CBKE
e-BIULETYN

Jednostka i państwo w dobie demokracji elektronicznej
Ochrona prywatności, życia osobistego i rodzinnego

Prof. dr hab. Jacek Gołaczyński

Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

Wprowadzenie

Coraz szybszy rozwój technologii informacyjnych oraz ogromna łatwość i skuteczność przekazywania informacji przekonują o ich rosnącej potędze. Ta światowa sieć informacyjna określana mianem Globalnej Infrastruktury Informacyjnej rozrasta się w szybkim tempie na oczach całego świata. Panuje powszechnie przekonanie o wielkiej potędze Internetu. Internet można traktować jako nowo powstałe medium, ale sprawa jego przewagi nad radiem czy telewizją jest tematem dyskusji wielu specjalistów. Jeśli chodzi o przewagę jakościową, to jest ona bardzo wyraźna. Główna różnica polega na sposobie, a właściwie na trybie komunikacji: on-line w przypadku Internetu oraz off-line w przypadku radia czy telewizji[2]. Specjaliści z dziedziny IT analizują wszystkie możliwe kierunki przemian technologicznych związanych z Internetem. W najbliższym czasie możliwości jej wykorzystania będą coraz większe. Internet stanie się prawdopodobnie nieodłącznym elementem życia większości ludzi na całym świecie. Rozwój ten nie może być oderwany od czynników kulturowych, politycznych i ekonomicznych. I to właśnie te czynniki powodują, że nie wszystkie możliwości, jakie niesie ze sobą rozwój technologii mogą zostać praktycznie rozwinięte. Powstają innowacyjne, nieznane uprzednio grupy zawodowe, dla których próżno szukać polskich nazw np. webmaster, webdeveloper, web designer, coraz ściślej przenikają się i łączą systemy komunikacji społecznej, wytworzonej przez informatykę i telekomunikację. Można zauważyć rozwijanie się nowego języka, jakim porozumiewają się

[2] http://globaleconomy.pl/?u=&a=6&b=1&c=&d=&e=&rk=120

między sobą internauci. Tworzą się nowe relacje społeczne, a co za tym idzie powstaje społeczeństwo informacyjne.

1.FORMY NARUSZEŃ DÓBR OSOBISTYCH ZA POŚREDNICTWEM INTERNETU

1.1.Zagadnienia ogólne

Przesyłanie informacji za pośrednictwem sieci jest bardzo proste – wystarczy dysponować bardzo łatwo osiągalnym i darmowym oprogramowaniem oraz oczywiście być podłączonym do sieci. Jednocześnie istnieje możliwość ukrycia w sieci swojej prawdziwej tożsamości, albo idąc dalej – stworzenia sobie tożsamości. W związku z tym jest sprawa oczywista, że Internet może być instrumentem naruszenia dóbr osobistych. Naruszenia ta mogą przybierać różne postaci. Wydaje mi się, że jest uzasadnione stosowanie w drodze twórczej wykładni przepisów art. 23 k.c. do tych nowych sytuacji. Mam tu na myśli znajdowanie nowych dóbr osobistych, które nie znalazły się w otwartym, kodeksowym katalogu, ale również zauważanie nowych form naruszeń dóbr osobistych, które mają już ugruntowaną pozycję w doktrynie i orzecznictwie. Do pierwszych sytuacji można zaliczyć np. wolności komunikacji. Konstytucja Rzeczpospolitej Polskiej wyraźnie stanowi w art. 49, iż zapewnia się wolność i ochronę tajemnicy komunikowania się. Jednocześnie art. 54 każdemu zapewnia wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. Te dobra, ze względu na łatwość ich naruszenia występują dość często w sieci. Do drugiej sytuacji należy zaliczyć nową formę naruszenia np. czci przez wypowiedź za pośrednictwem IRC[3] lub jego nowszej wersji – czata. Cześć, dobre imię były naruszane w środkach masowego przekazu i orzecznictwo zwracało uwagę na fakt dużej liczby odbiorców tych mediów. Internet stwarza możliwość dotarcia z jednostkową informacją do najszerszego kręgu osób. Wobec tego, że komunikacja następuje z wykorzystaniem tzw. kanałów, na których jednocześnie może przebywać kilka tysięcy ludzi, to jeden użytkownik może przebywać na kilku kanałach jednocześnie. Użytkownik przesyła „na kanał" lub do poszczególnych współużytkowników komunikaty tekstowe. Po pierwsze, można dotrzeć do specyficznie wyselekcjonowanej grupy ludzi, którzy tworzą np. środowisko związane tematycznie z jakąś dziedziną życia. Po drugie, (przy pewnych założeniach) praktycznie każdy jest w stanie brać udział w tworzeniu nowych informacji i w ich dystrybucji z pośrednictwem sieci. Powyższe uwagi powodują, że „ciężar gatunkowy" naruszenia czci, czy dobrego imienia w sieci będzie dużo większy niż przy „klasycznych" naruszeniach. Kolejne problemy rodzi kwestia dowodowa.

[3] Internet Relay Chat. Usługa oferująca możliwość komunikowaniu się wielu użytkowników w trybie rzeczywistym.

Tu również można dostrzec dwa aspekty: pierwszy, to udowodnienie, że nastąpiło naruszenie jakiegoś dobra, drugi to, udowodnienie sprawstwa określonej osoby. Należy pamiętać, że komunikacja w sieci polega na przesyłaniu między komputerami pakietów danych, które mogą przybierać postać pliku komputerowego, a takie pliki ze względu na łatwość modyfikacji nie mogą być wiarygodnym dowodem naruszenia. W wielu przypadkach ochrona będzie się ograniczała do usunięcia informacji (pliku) naruszającej dobra osobiste z serwera podłączonego do Internetu. W chwili obecnej jest to zagadnienie bardzo trudne, jednakże opracowane są już technologie, które w bardziej pewny sposób (niż przykładowo z zastosowaniem własnoręcznego podpisu) są w stanie wykazać, że dany dokument elektroniczny pochodzi od danej (konkretnej) osoby. Jednocześnie są już opracowane i wdrażane projekty, które umożliwią identyfikację osoby w sieci, ale jednocześnie umożliwią dokonywanie płatności, przechowywanie danych niezbędnych do egzystowania w informatycznym społeczeństwie (np. PGP[4]). Karty mikrochipowe na pewno przyczynią się do wyselekcjonowania kolejnych dóbr osobistych i kolejnych form naruszeń.

1.2.World Wide Web

Word Wide Web jest usługą umożliwiającą korzystanie z dokumentów hipertekstowych, udostępnionych na serwerach w dowolnym miejscu na kuli ziemskiej. Dokumenty hipertekstowe kodowane są w języku HTML (Hyper Text Markup Language). Jest to język opisu struktury wewnętrznej dokumentu (zdefiniowanego w SGML, czyli Standardized Generalized Markup Language; technologia SGML stała się międzynarodowym standardem ISO 8879). Publikacje elektroniczne prezentowane za pośrednictwem WWW to plik lub zespół plików, które wzajemnie się do siebie odwołują. Efekt końcowy w postaci wyświetlenia strony WWW będzie różny w zależności od przeglądarki WWW (browser). Ona tak naprawdę interpretuje i „składa w całość" pobrane z sieci informacje. Strona WWW to prezentacja wizualna, przedstawia tekst, grafikę, coraz częściej zawiera w sobie elementy muzyczne i video. Wraz z rozwojem technologii WWW zwiększa się dynamika prezentowanych za jej pomocą danych. Dzięki tzw. cookies strona WWW (specjalny program obsługujący cookies), którą kiedyś odwiedziliśmy może niejako pamiętać ten fakt, a także może, przy kolejnych odwiedzinach, pobierać z naszego[5].

[4] Więcej na temat Pretty Good Privacy można znaleźć pod adresem: http://www.pgpi.org komputera różne dane, które podaliśmy wcześniej. Strony WWW, poza prezentowaniem jakichś danych w postaci tekstu, grafiki, dźwięku czy video, mogą zawierać odesłania do bardzo skomplikowanych programów wykonywalnych.
[5] WWW.vagla.wiaara.pl

1.2.1 Negatywne kampanie

Niezwykle łatwo dziś umieścić i udostępnić stronę WWW w serwerze. Wystarczy odpowiednie pliki umieścić na serwerze WWW, który jest połączony z siecią. Coraz więcej osób dysponuje takimi możliwościami[6]. Problematyka stron jest niezwykle różnorodna i zależy od wyobraźni twórców. Może zdarzyć się tak, iż swoje negatywne emocje i uczucia przedstawiają w postaci ANTY stron.

„Antystrony" mogą dotyczyć różnorakich wątków. Mogą być to strony prześmiewczo traktujące muzykę znanego wykonawcy[7], ze stronami antynazistowskimi[8], antyfaszystowskimi[9], antystrony nauczycieli opracowane przez uczniów[10], antystrony mniejszości seksualnych[11]. W światowej sieci informacyjnej odnaleźć można także antystrony polityków[12]. Strony takie zwykle nie są napisane językiem obelżywym, co więcej mogą obejmować treści napisane w ramach wolności słowa i prawa do krytyki[13], nie naruszając żadnych dóbr osobistych. Niekiedy jednak takie strony zawierają treści uwłaczające, fikcyjne lub kompromitujące, godzące w dobre imię i cześć konkretnej osoby fizycznej lub prawnej. W przypadku, gdy na stronach znajduje się bezprawnie nazwisko, pseudonim lub zdjęcie (wizerunek) danej osoby – naruszane są również inne dobra osobiste. Zdarzyć się może również, że strony takie przybierają postać negatywnej kampanii skierowanej przeciwko określonej osobie fizycznej czy prawnej.

Przykładem negatywnej kampanii jest strona WWW o nazwie „Akta Norymberskie"[14]. Znajdowały się tam zdjęcia i precyzyjne dane o kilkuset lekarzach przeprowadzających w USA zabiegi usuwania ciąży. Spisy zawierały tak szczegółowe dane, jak: numery praw jazdy, adresy domowe, zdjęcia domów, imiona dzieci i daty ich urodzin. W prezentowanym serwisie nazwisko lekarza, który został ranny w wyniku ataku antyaborcyjnych fanatyków, było przekreślane czarna kreską. Sąd federalny w Portland w stanie Oregon zasądził 109 mln dolarów odszkodowania od właścicieli strony, gdyż -jak argumentował – nakłania ona do przemocy przeciw lekarzom dokonującym aborcji[15]. Jak podkreślił sędzia – właścicieli stron „Akta Norymberskie" nie chroni amerykańska konstytucja, bowiem nakłanianie do przemocy w stosunku do innych wykracza poza

[6] http://www.qs.pl/index.php?action=0504
[7] http://fuck-avril.xx.pl/
[8] http://free.polbox.pl/g/gannw/
[9] http://sierp.tc.pl/xpiotr35.htm
[10] http://www.friendsreunited.co.uk/
[11] http://free4web.pl/3/1,24415,17408,Threads.html;jsessionid=85A6C42180CBFB38247C3659FD8D9DF2
[12] http://www.karboch.gliwice.pl/~olejsystem/olejsystem/anty_lepper.html
[13] http://chrzanow.kik.opoka.org.pl/wsala/internet-nse.html
[14] http://www.christiangallery.com/
[15] http://dir.salon.com/news/feature/2001/05/31/nuremberg/index.html

granice wolności słowa[16]. Analogiczne orzeczenie na płaszczyźnie merytorycznej byłoby racjonalne z punktu widzenia polskiego prawa, gdyż zostały tu naruszone dobra osobiste lekarzy takie jak wizerunek, prawo do prywatności, nazwisko, w konsekwencji istnienia strony było zagrożone ich zdrowie a nawet życie. Za pośrednictwem Internetu można naruszyć dobro osobiste w postaci zdrowia. Pornografia, ale również jakiekolwiek opisy, rozmowy, prezentowanie dzieciom treści lub obrazów o charakterze seksualnym jest dokonywaniem wobec nich przemocy. Jest to o tyle niebezpieczne, że każda taka przemoc i doświadczenie tego typu przemocy niestety z jednej strony rodzi u odbiorcy tendencję do tego, by być ofiarą następnych form przemocy, a z drugiej strony rodzi również tendencje do tego, by być agresorem, tzn. jednocześnie upowszechnia się zachowania związane z tym, że ten, który doznał przemocy, staje się sam człowiekiem, który przemocy dokonuje. Przemoc rodzi przemoc i jest to społeczne dziedziczenie, które występuje zarówno w rodzinie, jak i w relacjach tego przekazu osobowego, chociaż pośredniego, w telewizji[17]. Prezentacja w środkach masowego przekazu, a tym bardziej w Internecie pewnych idei jako środowisku pozwalającym na swoistą interakcję z użytkownikiem może sugerować im pewien schemat zachowań. Dylemat ten dotyczy raczej rozważań aksjologicznych, albowiem trudno sobie wyobrazić powództwo o naruszenie dóbr osobistych w postaci zdrowia wytoczonego przeciwko autorowi serwisu prezentującego pornografię, bowiem wysoce prawdopodobne jest, że użytkownik strony pornograficznej zrobił to z własnej, nieprzymuszonej woli, powstaje też problem dowodowy, sprowadzający się do wykazania, iż potencjalne naruszenie zdrowia wywołane było zapoznaniem się z pornograficzną treścią konkretnych stron internetowych.

1.2.2 Podmiany stron WWW

Zamiana stron powoduje zwykle wzrost liczby odwiedzin na konkretnej stronie, przez co zwiększa się współczynnik odbiorców i obserwatorów naruszenia. Nie jest to bez znaczenia, może takie naruszenia są rozpowszechniane przez podanie ich do wiadomości za pośrednictwem grup dyskusyjnych *Usenetu.* I tak, np. przykład przedstawiciele hackerskiej grupy World of Hell, którzy poinformowali o swoim dokonaniu, które polegało na podmianie 679 stron internetowych w ciągu. jednej minuty. Hakerzy szykowali się do podmiany jednej strony skierowanej do fanów piosenkarza Ricky Martin'a (Rickymartin.com.mx) jednak po włamaniu się na serwer okazało się, że znajdują się na nim jeszcze setki innych stron internetowych. Wszystkie one zostały następnie podmienione z wykorzystaniem skryptu napisanego w języku Perl. Wszystkie strony znajdowały się na serwerze

[16] B. Węglarczyk: *Wolność słowa czy przemocy*, Gazeta Wyborcza 4 luty 1999.
[17] D. Kornas-Biela. Sejmowa Komisja Rodziny z dnia 13.03.98. *Problemy zagrożeń rodziny przez przemoc pornografię, ze szczególnym uwzględnieniem roli mediów*

firmy świadczącej usługi hosting'owe, a włamanie odbyło się z wykorzystaniem znanej już słabości systemy Windows 2000 i serwerze IIS 5.0 - Internet Printing Protocol http://www.eeye.com/html/Research/Advisories/AD20010501.html)[19]. Wspomagającą okoliczność stanowi fakt, iż osoby, które nie wiedziały o podmianie strony WWW łącząc się z określonym adresem na przykład: http://www.neo.pl/ spodziewają się znalezienia tam oficjalnego serwisu informacyjnego tej firmy. Zdarza się tak, iż osoby zmieniające strony posiłkują się niekiedy elementami graficznymi stron, które zmieniają, przez co część osób odwiedzających podmienioną stronę WWW może być przekonana, że prezentowane na niej treści pochodzą od tej właśnie firmy.

Przekierowanie usług takich jak WWW czy poczta można zrealizować właściwie w dowolnym miejscu sieci między odbiorcą a serwerem. Niewykluczone są równocześnie zamachy na usługi DNS, *routery* i całe mnóstwo innych. W praktyce bezpieczeństwo usług w Internecie w niemałym stopniu uzależnione jest od zabezpieczeń wszystkich dostawców po drodze." Na podmienionej stronie zatytułowanej „Zostań kowbojem", można było przeczytać: „Zadzwoń już dziś pod numer 0602256776 (musisz mieć ukończone 18 lat) i poproś o przybliżenie warunków promocji. W programie szkolenia znajdziesz wszystko, co chciałbyś wiedzieć o kowbojach, Dzikim Zachodzie. Wykłady poprowadzą nasi wybitni i znani, nad wyraz kompetentni eksperci, którym po raz pierwszy dano szansę zabrania głosu w temacie, o którym mają pojęcie."[20] . Przekierowanie stron WWW jednej z bardziej liczących się na płaszczyźnie bezpieczeństwa sieciowego firm w Polsce było powszechnie komentowane w ramach grupy dyskusyjnej *Usenetu*[21].

Włamanie na serwer Telekomunikacji Polskiej S.A. nastąpiło 1 grudnia 1998r. Przy okazji włamania nastąpiło podmienienie strony głównej serwisu spółki. Pod podmienioną stroną WWW podpisała się grupa hackerska „Gumisie". Na podmienionej stronie znajdowały się hasła dostępu do różnych serwerów, uzyskane z poprzedniego włamania tej grupy hackerskiej na serwer NASK'u[22] (NASK -Naukowa Akademicka Sieć Komputerowa). W trakcie tego włamania rozszyfrowano na podmienionych stronach ten skrót jako Niezwykle Aktywna Siatka Kretynów (włamanie nastąpiło 30 października 1995). Na stronie „Telekomuny Polskiej S.A." (zmieniona nazwa spółki) opublikowano uwłaczające animacje komputerowe[23].

Może się zdarzyć jednak ze sprawca podmiany działa w przekonaniu o prawdziwości swoich zarzutów. Jednak takie przeświadczenie nie uchyla odpowiedzialności z art. 24 k.c.[24]

[18] http://www.cert.pl/index2.html?action=show_news_more&nid=173
[19] http://www.cert.pl/index2.html?action=show_news_more&nid=173
[20] http://anonimuss.webpark.pl/ensi.htm
[21] http://www.man.lodz.pl/LISTY/POLIP/apr00/0161.html
[22] http://anonimuss.webpark.pl/nask.htm
[23] http://anonimuss.webpark.pl/tpsa.htm
[24] Wyrok SA z 24 września 1992 r., I ACr 340/92, OSAiSN 1993/6 poz. 39 s 32.

można, zatem założyć, że nastąpiło naruszenie prawa do prywatności administratora oraz naruszenie jego czci poprzez sugerowanie, że nie wywiązuje się z obowiązków pracowniczych.

Jak można dostrzec na podstawie powyższych przykładów nie tylko strony WWW należące do firm informatycznych zajmujących się bezpieczeństwem są narażone na ataki. Także firmy innego pokroju, nieopisane tutaj – jak np. Pizza Hut, Holiday Travel, Nestle - Lion[25] na serwery, której także się włamano zamieniając strony WWW. Osoby indywidualne posiadające własny prywatny „home page" także są narażone na tego typu podmiany, a w ich konsekwencji na naruszenie dóbr osobistych Jakiekolwiek zamienienie strony WWW można także uważać za ja naruszenie swoboda wypowiedzi osób uprawnionych z racji posiadania kont czy serwerów WWW za ich pośrednictwem. Nietrudno sobie wyobrazić naruszenie dóbr osobistych w postaci twórczości naukowej lub artystycznej przez podmienienie stron WWW, na których znajduje się dookreślone dzieło. Słuszne wydaje się również akceptacja samej strony WWW za utwór i objęcie ochroną jej autora. Dylemat z podmianą strony polega na tym, że często nie wykrywa się podejrzanego naruszenia dóbr osobistych[26]

1.2.3 Złośliwe aplety [27]

Z poziomu stron WWW możliwe jest instalowanie różnorakich aplikacji, które będą działały na lokalnym komputerze, ewentualnie będą konsolidować się z jego zasobami. Może to mieć miejsce w wyniku uruchomienia programu bez wiedzy i zgody osoby oglądającej z zasady niewinnie wyglądającą stronę WWW. Po rozruchu mogą udoskonalać system oglądającego, mogą udostępniać osobom postronnym wiadomości poufne na komputerze oglądającego, mogą powodować zablokowanie komputera (chodzi o atak typu DOS – Denial of Service[28] - metoda ataku na sieciowe systemy komputerowe, mająca na celu zakłócenie funkcjonowania systemu lub całkowite sparaliżowanie jego pracy[29]), który może wymagać jego ponownego uruchomienia Znikomą klasą zamachu dokonanego przez aplet jest utrudnianie pracy poprzez wypełnianie procedur niedogodnych dla eksploatatora. W konsekwencji na użytkowniku jest przymuszony do restartu przeglądarki.

Osoba umieszczająca je na swojej stronie WWW mogła wykorzystać je do całkowitej penetracji komputera osoby oglądającej daną stronę a w konsekwencji narazić lub wręcz naruszyć

[25] http://anonimuss.webpark.pl/wlamania.html
[26] http://www.vagla.pl/d_o/do3.htm
[27] Aplet – niewielki program wbudowany w inną aplikację. Leksykon Internetu http://leksykon.koti.com.pl
[28] Do ataków typu Denial of Service należą między innymi winnuke, ping of death, octopus (port fuck), syn flood itp. Są to ataki mające na celu unieruchomienie maszyny, lub któregoś z jej serwisów.
[29] http://www.webstyle.pl/cms.php/ws/netopedia/hardware/dos_denial_of_service

jej dobra osobiste. Dobra osobiste narażone przez tego typu działanie to prawo do prywatności, wolność komunikowania się, tajemnica komunikacji (jeśli wyodrębnić ją jako oddzielne dobro). Można również naruszyć cześć danej osoby przykładowo, gdy wykorzysta się opanowany komputer do ataków na inne maszyny, w taki sposób, jakby dokonywał tego właściciel.

> Oto przykłady: Atak polegający na obejściu reguły zezwalającej na otwarcie połączenia sieciowego tylko do serwera, z którego pobrano aplet. Taką lukę można wykorzystać na przykład w celu penetracji "zapory ogniowej" (ang. firewall). Aplet zostanie przepuszczony przez zaporę jako normalny pakiet danych WWW, po czym uruchomiony lokalnie zacznie atakować komputery w obrębie sieci lokalnej z maszyny nic nie podejrzewającego użytkownika, który po prostu przegląda strony WWW.
>
> Atak, który polega na oszukaniu przeglądarki przez aplet i spowodowaniu, że będzie ona traktować kod apletu jako swój własny. Ponieważ kod Javy dostarczany z przeglądarką uznawany jest za "bezpieczny", takie oszustwo sprawi, że aplet zyska nieograniczony dostęp do plików na lokalnym dysku.

1.2.4 Cytaty publikacji oraz publikacje własne autorów

Można zaobserwować sytuacje, gdy twórcy stron WWW zamieszczają na nich wiadomości, które pojawiły się w innych mediach, jak np. fragmenty programów publicystycznych czy reportaż wydany w prasie. Niewątpliwie pewne elementy takich działań będą naruszały prawa osobiste autorów tych materiałów, oraz ich dobra osobiste. Jeśli zdarzyłoby się tak, iż publikacje takie naruszały dobra osobiste innych osób wówczas należałoby dojść do wniosku, że gdyby nawet audycje telewizyjne stanowiły powtórzenie artykułów prasowych, to i tak nie można by podzielić poglądu, by nie miał obowiązku sprawdzenia prawidłowości stawianych powodom w tych artykułach zarzutów godzących w ich część i dobre imię. Zasięg przekazu telewizyjnego i masowość jego odbioru wymagają szczególnej ostrożności i wystrzegania się bezprawnego naruszenia czyjejś czci”[30]. Porównywalnie należy reagować na publikowanie w Internecie wydanych wcześniej artykułów prasowych, czy też urywek z programów telewizyjnych. Stosowne jest również, by radykalnie przyjąć, że rozmiar transmisji internetowej i liczebność jego odbioru wymagają specyficznej zapobiegliwości i wystrzegania się niepewnych naruszeń czyjejś czci, nie tylko przy cytowaniu innych materiałów, ale również przy umieszczaniu materiałów własnych

[30] Wyrok SN z 29 czerwca 1983 r., II CR 160/83, niepublikowany.

na stronach WWW[31]. Stoję na stanowisku, że odnosić się to do większości dóbr osobistych również prawa do prywatności, wizerunku, nazwiska.

1.3 E-mail i Usenet

Przesyłanie poczty elektronicznej (e-mail) jest niezwykle popularne. Ułatwia ono przekazywanie informacji ludziom z niebywałą jak dotąd efektywność i szybkością, pomaga w prowadzeniu wewnętrznych archiwów korespondencji, ułatwia przesyłanie otrzymanych listów do innych osób w postaci w gruncie rzeczy niezmienionej. Adres e-mail w związku z imieniem i nazwiskiem można uznać za dane osobowe w rozumieniu przepisów ustawy o ochronie danych osobowych. Adres e-mail w ograniczonym zakresie utożsamia daną osobę, a raczej – można przypuszczać, że list pochodzący z danego adresu pochodzi od konkretnej osoby. Oczywiście może nastąpić naruszenie dóbr osobistych za pośrednictwem poczty elektronicznej. Naruszenia te mogą przyjąć kształt wypowiedzi godzących w dobre imię lub cześć jakiejś osoby, mogą przybierać formę rozsyłania do osób trzecich zdigitalizowanej podobizny określonej osoby. Może to naruszać jej wizerunek. Poprzez „zwyczajne" rozsyłanie korespondencji można naruszyć również dobro osobiste w postaci nazwiska czy pseudonimu, a także twórczość naukową i artystyczną. Netykieta stwierdza: "Za szczególnie niegrzeczne uważa się rozpowszechnianie prywatnej poczty przez *mailing lists* lub *Usenet* bez zezwolenia autora", podaje się także, "aby być ostrożnym pisząc z humorem lub sarkazmem". "Bez osobistego kontaktu twój żart może być odebrany jako złośliwa krytyka"[32]. Te formy naruszeń nie różnią się praktycznie od podobnych, które można spotkać poza Internetem przy wykorzystaniu modelowej poczty. Wiele grup dyskusyjnych jest moderowanych (cenzurowanych) – czyli sprawdzanych, czy umieszczane na niej artykuły nadają się do publikacji. Niemniej przeważająca część grup dyskusyjnych nie podlega żadnej cenzurze, a wszystkie wiadomości są na nich umieszczane bez żadnej weryfikacji. W przypadku pisania listów (artykułów) na listy dyskusyjne i do Usenetu klasyczne naruszenie będzie miało większą skalę. Usługi tego typu pozwalają dyskutować na różne tematy wielu ludziom, w ten sposób, że list wysłany przez jedną osobę jest przez specjalne oprogramowanie rozsyłany do wszystkich subskrybentów (a więc osoby, które w specjalnej formie zgłosiły chęć udziału) danej listy dyskusyjnej. List (artykuł) w *Usenecie* jest opublikowany w ten sposób, że wysłany przez nadawcę trafia na serwer i stamtąd może być pobrany przez innych uczestników dyskusji. Ta ostatnia usługa przypomina „słup ogłoszeń", do którego w razie konieczności można podejść i zapoznać się z wiadomościami tam zawartymi i nie wiąże się to z przyzwoleniem innych członków dyskusji.

[31] http://www.vagla.wiaraa.pl/
[32] http://banita.pl/reg/netykieta.html

Zarówno listy dyskusyjne jak i grupy newsowe posiadają często wewnętrzne archiwa. Archiwa te przybierać mogą postać stron WWW. Wydaje się, że charakter publikacji artykułu na publicznej liście dyskusyjnej czy w grupie newsowej jest porównywalny do publikacji na stronach WWW. Wydaje się również, że do większości przypadków spotykanych w trakcie dyskusji na forum wspomnianych list będą miały zastosowanie uwagi Z. Bidzińskiego i J. Serdy[33] dotyczące sprawy dwu krytyków muzycznych, co, do których wypowiedział się Sąd Najwyższy w wyroku z dnia 19 września 1968 r. II CR 291/68[34]. Sąd Wojewódzki oddalił powództwo, a Sąd Najwyższy rewizję powoda od tego wyroku, stwierdzając m.in. iż krytyka zawarta w artykule pozwanego miała charakter polemiczny, przy którym „pewne przejaskrawienia są normalną i uznawaną jej właściwością". Ponadto „w środowisku muzycznym wyrażona przez pozwanego krytyka nie przekracza granic uważanych w tym środowisku za dopuszczalne". W konsekwencji Sąd Najwyższy nie dopatrzył się w sformułowaniach pozwanego przekroczenia granic krytyki akceptowanych w środowisku, dla którego jest przeznaczona i uznał, że nie nastąpiło naruszenie dóbr osobistych powoda. Stanowisko to spotkało się z krytyką A. Kopffa i A. Szpunara, ponieważ według tych autorów postępowania pozwanego nie można było usprawiedliwić w świetle zwyczajów środowiska muzycznego, skoro zwyczaje te są nieodpowiednie. Forma krytyki była niewłaściwa jako niezmiernie ostra. Autorzy uznają, zatem, że pozwany przekroczył granice potrzebne do osiągnięcia celu krytyki. Jak stwierdzają Z. Bidziński i J. Serda zwyczaje środowiska mogą mieć walor istotny jedynie w ramach tego środowiska, (co istotne z punktu widzenia rozważań na temat Internetu). Dalej natomiast stwierdzają, że skoro publikacja nastąpiła w ogólnospołecznym czasopiśmie, a nie w czasopiśmie zawodowym określonego środowiska, to powołanie się na takie zwyczaje nie może usprawiedliwiać zbyt ostrej formy wypowiedzi polemicznej[35]. Opisana okoliczność przypomina „flame war" (wojna ogniowa) czyli wysoce szybką wymianę listów (w żargonie internetowym: postów), nieprzemyślaną, niosącą w sobie bardzo duży ładunek emocjonalny, wykorzystującą obraźliwe słowa i wyrażenia. Pamiętać należy o tym, że list (artykuł) w Internecie można zamieścić z bardzo dużą łatwością.. Przyjmuje się powszechnie, że użycie w poczcie elektronicznej dużych liter oznacza krzyk lub, co najmniej podniesienie głosu. Należy zwracać również uwagę na tzw. uśmieszki internetowe (smails). Jest to obrazowa forma pokazywania emocji (emotikony) za pośrednictwem znaków typograficznych. Przedstawia ona twarze w różnych wyrazach (należy przekrzywić głowę by to odczytać), które mogą uosabiać dobry

[33] Z. Bidziński, J. Serda: *Cywilnoprawna ochrona dóbr osobistych w praktyce sądowej [w:] Dobra osobiste i ich ochrona w polskim prawie cywilnym,* Wrocław 1986, s. 37 – 38.
[34] OSNCP 1968 poz. 200 z glosami A. Kędzierskiej – Cieślakowej, PiP 1970, z. 5 s. 816 i n. oraz A. Kopffa, NP 1970, z 7-8, s. 1185 i n.

[35] Z. Bidziński, J. Serda: *op.cit., s.38.*

humor ·:-)", śmiech ":-D", smutek ·:-(", pokazanie języka ":-P" czy też żart z przymrużeniem oka ·;-)". Grupa Internautów wypracowała również szereg angielsko-polskojęzycznych skrótów nagminnie używanych w listach i w innych formach komunikacji. Trafny odczytanie transmisji może mieć wpływ na ocenę, czy dobra osobiste zostały naruszone lub zagrożone konkretną wypowiedzią czy to w liście elektronicznym prywatnym, czy to na forum listy dyskusyjnej[36].

1.3.1 Spamming

Spam – (ang. konserwa mięsna, mielonka, a w żargonie internetowym – niechciana korespondencja) to zjawisko, z którym każdy użytkownik Internetu spotyka się prawie codziennie podczas korzystania z poczty elektronicznej[37]. To zjawisko, które może zagrażać, lub naruszać dobra osobiste w postaci wolności, może powodować sytuacje, w których utrudniona będzie możliwość funkcjonowania osoby prawnej. Zgodnie z Konstytucją – każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym[38]. Konstytucja stanowi także, iż władze publiczne chronią konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu oraz przed nieuczciwymi praktykami rynkowymi. Zakres tej ochrony określa ustawa[39]. Bardzo szybko, pomimo stanowczo pejoratywnej postawy środowiska internetowego, praktyka mnogiego wysyłania niezamawianych przez odbiorców listów elektronicznych stała się powszednia w działalności marketingowej. Zakres jej wykorzystania był tak szeroki, że internauci określili ją jako prawdziwą plagę Internetu[40]. Innym powszechnie stosowanym określeniem jest UCE, skrót od *unsolicited commercial communication* (niezamawiana komunikacja handlowa)[41]. Tradycyjnie w przestrzeni internetowej pojęcie *spamu* używane jest powszechnie, do każdego listu elektronicznego, który nie jest oczekiwany przez adresata lub adresatów, niekoniecznie posiadającego komercyjny charakter [42]. Terminem zupełnie odrębnym jest *mailing*, który także odnosi się do przesyłania informacji reklamowych przy pomocy poczty elektronicznej, chociaż jest on przeznaczony dla poczty przesyłanej za zgodą odbiorców, co eliminuje jego zasadniczy ujemne cechy. W pewnym zakresie, usprawiedliwione jest porównanie praktyk spamingowych do materiałów reklamowych rozsyłanych tradycyjną pocztą, takich jak ulotki, katalogi itp[43]. Możemy wyróżnić kilka postaci *spamu* . Pierwsza z nich to *Excessive Multi-Posting*, czyli zbyt wiele kopii

[36] http://www.vagla.wiaraa.pl/
[37] http://www.mi.com.pl/index.php?section=article&id=171
[38] art. 47 *Konstytucji RP*
[39] art. 76 *Konstytucji RP*
[40] P. Podrecki, *Prawo Internetu,* Warszawa 2004, s. ?
[41] D. Kasprzycki, *Wybrane zagadnienia prawa reklamy, Miejsce wydania* s. 104
[42] P. Podrecki, *op. cit., s. ?*
[43] Tamże

tej samej wiadomości. Do kategorii tej zalicza się przesyłki, wszystkie zapytania, „propozycje nie do odrzucenia", łańcuszki szczęścia i inne wiadomości, które w identycznej lub w niewielkim stopniu zmodyfikowanej formie kierowane są do dużej ilości użytkowników lub grup dyskusyjnych, listy reklamujące po wielokroć tę samą usługę[44]. Drugą odmianą *spamu* jest *Excessive Crossposting*[45], czyli dużo postów do więcej niż jednej grupy newsowej lub więcej niż jednego użytkownika. Istnieją specyficzne procedury matematyczne, które administratorom serwerów pocztowych i newsowych potrafią pomóc określić stopień „agresywności" takiej partii przesyłek. Najbardziej dokuczliwe są przesyłki, które reklamują jakiś serwis, zachęcają do nabycia jakiegoś produktu (usługi) lub elektroniczna odmiana łańcuszka szczęścia, w którym należy wysłać do znajomych kopie otrzymanego listu wraz ze swymi danymi w zamian za obietnice otrzymania pieniędzy. Osoby, do których takie przesyłki docierają nie są w żaden sposób weryfikowane.

Do najpoważniejszych oskarżeń kierowanych wobec mnogich e-maili należą zarzuty natury pieniężnej. Otóż koszty aktywności marketingowej prowadzonej za pomocą poczty elektronicznej ponoszą nie osoby za nią odpowiedzialne, lecz podmioty pośredniczące w przesyłce oraz użytkownicy. To dostawcy usług internetowych są zobowiązani zadbać o to, aby ich infrastruktura techniczna, była w stanie podołać przyjęciu nadspodziewanej korespondencji. Oprócz tego listy określane nazwą spamu, posługują się zasobami ich komputerów (tzw. *bandwidth*), które mogłyby być wykorzystane w tym czasie do innych właściwych działań, jakkolwiek przesyłania wiadomości zamówionej. Użytkownicy także ponoszą koszty praktyk *spammingowych*, często w wymierny sposób, zwłaszcza w sytuacji, gdy opłata za podłączenie do Internetu jest uzależniona od czasu tego podłączenia. Takie rozłożenie akcentów określa się terminem przesunięcia kosztów działalności (*cost shifting*). Do tego dochodzą również koszty związane z potencjalnym filtrowaniem listów i stosowaniem zabezpieczeń. Wagę problemu unaocznił niedawno raport przeprowadzony na zlecenie Komisji Europejskiej odnoszący się niezamawianej korespondencji handlowej i ochrony danych osobowych[46]. Niezamawiana korespondencja elektroniczna przetrzymuje lub, co najmniej opóźnia korespondencję pożądaną. Staje się ona korespondencją dokuczliwą dla odbiorcy, pochłaniającą jego czas i nadmiernie absorbującą, ze względu na częstotliwość jej otrzymywania, a niejednokrotnie także i treść. Niejednokrotnie adresy zwrotne i inne wskazania źródeł korespondencji są fałszowane za pomocą tzw. *fake maila*, co poddaje tę działalność w dyskusyjność z etycznego punktu widzenia[47].

[44] http://www.mi.com.pl/index.php?section=article&id=237
[45] http://www.mi.com.pl/index.php?section=article&id=237
[46] http://www.europa.eu.int/comm/internal_market/privacy/docs/studies/spamstudy_en.pdf
[47] P. Podrecki, *op. cit*

Kilka lat temu zawiązała się nieformalna grupa *antyspamingowa* z powodu obserwowanej dużej ilości niechcianej korespondencji w Usenecie. Jeden z administratorów doliczył się aż miliona listów jednego dnia na serwerze Usenetu, z czego 40 % stanowiło właśnie spam. Kolejne 40 % listów w skutek niewydolności systemu przychodziło „w kawałkach". I jedynie 20 % stanowiły czytelne listy[48]. Administratorzy tworzący tę nieformalną, antyspamową grupę wyśledzili, że większość niechcianej korespondencji przychodzi z kont firmy UUNet, jednego z największych providerów. Administratorzy ci postanowili automatycznie kasować pochodzącą od klientów tej firmy pocztę bez względu na zawartość. W ciągu kolejnych kilku dni liczba niechcianej korespondencji została ograniczona do 94 sztuk. Następnie „wyrok śmierci" odwołano. Jak widać z powyższych przykładów spaming w dużej skali może naruszać dobra osobiste przedsiębiorstw (w tym osób prawnych) w ten sposób, że blokuje ich systemy informatyczne uniemożliwiając komunikowanie się ich pracowników lub klientów. Widać również, że taki stan rzeczy może rodzić sytuację, gdy w obronie przed spamem, naruszane są dobra osobiste osób trzecich. Naruszeniem takim (lub zagrożeniem) dóbr osobistych w postaci wolności komunikacji będzie tu kasowanie korespondencji. Na marginesie niechcianej korespondencji można przytoczyć następujący wyrok. „Dobro osobiste podlega ochronie prawnej, gdy jest zagrożone cudzym bezprawnym działaniem. Nie można wszakże przyjąć, iżby posłużenie się danymi osobowymi osoby fizycznej w ofercie handlowej do niej skierowanej było bezprawnym działaniem oferenta. Podstawowe dane osobowe człowieka (nazwisko i imię) są jego dobrem osobistym, ale jednocześnie są dobrem powszechnym w tym znaczeniu, iż istnieje publiczna zgoda na posługiwanie się nimi w życiu społecznym (towarzyskim, urzędowym, handlowym itd.). Dopóki, więc dane osobowe człowieka są używane zgodnie z regułami społecznymi, nie można mówić ani o bezprawności działań innych osób, ani o zagrożeniu dóbr osobistych tymi działaniami"[49]. Wydaje mi się, że bezprawnym działaniem, naruszającym dobra osobiste będzie właśnie wysyłanie na dużą skalę spamu, a zbierane za pomocą specjalnego oprogramowania dane osobowe (imię, nazwisko, pseudonim) są wykorzystywane w moim odczuciu zgodnie z regułami społecznymi oraz z obowiązującym prawem (ustawa o ochronie danych osobowych).

Celowe wydaje się przedstawienie dwóch metod podejścia do kwestii dopuszczalności rozsyłania poczty elektronicznej. Schematy te zdefiniowane zostały jako systemy *opt-in* oraz *opt-out*[50]. System *opt-out*[51] jest schematem postępowania, który udziela użytkownikowi opcję wycofania

[48] Do G: *Kara śmierci odwołana,* Biuro i Komputer, dodatek do Gazety.
[49] Wyrok Sądu Apelacyjnego z 15 marca 1996 r. I ACr 33/96, OSA 1996/7-8/31

[50] Zgodnie ze słownikiem Collinsa (Collins English Dictionary, 1992) *opt* oznacza możliwość (opcję) okazania preferencji lub wybrania określonego stanowiska dodania *in* lub *out* określa kierunek wyboru
[51] Art. 7 Dyrektywy 00/31 o handlu elektronicznym

się z niego. W przypadku poczty elektronicznej podawane są wtedy specjalne instrukcje pozwalające adresatowi na wypowiedzenie swego sprzeciwu i rezygnację z otrzymywania poczty elektronicznej w przyszłości. Konieczna jest, więc pewna aktywność użytkownika w celu zatamowania nagromadzenia kolejnej poczty elektronicznej. Instrukcje umożliwiające wyjście ze schematu, czyli tzw. instrukcje *opt-out* powinno być zrozumiałe i niezmuszające użytkownika do wielopłaszczyznowych działań ani powodować kosztów po jego stronie. W odwrotnym wypadku możliwość wycofania staje się mniej lub bardziej złudna. W doświadczeniu instrukcje *opt-out* doprowadzają do podania właściwego odnośnika, w który wystarczy kliknąć, albo wysłania zwrotnego listu z odpowiednią komendą. Rozsyłanie listów elektronicznych niezamawianych przez adresata pozostaje w tym układzie legitymowane aż do chwili wyrażenia sprzeciwu. Cały tok postępowania może odbywać się w sposób automatyczny bez udziału świadomości nadawcy. Warunkiem sprawnie działającego systemu *opt-out* jest bezproblemowość w posługiwaniu się nim, bezpłatność, świadomość użytkowników względem istnienia systemu. Oprócz tego produktywny system *opt-out* powinien ułatwiać szybkie do niego przystąpienie w racjonalnym terminie, powinien być systematycznie aktualizowany i oferować zwinny i osiągalny mechanizm postępowania z potencjalnymi skargami i reklamacjami. Zdaniem przeciwników systemu *opt-out* nie jest możliwe narodzenie się sprawnie działającego systemu. z uwagi na rozpiętość zjawiska i światowy charakter Internetu[52].

System *opt-in*[53] natomiast uzależnia rozsyłanie poczty elektronicznej do adresatów od uzyskania wcześniej ich zgody. W tym przypadku, jakikolwiek, nawet pierwszy e-mail przesłany do użytkownika bez jego zgody, także w sytuacji, kiedy nie jest wiadomy jego stosunek do przekazu, jest niedozwolony. Zgoda użytkownika powinna zostać wyrażona jednoznacznie, nadawca zaś może ją uzyskiwać w dowolny sposób. Należy też przyjąć, iż to bezwzględnie na nim spoczywa prawdopodobny ciężar dowodu na okoliczność istnienia zgody adresata.

System *opt-in* w zakresie poczty elektronicznej został utrwalony i rozwinięty w projekcie tzw. marketingu za zezwoleniem klienta (permission marketing). U założeń tej koncepcji leży teza o zupełnej kondensacji rynku reklamy, objawiającym się zobojętnieniem na możliwości dotarcia do nabywcy i zatrzymania jego uwagi na przekazie reklamowym Reklamodawcy. próbując przebić się przez natłok komunikatów, stają się coraz bardziej natarczywi. Bardzo często wytwarzają u odbiorcy skutek odwrotny od zamierzonego przez wywołanie zniechęcenia lub zmieszania. Ten sposób reklamowania się został nazwany „marketingiem przerywającym" (interruption marketing). Nowe podejście opiera się na stopniowym pozyskiwaniu przychylności klienta do działań

[52] P. Podrecki, *op. cit s.?*
[53] Art. 13 Dyrektywy 02/58 o ochronie prywatności i komunikacji elektronicznej

reklamowych, budowania jego zaufania, aż do stworzenia trwalszej więzi między nim a reklamodawcą. W myśl przedstawionego schematu wraz z pierwszym kontaktem, niekoniecznie o charakterze handlowym, pozyskiwana jest zgoda odbiorcy na otrzymywanie przekazów komercyjnych o mniej lub bardziej ograniczonym zakresie, stopniowo rozszerzana. Normy prawne regulujące dopuszczalność rozsyłania poczty elektronicznej opierają się w gruncie rzeczy na wyborze między systemami opt-in bądź opt-out. Za bardziej sprzyjający odbiorcom należy uznać system opt-in. Ostatnimi czasy można zaobserwować wyraźnie zarysowujące się różnice między unormowaniem europejskim, gdzie preferuje się system opt-in, a prawem Stanów Zjednoczonych, które z faktu największego udziału w regulacji Internetu, staje się często pierwowzorem rozwiązań stosowanych w cyberprzestrzeni.

1.3.2 Fake mail

Poczta elektroniczna jest drugą, co do popularności usługą wykorzystywaną w sieci[54]. We wstępie do tego rozdziału przedstawiona została historia powstania standardów przesyłania emalii w Internecie. Jak wspomniano – służy do tego specyficzny software zarówno klienckie, jak i specjalne oprogramowanie po stronie serwera wysyłającego i przyjmującego pocztę elektroniczną. Oprogramowanie serwera wysyłającego pocztę korzysta z informacji przekazanych mu przez oprogramowanie klienckie. Z reguły, na samym początku konfiguracji oprogramowania klienckiego – podajemy swoje dane: imię, nazwisko (ew. nazwa, pod którą chcemy być znani w sieci), adres naszej skrzynki e-mail (na ten adres będą przychodziły odpowiedzi na nasze listy), a zatem podajemy dane, które u odbiorcy zidentyfikują autora przekazanego przez sieć listu[55].

Można wpisać fikcyjne dane. W przypadku imienia i nazwiska – można podawać się za kogoś innego bez wpływu na doręczenie przesyłki. Stworzy to wrażenie, że osoba podająca się za osobę trzecią rozporządza znanym adresem pocztowym. Jeśli dany nazwisko należało do określonej osoby trzeciej – to zapewniona byłaby jej ochrona tego nazwiska. Wpisanie przy pomocy oprogramowania klienckiego sfingowanego adresu pocztowego, sprawi, że wysyłając pocztę nie otrzymamy na adres naszej autentycznej skrzynki pocztowej odpowiedzi. Aczkolwiek przesyłka dojdzie. Można w ten sposób uprawdopodobnić, że wysłana wiadomość pochodzi od wiadomej osoby trzeciej w ten sposób, że dysponuje ona poza danym imieniem i nazwiskiem dodatkowo konkretnym adresem poczty elektronicznej. Sfabrykowany w ten sposób list będzie mieścił w swoim nagłówku jak gdyby całą drogę, którą przebył przez poszczególne serwery pocztowe,

[54] przez wiele lat była najpopularniejszą usługą, aktualnie jest nią WWW.

[55] http://www.vagla.wiaara.pl

jednakże praktycznie będzie zawierał również „nazwę" maszyny, z której został wysłany. Na te informacje statystyczny użytkownik często nie zwraca w ogóle uwagi[56].

Możliwe jest też inne rozwiązanie. Korzystając z telnetu – usługi pozwalającej na zdalną pracę na innym komputerze w sieci – użytkownik posiadający zasadniczą wiedzę na temat mechanizmów przekazywania elektronicznej poczty jest w stanie połączyć się z *demonem sendmail.* Bez wątpienia jest on najczęściej spotykanym i używanym demonem do obsługi poczty. Jest on darmowy i dość łatwo konfigurowalny. Sendmail ze względu na swą popularność staje się często celem programistów piszących *exploity*[57]. Sendmail to program typu MTA (Mail Transport Agent), którego zadaniem jest nasłuchiwanie na określonym porcie, który odbiera wiadomości od innych serwerów pocztowych, wysyła je w świat oraz przesyła na konta lokalnych użytkowników. Do poprawnego działania Sendmail potrzebuje serwera DNS (np. BIND). Głównym plikiem konfiguracyjnym w demonie Sendmail jest plik /etc/sendmail.cf, w którym określane są parametry programu. Plik ten jest generowany podczas instalacji serwera i odczytywany za każdym razem przy starcie demona. Zawiera on opis ścieżek do pozostałych plików konfiguracyjnych, a także do katalogów, gdzie będą zapisywane obecnie przetwarzane listy. Każda linia tego pliku konfiguracyjnego odpowiada określonej komendzie. Wiersze rozpoczynające się od znaków # są komentarzami, natomiast te, które rozpoczynają się od pojedynczej litery, oznaczają funkcje. Plik konfiguracyjny składa się z siedmiu głównych działów. Plik ten jest generowany za pomocą programu m4. Generowanie owego pliku odbywa się na podstawie utworzonego wcześniej zbioru o rozszerzeniu .mc, który zawiera różnego typu makra[58].

Możemy również posłużyć się specjalnymi usługami istniejącymi w sieci, których przykładem jest *Remailer*. Remailer to jest usługa komputerowa, która anonimizuje pocztę elektroniczną. Remailer pozwala wysyłać list elektroniczny do kogoś, lub do grupy dyskusyjnej USENET, w taki sposób, że odbiorca listu nie pozna prawdziwej tożsamości, ani prawdziwego adresu e-mail. Kiedy pierwsza wersja tego FAQu, w 1995, roku została opublikowana w Internecie, wszystkie popularne remailery były darmowe. Dziś, niektóre z serwerów, które te usługi komputerowe udostępniają, wymagają opłat od użytkowników. Dzięki temu mechanizmowi istnieje możliwość naruszenia lub zagrożenia dóbr osobistych osób fizycznych i prawnych. Bo przecież nietrudno wyobrazić sobie sytuację, w której ktoś bezimiennie uczestniczy w dyskusji na forum grupy dyskusyjne *Usenetu* podając się za kogoś innego. Nie dość, że narusza dobro osobiste w postaci nazwiska (pseudonimu) danej osoby, to dodatkowo może głosić treści niezgodne z przekonaniami

[56] Tamże
[57] Exploity to programy wykorzystujące błędy w innych programach, które uruchomione w systemie pozwalają na nieupoważnione przejęcie kontroli nad nim (uzyskanie praw administratora).

[58] http://www.zajceff.de/webpage/psi.doc

osoby, pod którą się podszywa. Osoba podszywająca się prawdopodobnie ma możliwość obrażenia innych osób np. poprzez używanie epitetów, sformułowań kolokwialnie uznanych za ordynarne lub uwłaczające pod adresem osób trzecich. W ten sposób naruszone będzie dobre imię osoby, pod którą się podszyto w taki sposób, że zostanie ona uznana przez innych uczestników grypy dyskusyjnej za niekulturalną, ordynarną itp. Osoba, pod którą się podszyto nie koniecznie musi być równocześnie dyskutantem na tej grupie. Podszywający się może za każdym razem „podpisywać się" realnym adresem poczty elektronicznej ofiary i w ten sposób kierować do niej ewentualne odpowiedzi dyskutantów (*reposty*). Adres ten może przyciągnąć pełnych inwencji internautów, którzy dokonać mogą różnorodnych ataków na posiadacza danej skrzynki. Późniejsze *reposty* mogą spowodować pejoratywne odczucia dysponenta określonego adresu skrzynki pocztowej (poprzez sam fakt, że się pojawią lub przykładowo przez obraźliwe treści niosące w sobie w ramach „rewanżu"). Nie trudno sobie wyobrazić podszycie się pod pracowników danej firmy. Może to analogicznie rodzić konsekwencje w postaci uszczerbku na renomie tej firmy u części internautów, a w dalszej kolejności u innych osób .Należy pamiętać, że Internet to „wirtualna wioska", w której bardzo prosto znaleźć daną osobę, która z niego korzysta i nawiązać z nią kontakt. Należy również mieć na względzie to, że archiwa list dyskusyjnych lub archiwa dyskusji w *Usenecie* często są przechowywane w postaci stron WWW. Każdy, zatem zainteresowany znalezieniem informacji na temat danej osoby może dotrzeć do archiwalnych listów wysłanych przez kogoś, kto pod daną osobę się podszył, kreując jej negatywny obraz.

Przy wykorzystaniu *fake maila* można utrudnić atakowanej osobie użytkowanie swej skrzynki pocztowej. Procedura ta polega na podszyciu się pod daną osobę w chwili wysłania wniosku o zapisanie na listę dyskusyjną. Jeśli zasubskrybuje się taką osobę na kilka list dyskusyjnych, na których odbiorcy generują dla przykładu 20 listów dziennie – sumarycznie osoba atakowana dostaje bardzo dużą ich liczbę. Może dojść do zablokowania konta pocztowego tej osoby i w ostateczności naruszenia dobra osobistego w postaci wolności komunikacji. Zapisanie takie będzie efektywne tylko wtedy, gdy serwery obsługujące daną listę dyskusyjną nie wysyłają prośby o potwierdzenie subskrypcji na daną listę do nadawcy pierwszej prośby. Poświadczenie taki oczywiście w tym konkretnym przypadku przyjdzie na konto pocztowe atakowanej osoby i będzie mogło być przeczytane tylko przez nią. Nie spowoduje to zalania jej skrzynki dużą ilością korespondencji (*flood*). Bardzo zbliżone ograniczenia mogą się wiązać z *fake mailem* wysłanym na grupę *Usenetu* z jakąś interesującą ofertą, np. sprzedaży telefonu komórkowego, wynajęcia mieszkania. Osoby zaciekawione kupnem takiego telefonu po bardzo atrakcyjnej cenie będą spędzać sen z powiek ofierze ataku przesyłając jej oferty kupna. Prezentowane stanowisko może być dyskusyjne, gdyż jak

wspomniano wyżej – wolność może jest rozumiana przez niektórych autorów jako wolność poruszania się.[59]

5.4 Sniffing

Sniffing jest najczęściej spotykaną metodą ataków internetowych[60]. Gdy włamywaczowi uda się zainstalować specyficzne oprogramowanie do przechwytywania pakietów w sieci *(sniffer*), to za pomocą specjalnych filtrów może obserwować połączenia z konkretnej domeny – celu ataku. Jakiekolwiek połączenie protokołu FTP, telnet, rlogin czy SMTP może przyzwolić włamywaczowi na przechwycenie hasła, treści listu lub innych informacji. Włamywacz może również osadzić program do *„sniffowania"* w innym programie, w postaci wirusowej. Program taki zostałby rozpowszechniony i po uruchomieniu w systemie pokrzywdzonego, który niczego nie przewiduje, przechwytywałby odpowiednie informacje i przesyłał je do systemu włamywacza. Wchodząc w posiadanie takich danych włamywacz naruszałby prawo do prywatności danej osoby, naruszałby również inne dobra osobiste w szczególności tajemnicę komunikacji[61]. Można tu zacytować wypowiedź H. Hubmanna: „Osoba postronna narusza prawo osobiste wówczas, gdy uzyska nieuprawnioną wiadomość o tajemnicach drugiej osoby zarówno poprzez bezpośrednie wtargnięcie w sferę tajemnicy, jak i poprzez wybadanie czy wyśledzenie tajemnicy z rozmaitych okoliczności, które powinny być dla niej ukryte"[62]. Autorka w dalszej części swojego wywodu konstatuje, że już samo przygotowanie urządzeń podsłuchowych stanowi już zagrożenie dobra osobistego. W świetle powyższych uzasadnień należy przyjąć, że takim zagrożeniem będzie również zainstalowanie *sniffera* na którejś z tras internetowych, lub wygenerowanie odpowiedniego wirusa, który wykonywałby podobne funkcje i działał w systemie komputerowym bohatera napadu[63].

5.5 Inne przykładowe formy naruszeń

Dzięki wykorzystaniu techniki fake mail, ale również bez wykorzystania tej techniki – istnieje możliwość utrudnienia pracy telefonu komórkowego. Jest to możliwe dzięki usłudze udostępnianej w sieci Internet – tzw. bramki Internet -SMS[64]. Eksploatator może wysyłając e-mail na odpowiedni adres przesłać tą drogą SMS na dany numer telefonu. Można to również zrobić przy wykorzystaniu strony WWW. Długi list e-mail będzie dzielony na krótsze wiadomości i stopniowo przesyłany na numer telefonu adresata. Może to w konsekwencji spowodować tzw., flood (zalanie)

[59] www.vagla.wiaara.pl
[60] D. Atkins, P. Buis eds.: *Bezpieczeństwo Internetu. Profesjonalny Informator*,LT& P 1997,s. 461.
[61] I. Dobosz, *Procesy prasowe w Polsce w latach 1960-1975*, Kraków 1979*, s.*
[62] *Ibidem* s. 94
[63] WWW.vagla.wiaara.pl
[64] SMS -Short Message Service jest usługą polegającą na przesyłaniu krótkich (do 160 znaków) wiadomości między abonentami sieci komórkowych w standardzie GSM. SMS FAQ

telefonu komórkowego. Jeśli przyjąć za A. Szpunarem iż przedmiotem odrębnej ochrony jest „wolność od złośliwego niepokojenia”[65] opisane wyżej działanie będzie naruszało to dobro osobiste, ale może również naruszać wolności komunikacji, sferę życia prywatnego. Aktualnie serwisy oferujące taką usługę (bramkę) wprowadzają limit ilościowy przesyłek SMS na dany numer telefonu. Kolejnym z naruszeń jest Bluesnarfing. Znana jako "Bluesnarfing" technika wykorzystuje potencjalnie niebezpieczną lukę w systemie bezpieczeństwa najbardziej popularnych modeli Ericssona i Nokii. Mając na względzie sposób, w jaki moja komórka wymienia się z komputerem danymi "po bluetooth'ie" zacytuje: "Stojąc w pobliżu sali konferencyjnej, wprawny haker może na przykład wykraść kontakty i inne kluczowe informacje z telefonu konkurencyjnego biznesmena". Pedofil może z telefonu dziecka wykraść kontakty do swoich przyszłych ofiar[66]. W Internecie spotkamy się również z innymi formami naruszenia lub zagrożenia dóbr osobistych. Bardzo często narusza się autorskie prawa osobiste i z nimi związane autorskie dobra osobiste. Ma to miejsce zarówno przy wykorzystaniu utworów graficznych, muzycznych czy literackich opublikowanych w sieci jak i w przypadku udostępnianiu w sieci nielegalnego oprogramowania (lub specjalnych programów, tzw. cracków, które umożliwiają oszukanie programu w taki sposób, że uznaje on się za legalną kopię i udostępnia wszystkie swoje opcje. Podobnie, jeśli chodzi o sprawdzone i udostępnione w sieci numery seryjne, które pozwala na instalację danego oprogramowania). Mamy tu do czynienia z naruszeniem lub zagrożeniem autorskich dóbr osobistych, ale również przewidzianej w kodeksie twórczości naukowej lub literackiej. Wedle orzecznictwa „oprogramowanie komputerowe może być traktowane jako utwór o charakterze naukowym lub literackim, jeżeli posiada ono cenę oryginalności twórczej, spełnia przewidziany przez ustawę wymóg odpowiedniego ustalenia (verba legis: „ustalony w jakiejkolwiek postaci”) i zawiera elementy indywidualizujące twórcę programu”[67]. Innym przykładem naruszenia lub zagrożenia autorskich dóbr osobistych w Internecie będzie korzystanie z przez twórców stron WWW z ramek (frame), w których stosują odnośniki do innych stron. Tacy twórcy naruszać będą prawo do autorstwa integralności strony WWW jako utworu. Naruszenia autorskich dóbr osobistych oraz ich zagrożenie występujące w Internecie jest zagadnieniem bardzo obszernym i się mieści się w ramach niniejszego opracowania[68].

[65] A. Szpunar: *Zadośćuczynienie za szkodę niemajątkową*, Bydgoszcz 1999r., s. 100.
[66] http://www.vagla.pl/prawo_nws.htm
[67] Wyrok Sądu Apelacyjnego z 29 stycznia 1993 r. AG Cr 369/92, Wokanda 1993/9 s. 33.
[68] Szersze omówienie zagadnienia znajduje się w: J. Barta, R. Markiewicza, *Internet a prawo*, Kraków 1998.

2.CYWILNOPRAWNA OCHRONA DÓBR OSOBISTYCH

Przesłanka zawarta w art. 23 kodeksu cywilnego ma charakter generalny i przewiduje ochronę, jaką prawo cywilne roztacza nad instytucją dóbr osobistych. Ochrona dóbr osobistych na podstawie przepisów prawa cywilnego jest niezależna od ochrony przewidzianej innymi przepisami, np. przepisami prawa karnego[69]. Środki ochronne w razie bezprawnego naruszenia lub zagrożenia prawa osobistego przewidziane są w art. 24 kodeksu cywilnego[70]. Z jego treści wynika, że dobra osobiste są chronione w sposób uniwersalny, a więc środki ochrony mogą mieć zarazem charakter majątkowy jak i niemajątkowy. W jednym sprawie mogą być zgłoszone zarówno roszczenia mające naturę majątkową jak i te o naturze niemajątkowej.

Do środków o charakterze niemajątkowym zaliczamy: powództwo o ustalenie, roszczenie o zaniechanie oraz roszczenie o usunięcie skutków naruszenia. Do środków o charakterze majątkowym zaliczyć należy: zadośćuczynienie pieniężne lub zapłata za naruszenie dóbr osobistych oraz naprawienie szkody majątkowej przewidziane w art. 24 §2 k.c.[71] .

2.1. Niemajątkowe środki ochrony

Ochrona dóbr osobistych o charakterze niemajątkowym uregulowana jest w przepisach art. 24 k.c. Postanowienie art. 24 § 1 uzależnia ochronę dóbr osobistych od spełnienia dwóch przesłanek: zagrożenia lub naruszenia dobra osobistego oraz bezprawności działania[72]. Aczkolwiek nie powinno się ignorować możliwości ukazane przez art. 142, 423 i 424 k.c. albowiem mówią one o środkach ochrony, które przybierają postać obrony koniecznej oraz stanu wyższej konieczności. W tych wypadkach ustawodawca dopuszcza na zasadzie wyjątku zastosowanie pomocy własnej w celu zagwarantowania ochrony dóbr osobistych.[73].

2.2.Powództwo o ustalenie bezprawności naruszenia

Powództwo o ustalenie bezprawności naruszenia opiera się na ogólnym przepisie art. 189 KPC, według którego „powód może żądać ustalenia przez sąd istnienia lub nieistnienia stosunku prawnego lub prawa, gdy ma w tym interes prawny”[74]. Mimo początkowego oporu judykatury,

[69] S. Grzybowski, *Prawo cywilne zarys części ogólnej*, s. 136
[70] Z. Radwański, *Prawo cywilne – część ogólna*, Warszawa 2002, s. 166
[71] *Ibidem*
[72] Jest to pogląd panujący w piśmiennictwie polskim. Przykładowo: S. Grzybowski: *Zarys cześci ogólnej prawa cywilnego, Warszawa* , s. 136 ; A. Szpunar, *Ochrona dóbr osobistych*, Warszawa 1979, S. 235
[73] A. Cisek, *Dobra osobiste i ich niemajątkowa ochrona w kodeksie cywilnym*, Wrocław 1989, s. 114
[74] Z. Radwański, *op. cit.*, s. 167

zostało powszechnie uznane za dopuszczalny środek ochrony dóbr osobistych. [75]. Sąd Najwyższy zaobserwował bowiem, że dążeniem procesu o ochronę dóbr osobistych w razie bezprawnego wkroczenia w sferę cudzego życia rodzinnego jest uzyskanie sankcji cywilnoprawnej, dającej wyraz potępienia sprawcy bezprawnego zachowania. Przedmiotem procesu i rozstrzygnięcia sądowego nie jest skontrolowanie, które z faktów i ocen są prawdziwe i mają usprawiedliwienie, a które należy potraktować odmiennie[76]. W przypadku powództwa o ustalenie bezprawności naruszenia dóbr osobistych ustala się jednak, że dyskusyjna teza, mogąca naruszać dobra osobiste, jest autentyczne bądź nieautentyczne. Są to rzeczywiste ustalenia. Z drugiej strony powód domaga się stwierdzenia, że głoszenie pewnych wiadomości ignoruje jego prawo osobiste i w rezultacie mamy do czynienia z ustaleniem stosunku prawnego między stronami, jaki powstał w efekcie podniesienia i popularyzacji zarzutów. A. Szpunar zauważa, że powództwo o ustalenie może być wystarczającym środkiem zapobiegającym naruszeniu dobra osobistego, a także skutecznym środkiem ochrony w razie już dokonanego naruszenia[77]

2.3.Roszczenie o zaniechanie

Roszczenie o zaniechanie może pojawić się w pozwie albo jako jedyne żądanie główne, gdy dobro osobiste zostało tylko zagrożone cudzym działaniem albo też może wystąpić obok żądania usunięcia skutków naruszenia, gdy do naruszenia dobra osobistego już doszło[78]. Roszczenie o zaniechanie wzorowane jest na roszczeniu negatoryjnym z zakresu prawa rzeczowego (art. 222 § 2 , 344, 347 k.c.)[79]. Zgodnie z przyjętym w judykaturze i doktrynie poglądem przesłanką takiego roszczenia jest zagrożenie dobra osobistego cudzym działaniem lub uzasadniona obawa dalszych naruszeń[80]. Osoba uprawniona może żądać zaniechania tylko ściśle określonego działania[81]. Zaakcentować należy, iż według poglądu wyrażonego przez Sąd Najwyższy: „żądanie dopełnienia czynności potrzebnych do usunięcia skutków naruszenia dóbr osobistych przez złożenie oświadczenia odpowiedniej treści i 86w odpowiedniej formie powinno być skonkretyzowane przez osobę domagającą się ochrony, czyli, powinna ona ściśle określić treść oświadczenia, którego złożenia domaga się”[82].

2.4. Roszczenie o usunięcie skutków naruszenia

Z brzmienia zdania 2 § 1 art. 24 wynik, że w razie dokonanego już naruszenia dobra

[75] Wyrok Sądu Najwyższego z 30 sierpnia 1974r. , I CR 384/74, OSP 1977, Nr 10, poz. 161, Orzeczenie Sądu Najwyższego z 6 listopada 1986r., ICR 317/86 (niepublikowane)
[76] Wyrok Sądu Najwyższego z 18 stycznia 1984r., I CR 400/83, OSN 1984, poz. 195
[77] A. Szpunar: *op. cit.,* s. 253
[78] M. Pazdan: art. 24. [w:] K. Pietrzykowski (red.), *KC. Komentarz*, Warszawa 2004.
[79] A. Szpunar: *op. cit*. s. 237
[80] M. Pazdan [w:] K. Pietrzykowski (red.), *KC. Komentarz*, Warszawa 2004 ; w judykaturze Wyrok SN z 26 lutego 1965r., II CR 13/65, OSN 1965, Nr 10, poz. 174 z glosą S. Grzybowskiego , OSP 1966, Nr 10, poz. 221
[81] S. Dmowski, S. Rudnicki, *Komentarz do Kodeksu Cywilnego*, Warszawa 2003r.
[82] Wyrok Sądu Najwyższego z 22 grudnia 1997r. , II CKN 546/97 (OSNIC 7-8/98, poz. 119)

osobistego, ten czyje dobro osobiste zostało naruszone, może żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Treść zadania powinna być dostosowana do charakteru i rodzaju naruszenia dobra osobistego. Można w tym miejscu przytoczyć bogate orzecznictwo, wskazujące rozsądne wskazówki, co do sposobu ochrony[83]. Powód może, więc ograniczyć się do żądania usunięcia stanu naruszenia jego dobra osobistego np. zniszczenie nieprawdziwej opinii[84], zniszczenie przedmiotów za pomocą, których naruszono dobro osobiste. Powód może tez domagać się podjęcia czynności zmierzających do usunięcia skutków naruszenia. W kontekście naruszeń dóbr osobistych usunięciem skutków naruszenia może być przykładowo żądanie usunięcie z serwera określonej publikacji WWW naruszającej dobra osobiste, publiczne przeproszenie wysłane na listę dyskusyjną lub do Usenetu, usunięcie z archiwum grupy dyskusyjnej określonego listu. Za rodzaj oświadczenia prowadzącego do usunięcia skutków naruszenia dobra osobistego traktowane jest przeproszenie pokrzywdzonego lub złożenie wyrazów ubolewania[85]. Sąd Najwyższy w swojej stanowczej wypowiedzi[86] wyraził pogląd, że to sąd w sentencji wyroku decyduje, w jaki sposób i jakimi słowami pozwany ma przeprosić, skutkuje odebraniem charakteru osobistego moralnego przeprosinom. To, że sąd nakazuje przeprosić wcale nie znaczy, że przeprosiny będą nieudawane, a pozwany zmieni zdanie w stosunku do pokrzywdzonego. Takie przeprosiny niekoniecznie spowodują usunięcie skutków naruszenia. Tak, więc nierzetelnemu przeproszeniu powinien być odebrany status środka ochrony dóbr osobistych[87].

2.5. Majątkowe środki ochrony.

Uregulowanie przyjęte w Kodeksie cywilnym jest pod względem konstrukcyjnym niemalże tożsame z unormowaniem przedwojennym z Kodeksem zobowiązań, w którym odnośnie ekspiacji finansowej rządziły cztery zasady: zasada zadośćuczynienia pieniężnego jako wyjątku (w przypadkach, gdy przewiduje to ustawa) od reguły, że naprawieniu podlega jedynie szkoda o charakterze majątkowym, zasada fakultatywności zadośćuczynienia, zasada, w myśl, której pokrzywdzony mógł domagać się zadośćuczynienia alternatywnie na swoją rzecz lub na rzecz wskazanej przez siebie organizacji (Kodeks cywilny przyjął rozwiązanie odrębne, polegające na koegzystencji odpokutowania z nietypową i niemającą korelatu w obcych systemach

[83] Wyrok Sadu Apelacyjnego w Lublinie z 10 lipca 1998r. , I Aca202/98, OSA 2000, Nr 2, poz. 6
[84] Wyrok Sadu Najwyższego z 17 grudnia 1976r., I PR 15/76, OSN 1977, Nr 8, poz. 139
[85] M. Pazdan: *op. cit*. s. 92
[86] Wyrok Sądu Najwyższego z 19 stycznia 1982r., IV CR 500/81, OSN 1982, Nr 9-10, poz. 183
[87] Wyrok Sądu Najwyzszego 19.01.1982r., IV CR 500/81, OSN 1982 nr 9-10, poz. 183, wyraził pogląd, iż sentencja wyroku powinna zawierać dokładnie sformułowaną treść przeproszenia, co spotkało się z krytyką A. Szpunara w glosie OSP 1983, nr 10, poz. 220.

jurystyczny sankcją z art. 448 KC[88]), zasada ograniczająca dziedziczenie roszczenia o zadośćuczynienie[89]. Gdy idzie o normę, w myśl, której ofiara mogła domagać się rekompensaty alternatywnie na swoją rzecz lub na rzecz wskazanej przez siebie organizacji Art. 448 przewidywał w razie umyślnego naruszenia dóbr osobistych, że poszkodowany może żądać, niezależnie od innych środków potrzebnych do usunięcia skutków wyrządzonej szkody, ażeby sprawca uiścił odpowiednią sumę pieniężną na rzecz Polskiego Czerwonego Krzyża[90]. Współcześnie art. 448 przyjął inne brzmienie, a mianowicie: „w razie naruszenia dobra osobistego sąd może przyznać temu, czyje dobro osobiste zostało naruszone, odpowiednią sumę tytułem zadośćuczynienia pieniężnego za doznaną krzywdę lub[91] na jego żądanie zasądzić odpowiednią sumę pieniężną na wskazany przez niego cel społeczny, niezależnie od innych środków potrzebnych do usunięcia skutków naruszenia"[92].

Mając na uwadze na umiejscowienie przepisu art. 448 k.c. pomiędzy przepisami o czynach niedozwolonych i przyjmując równocześnie, że wina stanowi zasadniczą przesłankę odpowiedzialności z tego tytułu powinno się przyjmować, że podstawą zasądzenia zadośćuczynienia będzie najmniejszy nawet stopień zawinienia, a więc do granic *culpa levissima*[93] . W razie naruszenia dobra osobistego taka postać ochrony nie jest obligatoryjna i zależy od decyzji Sądu, na co wskazuje użyty w art. 448 k.c. zwrot „sąd może", niemniej jednak arbitralność oceny sędziego powinna mieć na względzie kryteria rozmiaru i intensywności doznanej krzywdy, stopień negatywnych konsekwencji dla pokrzywdzonego, również stopień zawinienia po stronie sprawcy[94]. Podstawą odmowy zadośćuczynienia, z art. 448 k.c. może być nieznaczny rozmiar szkody niemajątkowej (niekoniecznie jej znikomość)[95].

Kontrowersje budzi również możliwość kumulowania roszczeń przewidzianych w art. 448 i 445 k.c.. Ewentualność tę zakwestionował Radwański, bowiem jego zdaniem system prawny powinien unikać mnożenia jednorodnych satysfakcji za to samo naruszenie, a także nie dopuszczać do mnożenia sankcji za ten sam czyn. Jednakże uchwała Sądu Najwyższego z dnia 8 grudnia 1973r. przesądziła o dopuszczalności kumulowania obu sankcji. Możliwe było, więc zatem zasądzenie odpowiedniej sumy na PCK, a obok tego, zgodnie z art. 445 § 1 Sąd mógł zasądzić odpowiednią sumę tytułem zadośćuczynienia. Można, zatem przyjąć, że art. 448 w nowej treść podejmuje postulaty Z. Radwańskiego, gdyż obecnie będzie funkcjonować jedynie j źródło satysfakcji albo

[88] A. Szpunar, *op. cit.* , s. 203
[89] http://www.vagla.pl/dobra_os.htm
[90] A. Szpunar, *op. cit*. s. 203
[91] Z. Radwański, *op. cit*. 169
[92] http://wideofilm.internetdsl.pl/prawo/kc/3.html#t7
[93] A. Szpunar: *Zadośćuczynienie za szkodę niemajątkową*, Bydgoszcz 1999, s. 212.
[94] Z. Radwański, *op. cit*. s. 170
[95] A. Szpunar: Zadośćuczynienie, s. 185.

zadośćuczynienie albo zasądzenie sumy pieniężnej na wybrany cel. W sprawie wysokości zadośćuczynienia większość autorów jest zgodna, iż należy ją uzależnić od wielkości doznanej krzywdy (rozmiaru i intensywności krzywdy). Wysokość zadośćuczynienia z art. 448 k.c. powinna być umiarkowana[96].

Przepis artykułu 445 k.c. w wypadku naruszenia dóbr osobistych zadośćuczynienie pieniężne za doznaną krzywdę. Niezbędną przesłanka jest zaistnienie zdarzenia przewidzianego w tym artykule, z którym związana jest odpowiedzialność z tytułu czynów niedozwolonych i ażeby pomiędzy tym zdarzeniem a doświadczoną krzywdą istniał związek przyczynowy[97]. Ze względu na fakt, iż uszkodzenie ciała lub wywołanie rozstroju zdrowia a także skłonienie za pomocą podstępu, gwałtu lub nadużycia stosunku zależności do poddania się czynowi nierządnemu[98] w przypadku Internetu raczej nie będzie miało miejsca – art. 455 może być w omawianej kwestii zastosowany jedynie w przypadku pozbawienia wolności[99]. Przyjmuje się, że pozbawienie wolności może dotyczyć zarówno sytuacji fizycznego zniewolenia osoby, jak i w przypadkach skrajnych, pozbawienia osoby możliwości podejmowania decyzji o samej sobie[100]. Istnieje również inne, szersze rozumienie wolności chociażby wolność komunikacji, ochrona prowadzenia działalności statutowej osoby prawnej. Jak podkreślają autorzy Komentarza do Kodeksu cywilnego – majątkowa ochrona szerzej rozumianej wolności nie jest obecnie wykluczona na tle omawianego już art. 448 k.c.

[96] Z. Masłowski [w] *Komentarz do k.c.. ,* t. II s. 1130
[97] A. Szpunar, Zadośćuczynienie, s. 187
[98] http://wideofilm.internetdsl.pl/prawo/kc/3.html#t7
[99] http://www.vagla.pl/dobra_os.htm
[100] A. Szpunar*, Zadośćuczynienie, s*. 187