczególności odnoszą się do: komunikacji, wymogów dotyczących stron WWW, zasad korzystania z materiałów zamieszczonych w internecie i związanej z tym odpowiedzialności. Stąd niezbędna jest ciągła praca nad zasadami netykiety, ciągłe dostosowywanie ich do nowych realiów jakie niesie ze sobą, zmieniająca się rzeczywistość. Potrzebna jest nieustanna dyskusja na forum globalnym o zasadach netykiety, która będzie pobudzać świadomość społeczną o istnieniu zasad oraz wzmacniać konieczność ich przestrzegania dla dobra ogólnego. Konieczne jest pobudzenie globalnej świadomości o współodpowiedzialności wszystkich członków cyberświata za jego obecny oraz przyszły kształt. Kwestia ta jest istotna ze względu na wielonarodowy, wielokulturowy, zróżnicowany pod względem: wiekowym, rasowym, wyznania, światopoglądowym charakter tej społeczności. W publikacji zastosowano metodę analityczno-opisową.

Słowa kluczowe: podmiotowa odpowiedzialność, treści internetowe, samoregulacja, netykieta

Wstęp

Jeżeli mowa o konieczności przestrzegania przyjętych dla globalnej sieci przepisów prawa oraz pozaprawnych norm społecznych, należy przede wszystkim odpowiedzieć na pytania: kto ma prawo egzekwowania norm opracowanych dla internetu i kto powinien odpowiadać za ich naruszenie. Niezbędne jest wskazanie konstrukcji odpowiedzialności za naruszenia prawa i wskazanie podmiotów ją ponoszących. Dopełnienie tego obowiązku pozwoli z jednej strony na zagwarantowanie pewności prawa użytkownikom internetu, z drugiej zaś pozbawi krajowych prokuratorów i sędziów wątpliwości co do zakresu ich kompetencji w stosowaniu prawa krajowego. Zagadnienie to jest szczególnie ważne, jeśli mowa o odpowiedzialności za zawartość stron internetowych. Trudność w analizie prawnej tego aspektu internetu wynika z faktu szerokiego kręgu podmiotów zaangażowanych w powstawanie owych treści i posiadających faktyczny wpływ na ich kształt.

Celem artykułu jest przedstawienie mapy zagrożeń internetowych, wskazanie podmiotów ponoszących odpowiedzialność za zawartość stron internetowych (dostawcy internetu i użytkownicy globalnej sieci), analiza podstaw prawnych ich działalności (*Dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r.*, art. 12-15; *Ustawa z dnia 18 lipca 2002 r.*, art. 14). Ponadto weryfikacja podejmowanych działań samoregulacyjnych (*European Internet Service Providers Associations*) oraz omówienie kodeksów dobrej praktyki, z naciskiem na netykietę. W publikacji zastosowano metodę analityczno-opisową.

Zestawienie zagrożeń internetowych

Według Lucyny Kirwil dzieci, korzystając z globalnej sieci, mogą napotkać zagrożenia w czterech sferach funkcjonowania społecznego: relacjach międzyludzkich opartych na przemocy, agresji i okrucieństwie (typ „Agresja"), wypaczonych kontaktów erotycznych (typ „Seks"), ustalaniu hierarchii war-

Tabela 1. Klasyfikacja zagrożeń internetowych

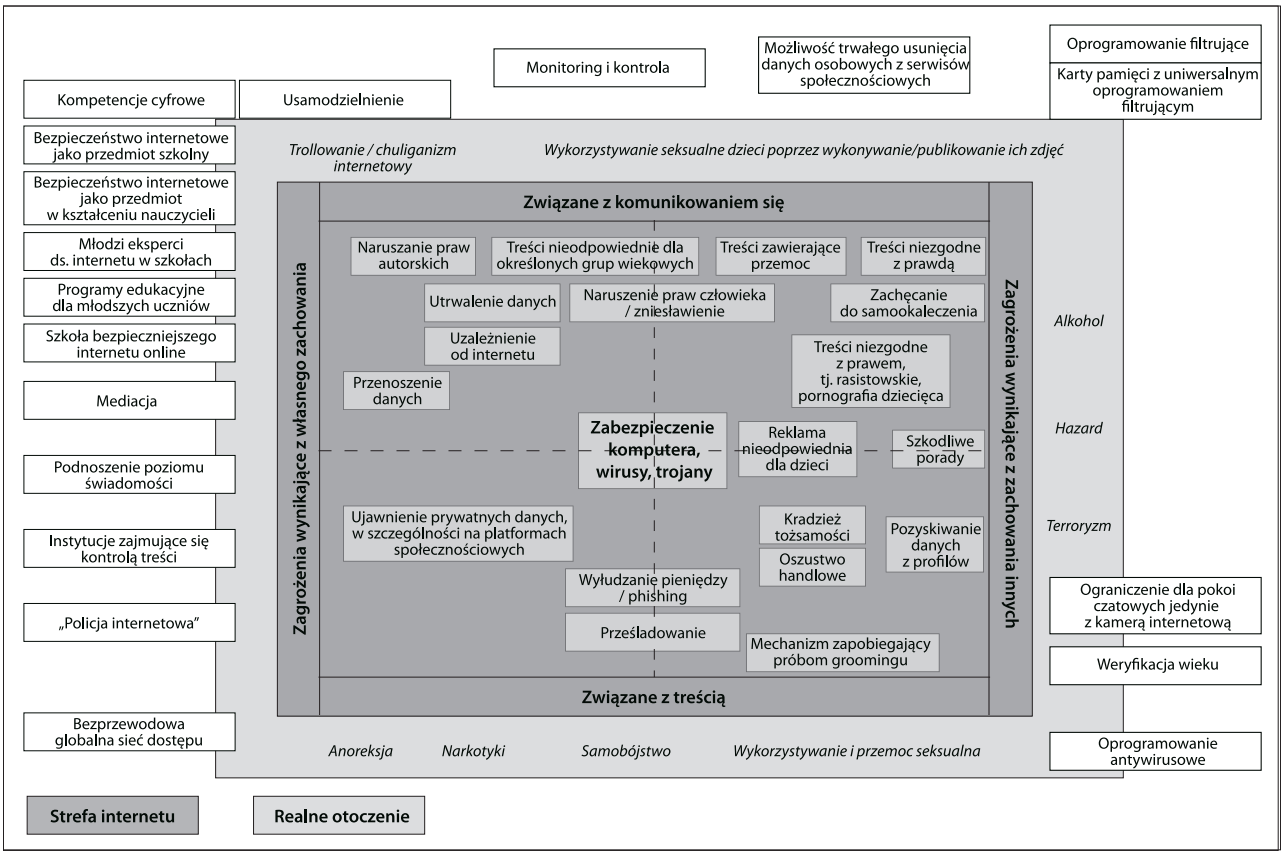
Typ zagrożenia	**Treść (zawartość)**	**Kontakt**	**Zachowanie**
Agresja	Przemoc/ okrucieństwo/ sceny drastyczne	Doznawanie dręczenia/znęcania się/agresywności/ napastliwości ze strony innych	Dręczenie/złośliwe zachowanie/ napastliwość (*cyberbullying)*
Seks	Pornografia	Doświadczenie bycia uwiedzionym (*grooming)*	Seksting
Wartości	Rasizm/ nienawiść	Perswazja ideologiczna	Samouszkodzenia
Komercyjne	Marketing, perswazja	Nadużycia prywatności/ wykorzystanie danych osobistych	Ściąganie filmów, dokumentów, hazard online

Źródło: L. Kirwil, Polskie dzieci w internecie. Zagrożenia i bezpieczeństwo na tle danych dla UE. Wstępny raport z badań EU Kids Online przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców, s. 10, http://www.saferinternet.pl/images/stories/pdf/raport_eu_kids_online_polska_28-10-2010.pdf, [21.09.2011]

tości i indoktrynacji w tym zakresie (typ „Wartości") oraz działaniach rynkowych (typ „Komercyjne"). Użytkownicy internetu mogą być narażeni na te zagrożenia poprzez zetknięcie się ze szkodliwymi treściami zamieszczonymi w globalnej sieci albo poprzez kontaktowanie się z innymi osobami w internecie (Kirwil 2010, s. 10). W obydwu przypadkach część zagrożeń wynika z zachowania samych internautów, pozostałe - ze sposobu postępowania innych. Istnieją też zagrożenia, których przypisanie do jednego z tych dwu wymiarów, wynika z przyjętej perspektywy - konsumenta lub producenta, szczególnie w przypadku treści generowanych przez użytkownika. Wynika skąd, że te dwa wymiary wzajemnie się przenikają (Zob. Gruchoła 2012, s. 37).

Dzięki uwzględnieniu powyższych czterech cech możliwe jest stworzenie mapy zagrożeń oraz form ochrony.

W kontekście treści internetowych ważne jest, by rozróżnić treści niezgodne z prawem i treści szkodliwe. Wykładnię treści nielegalnych oraz szkodliwych podaje uzasadnienie *Rekomendacji Komitetu Ministrów Rady Europy z dnia 31 października 2001 r.* Do pierwszych zalicza treści sprzeczne z prawem



Rysunek 1. Zestawienie zagrożeń
Źródło: Stiftung Digitale Chancen (2009), Zestaw zaleceń projektu Youth Protection Roundtable. SDC, Hamburg, s. 8

krajowym. Treści szkodliwe ujmuje jako niekoniecznie nielegalne, za to potencjalnie niosące szkodę, szczególnie dla fizycznego, psychicznego i moralnego rozwoju małoletnich. Przykładami szkodliwych stron są treści propagujące ruchy religijne, uznane za sekty, przedstawiające anoreksję i bulimię jako styl życia, a nie poważną chorobę; nawołujące do samobójstwa lub samookaleczeń; promujące narkotyki i inne używki oraz środki farmaceutyczne, takie jak tabletki gwałtu.

Do pierwszej grupy zagrożeń (związanych z treścią) zalicza się treści: nieodpowiednie dla określonych grup wiekowych (pornografia), zawierające przemoc, niezgodne z prawdą, zachęcające do autoagresji, naruszające prawa człowieka i jego godność. Ponadto nieodpowiednia reklama i działania marketingowe skierowane do dzieci, praktyki związane z utrwalaniem i przenoszeniem danych czy naruszaniem praw autorskich.

Drugą grupę zagrożeń stanowią zagrożenia związane z kontaktowaniem się przez internet. Zalicza się do nich: stalking, bias bullying, mobbing elektroniczny, zmiany tożsamości i zachowań online, szkodliwe porady, internetowe kluby samobójców, uzależnienie od internetu *(Internet Addiction Disorder),* kradzież tożsamości, utrata pieniędzy/ phishing, oszustwo handlowe, uwodzenie dzieci (*grooming*), cyberprzemoc (*cyberbullying*), *trollowanie* i *flaming,* ujawnianie prywatnych informacji, pozyskiwanie danych z profili internetowych, wykluczenie społeczne oraz cyfrowe i inne. Grupami zagrożonymi wykluczeniem cyfrowym, podobnie jak wykluczeniem społecznym w ogóle, są przede wszystkim osoby słabiej wykształcone, bezrobotni, osoby niepełnosprawne oraz starsze, a także nieposiadające środków dostępu do komputera i internetu (Wiecej zob. Gruchoła 2012, s. 37-48, Gruchoła 2011, s. 78-100).

Możliwe formy ochrony użytkowników globalnej sieci omawiam w odrębnej monografii (Zob. M. Gruchoła (2012), *Ochrona użytkowników internetu w państwach Unii Europejskiej.* Wydawnictwo KUL, Lublin, ss. 381). Przypomnę tylko najważniejsze: regulacje prawne, kompetencje cyfrowe, samoregulacja dostawców internetu, działania „oddolne" użytkowników globalnej sieci, stosowne oprogramowanie oraz techniczne urządzenia wspierające ochronę.

Podmioty odpowiedzialne za zawartość stron internetowych

Termin *Internet Service Providers* (dalej: ISP) jest często używany w sposób ogólny, bez różnicowania pomiędzy usługą dostarczania dostępu do internetu *(access providers)* a usługami przechowywania *(hostowania)* i przekazywania treści *(tzw. content providers).* Jedna i ta sama firma może należeć do różnych kategorii, a różnice między nimi precyzuje *Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego* (art. 12-15) *(Dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r.).* W praktyce dostawcy usług internetowych oferują kilka rodzajów usług, w tym z usługą podłączenia do internetu. Gdyby taki dostawca na tym poprzestał, byłby on rzeczywiście jedynie dostawcą usługi dostępowej, a korzystanie z globalnej sieci zależałoby wówczas całkowicie od użytkownika. Jednak tylko nieliczni usługodawcy ograniczają się do tak prostej usługi. Większość z nich oferuje pocztę elektroniczną, grupy dyskusyjne, serwery WWW, utrzymywanie stron domowych, serwery gier albo oprogramowanie dla chatów. W takim przypadku, w świetle powyższej dyrektywy (art. 14) ich odpowiedzialność może być większa.

Odpowiedzialność za treści znajdujące się na stronach internetowych ponosić więc mogą teoretycznie cztery grupy podmiotów:

1. dostawcy treści (*Internet Content Providers*, dalej: ICP);
2. dostawcy usług internetowych (*Internet Service Providers,* dalej: ISP);
3. dostawcy dostępu do internetu (*Internet Access Providers,* dalej: IAP)
4. użytkownicy internetu (Zob. Kulesza 2010, s. 160)[1].

Dostawca treści internetowych to najczęściej sam twórca zamieszczonych w globalnej sieci informacji czy danych. Dostawca usług internetowych to przedsiębiorca, który świadczy usługi polegające na umożliwieniu połączenia z internetem (wielu z nich to firmy telekomunikacyjne).

O ile nie budzi wątpliwości odpowiedzialność samych twórców treści umieszczanych w internecie czy we wskazanych przez prawo sytuacjach odpowiedzialność internautów (gdzie samo posiadanie informacji czy materiałów o określonym charakterze jest karalne, np. pornografii dziecięcej), o tyle - zdaniem Janusza Barty i Ryszarda Markiewicza - zagadnienie odpowiedzialności dostawców dostępu do internetu jest wciąż przedmiotem ożywionej dyskusji (Barta, Markiewicz 2002). Dotyczy to podmiotów, które udostępniają pozostające do ich dyspozycji miejsca w sieci (serwery) w celu przechowania na nich i udostępniania cudzych materiałów *(host providers).* Wyjątkowość tej kategorii podmiotów polega na tym, że w odróżnieniu od *access provider'ów* mają oni wpływ na przepływ treści w obrębie globalnej sieci. Mogą kontrolować przechowywane dane, a nawet je usunąć, jeżeli uznają to za stosowne. Niemniej jednak sporne jest, w jakim zakresie powinni z tej władzy korzystać i w oparciu o jakie podstawy. Pytania te są szczególnie aktualne w kręgu państw uznawanych za demokratyczne, w kontekście problemu wolności słowa w globalnej sieci. W tych państwach zakres odpowiedzialności dostawców internetu jest ogra-

[1] J. Kulesza utożsamia zakres odpowiedzialności dostawców usług internetowych (*Internet Service Providers)* z dostawcami dostępu do internetu (*Internet Access Providers*).

niczony, jeśli występuje w ogóle. „Niektórzy przedstawiciele doktryny postulowali, aby *host provider* był zobowiązany do kontroli w takim stopniu jak wydawca przyjmujący ogłoszenie do publikacji, a zatem by na bieżąco badał, czy użytkownik nie dopuścił się naruszenia przepisów ustawowych" (Barta, Markiewicz 2002, s. 76).

Przepisy decydujące o charakterze odpowiedzialności ISP w prawie wspólnotowym zawarte są w art. 12-15 *Dyrektywy o handlu elektronicznym* (*Dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r.*). Zgodnie z treścią ww. artykułów, ISP nie ponoszą odpowiedzialności za działania polegające na świadczeniu usługi „zwykłego przekazu" (art. 12)[2], catchingu (art. 13)[3] i hostingu (art. 14)[4]. Zapis Dyrektywy pozostawia jednak państwom członkowskim możliwość wymagania od usługodawcy przez sąd lub organ administracyjny, zgodnie z systemem prawnym państwa, żeby przerwał on naruszenia prawa lub im zapobiegł. Ogólna klauzula artykułu 15 *Dyrektywy o handlu elektronicznym* zwalnia usługodawców z obowiązku nadzoru nad dostarczanymi treściami. Z przepisów wewnętrznych państwa może jednak wynikać obowiązek niezwłocznego powiadomienia przez ISP właściwych władz publicznych o rzekomych bezprawnych działaniach podjętych przez ich usługobiorców lub przekazanych przez nich informacjach. Ponadto często są oni zobowiązani do przekazania właściwym władzom, na ich żądanie, informacji pozwalających na ustalenie tożsamości usługobiorców z którymi wiążą ich umowy o przechowywanie danych (art. 15 ust. 2)[5]. W polskim prawie wynika to z ustawowego wprowadzenia wyłączeń odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną (*Ustawa z dnia 18 lipca 2002 r.*, art. 14).

W myśl ustawy z 2002 roku: usługodawca świadczący usługi drogą elektroniczną obejmujące zapewnienie dostępu do sieci telekomunikacyjnej lub transmisję danych, nie ponosi odpowiedzialności za treść tych danych, jeżeli:

- nie jest inicjatorem przekazu danych;
- nie wybiera odbiorcy przekazu danych;
- nie wybiera oraz nie modyfikuje informacji zawartych w przekazie.

Wyłączenie odpowiedzialności, o którym powyżej mowa obejmuje także automatyczne i krótkotrwałe pośrednie przechowywanie danych w celu zrealizowania oraz przeprowadzenia transmisji danych (*Ustawa z dnia 18 lipca 2002 r.*, art. 12). Ponadto: nie ponosi odpowiedzialności za przechowywane dane każdy, kto transmitując dane oraz zapewniając automatyczne i krótkotrwałe pośrednie przechowywanie tych danych w celu przyspieszenia ponownego dostępu do nich na żądanie innego podmiotu:

- nie modyfikuje danych;
- posługuje się uznanymi i stosowanymi zwykle w tego rodzaju działalności technikami informatycznymi określającymi parametry techniczne dostępu do danych i ich aktualizowania;

[2] Artykuł 12. Zwykły przekaz
1. Państwa członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na transmisji w sieci telekomunikacyjnej informacji przekazanych przez usługobiorcę lub na zapewnianiu dostępu do sieci telekomunikacyjnej usługodawca nie był odpowiedzialny za przekazywane informacje, jeżeli:
   a) nie jest inicjatorem przekazu;
   b) nie wybiera odbiorcy przekazu oraz
   c) nie wybiera oraz nie modyfikuje informacji zawartych w przekazie.
2. Czynności polegające na transmisji oraz zapewnianiu dostępu określone w ust. 1 obejmują automatyczne, pośrednie i krótkotrwałe przechowywanie przekazywanych informacji w zakresie, w jakim służy to wyłącznie wykonywaniu transmisji w sieci telekomunikacyjnej oraz że okres przechowywania nie przekracza czasu rozsądnie koniecznego do transmisji.
3. Artykuł nie ma wpływu na możliwość wymagania od usługodawcy przez sąd lub organ administracyjny, zgodnie z systemem prawnym państw członkowskich, żeby przerwał on naruszenia prawa lub im zapobiegł.

[3] Artykuł 13. Caching
1. Państwa członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na transmisji w sieci telekomunikacyjnej informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny z tytułu automatycznego, pośredniego i krótkotrwałego przechowywania tej informacji dokonywanego w celu usprawnienia późniejszej transmisji informacji na żądanie innych usługobiorców pod warunkiem że:
   a) usługodawca nie modyfikuje informacji;
   b) usługodawca przestrzega warunków dostępu do informacji;
   c) usługodawca przestrzega zasad dotyczących aktualizowania informacji, określonych w sposób szeroko uznany i używany w branży;
   d) usługodawca nie zakłóca dozwolonego posługiwania się technologią, szeroko uznaną i używaną w branży w celu uzyskania danych o korzystaniu z informacji oraz
   e) usługodawca niezwłocznie usuwa lub uniemożliwia dostęp do przechowywanych informacji, gdy uzyska wiarygodną wiadomość, że informacje zostały usunięte z początkowego źródła transmisji lub dostęp do nich został uniemożliwiony albo gdy sąd lub organ administracyjny nakazał usunięcie informacji lub uniemożliwienie dostępu do niej.
2. Artykuł nie ma wpływu na możliwość wymagania od usługodawcy przez sądy lub organy administracyjne, zgodnie z systemem prawnym państw członkowskich, żeby przerwał naruszenia prawa lub im zapobiegł.

[4] Artykuł 14. Hosting
1. Państwa członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem że:
   a) usługodawca nie ma wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji, a w odniesieniu do roszczeń odszkodowawczych - nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności; lub
   b) usługodawca podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony.
2. Ustęp 1 nie ma zastosowania, jeżeli usługobiorca działa z upoważnienia albo pod kontrolą usługodawcy.
3. Niniejszy artykuł nie ma wpływu na możliwość wymagania od usługodawcy przez sądy lub organy administracyjne, zgodnie z systemem prawnym państw członkowskich, żeby przerwał on naruszenia prawa lub im zapobiegł oraz nie ma wpływu na możliwość ustanowienia procedur regulujących usuwanie lub uniemożliwianie dostępu do tych informacji przez państwa członkowskie.

[5] Artykuł 15. Brak ogólnego obowiązku w zakresie nadzoru
1. Państwa członkowskie nie nakładają na usługodawców świadczących usługi określone w art. 12-14 ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność.
2. Państwa członkowskie mogą ustanowić w stosunku do usługodawców świadczących usługi społeczeństwa informacyjnego obowiązek niezwłocznego powiadamiania właściwych władz publicznych o rzekomych bezprawnych działaniach podjętych przez ich usługobiorców lub przez nich przekazanych informacjach lub obowiązek przekazywania właściwym władzom, na ich żądanie, informacji pozwalających na ustalenie tożsamości ich usługobiorców, z którymi mają umowy o przechowywanie.

- nie zakłóca posługiwania się technikami informatycznymi uznanymi i stosowanymi zwykle w tego rodzaju działalności w zakresie zbierania informacji o korzystaniu ze zgromadzonych danych (art. 13.1).

Również nie ponosi odpowiedzialności za przechowywane dane ten, kto przy zachowaniu warunków, o których mowa wyżej, niezwłocznie je usunie albo uniemożliwi do nich dostęp, gdy uzyska wiadomość, że dane zostały usunięte z początkowego źródła transmisji lub dostęp do nich został uniemożliwiony. Ponadto w sytuacji, gdy sąd lub inny właściwy organ nakazał usunięcie danych lub uniemożliwienie do nich dostępu (*Ustawa z dnia 18 lipca 2002 r.*, art. 13.2). W myśl art. 14.1.: [...] „nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych" (*Ustawa z dnia 18 lipca 2002 r.*, art. 14).

Jak wynika z powyższych przykładów w państwach Unii Europejskiej, w tym w Polsce, powszechna jest praktyka zwalniania dostawców usług z odpowiedzialności za dostarczane przez nich treści. Zdaniem, więc Barty i Markiewicza odpowiedzialność dostawców usług internetowych można porównać do odpowiedzialności bibliotekarzy, sprzedawców książek lub retransmitujących programy (Barta, Markiewicz 1998, s. 221). „Nie możemy ponosić odpowiedzialności za działania naszych użytkowników - twierdzą dostawcy usług internetowych i dlatego w regulacjach świadczenia usług drogą elektroniczną wylobbowali na całym świecie - czy to w USA na podstawie DMCA, czy to w Polsce, na podstawie art. 14 *ustawy o świadczeniu usług drogą elektroniczną* - wprowadzenie wyłączeń odpowiedzialności (gdy nie wiedzą, co w tych łączach między użytkownikami jest przesyłane") (Waglowski 2010, s. 1). Rzecz ma się jednak diametralnie inaczej w państwach azjatyckich - tam dostawcy usług są prawnie zobowiązani do filtrowania dostarczanych treści oraz ponoszą odpowiedzialność za treści, których nie udało się zablokować.

Jakie są praktyczne konsekwencje wyżej zanalizowanych regulacji prawnych?

Należy podkreślić, iż ISP jest zorganizowany w sposób samorządny, podlega prawu właściwemu dla terytorium, na którym się znajduje. Przykładem braku możliwości egzekwowania przepisów prawa krajowego w innych państwach są działania niemieckiego Ministerstwa Sprawiedliwości, które od 2000 roku przegląda adresy stron WWW o wydźwięku neonazistowskim (np. nsdap.de) i domaga się ich usunięcia. Obowiązujące tam prawo, zabraniające kwestionowania Holokaustu i szerzenia propagandy nazistowskiej, rozciąga się także na internet, nawet, jeśli takie treści powstają za granicą. Prawo umożliwia prokuratorom ściganie propagatorów ww. treści, gdziekolwiek się oni znajdują i bez względu na obywatelstwo, o ile tylko ich strony internetowe są dostępne w Niemczech. Mimo tak surowych niemieckich regulacji prawnych liczba stron internetowych o treści radykalno-prawicowej wciąż wzrasta (Kulesza 2010, s. 109). Źródłem problemu są przepisy prawa, które wyłączają odpowiedzialność dostawców dostępu do internetu (czyli tych, którzy umożliwiają dostęp do treści). Obowiązujące przepisy prawne obejmują tylko właścicieli stron internetowych.

Powyższy problem ilustruje kolejny przykład. W 2001 roku władze Nadrenii Północnej-Westfalii nakazały osiemnastu działającym tam dostawcom internetu, aby ci zablokowali dostęp do dwóch amerykańskich serwisów internetowych „głoszących" nazistowskie idee. Dostawcy, odwołujący się od administracyjnego nakazu, argumentowali, że nie mogą ponosić odpowiedzialności za treści publikowane na różnych, niebędących pod ich kontrolą stronach WWW (Waglowski 2009, s. 1). Stąd często amerykańskie serwisy stają się schronieniem tych, którzy łamią krajowe czy europejskie przepisy prawne.

Kolejnym problemem jest rozbieżność europejskich i amerykańskich regulacji prawnych. Przykładem jest sprawa aukcji pamiątek nazistowskich we francuskiej filii amerykańskiego portalu Yahoo!, która wciąż nie znalazła swojego definitywnego rozwiązania. Na początku 2003 roku francuski sąd orzekł, że Francuzi nie powinni mieć dostępu do aukcji organizowanych na stronach amerykańskiego giganta, gdyż prawo zakazuje prezentowania lub sprzedaży pamiątek nazistowskich. Po tym orzeczeniu serwis Yahoo! starał się uniemożliwić Francuzom dostęp do takich aukcji. Równolegle, sąd federalny USA zdecydował, że Yahoo! nie musi spełniać wymogów francuskiego prawa. Konsekwencją tego orzeczenia było m.in. postępowanie przed sądem we Francji, w którym trzy niezależne organizacje oskarżały Tima Koogle (szefa Yahoo!) o usprawiedliwianie przestępstw wojennych i zbrodni przeciwko ludzkości. Sąd w Paryżu stwierdził, że usprawiedliwianie takie oznaczałoby „wychwalanie, albo co najmniej prezentację przestępstwa w korzystnym świetle". Działalność portalu nie spełniało zdaniem sądu znamion tego przestępstwa (Waglowski 2009, s. 3).

Przytoczone wyżej przykłady wskazują na transgraniczny problem odpowiedzialności za treści zamieszczane w globalnej sieci. Dotyczy on stosowania norm prawa krajowego wobec internetu, a dokładniej braku możliwości egzekwowania przepisów prawa krajowego w innych państwach, i ich bezskuteczności. Skuteczna odpowiedzialność wymaga łączenia doświadczeń z różnych państw na bazie wspólnego, ujednoliconego prawa globalnego.

Innym problemem jest blokowania dostępu do określonych stron internetowych. Blokowanie stron WWW jako środek walki z pedofilią w internecie

niejednokrotnie był analizowany w Polsce, w Unii Europejskiej i poza jej granicami. Koniecznością walki z pornografią dziecięcą uzasadniano pomysł wprowadzenia w Polsce Rejestru Stron i Usług Niedozwolonych. Ochrona przed pedofilią może stać się pretekstem do monitorowania wyszukiwarek internetowych. Przeciwnicy obawiają sie, iż blokowanie stron będzie środkiem nadużywanym i/lub rozszerzanym na inne naruszenia (np. praw autorskich) i treści (np. krytykujące władzę). Natomiast zwolennicy blokowania powołują sie na dobro dzieci.

W październiku 2011 r. Parlament Europejski UE przyjął kompromisowe rozwiązanie, w myśl którego blokowanie na poziomie unijnym jest środkiem fakultatywnym, nieobowiązkowym. Europosłowie uznali, iż w sytuacjach, gdy niemozliwe jest usunięcie stron z materiałami pedofilskimi, konieczne może być ich zablokowanie. Ewentualna blokada powinna być zastosowana w sposób przejrzysty. Nie będzie to jednak środek wymagany bezwzględnie przez dyrektywę. Decyzję w tej sprawie będą musiały podjąć państwa członkowskie. Będą miały one dwa lata na dostosowanie przepisów krajowych do wymagań analizowanej dyrektywy *(UE: Zgoda Parlamentu ...* 2011).

Wcześniej, bo już w 2005 roku finlandzki rząd doszedł do porozumienia z firmami ISP w sprawie blokowania dostępu do witryn z pornografią dziecięcą. Jak podaje Polska Agencja Prasowa: „Policja przekaże firmom internetowym listę około tysiąca adresów internetowych, które powinny zostać zablokowane. Minister Łączności Leena Luhtanen wyraziła nadzieję, że porozumienie rządu z dostawcami usług internetowych sprawi, iż nie będzie trzeba uchwalać przepisów, zmuszających do blokowania witryn z pornografią dziecięcą" *(Porozumienia policji i rządu...* 2011, s.1). Na podobnych zasadach blokuje się również w Norwegii i Szwecji. Dlaczego blokuje się treści, zamiast ścigać sprawców przestępstw? Ci ostatni pozostają niezidentyfikowani albo znajdują się poza zasięgiem organów ścigania w danym państwie. Obowiązujące przepisy prawa nie są więc skuteczne.

Pomimo powszechnej zgody co do odpowiedzialności dostawców treści internetowych jako podmiotów mających bezpośredni wpływ na kształt treści umieszczanych w globalnej sieci ich obecna sytuacja prawna - jak słusznie podkreśla Joanna Kulesza - budzi wiele obaw i pytań (Kulesza 2010, s. 164). Podstawowe zagadnienie, jakie wiąże się z pytaniem o zakres odpowiedzialności ICP, obejmuje pytanie o podmiot kompetentny do prawnej oceny tych treści - czy będzie to suweren, z terytorium którego działa ICP, czy internauta, który uzna się za poszkodowanego skutkami owego działania? Ten brak porozumienia pomiędzy państwami administratorzy i właściciele stron internetowych starają się rozwiązywać we własnym zakresie, przede wszystkim przy wykorzystaniu opracowywanych przez siebie regulaminów. Ich zadaniem jest ustrzeżenie operatora przed odpowiedzialnością we wszystkich lokalizacjach, w których dostępna jest administrowana przez niego strona. Wiele witryn internetowych zawiera na którejś ze swoich podstron ogólne warunki użytkowania, wśród których zawarte są często także regulacje dotyczące porządku prawnego, któremu podlega dane „miejsce" w cyberprzestrzeni. Naturalnie operatorzy czy administratorzy stron internetowych powołują w nich najkorzystniejszy czy najwygodniejszy dla siebie porządek prawny, jako regulujący wzajemne relacje z użytkownikami stron. Podstawowa wada tego rodzaju zapisów polega na tym, że użytkownicy najczęściej po prostu nie zapoznają się z ich treścią, lekceważą ich czy też w ogóle nie mają świadomości ich istnienia. Stąd też wątpliwa jawi się skuteczność tak wyrażanej zgody użytkownika serwisu na poddanie się wskazanych przez operatora strony przepisom prawnym. Jednocześnie jest to najpopularniejszy sposób uniknięcia przez administratora strony problemów z obcymi jurysdykcjami, pozwala na jednoznaczne określenie porządku prawnego rządzącego stroną i relacjami pomiędzy jej twórcą, administratorem a użytkownikami. Dla wzmocnienia skuteczności zapisów owych regulaminów zasadne byłoby jednak rozważenie praktycznej możliwości zagwarantowania, że wszyscy korzystający z danej strony faktycznie posiadają świadomość, że korzystając z jej usług wyrażają zgodę na poddanie się reżimowi prawnemu państwa wybranego przez właściciela czy administratora. W tym celu powinny być prowadzone działania mające na celu podniesienie świadomości użytkowników internetu, wyrażających zgodę na owe warunki. Obecnie częstym sposobem na zwolnienie się od zarzutu małej „widoczności" warunków umowy jest rozwiązanie, w którym internauta musi nacisnąć ekranowy „przycisk", potwierdzający zgodę na warunki i regulamin korzystania ze strony. Takie zabezpieczenie pozwala podnosić twórcy strony argument wyraźnego wskazania użytkownikowi stosownych regulacji, którymi rządzi się jego serwis. Są to jednak najczęściej dokumenty o znacznej objętości i większość internautów nie zadaje sobie trudu ich przeczytania, co więcej - trudno wykazać, kto faktycznie wyraził ową zgodę. Moc wiążąca owych umów podważana jest z podanych wyżej powodów - większość z wyrażających na nie zgodę najczęściej nie zapoznaje się z ich treścią (Kulesza 2010, s. 165).

Stowarzyszenia dostawców usług internetowych

Bez względu na zobowiązania prawne dostawcy usług internetowych tworzą zrzeszenia (*Internet Service Providers Association*, dalej: ISPA), w ramach których ustalają wewnętrzne reguły działania, ograniczające swobodę zamieszczanych nielegalnych i szkodliwych treści w globalnej sieci. Największym stowarzyszeniem grupującym europejskich dostawców usług internetowych jest działające od

1997 roku European Internet Service Providers Associations (dalej: EuroISPA), reprezentujące ponad 1700 dostawców z UE oraz krajów EFTA. Celem Stowarzyszenia jest reprezentowanie europejskiego przemysłu internetowego w polityce UE oraz ułatwienie wymiany najlepszych praktyk między krajowymi stowarzyszeniami ISP (*European Internet Service Providers Associations 2011*)[6]. Stowarzyszenie przyjęło ustalone przez Radę Europy zasady polityki na rzecz dobrowolnej współpracy między providerami internetowymi a wymiarem sprawiedliwości w zakresie usuwania nielegalnych i szkodliwych treści i usług internetowych.

Innym przykładem jest niemieckie Stowarzyszenie Dobrowolnej Samokontroli Dostawców Usług Multimedialnych (*Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V).* Głównym jego zadaniem jest zapewnienie ochrony dzieci i młodzieży w internecie. Każdy jest uprawniony do złożenia w biurze Stowarzyszenia skargi na nielegalne i szkodliwe treści udostępniane w globalnej sieci, w innych sieciach lub w usługach online. Także członkowie Biura mogą z własnej inicjatywy wystąpić przeciw stowarzyszeniom członkowskim, łamiącym podstawowe jego cele (*Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V* 2011*)*. Działalność Stowarzyszenia reguluje §19 *Traktatu na rzecz ochrony małoletnich i godności ludzkiej w mediach (Jugendmedienschutz-Staatsvertrag*) (*Jugendmedienschutz-Staatsvertrag z dnia 1 kwietnia 2003 r.*, art. 5).

Na odnotowanie zasługuje także pierwsze europejskie dobrowolne porozumienie *The Safer Social Networking Principles for the EU,* na rzecz poprawy bezpieczeństwa nastolatków korzystających z portali społecznościowych. Zostało podpisane w dniu 10 lutego 2009 r. przez 17 firm internetowych[7]. Dokument ten wyznacza zalecenia oraz zasady, którymi powinni kierować się właściciele serwisów społecznościowych, chcąc zminimalizować zagrożenia na jakie narażone są dzieci i młodzież (Swetenham 2010, s. 20). Siedem głównych zaleceń to: 1) Poszerzenie wiedzy na temat bezpiecznego korzystania z internetu wśród dzieci, rodziców oraz opiekunów w prosty i przystępny dla danej grupy wiekowej sposób. 2) Dostosowanie treści serwisów internetowych do wieku grupy docelowej. 3) Udostępnienie internautom narzędzi i technologii zwiększających bezpieczeństwo online. 4) Dostarczenie łatwych w obsłudze mechanizmów do zgłaszania przypadków naruszenia bezpieczeństwa i prywatności internautów. 5) Reakcja na zgłoszenia nielegalnych treści lub zachowań. 6) Dbałość o prywatność użytkowników. 7) Ocena środków kontroli nad nielegalnymi lub zakazanymi treściami i działaniami.

Administratorzy portali zobowiązali się ograniczyć zagrożenia przez zagwarantowanie:

- prostego w użyciu przycisku „zgłoś nadużycie", umożliwiającego jednym kliknięciem zgłoszenie niewłaściwego kontaktu lub zachowania innego użytkownika;
- domyślnego ustawienia *prywatne/poufne* w przypadku pełnych profili i list kontaktów tych użytkowników portali, którzy są zarejestrowani jako osoby niepełnoletnie (utrudnienie nawiązania kontaktu z małoletnimi);
- braku możliwości przeszukiwania prywatnych profili użytkowników poniżej 18. roku życia (na stronach internetowych lub przez wyszukiwarki);
- stałej widoczności i dostępności opcji ochrony prywatności, tak by użytkownicy mogli łatwo sprawdzić, czy tylko ich znajomi, czy też wszyscy internauci widzą to, co umieszczają w globalnej sieci;
- zapobieganiu korzystania z usług przez zbyt młodych użytkowników, jeżeli portal społecznościowy jest przeznaczony dla nastolatków powyżej 13. roku życia (zarejestrowanie się osób młodszych będzie utrudnione) (*Społeczności sieciowe* 2011).

Wszyscy sygnatariusze zostali zobowiązani do złożenia informacji, określających w jaki sposób powyższe zasady zostały wdrożone w prowadzonych przez nich serwisach. Jedną z takich deklaracji są ograniczenia wprowadzone przez MySpace, mające utrudnić dorosłym użytkownikom serwisu zawieranie przyjaźni z dziećmi. Internauci powyżej 18. roku życia nie mogą być dodawani do sieci znajomych przez 14 i 15-latków (wyjątek: gdy znają pełne imię i nazwisko lub adres e-mail). Aktualnie dzieci poniżej 13. roku życia nie mogą zakładać kont, a profile 14 i 15-latków pokazywane są tylko częściowo. Serwis MySpace zmienił także sposób emitowania reklam; reklamy hazardu i randek nie wyświetlają się najmłodszym internautom. Impulsem, który spowodował te działania był 30 -milionowy pozew, jaki na serwis złożyła 14-letnia Amerykanka twierdząc, że była molestowana przez 19-latka, poznanego na serwisie MySpace (*Serwis internetowy MySpace zaostrza ograniczenia dla użytkowników* 2011).

Kodeksy dostawców usług internetowych

Jednym z podstawowych narzędzi używanych w ramach samoregulacji są kodeksy dobrej praktyki (kodeksy postępowania). Są opracowywane przez sam przemysł internetowy i zatwierdzane (w przypadku Australii również rejestrowane) przez właściwy organ regulacyjny, monitorujący ich przestrzeganie[8]. Kodeksy te zawierają zbiory reguł

[6] Członkami EuroISPA są: AFA - *Association des Fournisseurs d'Accès et de Services Internet*; AIIP - *Associazione Italiana Internet Providers;* ANISP - *The National Association of ISPs of Romania;* CZ.NIC - *Czech Internet Association;* ECO - *Verband der deutschen Internetwirtschaft;* FiCom - *Finnish Federation for Communications and Teleinformatics;* ICT-Norway - *Internet Service Providers Association of Norway;* ISPA Austria - *Internet Service Providers Austria;* ISPA Belgium - *Internet Service Providers Association Belgium;* ISPAI - *Internet Service Providers Association of Ireland;* ISPA UK - *Internet Services Providers Association UK* oraz LINX - *The London Internet Exchange.*

[7] Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google/YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klasa.pl, Netlog, One.lt, Skyrock, StudiVZ, Sulake/Habbo Hotel, Yahoo!Europe oraz Zap.lu.

[8] *Codes for industry co-regulation in areas of internet and mobile kontent*

i procedur stosowanych przez dostawców usług internetowych. Duży nacisk położony jest na wypracowanie wspólnych procedur usuwania z globalnej sieci materiałów nielegalnych oraz szkodliwych (Murawska-Najmiec 2005, s. 51).

Warto przypomnieć, że już w oświadczeniu *Nielegalne i szkodliwe treści w internecie* z 1996 roku, Komisja Europejska zachęcała ISP do przyjęcia ich własnych kodeksów etycznych. *Konwencja o Cyberzawartości z 2001 roku,* jak i dyrektywy unijne nie przewidują obowiązku tworzenia takich kodeksów. *Dyrektywa 2000/31/WE o handlu elektronicznym* pisze tylko o wspieraniu ich opracowywania na poziomie wspólnotowym (art. 16). Mają one przyczyniać się do sprawnej realizacji innych postanowień dyrektywy, zwłaszcza tych, które dotyczą odpowiedzialności prawnej ISP za materiały umieszczane w internecie przez osoby trzecie. Nowym elementem *Decyzji nr 854/2005WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. w sprawie kontynuacji wieloletniego programu wspólnotowego na rzecz bezpieczniejszego korzystania z internetu i nowych technologii sieciowych* jest przeznaczenie wsparcia finansowego na opracowanie transgranicznych, (a nie tylko krajowych) kodeksów postępowania w ramach programu *Safer Internet* (*Decyzja nr 854/2005WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r.*). Program dostrzega konieczność działań na poziomie wspólnotowym na rzecz zachęcania europejskiego przemysłu internetowego i nowych technologii sieciowych do wdrażania kodeksów postępowania. Zaleca tworzenie przejrzystych i sumiennych kodeksów postępowania, informowanie internautów o istnieniu linii interwencyjnych dla zgłaszania treści sprzecznych z prawem (np. Hotline, Dyżurnet.pl) (Murawska-Najmiec 2005).

W odpowiedzi na powyższe zalecenia w wielu państwach dostawcy usług internetowych dobrowolnie opracowali i przyjęli kodeksy postępowania. Są to m.in. *Spam code of conduct of ISPA* - Austria (*Spam code of ...* 2011); *Evropská Asociace Státnich Loterii A Toto Spolecnosti* - Czechy (*Evropská Asociace Státnich ...* 2011); *Code for the Chat Check Badge* - Dania (*Code for the Chat...* 2011); *Code of Conduct for search engines/Verhaltenssubkodex fur Suchmaschinenanbieter der FSM* - Niemcy (*Code of Conduct...* 2011); *Convenio de Autorregulación para promover el buen uso de Internet es Espańa* - Hiszpania (*Convenio de Autorregulación...* 2011); *Código deontológico de la Agencia de Calidad de Internet* - Hiszpania (*Código deontológico de la Agencia...* 2011) oraz *Good Practice Guidance for search service providers and advice providers and advice to the public on how to search safely* - Wielka Brytania (*Good Practice Guidance...* 2011).

Analizując powyższe kodeksy można zauważyć pewne cechy wspólne. Dostawcy usług internetowych zobowiązują się do podjęcia działań gwarantujących internautom swobodę wypowiedzi, prywatność, poufność komunikacji oraz ochronę danych osobowych i łączności elektronicznej. Ponadto: udostępniania w sposób jasny i rzetelny informacji o cenach świadczonych usług internetowych oraz o warunkach umowy przed jej podpisaniem, a także przestrzegania praw własności intelektualnej. Natomiast internauta jest zobowiązany do unikania świadomego tworzenia, przechowywania lub rozpowszechniania treści sprzecznych z prawem. Przestrzegania regulaminu korzystania z usług internetowych, w tym przepisów prawa autorskiego i praw własności intelektualnej oraz zakazu promowania spamu. W zakresie ochrony dzieci ISP zobowiązali się nie oferować płatnych usług abonamentowych małoletnim bez pisemnej zgody rodzica lub opiekuna oraz zapewnić procedury i techniczne aplikacje niezbędne do kontroli i monitorowania ich zachowań w internecie.

ISP nie mają obowiązku monitorowania treści zamieszczanych przez osoby trzecie, ale są zobowiązani do podjęcia odpowiednich działań w przypadku otrzymania zgłoszenia o niezgodnych z prawem treściach i zachowaniach w globalnej sieci. Ponadto nie mogą świadomie hostować hiperłączy do nielegalnych treści, z wyjątkiem, gdy jest to wymagane przez regulacje prawne. W sytuacji, gdy dostawca internetu dowiedział się o działaniach lub treściach, które zostały uznane za sprzeczne z przepisami prawa, musi zawiesić lub zamknąć stronę oraz przekazać informację do właściwego organu ścigania. W tym celu stowarzyszenia opracowały wspólne procedury zgłoszeń. Powinny prowadzić rejestr wszystkich przyjmowany zgłoszeń oraz wszelkich materiałów usuniętych z internetu przez okres co najmniej trzech lat.

Kodeksy internautów – netykieta

Drugim, obok dostawców usług internetowych podmiotem ponoszącym odpowiedzialność za treści zamieszczane w globalnej sieci są sami użytkownicy internetu. Reguły rządzące postępowaniem internautów były i nadal są tworzone na dwa sposoby. Odgórny - z inicjatywy prawodawców, reagujących na pojawienie się nowej przestrzeni aktywności społecznej, w której muszą obowiązywać normy prawne oraz oddolny: z inicjatywy użytkowników sieci, dostrzegających potrzebę takiego samoograniczenia. Rezultatem działań odgórnych są regulacje prawne (ustawy oraz przepisy prawa międzynarodowego). Natomiast inicjatywy oddolne doprowadziły do powstania pozaprawnych norm społecznych (m.in. netykieta). W niniejszym artykule zostały pominięte kwestie prawne, są one przedmiotem analizy w innych publikacjach (Zob. Gruchoła 2011, Gruchoła 2012). Autorka koncentruję sie na pozaprawnych normach społecznych. Zdaniem Karola Dobrzenieckiego „jest to kategoria

został opracowany przez krajowe stowarzyszenie *Internet Industry Association* na podstawie wymagań zawartych w *Ustawie Broadcasting Services Act.* Jego rejestracja przez organ regulacyjny miała miejsce w maju 2005 r. Kodeks reguluje obowiązki dostawców usług internetowych w zakresie hostowania zawartości internetu na terytorium Australii oraz w zakresie dostarczania dostępu do zawartości sieci pochodzącej zarówno z Australii, jak i spoza jej granic.

zbiorcza, na którą składają się normy religijne, obyczajowe, praktyki postępowania – systemy niejako zapożyczone ze świata materialnego. Egzekucja tych norm jest zdecentralizowana, a na straży ich przestrzegania stoi samo społeczeństwo, a nie organy państwowe. Odgrywają one ważną rolę w procesie samoregulacji cyberprzestrzeni" (Dobrzeniecki 2004, s. 38).

Za pierwszy kompleksowy zbiór zasad korzystania z internetu, powszechnie określany jako netykieta przyjmuje się opracowanie Arlene H. Rinaldi z Florida Atlantic University (dalej: FAU) z 1992 roku. Wskazała ona, iż naruszenie umownych zasad zachowania, dobrych obyczajów w globalnej sieci może spowodować pewne działania względem sprawcy takich czynów, czyli internauty (Kubas 2004, s. 17).

Definicja netykiety, choć nie jest najnowszym terminem, nie doczekała się encyklopedycznego przedstawienia. Netykieta (ang. *netiquette: network* - sieć i *etiquette* - etykieta) to „internetowy kodeks zachowań, zawierający zbiór specyficznych reguł zachowania, sposobów komunikowania się internautów, w szczególności biorących udział w dyskusjach, czatach czy na forach" (*Czym jest netykieta?,* s. 1). Netykieta to „normy postępowania w określonej grupie użytkowników wydzielonej części sieci internet, zawierające zbiór zasad, zgodnie z którymi należy postępować, aby uczynić korzystanie z sieci bardziej przyjaznym" (Brzozowski 1999, s. 39). To „żartobliwa nazwa zbioru zachowań etycznych umownie obowiązujących w internecie. Właściwy sposób zachowania się internautów pozwala na <współistnienie> w internecie osób z wielu obszarów kulturowych i sprzyja rozwojowi sieci" (*Czym jest netykieta?,* s. 1). Inna definicja określa netykietę jako „prawo internetu, spisane oraz zabezpieczone przymusem społecznym, nie państwowym. Naruszenie etykiety spotyka się z sankcją ze strony internautów wobec tego, kto dopuścił się naruszenia" (Gajowniczek 1999, s. 63).

Etykieta internetu czyli tzw. netykieta stanowi zbiór zasad, norm i dobrych praktyk określających zachowanie użytkowników internetu, obowiązujących w globalnej sieci. Ma charakter dobrych obyczajów, luźnych zaleceń, których przestrzeganie ułatwia życie wszystkim internautom. M.in. zakaz: umieszczania w sieci nielegalnych i szkodliwych treści oraz informacji, używania wulgarnego języka, wysyłania tzw. „listów łańcuszkowych" czy spamu itp. Ponadto nie należy publikować w internecie treści niezgodnych z przepisami prawa krajowego. W polskim prawie, będą to w szczególności:

- treści określone w *Kodeksie karnym*, które naruszają godność człowieka (zniesławienie: art. 202, art. 212 oraz znieważenie: art. 216); nakłaniają do popełnienia lub doradzają w popełnieniu samobójstwa lub samookaleczenia (art. 151). Zagrażają innym osobom popełnieniem przestępstwa na jego szkodę lub szkodę osoby jego najbliższej, umieszczają groźby w internecie (art. 190-191). Ponadto stosują „stalking" rozumiany jako uporczywe, złośliwe nagabywanie, naprzykrzanie się, które może wywołać u innej osoby poczucie zagrożenia (art. 190a). Obrażają inne narodowości, religie, rasy ludzkie (art. 194-196, art. 257); propagują totalitarny ustrój państwa lub nawołują do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość (art. 256). Dokonują kradzieży tożsamości **(**art. 267-268a); nawołują do popełnienia przestępstwa (art. 255); (*Kodeks karny; Ustawa z dnia 6 czerwca 1997 r.*);
- treści określone w *Kodeksie cywilnym*, które poniżają godność ludzką; zawierają pomówienia - informacje obarczające niepotwierdzonymi zarzutami inne osoby oraz obrażają inne narodowości, rasy ludzkie, religie (art. 23) (*Kodeks cywilny; Ustawa z dnia 23 kwietnia 1964 r.*, art. 23);
- treści określone w ustawach szczególnych, które przyczyniają się do łamania praw autorskich lub naruszają prawa autorskie i licencje podmiotów trzecich (*Ustawa z dnia 4 lutego 1994 r.*). Promują środki odurzające, narkotyki *(Ustawa z dnia 29 lipca 2005 r.).* Ujawniają bez wyraźnej zgody dane osobowe, identyfikatory komunikatorów internetowych, fotografie, adresy poczty elektronicznej, miejsce zamieszkania, pracy, przebywania, numery telefonów, tablic rejestracyjnych i inne poufne dane (*Ustawa z dnia 29 sierpnia 1997 r.)*. Zawierają słowa powszechnie uznane za niecenzuralne, wulgaryzmy (*Ustawa z dnia 7 października 1999 r.; Kodeks wykroczeń; Ustawa z dnia 20 maja 1971 r.)* i inne (Zob. Gruchoła 2011).

Jak dotąd, nie wytworzyła się jedna, powszechna netykieta. Najbardziej znanym jej opracowaniem, traktowanym nierzadko przez internautów jako wzorzec jest dokument Network Working Group RFC 1855: *Netiquette Guidelines* (*Netiquette Guidelines* 2011). Rodzaj netykiety uzależniony jest m.in. od osoby redagującej zasady właściwego zachowania w globalnej sieci, od miejsca, w którym korzysta z internetu. Inne są zasady w pracy, inne w domu, czy w szkole. Przede wszystkim netykieta różni się od „miejsca w sieci". Cyberprzestrzeń zawiera w sobie różne kultury zwane także wirtualnymi wspólnotami. Każda z tych wspólnot ma swoje własne reguły i zwyczaje. Ponadto poszczególne usługi internetowe np. grupy dyskusyjne, IRC przyjmują własne katalogi reguł postępowania co do, np. objętości nadsyłanej korespondencji. Sankcje za naruszenie zasad współżycia mogą przybrać różną postać. Osoba, która wypowiada się w ramach danej grupy w sposób niestosowny, może spotkać się z uprzejmym zwróceniem uwagi, ze strony bardziej doświadczonego użytkownika, ostrzeżeniem, a nawet gniewną słowną reprymendą, czyli tzw. *flamin-*

giem. Inne „prywatne" sankcje w takiej sytuacji to m.in. zablokowanie możliwości przesyłania wiadomości lub usunięcie z grona członków danej grupy dyskusyjnej czy też swoisty ostracyzm. Ostateczną karą w tym systemie jest rozłączenie (*disconnection),* które może być horyzontalne (tzn. pozbawianie możliwości komunikacji pomiędzy siecią lokalną a innymi sieciami) albo wertykalne (polegające na „odcięciu" użytkownika od internetu) (Dobrzeniecki 2004, s. 39-40).

Obok szczegółowych netykiet, regulujących zachowania określonych grup internautów wiele reguł odnosi się oraz obowiązuje w całej cyberprzestrzeni. Bardzo często zasady netykiety formułowane są w formie 10 przykazań. Zestawienie takie zaproponowała Virginia Shea w publikacji *Netiquette* (Shea 2009).

Nawiązując do tytułowego problemu kluczowym zagadnieniem są uprawnienia i ocena zachowania administratorów sieci. Umożliwiają one podgląd zawartości kont, a co więcej, dokonywanie w nich rozmaitych zmian, m.in. usuwanie danych. Netykieta powinna więc wskazywać na granice dopuszczalnej ingerencji administratorów w prywatne konta internautów. Kolejne zagadnienie dotyczy „nadzorowania", a dokładniej śledzenia „cyfrowych kroków" internauty przez różnego rodzaju agencje rządowe oraz firmy komercyjne. Proceder ten prowadzony jest między innymi przy wykorzystaniu programów typu *spyware* lub *sniffer*, których działanie polega na rejestrowaniu działań osoby w internecie. Informacje te są gromadzone na serwerach i na ich podstawie tworzone są profile poszczególnych internautów. Powszechną jest także praktyka „podpinania" spyware'ów pod wersje instalacyjne innych programów (np. wygaszacze ekranów i inne) bez wiedzy i zgody użytkowników internetu (Kubas 2004, s. 68-70).

Netykieta, jako honorowy kodeks internautów, powinna jasno wskazać na moralną odpowiedzialność jaka związana jest zarówno z samym celem komunikacji w globalnej sieci jak i wykorzystaniem do tego celu technologii umożliwiających kodowanie danych. Kolejnym zagadnieniem, które powinno mieć swoje odzwierciedlenie w netykiecie jest problem związany z szeroko pojętą wiarygodnością, a dokładniej z podszywaniem się, udawaniem kogoś innego podczas komunikacji online. Temat ten jest obecnie szczególnie aktualny w związku z nowelizacją prawa wprowadzającą karalność *groomingu*.

Istnieje również cała gama niebezpieczeństw związanych z netykietą. Jest to jakość opracowań tego rodzaju - każdy może napisać własną wersję i umieścić ją w internecie. Ponadto możliwość zatracenia znaczeń opracowań dobrych, czy stagnacja jej zaleceń. Sytuacja taka może mieć miejsce wówczas, jeżeli o netykietach internetowych przestanie się mówić, dyskutować na ich temat, jeśli ich twórcy poprzestaną na jednorazowym ich ogłoszeniu.

Podsumowanie

Odpowiedzialność za treści znajdujące się na stronach internetowych ponoszą trzy grupy podmiotów: dostawcy treści, dostawcy usług internetowych oraz użytkownicy internetu. Odpowiedzialność za prowadzone przez siebie strony internetowe z pewnością powinni ponosić ci, którzy mają bezpośredni wpływ na ich treść. Niezasadne wydaje się natomiast nakładanie odpowiedzialności na dostawców dostępu do internetu, którzy z jednej strony nie są w stanie faktycznie wywiązać się z tego obowiązku, z drugiej zaś otrzymują władzę znacznie wykraczającą poza kompetencje wynikające z ich funkcji. Obecnie, ani unijne, ani polskie ustawodawstwo nie przewiduje obowiązku administratorów serwera czynienia swoistego prewencyjnego *screeningu* stron internetowych udostępnianych za pomocą konkretnego serwera, celem odnalezienia bądź usunięcia nielegalnych treści. Przyznanie takiego uprawnienia, względnie obowiązku, mogłoby się łączyć z kolejnymi protestami. Administratorzy serwerów dysponowaliby uprawnieniami cenzora, a od ich uznaniowej decyzji miałoby zależeć stwierdzenie, że dana strona prezentuje nielegalne czy szkodliwe treści. Zarzut ten można jednak zanegować, powierzając kompetencje decyzyjne, co do dalszego udostępniania serwera organom ścigania. Reprezentowane też jest odmienne stanowisko, postulujące prawne określenie zakresu obowiązku ISP odnośnie kontrolowania i eliminowania niebezpiecznych treści z internetu oraz unormowanie ich współpracy z organami ścigania w zakresie monitorowania zasobów globalnej sieci i działań operacyjnych (Maroń 2008, s. 235).

Bez względu na różne stanowiska w tej kwestii nie ulega wątpliwości, że pewne mechanizmy prawne regulujące działania firm internetowych zobowiązujące je do kontroli i eliminowania niebezpiecznych treści z internetu są niezbędne. Technicznie nie jest możliwe kontrolowanie wszystkich materiałów publikowanych w globalnej sieci, przepisy prawne (o ile istnieją) zobowiązują zazwyczaj ISP do usuwania niebezpiecznych stron dopiero po każdorazowym powiadomieniu o ich istnieniu czy to przez policję, czy przez internautów. Najczęściej, po ich wcześniejszym wyświetleniu.

Ponadto obowiązujące przepisy prawa nie zawsze są skuteczne. Po pierwsze, nie umożliwiają egzekwowania przepisów prawa krajowego w innych państwach. Jest to istotne przy transgranicznym charakterze internetu. Po drugie, zauważa się rozbieżności europejskich i amerykańskich regulacji prawnych. Po trzecie, wszelkie próby wprowadzenia blokowania szkodliwych czy nielegalnych treści spotykają sie z protestami w imię wolności słowa.

Netykiety sieciowe będące rodzajem przewodników, drogowskazów dla nowicjuszy w cyberświecie oraz przypomnieniem o tych zasadach dla użytkowników, którzy je zatracili wskazują na konkretne zachowania, postawy, sytuacje, a nawet słowa

wyjaśniając, które z nich są dobre, a które niedopuszczalne. Służą standaryzacji praktyk internautów. W szczególności odnoszą się do: komunikacji, wymogów dotyczących stron WWW, zasad korzystania z materiałów zamieszczonych w internecie i związanej z tym odpowiedzialności. Wskazują na pewne normy etyczne, chociaż w ograniczonym zakresie. Stąd niezbędna jest ciągła praca nad zasadami netykiety, ciągłe dostosowywanie ich do nowych realiów jakie niesie ze sobą rozwój techniczny i społeczny, zmieniająca się rzeczywistość. Potrzebna jest nieustanna dyskusja na forum globalnym o zasadach netykiety, która będzie pobudzać świadomość społeczną o istnieniu zasad oraz wzmacniać konieczność ich przestrzegania dla dobra ogólnego. Konieczne jest pobudzenie globalnej świadomości o współodpowiedzialności wszystkich członków cyberświata za jego obecny oraz przyszły kształt. Netykieta mogłaby się stać aksjologicznym układem odniesienia dla użytkowników internetu wobec ich praktyk. Wymagałoby to jednak globalnej współpracy w zakresie aktualizacji jej zasad oraz ich promocji wśród wszystkich internautów. Kwestia ta jest bardzo istotna ze względu na wielonarodowy, wielokulturowy, zróżnicowany pod względem: wiekowym, rasowym, wyznania, światopoglądowym charakter tej społeczności.

Literatura:

1. Barta J., Markiewicz R. (1998), *Internet a prawo*. Wydawnictwo Universitas, Kraków.
2. Barta J., Markiewicz R. (2002), *Świadczenie usług drogą elektroniczną - nowa rzeczywistość dla prawników.* „Radca Prawny", nr 4-5, s. 66-78.
3. Brzozowski M. (1999), *Biznesowa etyka.* „WWW", nr 2, s. 36-39.
4. *Code for the Chat Check Badge,* http://www.fdim.dk/?pageid=52, [23.10.2011].
5. *Code of Conduct for search engines/Verhaltenssubkodex fur Suchmaschinenanbieter der FSM,* http://www.fsm.de/en/SubCoC_Search_Engines, [23.10.2011].
6. *Convenio de Autorregulación para promover el buen uso de Internet es Espańa,* http://www.aui.es/../biblio/documentos/legislacion/proteccion_menores/convenio/tex_conv.htm, [23.10.2011].
7. *Código deontológico de la Agencia de Calidad de Internet,* http://www.iqua.net/Codigos_de_conducta/Codigo_de_conducta/?go=WWiW6aWP3cIUyUj7fiM3LUP2TC+MOm3NphIdSA2vOCa_qmvpV3BPk GOo8, [23.10.2011].
8. *Czym jest netykieta?* http://www.netykieta.net/definicje.php, [03.08.2011].
9. *Decyzja nr 854/2005WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. w sprawie kontynuacji wieloletniego programu wspólnotowego na rzecz bezpieczniejszego korzystania z internetu i nowych technologii sieciowych,* Dz. Urz. L 149 z 11.05.2005.
10. Dobrzeniecki K. (2004), *Prawo a etos cyberprzestrzeni.* Wydawnictwo Adam Marszałek, Toruń.
11. *Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego,* Dz. Urz. L 178 z 17.07.2000.
12. *European Internet Service Providers Associations - EuroISPA*, http://www.euroispa.org/, [15.07.2011].
13. *Evropská Asociace Státnich Loterii A Toto Spolecnosti,* http://www.sazka.cz/o-nas/vice-osazka/zakony/kodex.php, [23.10.2011].
14. *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V,* http://www.fsm.de/, [19.08.2011].
15. Gajowniczek A. (1999), *Wykorzystanie internetu w celu reklamy. Wybrane zagadnienia prawne,* pracy magisterskiej. Dostępna na stronie: http://www.vagla.pl, [16.09.2009].
16. *Good Practice Guidance for search service providers and advice providers and advice to the public on how to search safely,* http://police.homeoffice.gov.uk, [24.10.2011].
17. Gruchoła M. (2012), *Ochrona użytkowników internetu w państwach Unii Europejskiej.* Wydawnictwo KUL, Lublin.
18. Gruchoła M. (2011), *Dangers in the Internet Communication and the Protection of Internet Users in the Era of Media Convergenc.* W: *Konwergencja mediów - media convergence - Medienkonvergenz".* Wydawca niemiecki, ss. 18, złożony do druku.
19. Gruchoła M. (2011), *Ochrona małoletnich internautów w prawie i praktyce państw Unii Europejskiej.* „Rozprawy Społeczne", T. V, s. 78-100.
20. *Jugendmedienschutz-Staatsvertrag z dnia 1 kwietnia 2003 r. - JMStV;* http://www.artikel5.de/gesetze/jmstv.html, [02.10.2011].
21. Kirwil L., *Polskie dzieci w internecie. Zagrożenia i bezpieczeństwo na tle danych dla UE. Wstępny raport z badań EU Kids Online przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców,* http://www.saferinternet.pl/images/stories/pdf/raport_eu_kids_online _polska_28-10-2010.pdf, [21.09.2011].
22. *Kodeks cywilny; Ustawa z dnia 23 kwietnia 1964 r.,* Dz. U. z 1964 r. Nr 16, poz. 93.
23. *Kodeks karny; Ustawa z dnia 6 czerwca 1997 r.,* Dz. U. z 1997 r. Nr 88, poz. 553 ze zm.
24. *Kodeks wykroczeń; Ustawa z dnia 20 maja 1971 r.,* Dz. U. z 1971 r. Nr 109, poz. 756.
25. Kubas G., *Netykieta - kodeks etyczny czy prawo internetu?,* Kraków: Uniwersytet Jagielloński 2004, s. 17, praca magisterska. Dostępna na stronie: http://www.vagla.pl, [16.09.2011].
26. Kulesza J. (2010), *Międzynarodowe prawo internetu.* Przedsiębiorstwo Wydawnicze *Ars boni et aequi,* Poznań.
27. Maroń G. (2008), *Ochrona małoletnich przed pornografią i pedofilią internetową*. W: R. Grabowski (red.), *Wpływ internetu na ewolucję państwa*

i prawa. Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów.
28. Murawska-Najmiec E. (2005), *Informacja na temat działań społeczności międzynarodowej na rzecz objęcia internetu systemem prawa przy jednoczesnej ochronie swobody wypowiedzi i informacji.* KRRiT, Warszawa.
29. *Porozumienia policji i rządu w sprawie blokowanie treści,* http://prawo.vagla.pl/node/5426, [27.08.2005].
30. *Serwis internetowy MySpace zaostrza ograniczenia dla użytkowników,* http://wirtualnemedia.pl/document,,1309742,Serwis_internetowy_MySpace_zaostrza_ograniczenia_dla_uzytkownikow.html, [22.06.2011].
31. Shea V., *Netiquette,* www.albion.com/netiquette/book/TOC09633702513.html, [09.09.2009].
32. *Spam code of conduct of ISPA,* http://www.ispa.at/downloads/COC_spam_english.pdf, [23.10.2011].
33. *Społeczności sieciowe: Komisja pośredniczy w porozumieniu głównych firm internetowych,* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/232& format=HTML&aged=0&language=PL&guiLanguage=en, [12.05.2011].
34. Stiftung Digitale Chancen (2009), *Zestaw zaleceń projektu Youth Protection Roundtable.* SDC, Hamburg.
35. Swetenham R. (2010), *Europejskie porozumienie dotyczące samoregulacji w zakresie bezpieczeństwa w portalach społecznościowych.* W: *Materiały konferencyjne z IV Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie.* Fundacja Dzieci Niczyje, Warszawa.
36. *UE: Zgoda Parlamentu na blokowanie pedofilskich treści,* http://di.com.pl/news/41219,0,UE_Zgoda_Parlamentu_na_blokowanie_pedofilskich_tresci.html, [29.10.2011].
37. *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,* Dz. U. z 2002 r. Nr 144, poz. 1204.
38. *Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii*, Dz. U. z 2009 r. Nr 98, poz. 817.
39. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,* Dz. U. z 1997 r. Nr 133, poz. 883 ze zm.
40. *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,* Dz. U. z 1994 r. Nr 24, poz. 83.
41. *Ustawa z dnia 7 października 1999 r. o języku polskim,* Dz. U. z 2002 r. Nr 37, poz. 349.
42. Waglowski P., *Niebezpieczne ideologie i nawoływanie do waśni,* http://prawo.vagla.pl/node/4773, [04.12.2009].
43. Waglowski P., *Szwedzi witają nowy porządek, czyli retencja danych na granicach,* http://prawo.vagla.pl/node/7961, [01.07.2010].

SUPPLIERS' AND USERS' RESPONSIBILITY FOR THE CONTENTS OF INTERNET PAGES UNDER THE LEGAL AND SOCIAL REGULATIONS

Social Dissertations, Issue 1 (VI), 2012

Małgorzata Gruchoła

The John Paul II Catholic University of Lublin

Summary: The aim of this paper is to present a map of hazards for the global network and identify entities responsible for the content of web pages (Internet Content Providers, Internet Service Providers and users of global networks), an analysis of the legal basis of their activities and the responsibility resulting from them in the title field (Directive 2000/31/EC of 8 June 2000, Art. 12-15, Act of 18 July 2002, Art. 14). In addition, the verification of self-regulatory actions (European Internet Service Providers Associations) and a discussion on the codes of content providers and Internet Service Providers (among others: Spam code of Conduct of ISPA - Austria, Evropská Asociace Státnich Loterii A Toto Spolecnosti – the Czech Republic, Code of Conduct for search engines/Verhaltenssubkodex Suchmaschinenanbieter der FSM - Germany and others). The article is concluded by an analysis of the codes of Internet users, that is, Netiquette, and summarising conclusions and demands.

The responsibility for the content found on websites is borne by three groups of entities: Internet Content Providers, Internet Service Providers and Internet users. The applicable law is not always effective. First, it does not allow for the enforcement of national laws in other countries. This is crucial for the cross-border nature of the Internet. Secondly, there is a divergence between European and American regulations. Third, any attempt to block of harmful or illegal content is met with protests calling for freedom of speech. Effective responsibility requires combining the experiences of various countries on the basis of a common, unified, global law.

Network Netiquettes as some kind of guides and signposts are designed to standardise the practices of Internet users. In particular, they relate to communication, requirements for websites, rules for the use of any material contained on the Internet and the related liability. Hence it is necessary to continuously work on Netiquette, and strive to adapt to the new realities posed by the changing reality. There is a need for a constant global forum discussion on the principles of Netiquette, which will foster social awareness of the existence of rules and reinforce the necessity of perceiving them in the context of the general well-being. It is necessary to foster global awareness of the common responsibility of all the members of the cyberworld for its current and future shape. This issue is important because of the multinational, multicultural and diverse (in terms of: age, race, religion and world outlook) nature of this community. The paper uses the analytical descriptive method.

Key words: subjective responsibility, Internet content, self-regulation, Netiquette

Introduction

Speaking of the need to observe the global network of legislation and non-legal social norms, one must first answer the questions: who has the right to enforce the standards developed for the Internet and who should be accountable for their violation? It is essential to identify the structure of responsibility for violating the law and to identify the entities bearing it. The fulfillment of this duty will on the one hand ensure legal certainty for Internet users, and on the other it will leave no doubt for national prosecutors and judges as for the scope of their competence in the application of national law. This issue is especially important when it comes to responsibility for the content of websites. The difficulty of the legal analysis of this aspect of the Internet stems from the fact of a wide range of entities involved in the emergence of such content aspect and having a positive impact on their shape.

The aim of this article is to present a map of Internet threats, identify the entities responsible for the content of websites (Internet Service providers and users of global network), to analyse the legal basis of their activities (Directive 2000/31/EC of 8 June 2000, Art. 12-15 , Act of 18 July 2002, Art. 14). In addition, it is also to verify self-regulatory actions (European Internet Service Providers Associations) and to discuss the codes of good practice, with an emphasis on Netiquette. The paper uses the analytical descriptive method.

List of Internet threats

According to Lucyna Kirwil children,,using the global network may face threats in four areas of social functioning: interpersonal relations based on violence, aggression and cruelty (the "Aggression" type), perverted sexual contacts (the "Sex" type), establishing a hierarchy of values and indoctrination in this field (the "Values" type) and market activities (the "Commercial" type). Internet users may be exposed to these hazards through contact with harmful content on the global network or through contact with other people on the Internet (Kirwil 2010, p 10). In both cases, part of the hazard results from the behaviour of Internet users, the other from

Table 1. The Classification of Internet threats

Threat type	Content (subject)	Contact	Behavior
Aggression	Violence /cruelty / experiencing drastic scenes	Harassment / bullying / aggressiveness on the part of others	Harassment / malicious behavior / aggressiveness (*cyberbullying)*
Sex	Pornography	Experiencing being seduced (*grooming)*	Sexting
Values	Racism / hatred	Ideological persuasion	Self-harm
Commercial	Marketing, persuasion	Abuse of privacy / use of personal data	Download of videos, documents, online gambling

Source: L. Kirwil, Polish children on the Internet. Hazards and safety against background data for the EU. Preliminary report on the EU Kids Online research conducted among children aged 9-16 years and their parents (Polskie dzieci w internecie. Zagrożenia I bezpieczeństwo na tle danych dla UE. Wstępny raport z badań EU Kids Online przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców), p.10, http://www.saferinternet.pl/images/stories/pdf/raport_eu_kids_online_polska_28-10-2010.pdf, [21. September 2011]

the manner of conduct of others. There are also threats with the assignment to one of these two dimensions resulting from the adopted perspective - the consumer or the manufacturer, especially for user-generated content. It hence follows that these two dimensions intermingle (See Gruchoła 2012, p 37).

By considering these four characteristics, it is possible to draw up maps of threats and forms of protection.

In the context of Internet content, it is important to distinguish between illegal content and harmful content. The interpretation of illegal and harmful content is provided by the justification for *Recommendations of the Committee of Ministers of the Council of Europe of 31 October 2001*. The first type includes the content of the conflict with national law. Harmful content is recognised as not necessarily illegal, but potentially carrying damage, especially

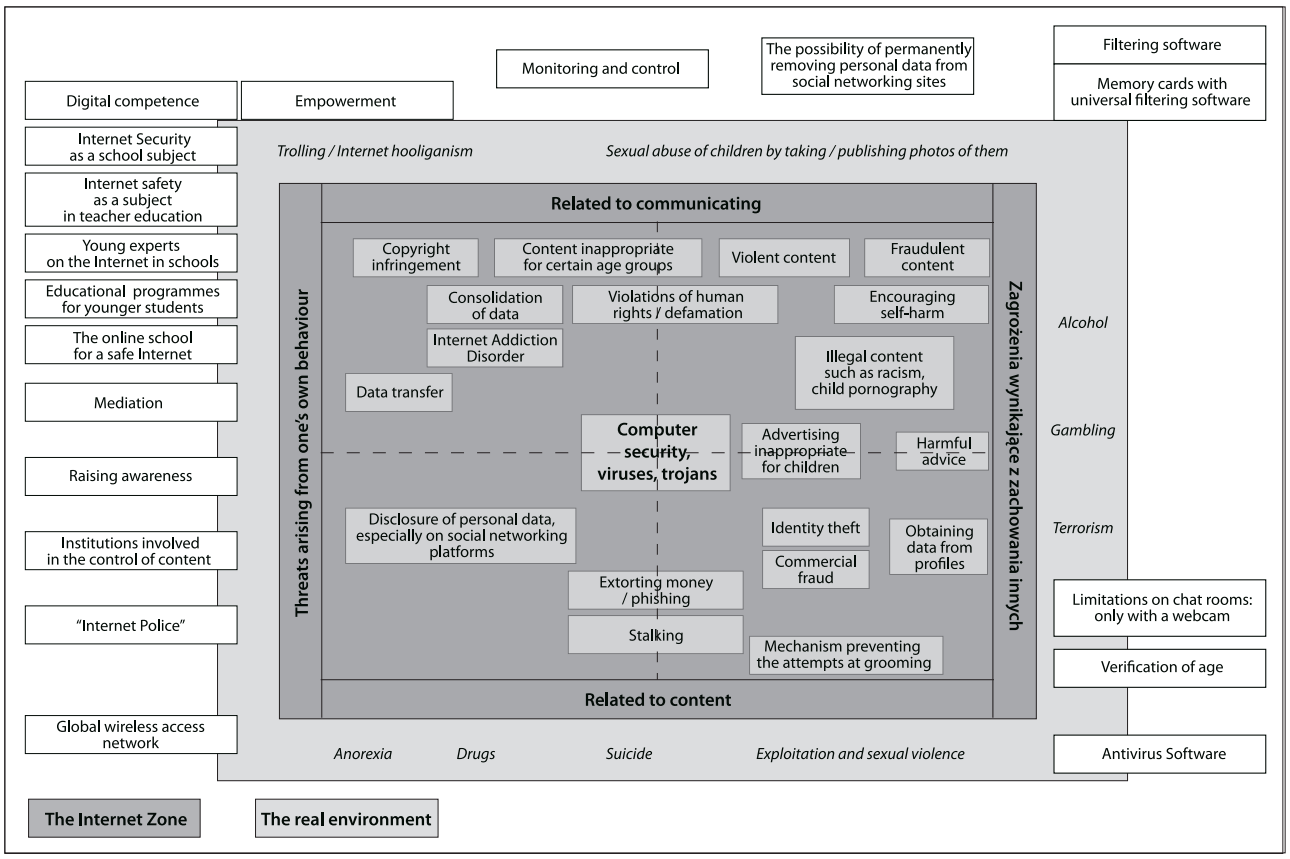


Figure 1. Summary of threats
Source: Stiftung Digitale Chancen (2009), The set of recommendations of the Youth Protection Roundtable. SDC, Hamburg, page 8

for the physical, mental and moral development of minors. The examples of harmful sites include content promoting religious movements, considered to be sects that present anorexia and bulimia as a lifestyle, and not a serious disease, instigating to suicide or self-harm, promoting drugs and other stimulants and pharmaceuticals such as rape pills.

The first group of threats (associated with content) comprises: unsuitablefor certain age groups (pornography), including violence, fraudulent, encouraging self-harm, violating human rights and dignity. In addition, inappropriate advertising and marketing directed at children, a practice associated with the retention and transfer of data or copyright violations.

The second group of threats comprises the ones related to communicating via the Internet. These include: stalking, bias bullying, electronic mobbing, change of identity and behaviour online, harmful advice, Internet clubs of suicides, Internet Addiction Disorder, identity theft, extorting money / phishing, commercial fraud, seducing children (grooming), cyberbullying, trolling and flaming, disclosure of personal data information, obtaining data from Internet profiles, social and digital exclusion and others. Groups at risk of digital exclusion, as well as social exclusion in general, are mostly badly-educated people, the unemployed, the disabled and the elderly, and also those who lack access to computers and the Internet (See more Gruchoła 2012, pp. 37-48, 2011 Gruchoła , pp. 78-100).

The possible forms of protection for global networks users are discussed in a separate monograph (See M. Gruchoła (2012), *Protection of Internet Users in the European Union Countries* (Ochrona użytkowników internetu w państwach Unii Europejskiej). Published by KUL, Lublin, p. 381). The most significant ones that deserve to be recalled are: legal regulations, digital competence, self-regulation of Internet providers, „bottom up" actions of global network users, appropriate software and technical equipment in support of protection.

The entities responsible for the content of web pages

The term *Internet Service Providers* (hereinafter ISPs) is often used in a general way, without distinguishing between the service of the Internet access provision (*access providers*) and storage services (*hosting*), and the transmission of content (*so-called content providers*). One and the same company may belong to different categories, and the differences between them are specified by *Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Articles 12-15) (Directive 2000/31/EC of 8 June 2000)*. In practice, Internet Service Providers offer several types of services, including the service of connection to the Internet. If the suppliers limit themselves to that, they would actually be only an access service provider, and the use of the global network would depend entirely on the user. However, very few providers are limited to such a simple service. Most of them offer e-mail, newsgroups, web servers, maintaining personal web pages, servers, game servers or software for chats. In this case, in the light of the aforementioned Directive (Article 14), their responsibility may be greater.

The responsibility for the content contained on the website can theoretically be borne by four groups of entities:

1. *Internet Content Providers*, hereinafter ICP;
2. *Internet Service Providers*, hereafter ISP;
3. *Internet Access Providers*, hereafter IAP
4. the Internet users (See Kulesza 2010, p 160)[1].

The Internet Content Provider is most frequently the creator itself of the information or data placed on the global network. The ISP is an entrepreneur who provides the services of allowing connections to the Internet (many of them are telecommunications companies).

Where the responsibility of the authors themselves for the content of the Internet is unquestionable or, in the cases specified by law, the responsibility of Internet users (where the mere possession of information or materials of the specified character is a felony, e.g. child pornography), then - according to Janusz Barty and Richard Markiewicz - the issue of Internet content providers is still the subject of heated discussion (Barta, Markiewicz, 2002). This applies to the entities that make their material on the network (servers) available in order to store and share other people's material (host providers).

The uniqueness of such a type of entities is that, unlike the *access providers* they have an impact on the flow of content within the global network. They can check the stored data, and even remove them, if they deem it appropriate. However, the question is to what extent this power should be used and on what grounds it should be based. These questions are particularly relevant to the circle of countries regarded as democratic, in the context of the problem of freedom of speech in the global network. In these countries the responsibility of Internet Service Providers is limited, if any at all. „Some representatives of the doctrine postulated that the *host provider* is required to be controlled as much as the publisher accepting the advertisement for publishing, and thus remain under scrutiny, if the user did not commit a violation of the statutory laws" (Bart, Markiewicz, 2002, p 76).

The laws determining the nature of ISP responsibility in Community law are set out in Art. 12-15 of the *Directive on electronic commerce (Directive 2000/31/EC of 8 June 2000).* According to the above Articles, ISPs are not responsible for activities involving the provision of „mere conduit" services (Ar-

[1] J. Kulesza compares the responsibilities of *Internet Service Providers to Internet Access Providers*.

ticle 12)[2], caching (Article 13)[3] and hosting (Article 14)[4]. However, the provision of the Directive gives the Member States the possibility of the requirement from a service provider through a court or an administrative body, under the laws of the State, to terminate an infringement or prevent it. The general clause of Article 15 of the *Directive on electronic commerce* exempts service providers from the supervision of the provided content.

The internal regulations of the State may, however, result in immediate notification by the ISP of the competent public authorities of the alleged illegal activities undertaken by the recipients of their service or the information provided by them. In addition, they are often required to report to the competent authorities, at their request, on the information enabling the identification of recipients with whom they have concluded data storage agreements (Article 15 paragraph. 2)[5]. Under Polish law, it results from the statutory introduction of a responsibility exemptions of a service provider from the provision of electronic services (*Act of 18 July 2002, Art. 14*).

Under the Act of 2002: the service provider providing services electronically, including providing access to a telecommunications network or data, is not responsible for the content of this data, if they:

- do not initiate the transmission of data;
- do not select the receiver of data transfer;
- do not select or modify the information contained in the transmission.

Exemption from the responsibility, as mentioned above, also includes automatic and short-term intermediate storage of data in order to realise and carry out data transmission (*Act of 18 July 2002, Article 12*). Moreover: anyone transmitting data, and providing automatic and short-term intermediate storage of these data in order to accelerate access to them again at the request of another entity, is not responsible for the stored data if:

- they do not modify the data;
- they use recognised and commonly-used IT techniques in this type of activity, defining the technical parameters of the data access and updating it;
- they do not interfere with the use of information techniques, recognised and commonly applied in this type of activity for obtaining the information about the usage of the collected data (Article 13.1).

Also, anyone who under the conditions referred to above, removes them immediately, or prevents access to them, is not responsible for the stored data if they receive the message that the data has been removed from the initial source of transmission or access to it has been prevented. Furthermore, when a court or another responsible body has ordered its removal or prevented access to it (*the Act of 18 July 2002, Art. 13.2*). According to Art. 14.1.: [...] "Anyone providing the resources of a teleinformatics system for storing data by the recipient who is not aware of the illegal nature of the data or the related activities, and in the event of receiving an official notification or obtaining a reliable message about the illegal nature of the data or the related activities immediately prevents access to the data, is not responsible for the content of this data "(*Act of 18 July 2002, Art. 14*).

As the above examples show the European Union

[2] Article 12 Mere conduit
1. Member States shall ensure that in the case of an information society service consisting of the transmission in a communication network of information provided by the customer or to provide access to the telecommunications network the provider is not responsible for the information if they:
   a) do not initiate the transmission;
   b) do not select the receiver of the transmission and
   c) do not select or modify the information contained in the transmission.
2. Acts of transmission and the provision of access referred to in paragraph. 1 include the automatic, intermediate and transient storage of information transmitted in so far as this serves only to carry out the transmission on a communication network, and that the storage period is no longer than is it reasonably necessary for the transmission.3. This article does not affect the possibility of demanding from a service provider through a court or an administrative body, under the laws of the State to terminate an infringement or prevent it.

[3] Article 13. Caching
1. Member States shall ensure that in the case of the provision of an information society service consisting of the transmission on a communication network of information provided by the service provider is not responsible for the automatic, intermediate and temporary storage of that information, performed in order to improve the onward transmission of information at the request of other recipients, provided that:
   a) the provider does not modify the information;
   b) the provider complies with the conditions of access to information;
   c) the provider complies with Internet service providers rules regarding the updating of the information referred to in a manner widely recognised and used by the industry;
   d) the provider does not interfere with the lawful use of technology, widely recognised and used by the industry to obtain data on the use of information and
   e) the service provider promptly removes or prevents access to stored information, upon obtaining a reliable message that information has been removed from the initial source of transmission or access to it has been prevented or if a court or administrative body has ordered the removal of information or prevented access to it.
2. The Article shall not affect the possibility for a court or administrative body, under the laws of the Member States, to terminate the infringement or prevent it.

[4] Article 14 Hosting
1. Member States shall ensure that in the case of the provision of an information society service consisting of the storage of information provided by the recipient the provider was not responsible for the information stored on the request of the recipient, provided that:
   a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages – they are not aware of facts or circumstances that clearly testify to the illegality, or
   b) the provider acts expeditiously to remove or prevent access to information, upon obtaining such message or being informed about it.
2. Paragraph 1 shall not apply if the recipient operates under the authority or under the control of the provider.
3. This Article shall not affect the possibility for a court or administrative body, under the laws of the Member States, to terminate an infringement or prevent it, and it does not affect the possibility of establishing procedures governing the removal or prevention of access to information by Member States.

[5] Article 15 No general obligation for monitoring.
1. Member States shall impose on providers of the service as defined in Article. 12-14 neither the general obligation to monitor the information which they transmit or store, nor a general obligation to search actively for facts or circumstances indicating illegal activity.
2. Member States may provide in relation to providers of information society services the obligation to immediately inform the responsible public authorities of alleged illegal activities undertaken by the recipients of their service or the information provided by them or to provide the competent authorities, on their request, with the information enabling to identify their recipients, with whom they have concluded storage agreements.

Member States, including Poland, widely practices releasing service providers from responsibility for the content they provide.

According to Barta and Markiewicz the responsibility of Internet Service Providers can be then compared to the responsibility of librarians, booksellers, or those retransmitting programmes (Barta, Markiewicz 1998, p. 221). "We cannot be held responsible for the actions of our users - say Internet Service Providers, and, therefore, in the regulations, they lobbied for providing electronic services around the world - whether in the U.S. under the DMCA, or in Poland, under Art. 14 of the *Act on Electronic Services* – the introduction of the responsibility exemptions (if they do not know what is sent in those links between the users ") (Waglowski 2010, p 1). The situation is, however, completely different in Asian countries, where service providers are legally required to filter the content delivered and bear the responsibility for content which cannot be blocked.

What are the practical implications of the above-analysed legal regulations?

It should be emphasised that, if the ISP is organised as self-governing, it is subject to the law applicable to the territory on which it is located. An example of the lack of capacity to enforce national laws in other countries is the actions of the German Ministry of Justice, which since 2000 has been browsing the Web addresses of a neo-Nazi character (e.g. nsdap.de) and has been calling for their removal. The law that applies there, and prohibits the questioning of the Holocaust and spreading Nazi propaganda, also extends to the Internet, even if such content is generated abroad. The law allows prosecutors pursuing promoters of the above content, wherever they are and whatever their nationality is, provided that their websites are available in Germany. Despite such stringent German regulations the number of web pages with the radical-right content continues to rise (Kulesza 2010, p 109). The source of the problem is the law, which exempts the responsibility of Internet access providers (i.e. those who provide access to content). The existing law contains only website owners.

This above issue is illustrated by another example. In 2001, the authorities of North Rhine-Westphalia ordered eighteen Internet providers operating there to block access to two American websites "proclaiming" Nazi ideas. The providers, referring to the administrative order, argued that they could not be held responsible for the content of various websites exempted from their control (Waglowski 2009, p. 1). Hence, U.S. sites are often a refuge for those who break national or European regulations.

Another problem is the divergence between European and American regulations. An example is the issue of a Nazi memorabilia auction on the French branch of the U.S. portal Yahoo!, which still has not found its definitive solution. In early 2003, a French court decided that the French should not have access to the auctions held on the pages of the American giant, because the law prohibits the display or sale of Nazi memorabilia. After this decision the Yahoo! site tried to prevent the French from having access to such listings. In parallel, the U.S. federal court decided that Yahoo! did not need to comply with French law. The consequence of this decision was, among others, court proceedings in France, where three independent organisations accused Tim Koogle (head of Yahoo!) of justifying war crimes and crimes against humanity. The court in Paris found that such justification would mean "praising crime, or at least presenting it in a positive light." The activities of the portal did not constitute a criminal offence according to the court (Waglowski 2009, p. 3).

The examples quoted above show the cross-border issue of responsibility for content on the global network. It concerns the application of domestic law norms to the Internet, and more specifically the lack of capacity to enforce national laws in other countries, and their ineffectiveness. Effective responsibility requires combining the experiences of various countries on the basis of a common, unified global law.

Another problem is blocking access to certain websites. Blocking the Web as a means to combat pedophilia on the Internet has often been analysed in Poland, the European Union and beyond its borders. The need to combat child pornography gave the reason for the idea of introducing the Registry of Sites and Services Prohibited in Poland. Protection against pedophilia may become a pretext to monitor search engines. Opponents fear that the blocking of sites will be a measure abused and / or expanded to other violations (e.g. copyrights) and content (e.g. criticising the authorities). In turn, the supporters of blocking focus on the welfare of children.

In October 2011 the EU Parliament adopted a compromise solution whereby blocking at the EU level is an optional measure, not mandatory. MEPs agreed that in situations where it is impossible to remove sites with pedophiliac materials it may be necessary to block them. Any block should be applied in a transparent manner. But this is not necessarily a measure required by the Directive. The decision on this matter will have to be made by the Member States. They will have two years to adapt national legislation to the requirements of Directive (the EU: Parliament's Consent ... 2011).

Earlier, in 2005 Finnish Government reached an agreement with the ISP companies on blocking access to websites containing child pornography. According to the Polish Press Agency: "The police will provide online businesses with a list of about a thousand Internet addresses that should be blocked. The Minister of Communications Leena Luhtanen hopes that the Government's agreement with ISPs means that it will not need to enact legislation enforcing the blocking of child porn sites "(Agreement, the police and the Government ... 2011, p.1). The block is also applied on a similar basis in Norway and Sweden. Why block content rather than prosecute offenders? The latter remain unidentified or are beyond the

reach of law enforcement in the country. The existing provisions of law are not so effective then.

Despite widespread agreement for the responsibility of Internet content providers as the entities having a direct influence on the shape of the content on the global network, their current legal situation - as rightly pointed out by Joanna Kulesza - raises many concerns and questions (Kulesza 2010, p 164). The basic problem, which involves the question of the responsibility of the ICP, involves the question of the legal entity qualified to assess the content - whether it is sovereign, where the ICP operates, or a surfer who considers themselves to be the victim of that action? This lack of agreement between States is being attempted to be solved by administrators and website owners on their own, especially with the use of regulations drawn up by themselves. Their task is to preclude the operator from responsibility in all locations where the site administered by them is available. Many websites contain General Terms of Use on one of their subpages, which often also include regulations on the legal system, which governs the "place" in cyberspace. Naturally, the operators and administrators of websites rely on the most beneficial or most convenient legal system for them, as regulating their interactions with the site users. The main drawback of such records is that users are often simply not familiar with their content, ignore them, or are not aware of their existence at all. Hence, the effectiveness of the consent to be subject to the laws and regulations designated by the website operator thus expressed by the website user appears questionable. At the same time, it is the most popular usual way to avoid problems with foreign jurisdictions site administrator, allowing the unambiguous definition of the legal system governing the party and the relationship between its author, administrator and users. To enhance the effectiveness of the provisions of these regulations, however, it would be appropriate to consider the practical possibility of ensuring that all the users of a particular site are actually aware of the fact that by using its services they agree to subject themselves to the legal regime of the State selected by the owner or administrator. For this purpose, activities aimed at raising awareness of the Internet users who have consented to these conditions should be carried out. Currently, a common way to alleviate complaints about the small "visibility" of the conditions of the contract is a solution in which an Internet user must press the screen "button", confirming the conditions and terms of use. Such protection allows a website author to raise the argument for the clear presentation of the relevant regulations which are to be obeyed in his service. However, they are usually documents of a large volume, and most Internet users do not bother reading them,; what's more - it is difficult to prove who actually gave this consent. The binding force of these agreements is undermined for those reasons - the majority expressing their consent usually do not get acquainted with content of them (Kulesza 2010, p. 165).

Associations of Internet Service Providers

Regardless of their legal obligations ISPs make associations (Internet Service Providers Association, hereinafter: ISPA), which determine the internal rules of operation, restricting the freedom of the posted illegal and harmful content on global networks. The largest association bringing together European Internet Service Providers is the European Internet Service Providers Association (hereinafter referred to EuroISPA) operating since 1997, representing more than 1 700 suppliers from EU and EFTA countries. The Association aims to represent the European Internet industry in EU policy and to facilitate the exchange of best practice between national ISP associations (European Internet Service Providers Associations 2011)[6]. The Association has adopted the policies established by the Council of Europe for voluntary cooperation between Internet providers and the justice system to remove illegal and harmful content and Internet services.

Another example here is the German Association of Voluntary Self-Control of Multimedia Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter eV). Its main task is to ensure the protection of children and young people on the Internet. Everyone is entitled to make a complaint to the office of the Association on illegal and harmful content available on the global network, on other networks or online services. Also, members of the Bureau may oppose on their own initiative State associations, breaking its basic objectives (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter eV 2011). The Association's activity is regulated by the § 19 of the Treaty on the protection of minors and human dignity in the media (Jugendmedienschutz-Staatsvertrag) (Jugendmedienschutz-Staatsvertrag of 1 April 2003, Art. 5).

Also, the first European voluntary agreement on Safer Social Networking Principles for the EU, to improve the safety of teens using social networking sites, is worth noting. It was signed on 10 February 2009 by 17 online companies[7]. This document sets the recommendations and principles to guide the owners of social networking sites, in order to minimise the threats faced by children and adolescents (Swetenham 2010, p. 20). The seven main recommendations are: 1) Increasing knowledge on the safe use of the Internet among children, parents and guardians in a simple and accessible way to a given age group. 2) Adjusting the content of websites to

[6] EuroISPA members are: AFA - Association des Fournisseurs d'Accès et de Services Internet, AIIP - Associazione Italiana Internet Providers; ANISP - The National Association of ISPs of Romania; CZ.NIC - Czech Internet Association, ECO - Verband der deutschen Internetwirtschaft; FiCom - Finnish Federation for Communications and Teleinformatics, ICT-Norway - Internet Service Providers Association of Norway, Austria ISPA - Internet Service Providers Austria, ISPA Belgium - Internet Service Providers Association Belgium; ISPAI - Internet Service Providers Association of Ireland, ISPA UK - Internet Services Providers Association UK and LINX - The London Internet Exchange.

[7] Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google / YouTube, Hyves, Microsoft Europe, Myspace, Nasza-klasa.pl, Netlog, One.lt, Skyrock, StudiVZ, Sulake / Habbo Hotel, Yahoo! Europe, and Zap. lu.

the age of the target group. 3) Providing Internet tools and technologies for users to increase online safety. 4) Providing user-friendly mechanisms for reporting breaches of security and the privacy of Internet users. 5) Responding to the reports on illegal content or behaviour. 6) Care for the privacy of users. 7) The evaluation of control measures on illegal or prohibited content and activities.

Portal administrators pledged to reduce threats by ensuring:

- a simple-to-use "report abuse" button allowing a one-click report on inappropriate contact or conduct by another user;
- a default setting for private / confidential in the case of the full online profiles and contact lists of those website users who are registered as minors (difficulty in establishing contact with minors);
- the inability to search private profiles of users under 18 (on websites or via search engines);
- the constant visibility and accessibility of a privacy protection option so that users can easily work out if only their friends, or all Internet users, see what they post in the global network;
- the prevention of the use of services by underage users, if a social networking site targets teenagers over 13 (registration by younger people will be more difficult) (Network Communities 2011).

All signatories are obliged to provide information determining how the above principles have been implemented on the websites run by them. One such declaration is the limitations established by MySpace, intended to hinder making friends with children by adult website users. Internet users aged over 18 cannot be added to the network of friends by 14 and 15-year- olds (except when they know your full name or e-mail). Currently, children under 13 cannot create online accounts, and profiles of 14 and 15-year-olds are shown only partially. The MySpace service has also changed the method of issuing advertisements - advertisements for gambling and dating are not displayed to the youngest Internet users. The impulse that caused these activities was a $30-million lawsuit filed by a 14-year-old American who said she was being molested by a 19-year-old she met on MySpace (MySpace Internet service tightens restrictions for users 2011).

Codes of Internet service providers

One of the basic tools used within self-regulation is codes of good practice (codes of conduct). They are developed by the Internet industry itself and approved (in the case of Australia also registered) by the appropriate regulatory body that monitors compliance with them[8]. These codes contain sets of rules and procedures used by Internet service providers. A strong emphasis is put on developing common procedures for removing illegal and harmful materials from a global network of (Murawska-Najmiec 2005, p. 51).

It is worth recalling that in the declaration on Illegal and harmful content on the web of 1996, the European Commission urged ISPs to adopt their own codes of ethics. Convention on Cyber Value of 2001, as well as the EU directives do not require the creation of such codes. Directive 2000/31/EC on electronic commerce says only about supporting their development at Community level (Article 16). They are to contribute to the smooth implementation of other provisions of the Directive, particularly those relating to ISP responsibility for the material posted on the Internet by third parties. The new element in Decision No. 854/2005WE European Parliament and the Council of 11 May 2005 on the continuation of multiannual Community Programme on promoting safer use of the Internet and new network technologies is the allocation of financial support for the development of cross-border (and not just national) codes of conduct under the Safer Internet Programme (Decision No 854/2005WE European Parliament and the Council of 11 May 2005). The programme recognises the need for action at Community level to encourage European Internet industry and new network technologies to implement codes of conduct. It recommends the creation of transparent and conscientious codes of conduct, informing Internet users about the existence of hotlines for reporting illegal content (e.g. Hotline, Dyżurnet.pl) (Murawska-Najmiec 2005).

In response to these recommendations, Internet Service Providers in many countries have voluntarily developed and adopted codes of conduct. Evropská Asociace Státnich Loterii A Toto Spolecnosti – Czech Republic (Evropská Asociace Státnich ... 2011); Code for the Chat Check Badge – Denmark (Code for the Chat... 2011); Code of Conduct for search engines/ Verhaltenssubkodex fur Suchmaschinenanbieter der FSM – Germany (Code of Conduct... 2011); Convenio de Autorregulación para promover el buen uso de Internet es España - Spain (Convenio de Autorregulación... 2011); Código deontológico de la Agencia de Calidad de Internet – Spain (*Código deontológico de la Agencia...* 2011) and *Good Practice Guidance for search service providers and advice providers and advice to the public on how to search safely* – Great Britain (*Good Practice Guidance...* 2011).

By analysing these codes some common features can be noticed. Internet Service Providers are obliged to take action to ensure Internet users freedom of speech, privacy, confidentiality of communications and protection of personal data and electronic communications. In addition, sharing in a clear and reliable way information on the prices

[8] Codes for industry co-regulation in the areas of Internet and mobile phone content was developed by the National Association of the Internet Industry Association on the basis of the requirements contained in the Broadcasting Services Act. Its registration by the regulatory body took place in May 2005; the Code regulates the obligations of Internet Service Providers within hosting Internet content on the territory of Australia and providing access to Web content both from Australia and beyond it.

of Internet services and on the terms of the contract before signing it, and respecting intellectual property rights. The Internet user, however, is required to avoid the conscious creation, storage, or distribution of illegal content, to comply with the regulations for the use of Internet services, including the rules of copyright and intellectual property rights and the ban on the promotion of spam. In the field of child protection ISPs have committed themselves not to offer paid subscription services to minors without the written consent of a parent or guardian and to provide technical procedures and applications necessary to control and monitor their behaviour on the Internet.

ISPs are not obliged to monitor the content posted by third parties, but they are required to take appropriate action on receiving reports on illegal content and behaviour in global networks. In addition, they are not permitted to host illegal content intentionally, except where the content is required by the regulations. In the situation where the Internet service provider knows about activities or content that has been declared contrary to the law, they shall suspend or close the page and provide information for the relevant enforcement body. For this purpose, the association has developed a common application procedure. They should keep the records of all the accepted applications, and any materials removed from the Internet for at least three years.

Codes of the Internet users – Netiquette

The second entity, in addition to Internet Service Providers, bearing the responsibility for the content of the global network, is the Internet users themselves. The rules governing the conduct of Internet users have been and still are created in two ways. The top-down; the initiative of lawmakers, responding to the emergence of a new sphere of social activity in which the legal standards must be applied; and the bottom-up: at the initiative of web users who see the need for such self-restraint. The result of the top-down actions are regulations (laws and rules of international law), whereas, the bottom-up initiatives have resulted in extra-legal social norms (such as Netiquette). This article has omitted legal issues - these are analysed in other publications (See Gruchoła 2011, Gruchoła 2012). The author focusses on extra-legal social norms. According to Karol Dobrzeniecki "this is a common category, which consists of religious norms, customs, and practices of conduct – the kind of systems borrowed from the material world. Enforcement of these standards is decentralised, and the society itself guards its observance, not the authorities. They play an important role in the process of the self-regulation of cyberspace "(Dobrzeniecki 2004, p. 38).

The first comprehensive set of rules for the use of the Internet, commonly referred to as Netiquette, is assumed to have been developed by Arlene H. Rinaldi of Florida Atlantic University (hereinafter FAU) in 1992. She indicated that the breach of the conventional rules of conduct and good manners on the global network could lead to some action against the perpetrators of such acts,that is an Internet user (Kubas, 2004, p. 17).

The definition of Netiquette, although it is not the most recent term, has never entered an encyclopedia. Netiquette (Eng. Netiquette: network and etiquette) is the "Internet code of conduct, which contains a set of specific rules of behaviour, ways of communicating by Internet users, in particular taking part in discussions, chats or forums" (*What is Netiquette?*, p. 1). Netiquette is the "standards of conduct in a particular group of users of a particular part of the Internet, containing a set of rules which are to be obeyed to make use of the network more friendly" (Brzozowski, 1999, p. 39). This is a "lighthearted name for established ethical behaviour conventionally binding on the Internet. The right way to behave on the Internet allows the online "coexistence" of people from many cultural regions and it promotes the development of a network "(*What is Netiquette?*, p.1). Another definition identifies Netiquette as "the Internet law, written and secured by social coercion, and not by the State. Violation of the label met with sanctions from the Internet users against the person who committed the violation "(Kolbe, 1999, p. 63).

Internet etiquette i.e. Netiquette, is a set of rules, standards and best practices, defining the behaviour of Internet users, in force on the global network. Its essence is good morals, loose guidelines whose observance makes life easier for all Internet users. Among other things, the prohibition of: placing of illegal and harmful content and information on the Internet, using foul language, sending so-called "chain letters" or spam, etc. Also, it is prohibited to publish content inconsistent with the provisions of national law on the Internet. In Polish law, this shall include in particular:

- content specified in the *Penal Code* that violates human dignity (defamation: Art. 202, Art. 212 and insulting: Art. 216), encourages to commit or advise on the commission of suicide or self-harm (Article 151). It coerces other persons to commit an offence of damage or injury to one or their closest persons, it places a threat on the Internet (Articles 190-191). In addition, it uses the word "stalking", understood as persistent, malicious solicitation and molestation, which may create another person's sense of danger (Art. 190a). It offends other nationalities, religions, and human races (Article 194-196, Art. 257); it promotes the totalitarian system of the State or incites hatred on national, ethnic, racial and religious grounds, or because of denomination (Article 256). It commits identity theft (Article 267-268a); it calls for committing a crime (Article 255), *(Penal Code, Act of June 6, 1997)*;

- the content specified in the *Civil Code*, which humiliates human dignity; contains slander - uncorroborated allegations blaming others and offends other nationalities, races, and religions (Article 23) (*Civil Code, Act of April 23, 1964, Art. 23*);
- the content specified in the specific Acts that contributes to a violation of copyright laws or infringes the copyrights and licences of third parties (*the Act of February 4, 1994*). It promotes narcotics and drugs (*Act of 29 July 2005*). I reveals, without express permission, personal data, Internet messaging IDs, photos, email addresses, place of residence, employment, residence, phone numbers, licence plates and other confidential data *(Act of August 29, 1997*). It contains words commonly regarded as obscene, profane *(Act of 7 October 1999; Code of offences, Act of May 20, 1971)* and others (See Gruchoła 2011).

So far, not a single common Netiquette has been developed. Its most popular development, often treated as a standard by Internet users, is the document Network Working Group RFC 1855: *Netiquette Guidelines* (*Netiquette Guidelines* 2011). The type of Netiquette depends, among other things, on the person editing the principles of the proper conduct in the global network, from the point they use the Internet. Others are the principles at work, others at home or at school. First of all Netiquette is different from the "Web Site". Cyberspace contains a variety of cultures, also called virtual communities. Each of these communities has its own rules and customs. Furthermore, the individual Web services such as newsgroups and the IRC, adopt their own rules of behaviour catalogues as to, e.g., the volume of sent correspondence. Sanctions for the violation of intercourse may take various forms. A person who speaks for the group in an inappropriate manner may meet with a polite admonition from the more experienced user, warning, or even an angry verbal rebuke, i.e. *flaming*. Other "private" sanctions in this case include blocking the possibility of sending messages, or the removal by a member of a particular newsgroup or a kind of ostracism. The ultimate punishment in this system is disconnection, which can be horizontal (i.e. deprived of the possibility of communication between the local network and other networks) or vertical (consisting of "cutting off" the user from the Internet) (Dobrzeniecki 2004, pp. 39-40) .

In addition to the detailed Netiquettes governing the behaviour of specific groups of Internet users a lot of rules relate to, and applies throughout cyberspace. Very often, the rules of Netiquette are formulated in the form of 10 commandments. The list was offered by Virginia Shea in her publication *Netiquette* (Shea 2009).

Referring to the title problem the key issue is permission and the assessment of the behaviour of network administrators. They allow viewing the contents of accounts and, more importantly, they make various changes, including deleting data. Netiquette should therefore indicate the limits of acceptable interference by administrators in the private accounts of Internet users. Another issue relates to "supervising", namely tracking the "digital steps", of an Internet user by various Government agencies and commercial firms. This practice is carried out, inter alia, by means of *spyware* or *sniffers*, the activity of recording person's activities on the Internet. This information is stored on servers and on its basis individual profiles of surfers are created. A universal practice is also that of "hooking" spyware installers for other applications (such as screensavers and others) without the knowledge or consent of Internet users (Kubas, 2004, pp. 68-70).

Netiquette, as an honorable code of Internet users, should clearly indicate the moral responsibility which is associated both with the same communications purpose in the global network and the use of the technology of data coding for that purpose. Another issue that should be reflected in Netiquette is a problem related to the wider credibility, and more specifically with forgery, and pretending to be someone else while communicating online. This subject is now particularly valid in relation to the amendment of the law introducing criminal responsibility for *grooming.*

There is also a whole range of dangers associated with Netiquette. It is the quality of studies of this kind - anyone can write their own version and put it on the Internet. Moreover, the possibility of the destruction of the meaning of good studies, or the stagnation of its recommendations. This situation can occur if Internet Netiquettes are stopped being talked about, if their authors confine themselves to one-time notification of them.

Summary

The responsibility for the content found on websites is borne by three groups of entities: content providers, Internet Service Providers, and Internet users. The responsibility for the run websites should definitely be borne by those who have a direct impact on their content. Imposing responsibility on Internet access providers, who on one hand are unable to effectively fulfill this obligation, and on the other become empowered far beyond the competence based on their functions, seems unjustified. Currently, neither EU nor Polish legislation requires server administrators to perform preventive screening of the sites accessed through a specific server, or to locate or remove infringing content. Granting such powers or obligations could lead to further protests. Server administrators would be privileged with the powers of the censor, and their discretionary decision would be crucial for finding whether the website presents illegal or harmful content. However, this objection may be negated by delegating decision-making powers as for providing greater

access to the server to the law enforcement. Also, a different approach is represented, postulating the legal obligation to determine the scope of ISPs for the control and elimination of hazardous Internet content and regulate their cooperation with law enforcement to monitor global network resources and operations (Maroń 2008, p. 235).

Notwithstanding the different positions on this issue, it is clear that some regulatory mechanisms governing the operation of online companies require them to control and eliminate dangerous content from the Internet are essential. Technically it is not possible to control all the materials published on the global network; the legislation (if any) usually requires ISPs to remove dangerous sites only after every notification of their existence, either by police or by the Internet. Frequently, having displayed them.

Moreover, the current laws are not always effective. First, they do not allow the enforcement of national laws in other countries. This is important in the cross-border nature of the Internet. Secondly, there is a divergence between European and American regulations. Third, any attempt to block the introduction of harmful or illegal content meets with protests in the name of freedom of speech.

Network Netiquette, is a kind of guide, a signpost for novices in the cyber world, and a reminder of these rules for users who have lost them. They point to specific behaviours, attitudes, situations, and even words explaining which ones are good and which are unacceptable. They serve the standardisation of Internet users' practices. In particular, they relate to: communications, requirements for websites, rules for the use of any material from the Internet and the related responsibilities. They point to certain ethical standards, although in a limited way. Hence it is necessary to continuously work on Netiquette, to continuously adjust it to the new realities posed by technological and social development, and the changing reality. We need a constant global forum discussion on the principles of Netiquette, which will stimulate the social awareness of the existence of rules and reinforce the need to obey them for the sake of the general good. It is necessary to stimulate global awareness of the responsibility of all the members of the cyber world for its current and future design. Netiquette could become the axiological frame of reference for Internet users to their practices. This would require global cooperation, however, to update its rules and promote them among all the Internet users. This issue is very important, due to the multinational, multicultural and diverse - in terms of: age, race, religion, and world view - nature of this community.

References:

1. Barta J., Markiewicz R. (1998), *Internet a prawo*. Wydawnictwo Universitas, Kraków.
2. Barta J., Markiewicz R. (2002), *Świadczenie usług drogą elektroniczną – nowa rzeczywistość dla prawników.* „Radca Prawny", Issue 4-5, pp. 66-78.
3. Brzozowski M. (1999), *Biznesowa etyka.* „WWW", Issue 2, pp. 36-39.
4. *Code for the Chat Check Badge,* http://www.fdim.dk/?pageid=52, [23.10.2011].
5. *Code of Conduct for search engines/Verhaltenssubkodex fur Suchmaschinenanbieter der FSM,* http://www.fsm.de/en/SubCoC_Search_Engines, [23.10.2011].
6. *Convenio de Autorregulación para promover el buen uso de Internet es Espańa,* http://www.aui.es/../biblio/documentos/legislacion/proteccion_menores/convenio/tex_conv.htm, [23.10.2011].
7. *Código deontológico de la Agencia de Calidad de Internet,* http://www.iqua.net/Codigos_de_conducta/Codigo_de_conducta/?go=WWiW6aWP3cIUyUj7fiM3LUP2TC+MOm3NphIdSA2vOCa_qmvpV3BPk GOo8, [23.10.2011].
8. *Czym jest netykieta?* http://www.netykieta.net/definicje.php, [03.08.2011].
9. *Decyzja nr 854/2005WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. w sprawie kontynuacji wieloletniego programu wspólnotowego na rzecz bezpieczniejszego korzystania z internetu i nowych technologii sieciowych,* Dz. Urz. L 149 z 11.05.2005.
10. Dobrzeniecki K. (2004), *Prawo a etos cyberprzestrzeni.* Wydawnictwo Adam Marszałek, Toruń.
11. *Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego,* Dz. Urz. L 178 z 17.07.2000.
12. *European Internet Service Providers Associations – EuroISPA*, http://www.euroispa.org/, [15.07.2011].
13. *Evropská Asociace Státnich Loterii A Toto Spolecnosti,* http://www.sazka.cz/o-nas/vice-osazka/zakony/kodex.php, [23.10.2011].
14. *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V, http://www.fsm.de/, [19.08.2011*].
15. Gajowniczek A. (1999), *Wykorzystanie internetu w celu reklamy. Wybrane zagadnienia prawne.* Master's thesis, available at: http://www.vagla.pl, [16.09.2009].
16. *Good Practice Guidance for search service providers and advice providers and advice to the public on how to search safely,* http://police.homeoffice.gov.uk, [24.10.2011].
17. Gruchoła M. (2012), *Ochrona użytkowników internetu w państwach Unii Europejskiej.* Wydawnictwo KUL, Lublin.

18. Gruchoła M. (2011), *Dangers in the Internet Communication and the Protection of Internet Users in the Era of Media Convergenc.* In: *Konwergencja mediów – media convergence - Medienkonvergenz".* German publisher, p. 18, submitted for printing.
19. Gruchoła M. (2011), *Ochrona małoletnich internautów w prawie i praktyce państw Unii Europejskiej.* „Rozprawy Społeczne", Vol. V, pp. 78-100.
20. *Jugendmedienschutz-Staatsvertrag z dnia 1 kwietnia 2003 r. – JMStV;* http://www.artikel5.de/gesetze/jmstv.html, [02.10.2011].
21. Kirwil L., *Polskie dzieci w internecie. Zagrożenia i bezpieczeństwo na tle danych dla UE. Wstępny raport z badań EU Kids Online przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców,* http://www.saferinternet.pl/images/stories/pdf/raport_eu_kids_online _polska_28-10-2010.pdf, [21.09.2011].
22. *Kodeks cywilny; Ustawa z dnia 23 kwietnia 1964 r.,* Dz. U. z 1964 r. Nr 16, poz. 93.
23. *Kodeks karny; Ustawa z dnia 6 czerwca 1997 r.,* Dz. U. z 1997 r. Nr 88, poz. 553 ze zm.
24. *Kodeks wykroczeń; Ustawa z dnia 20 maja 1971 r.,* Dz. U. z 1971 r. Nr 109, poz. 756.
25. Kubas G., *Netykieta - kodeks etyczny czy prawo internetu?,* Kraków: Uniwersytet Jagielloński 2004, s. 17, master's thesis. Available at: http://www.vagla.pl, [16.09.2011].
26. Kulesza J. (2010), *Międzynarodowe prawo internetu.* Przedsiębiorstwo Wydawnicze *Ars boni et aequi,* Poznań.
27. Maroń G. (2008), *Ochrona małoletnich przed pornografią i pedofilią internetową*, In: R. Grabowski (red.), *Wpływ internetu na ewolucję państwa i prawa.* Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów.
28. Murawska-Najmiec E. (2005), *Informacja na temat działań społeczności międzynarodowej na rzecz objęcia internetu systemem prawa przy jednoczesnej ochronie swobody wypowiedzi i informacji.* KRRiT, Warszawa.
29. *Porozumienia policji i rządu w sprawie blokowanie treści,* http://prawo.vagla.pl/node/5426, [27.08.2005].
30. *Serwis internetowy MySpace zaostrza ograniczenia dla użytkowników,* http://wirtualnemedia.pl/document,,1309742,Serwis_internetowy_MySpace_zaostrza_ograniczenia_dla_uzytkownikow.html, [22.06.2011].
31. Shea V., *Netiquette,* www.albion.com/netiquette/book/TOC09633702513.html, [09.09.2009].
32. *Spam code of conduct of ISPA,* http://www.ispa.at/downloads/COC_spam_english.pdf, [23.10.2011].
33. *Społeczności sieciowe: Komisja pośredniczy w porozumieniu głównych firm internetowych,* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/232& format=HTML&aged=0&language=PL&guiLanguage=en, [12.05.2011].
34. Stiftung Digitale Chancen (2009), *Zestaw zaleceń projektu Youth Protection Roundtable.* SDC, Hamburg.
35. Swetenham R. (2010), *Europejskie porozumienie dotyczące samoregulacji w zakresie bezpieczeństwa w portalach społecznościowych.* In: *Materiały konferencyjne z IV Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie.* Fundacja Dzieci Niczyje, Warszawa.
36. *UE: Zgoda Parlamentu na blokowanie pedofilskich treści,* http://di.com.pl/news/41219,0,UE_Zgoda_Parlamentu_na_blokowanie_pedofilskich_tresci.html, [29.10.2011].
37. *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,* Dz. U. z 2002 r. Nr 144, poz. 1204.
38. *Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii*, Dz. U. z 2009 r. Nr 98, poz. 817.
39. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,* Dz. U. z 1997 r. Nr 133, poz. 883 ze zm.
40. *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,* Dz. U. z 1994 r. Nr 24, poz. 83.
41. *Ustawa z dnia 7 października 1999 r. o języku polskim,* Dz. U. z 2002 r. Nr 37, poz. 349.
42. Waglowski P., *Niebezpieczne ideologie i nawoływanie do waśni,* http://prawo.vagla.pl/node/4773, [04.12.2009].
43. Waglowski P., *Szwedzi witają nowy porządek, czyli retencja danych na granicach,* http://prawo.vagla.pl/node/7961, [01.07.2010].