Uniwersytet Warszawski

Wydział Prawa i Administracji

Piotr Waglowski

Naruszenie dóbr osobistych w Internecie i ich cywilnoprawna ochrona na podstawie przepisów Kodeksu cywilnego

Praca napisana w

Katedrze Prawa Cywilnego

Pod kierunkiem

prof. dr hab. Marka Safjana

Warszawa 1999

Spis treści

1 WSTĘP ... 3

1.1 Uzasadnienie wyboru tematu ... 3
1.2 Zakres pracy ... 4

2 Internet ... 5

2.1 Historia Internetu ... 5
2.2 Charakterystyka środowiska Internautów w Polsce ... 6
2.3 Netykieta ... 11

3 Dobra osobiste ... 12

3.1 Pojęcie ... 12
3.2 Konstrukcja prawna – prawo podmiotowe ... 15
3.3 Inne gałęzie prawa ... 16
3.4 Otwarty katalog dóbr osobistych ... 17
3.5 Ewentualna kolizja wartości ... 23
3.6 Dobra osobiste osób prawnych ... 25

4 Przesłanki ochrony ... 26

4.1 Zagrożenie i naruszenie dóbr osobistych ... 26
4.2 Bezprawność ... 26
4.3 Wyłączenie bezprawności ... 28

5 Naruszenia dóbr osobistych w Internecie ... 30

5.1 Zagadnienia wstępne ... 30
5.2 World Wide Web ... 32
5.3 E-mail i Usenet ... 45
5.4 Sniffing ... 55
5.5 Inne przykładowe formy naruszeń ... 56

6 Cywilnoprawna ochrona dóbr osobistych ... 61

6.1 Niemajątkowe środki ochrony ... 61
6.2 Majątkowe środki ochrony ... 63
6.3 Odpowiedzialność *providera* ... 66

7 Zakończenie ... 71

8 Bibliografia ... 74

9 Autor ... 77

1 WSTĘP

1.1 Uzasadnienie wyboru tematu

W 1999 roku Internet obchodzi trzydziestolecie swoich narodzin. Od swych początków *stricte* militarnych przeszedł długą ewolucję i wciąż następuje jego bardzo szybki rozwój. Wielu obserwatorów zadziwia ekspansja Internetu. W chwili obecnej spełnia on coraz częściej funkcję codziennej gazety, telefonu, faxu, biblioteki. Za jego pośrednictwem można kupić *on line* szereg towarów z bogatego asortymentu wirtualnych sklepów: poprzez samochody, książki, oprogramowanie, wszelki sprzęt gospodarstwa domowego, na artykułach spożywczych kończąc. Następuje stopniowa komercjalizacja Internetu. Internet jako zjawisko zarówno techniczne jak i społeczne przekracza granice państw, utrwalonych systemów prawnych, grup społecznych, etnicznych, zawodowych czy religijnych. Ma globalny charakter.

Wraz z rozrastającą się „siecią sieci" wzrasta liczba jej użytkowników. Powstają nowe, nieznane wcześniej grupy zawodowe, dla których (w większości przypadków) próżno szukać polskich nazw (webmaster, konsultant ds. e-business, web designer), coraz ściślej przenikają się i splatają systemy komunikacji społecznej, wytworzonej przez informatykę i telekomunikację. Można zaobserwować rozwijanie się nowego języka, jakim porozumiewają się między sobą internauci. Tworzą się nowe relacje społeczne, a tym samym powstaje społeczeństwo informacyjne.

Józef Wierzbołowski w swoim referacie przedstawionym na Konferencji naukowej nt. "Integracja europejska wobec wyzwań ery informacyjnej (postindustrialnej)[1]" zorganizowanej przez Centralny Urząd Planowania i Instytut Rozwoju i Studiów Strategicznych przedstawił następującą definicję społeczeństwa informacyjnego: „Jako społeczeństwo informacyjne traktuje się społeczeństwo, w którym informacja stała się zasobem produkcyjnym określającym nowe przewagi konkurencyjne w stosunku do otoczenia, a równocześnie zapewniającym rosnący poziom adaptacyjności społecznej, w wyrazie ogólnym i w wyrazie jednostkowym, do

[1] Referat można znaleźć pod adresem: http://eris.kbn.gov.pl/Pl-iso/pub/info/dep/integracja/index.html

zwiększającej się lawinowo zmienności tego otoczenia. Jak z tego wynika, w podejściu do społeczeństwa informacyjnego akcentuje się nie tyle aspekt technologiczny (technologie informacyjne), ile aksjologiczny, wykształcenie się nowej formacji cywilizacyjnej z nowym sposobem postrzegania świata i zmodyfikowanym systemem wartości społecznych."

Dobra osobiste są wartością chyba najbliższą naturze ludzkiej, ich lekceważenie wydaje się niemożliwe, ze względu na ścisły związek życia, zdrowia, czci, nietykalności osobistej itp. z osobą każdego z nas. J. St. Piątkowski za podstawową przyczynę wzrostu znaczenia ochrony dóbr osobistych w drugiej połowie XX wieku uznaje postęp techniki[2]. Ciągły rozwoju techniki, kultury, tworzenie się wspomnianego nowego rodzaju społeczeństwa powoduje, że należy przyjrzeć się dotychczasowym regulacjom prawnym dotyczącym właśnie dóbr osobistych pod kątem ich adekwatności do nowych warunków.

1.2 Zakres pracy

Niniejsza praca ma na celu opisanie pewnych zjawisk w sieci Internet, które można zakwalifikować jako naruszenie lub zagrożenie dóbr osobistych osób uczestniczących w wymianie informacji za pośrednictwem Internetu. Zjawiska te po części stanowią naruszenia klasycznych, znanych polskiemu systemowi prawnemu dóbr osobistych, po części stanowią naruszenie nowych, specyficznych dóbr, mających związek z funkcjonowaniem społeczeństwa informacyjnego. Praca ta ma na celu zwrócenie uwagi na to, że Internet (jako medium komunikacyjne) nie może pozostawać poza państwowym systemem prawnym.

Stawiam tezę, iż nie trzeba tworzyć nowego prawa dotyczącego dóbr osobistych w związku z pewnymi nowymi zachowaniami spotykanymi w sieci. Całkowicie wystarczające wydaje się oparcie na niezamkniętym ich katalogu przewidzianym w kodeksie cywilnym (zasady ogólne). Ewentualne (pożądane) unormowanie ustawowe całości kwestii związanych z Internetem powinno jedynie odsyłać do tych właśnie przepisów, ponieważ art. 23 k.c. *in fine* stanowi, że dobra

osobiste pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

Internet jako sieć globalna, przenika granice państw i systemów prawnych. Jednakże praca ta nie będzie zasadniczo zajmować się ustawodawstwem innych państw. Na marginesie tej pracy pozostaje również ochrona dóbr osobistych przewidziana w polskim prawie międzynarodowym prywatnym i w międzynarodowym prawie publicznym.

Różnorodność zachowań, które mogą naruszać cudze dobra osobiste, a które spotykamy w Internecie, jest tak duża, że z zakresu przedmiotowego niniejszej pracy postanowiłem usunąć kwestie ochrony dóbr osobistych związanych z ochroną wynalazczości, autorskich dóbr osobistych związanych z technologiczną i fizyczną stroną internetu, a także inne, uregulowane w szeregu ustaw szczegółowych. Kwestie te poruszane są coraz częściej w literaturze.

2 INTERNET

2.1 Historia Internetu

Historia Internetu liczy sobie już 30 lat. W pierwszej swej postaci stworzony został do celów militarnych. Armia amerykańska, ze względu na przyjęcie możliwości ataku nuklearnego na USA, rozpoczęła prace nad stworzeniem sieci komputerowej, mogącej funkcjonować pomimo uszkodzenia jej fragmentu - zniszczenie jednego z węzłów nie powodowałoby unieruchomienia całej sieci. Pierwszą koncepcję rozległej sieci o tych cechach zakładała, że każdy węzeł sieci będzie pełnić dokładnie takie same funkcje, a więc nie będzie centralnego komputera zarządzającego. Dzięki agencji rządowej DARPA (*Defence Advanced Research Projects Agency*), która w 1969 roku sfinansowała projekt - powstała pierwsza sieć tego typu o nazwie ARPANET. Pierwszy węzeł zainstalowano 1 września 1969 roku w Uniwersytecie Kalifornijskim w Los Angeles (UCLA). Wkrótce potem w trzech następnych uniwersytetach powstały pierwsze węzły sieci ARPANET - bezpośredniego przodka dzisiejszego

[2] J. St. Piątkowski, Ewolucja ochrony dóbr osobistych [w:] E. Łętowska (red.), Tendencje rozwoju prawa cywilnego, Ossolineum 1983, s. 9.

Internetu[3]. Sieć ARPANET pozwalała swoim użytkownikom przesyłać pocztę i pliki pomiędzy podłączonymi do niej komputerami. ARPANET w swej pierwszej postaci składał się tylko z czterech węzłów, jednakże z upływem lat ulegał szybkiemu rozwojowi. W 1973 r. po raz pierwszy w historii dokonano próby przesłania danych pomiędzy węzłami położonymi po obu stronach oceanu. Zaczął się tworzyć szkielet jednorodnego zestawu technologii sieciowych, co zaowocowało opracowaniem protokołu TCP/IP[4]. Agencja DARPA naciskała na rozwój alternatywnych form transmisji, które byłyby oparte na połączeniach satelitarnych i radiowych, a jednocześnie prowadziła prace nad tanią implementacją protokołu TCP/IP do systemu BSD Unix. W roku 1983 TCP/IP został oficjalnie uznany za obowiązujący w sieci ARPANET. W tym samym czasie zaczęła się coraz częściej pojawiać nazwa Internet. Obecnie Internet nie jest pojedynczą siecią; jest to raczej zbiór tysięcy pojedynczych sieci, którym umożliwiono wymianę informacji pomiędzy sobą.

2.2 Charakterystyka środowiska Internautów w Polsce

Jeśli mówi się o społeczeństwie informacyjnym – można również mówić o jego charakterystyce. Wszelkie szacowania ilości osób korzystających z internetu na świecie oraz w Polsce są jedynie przybliżone. Umieszczenie ich w tej pracy ma na celu pokazanie, że środowisko Internautów jest środowiskiem specyficznym, co może mieć znaczenie przy ocenie, czy cudze dobra osobiste zostały naruszone w Internecie czy też nie.

Niewiele firm specjalizuje się w badaniach użytkowników Internetu w Polsce. Wiadomo jednak, że wśród krajów Europy Wschodniej, w Polsce jest obecnie najwięcej komputerów podłączonych do sieci oraz jej użytkowników. Tendencje w dziedzinie wykorzystania Internetu są podobne jak w krajach Europy Zachodniej, mimo iż skala tych działań jest mniejsza. Pierwszy komputer w Polsce podłączono do międzynarodowej sieci Internet w roku 1991.

[3] M. Kuchciak, Geneza i rozwój Internetu, http://www.ccs.pl/~mkc/internet/genrozw.html
[4] TCP/IP – to zestaw protokołów transmisji danych, pozwalające kierować danymi przesyłanymi z jednej maszyny do drugiej. Nazwa odnosi się do dwóch głównych protokołów – *Transmission Control Protocol* i *Internet Protocol*. Szerzej na ten temat: D. Atkins, P. Buis eds.: Bezpieczeństwo Internetu. Profesjonalny Informator. LT&P 1997, s. 6.

Dynamika przyrostu użytkowników Internetu w Polsce jest wysoka. Po pierwszych trzech latach było ich około 60 tys., po następnych trzech - ponad 900 tys.. Wiosną 1997 roku szacowano liczbę osób korzystających z Internetu w Polsce na około 900 tys. do 1 mln osób[5]. Pod koniec roku 1999 mówi się o dwóch milionach internautów. Według optymistycznych ocen liczba internautów w Polsce podwaja się co rok, aczkolwiek nie będzie to proces ciągły.

W połowie stycznia 1997 roku NASK (Naukowa i Akademicka Sieć Komputerowa) udostępnił wyniki drugiego ogólnopolskiego badania potrzeb i oczekiwań społeczności użytkowników sieci Internet w Polsce. Badanie zostało zrealizowane w oparciu o próbę losowo-celową, w ramach której przeprowadzono wywiady w ponad 200 wylosowanych instytucjach z 204 administratorami sieci i 785 użytkownikami (w sumie wywiady przeprowadzono z 989 osobami). Wyniki badania dają obraz polskiego Internetu od strony geograficznej, demograficznej i społecznej, pozwalają na zarysowanie postaci typowego użytkownika sieci w Polsce, jego problemów, preferencji, sposobów korzystania z sieci, itd.

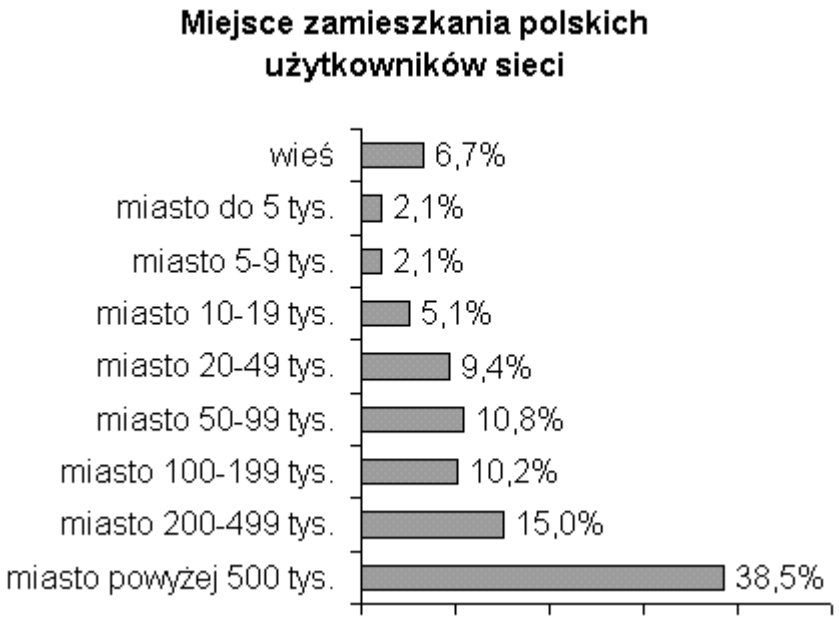
W 1997 roku Internet był używany głównie w wielkich i dużych miastach. Większość zbadanych instytucji (60%) miała swoje siedziby w miastach powyżej 500 tys. mieszkańców. W tych ośrodkach skupia się życie naukowe i gospodarcze kraju. Około 20% badanych instytucji znajdowało się w miastach od 200 do 500 tys. mieszkańców, a 12% to instytucje zlokalizowane w miastach od 100 do 200 tys. mieszkańców. W sumie więc 92% użytkowników Internetu grupowało się w miastach powyżej 100 tys. mieszkańców, a zaledwie 8% przypada na miasta mniejsze i całkiem małe. Sytuacja w 1999 roku (rysunek nr 1) zmieniła się w ten sposób, że coraz więcej osób i instytucji w mniejszych miastach ma dostęp do Internetu, jednakże nadal większe miasta skupiają większość użytkowników.

Wśród użytkowników występuje zdecydowana przewaga mężczyzn. Wedle badań przeprowadzonych przez Katedrę Marketingu Akademii Ekonomicznej w

[5] S. Zembrzuski: Milion Polaków w sieci, Teleinfo 14/97; http://www.teleinfo.com.pl/ti/1997/14/f05.html

Krakowie (http://badanie.ae.krakow.pl) – w roku 1999 z Internetu korzysta 81,3 % mężczyzn oraz 18, 7% kobiet.

Ośrodek Badania Opinii Publicznej (OBOP) przeprowadził dwa badania w roku 1997. I badanie odbyło się między 13 a 15 czerwca 1997 roku, OBOP przebadał reprezentatywną próbę mieszkańców kraju od 16-go roku życia (zrealizowano 1077 wywiadów). Maksymalny błąd statystyczny dla takiej wielkości próby nie przekracza +/- 3% przy wiarygodności oszacowania równej 95%. II badanie zostało przeprowadzone między 4 a 7 października 1997 roku, zrealizowano 1065 wywiadów (błąd jw.).



Rysunek 1: Miejsce zamieszkania polskich użytkowników internetu (1999 rok)

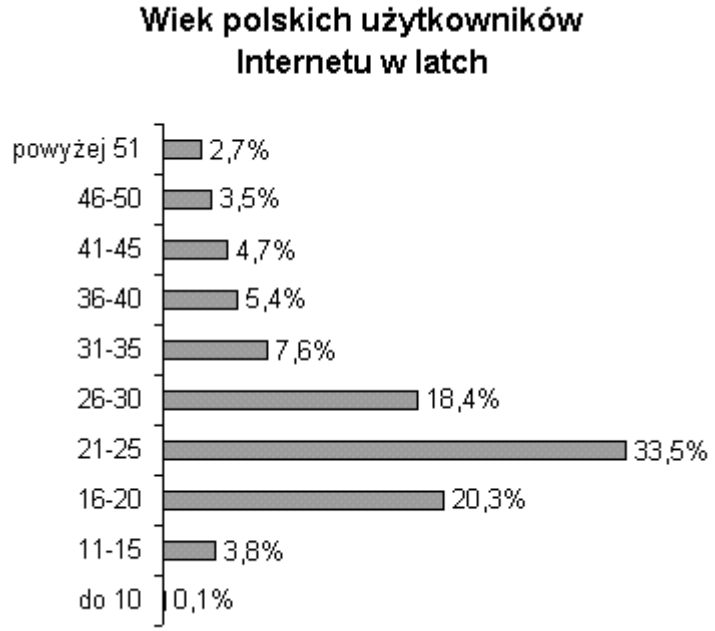
Możliwość korzystania Polaków z Internetu (badania OBOP-u), w % danej grupy, w roku 1997, przedstawia poniższa tabela:

Wybrane grupy użytkowników	I badanie	II badanie
Kierownicy i specjaliści	25	28
Uczniowie i studenci	17	27
Pracownicy szeregowi	11	-
osoby z wyższym wykształceniem	19	-
osoby z dobrą sytuacją materialną	13	17
pow. 20 lat	11	17

Istnieje także powiązanie między dostępem do Internetu a miejscem zamieszkania badanych oraz poziomem wykształcenia. Im wyższy status wykształcenia mieli ankietowani i im w większej miejscowości mieszkali, tym częściej deklarowali możliwość korzystania z Internetu.

Wśród osób korzystających z Internetu w Polsce przeważają osoby z wykształceniem wyższym ukończonym bądź nieukończonym. Nadal utrzymuje się wysoki udział osób, które ukończyły studia w dziedzinie nauk ścisłych.

Sondaże potwierdzają wyraźne obniżenie się wieku użytkowników Internetu. W 1999 roku w gronie respondentów zdecydowanie przeważają użytkownicy w wieku 16 – 30 lat..

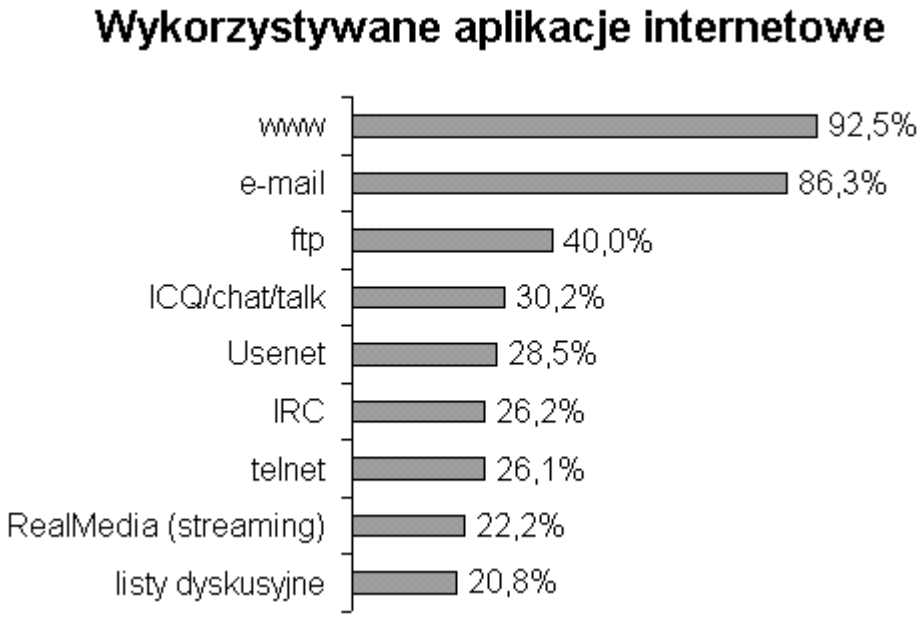


Rysunek 2: Struktura wiekowa użytkowników polskiego Internetu (1999 rok)

Strukturę wiekową użytkowników polskiego Internetu w 1999 roku[6] przedstawia rysunek nr 2. Polski Internet już nie składa się z naukowców i studentów korzystających z sieci na swoich uczelniach. Ten obraz powoli odchodzi w przeszłość. Z jednej strony coraz więcej szkół średnich i podstawowych podłącza się do sieci, z

drugiej: następuje coraz większa komercjalizacja sieci, firmy komercyjne umożliwiają dostęp do sieci swoim pracownikom.

Internet nie stanowi jednorodnej płaszczyzny komunikacyjnej. Za jego pośrednictwem można korzystać z wielu różnych usług. Z punktu widzenia zagadnienia, którym się zajmujemy – naruszeń dóbr osobistych w Internecie – interesujące może być przyjrzenie się z jakich usług internauci korzystają w sieci najczęściej. Do niedawna najczęściej używaną usługą była poczta elektroniczna[7]. Prawdziwą rewolucję zaczął jednak WWW (*World Wide Web*). Jest to aplikacja umożliwiająca korzystanie z dokumentów hipertekstowych udostępnionych na dowolnym serwerze w dowolnym miejscu na kuli ziemskiej. Dokumenty hipertekstowe, kodowane w języku HTML (*Hyper Text Markup Language*), mogą przedstawiać tekst, grafikę, coraz częściej zawierają w sobie elementy muzyczne i video. Wraz z rozwojem technik informacyjnych dokumenty prezentowane poprzez WWW pozwalają na wysoką personalizację wyglądu stron tworzonych dynamicznie dla potrzeb konkretnego adresata.



Rysunek 3: Korzystający z poszczególnych usług w Polskim Internecie (1999 rok)

[6] badania społeczności Internetu przeprowadzone przez Katedrę Marketingu Akademii Ekonomicznej w Krakowie: http://badanie.ae.krakow.pl.
[7] M. Baranowska, NASK, Wyniki badania zbiorowości użytkowników Internetu w Polsce, Internet 2/97.

Pierwszy serwer WWW został uruchomiony w listopadzie 1990 r. przez Tima Berners-Lee z Europejskiego Centrum Badań Jądrowych. W roku 1992 WWW został udostępniony do użytku publicznego. Obecnie przeglądanie Internetu za pośrednictwem tej aplikacji staje się coraz bardziej popularne. Jednocześnie można zaobserwować coraz mniejszą popularność takich usług jak ghoper (prekursor www), czy archie – systemy baz danych (nie uwzględnione wogóle wśród wyników na rysunku nr 3). WWW wypiera te usługi, gdyż spełnia te same funkcje, a dodatkowo oferuje coraz to nowe rozwiązania. Coraz więcej użytkowników Internetu korzysta z grup newsowych (*Usenet*).

Jak wynika z przedstawionych badań można mówić o specyficznym środowisku użytkowników internetu w Polsce.

2.3 Netykieta

Na uwagę zasługuje fakt, że w światowym Internecie funkcjonuje tzw. Netykieta[8]. Jest to zespół podstawowych zasad pracy w Internecie napisanych przez Arlene H. Rinaldi z *Florida Atlantic University* we wrześniu 1992 roku[9]. Na język polski została przetłumaczona przez Krzysztofa Snopka w grudniu 1993.

Jak czytamy we wstępie tej publikacji: „Motywacją do powstania tego opracowania była potrzeba opracowania jednolitych wskazówek dla wszystkich protokołów Internetu, które pozwoliłyby użytkownikom [z Uniwersytetu Floryda] wykorzystywać wszystkie potencjalne zasoby Internetu, zapewniając jednocześnie pełna ich [użytkowników] odpowiedzialność za sposób dostępu i transmisji informacji poprzez siec Internet."

Dość szczegółowo potraktowane zasady przedstawione w Netykiecie wraz z rozwojem technik teleinformatycznych stopniowo dezaktualizują się („usuwaj niezwłocznie niepotrzebne przesyłki, ponieważ zajmują one miejsce na dysku"[10].). Wielu Internautów, nie będąc świadomych norm prawnych kieruje się jednak Netykietą w swoich kontaktach z Internetem. Mimo, że nie są to zasady mające swoje

[8] angielski neologizm netiquette – „net" (sieć) i „etiquette" (etykieta)
[9] Netykieta: http://urethan.chem.pg.gda.pl/docs/S_S_vivre.txt

korzenie w obowiązującym polskim systemie prawnym, to jednak mogą mieć doniosłość prawną. Mianowicie można uznać Netykietę za spisaną w jednym dokumencie część zasad współżycia społecznego (o których mówi art. 5 kc).

Pojawiły się już pierwsze orzeczenia sądowe na świecie, które opierają się właśnie na Netykiecie. Orzeczenie to wydał Sad Najwyższy Prowincji Ontario, rozpoznający sprawę z powództwa nie wymienionego z nazwy użytkownika przeciwko Nexx Online, ISPowi (*Internet Service Provider* – dostawca usług internetowych) z Toronto, który zlikwidował konto użytkownika za wysyłanie *spamu* w ilości 200,000 listów dziennie. Użytkownik pozwał Nexx za zerwanie umowy. ISP z kolei oskarżył tegoż użytkownika o łamanie warunków tej umowy. Sąd stwierdził, że jeśli umowa między *providerem* a użytkownikiem nie stanowi inaczej, masowe rozsyłanie niezamawianej, komercyjnej korespondencji elektronicznej łamie zasady zawarte w Netykiecie[11].

3 DOBRA OSOBISTE

Znajdujące się w niniejszym rozdziale rozważania dotyczące dóbr osobistych i ich charakteru stanowią jedynie wprowadzenie oraz pewne tło głównego tematu pracy. Przedstawiają one tematykę w sposób uproszczony i niewyczerpujący i są o tyle istotne o ile pomagają w zaprezentowaniu nowych form (sposobów) naruszeń dóbr osobistych, które mogą mieć miejsce z wykorzystaniem Internetu.

3.1 Pojęcie

Dobra osobiste są atrybutem wszystkich osób fizycznych. Jednakże przepisy prawa cywilnego nie zawierają definicji tego pojęcia. Kodeks cywilny poprzestaje na przykładowym katalogu dóbr osobistych.

Na kształtowanie się poglądów dotyczących ochrony dóbr osobistych początkowo miały największy wpływ prace S. Grzybowskiego. Jego definicja dóbr osobistych odwołująca się do kryteriów subiektywnych spotkała się jednak z krytyką.

[10] Ibidem

Według Grzybowskiego dobra osobiste należy traktować jako niemajątkowe, indywidualne wartości świata uczuć, stanu życia psychicznego określonej osoby[12]. Z Radwański stwierdza jednak, że subiektywny punkt widzenia w odniesieniu do dóbr osobistych nie stanowi dogodnej podstawy dla ich zrozumienia, oraz że obecnie przeważa pogląd, iż należy się posługiwać w tym celu kryterium obiektywnym, odwołując się do przyjętych w społeczeństwie ocen[13]. Z. Radwański przyjmuje, że jeśli chodzi o dobra osobiste człowieka to można przyjąć, że chodzi tu o uznane przez system prawny wartości, obejmujące fizyczną i psychiczną integralność człowieka, jego indywidualność oraz godność i pozycję w społeczeństwie, stanowiącą przesłankę samorealizacji osoby ludzkiej[14].

Zdaniem A. Szpunara, dobra osobiste to niemajątkowe wartości związane z osobowością człowieka, uznawane powszechnie w danym społeczeństwie[15]. Kolejną definicję podaje A. Wojciechowska. Charakteryzuje dobra osobiste jako wartości niemajątkowe, związane z indywiduum, z osobowością określonego człowieka i przez niego jako dobra odczuwane, ale jednocześnie wartości o zmiennym w czasie zakresie. Zmienny zakres tych wartości jest wg A. Wojciechowskiej skutkiem przemian warunków życia społecznego i ewolucji poglądów ich dotyczących[16]. Za koncepcją obiektywną opowiada się również A. Cisek, podkreślając, że dobro osobiste powinno odpowiadać interesom przeciętnej jednostki ludzkiej, jako, że prawo nie może chronić osób zbytnio przewrażliwionych, pozostawiając jednocześnie poza wszelką ochroną te jednostki, które z jakichś powodów nie są zdolne do określonych przeżyć o charakterze pozytywnym bądź negatywnym[17]. Jak stwierdza SN: przy ocenie naruszenia czci należy mieć na uwadze nie tylko subiektywne odczucie osoby

[11] "Sending unsolicited bulk commercial email is in breach of the emerging principles of netiquette, unless it is specifically permitted in the governing contract"; Moi@w.pl: SPAM a Netykieta - kanadyjski precedens sądowy, pl.internet.polip

[12] S. Grzybowski: Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego, Warszawa 1957, s. 78

[13] Z. Radwański: Prawo cywilne – część ogólna, Warszawa 1993, s. 121.

[14] Ibidem

[15] A. Szpunar: Ochrona dóbr osobistych, Warszawa 1979, s. 104.

[16] A. Wojciechowska: Czy autorskie dobra osobiste są dobrami osobistymi prawa cywilnego?, „Kwartalnik Prawa Prywatnego" 1994, z. 3 s. 375.

[17] A. Cisek: Dobra osobiste i ich niemajątkowa ochrona w kodeksie cywilnym, Wydawnictwo Uniwersytetu Wrocławskiego 1989, s. 37-38.

żądającej ochrony prawnej, ale także obiektywną reakcję w opinii społeczeństwa. Nie można też przy tej ocenie ograniczać się do analizy pewnego zwrotu w abstrakcji, ale należy zwrot ten wykładać na tle całej wypowiedzi[18].

Obecnie dominują definicje dóbr osobistych odwołujące się do koncepcji obiektywnych, a więc osadzonych w kontekście danego społeczeństwa. Ma to znaczenie z punktu widzenia niniejszej pracy, gdyż środowisko użytkowników Internetu oraz niepisane zasady obowiązujące w tzw. *cyber space* są specyficzne. Panujące w różnych środowiskach opinie i oceny mogą bardzo się różnić, a z czasem ulegać zmianom. Trzeba więc zawsze pamiętać, że treść konkretnego dobra jest zrelatywizowana do określonej społeczności[19].

Według konkluzji P. Suta[20] różnorodne definicje stworzone przez doktrynę, które jednak nie są pozbawione pewnych uproszczeń, wskazują, iż tworzenie legalnego określenia pojęć „dobo osobiste" czy też „dobra osobiste" nie jest możliwe. Zgadza się jednak z potrzebą poszukiwania wspólnych cech wszystkich dóbr osobistych, zwłaszcza, że prawo cywilne zapewnia ochronę wszystkim dobrom osobistym, a nie wszystkie te dobra są wskazane w ustawach.

Dobra osobiste mają charakter niemajątkowy, co podkreślają liczni autorzy[21]. Jak stwierdza Z. Radwański: dobra osobiste nie dają się wyrazić w jakichkolwiek kategoriach ekonomicznych, aczkolwiek pośrednio mogą wpływać na sytuację ekonomiczną człowieka (np. opinia dobrego pracownika na jego zarobki)[22]. W podobnym duchu wypowiada się A. Cisek[23]. Naruszenie dobra osobistego może mieć wymiar majątkowy (firma i dobre imię podmiotu gospodarczego, „nazwisko" adwokata, wizerunek aktora, zdrowie pracownika).

[18] Orzeczenie SN z 16 stycznia 1976 r., II CR 692/75, OSN 1976, nr 11, poz. 251.
[19] P. Sut: Problem twórczej wykładni przepisów o ochronie dóbr osobistych, PiP 1997, z. 9, s. 37.
[20] Ibidem, s. 31.
[21] Por. A. Szpunar: op. cit., s. 96.
[22] Z. Radwański: op. cit., s. 121.
[23] A. Cisek: op. cit., s. 39.

Dobra osobiste pozostają w ścisłym związku z podmiotem, któremu służą[24] i jako takie nie mogą być przenoszone. Nie można również się ich zrzec. Gasną wraz ze śmiercią podmiotu upr awnionego.

Jak stwierdza A. Szpunar: „każda osoba jest podmiotem tych praw, które są wyrazem poszanowania osobowości i godności ludzkiej[25].” Konsekwencją powyższego jest fakt, że dobro osobiste określonego podmiotu może zaistnieć dopiero z chwilą powstania tego podmiotu (tak będzie w przypadku osób prawnych) czy też z chwilą narodzin (gdy w grę wchodzą dobra osobiste osoby fizycznej). A. Cisek proponuje podział dóbr osobistych na te właśnie, które powstają z momentem zaistnienia podmiotu, czyli np. życie, zdrowie, wolność, cześć, oraz takie, które są nabywane przez podmioty w następstwie określonych działań – choćby dobra związane z przynależnością do rodziny, np. tajemnica przysposobienia[26]. Według S. Grzybowskiego: „Prawa osobiste powstają z chwilą powstania podmiotu, którego dotyczą, a następnie istnieją dopóty, dopóki istnieje ten podmiot[27].” Jak z tego wynika: dobra osobiste wygasają z chwilą śmierci podmiotu uprawnionego. Niektóre dobra osobiste związane z osobą zmarłego – np. jego dobra sława, osobiste prawa autorskie – nie pozostają jednak bez ochrony. Mogą je realizować osoby bliskie zmarłemu lub organizacje służące ochronie określonych wartości (np. związek literatów) – jako swoje własne prawa podmiotowe[28].

3.2 Konstrukcja prawna – prawo podmiotowe

Prawo cywilne opiera ochronę dóbr osobistych na przyznaniu jednostce praw podmiotowych[29]. Panujące zapatrywanie przyjmuje zarazem koncepcję wielości praw osobistych, wychodząc z założenia, że dla poszczególnych typów dóbr osobistych należy konstruować odpowiadające im typy praw podmiotowych[30]. Inna koncepcja zakłada istnienie jednego prawa podmiotowego osobistego. Podnosi się, że ta

[24] A. Cisek: op. cit., s. 40.
[25] A. Szpunar: op. cit., s. 96.
[26] A. Cisek: op. cit., s. 41.
[27] S. Grzybowski: op. cit., s. 18.
[28] Z Radwański: op. cit., s. 123.
[29] S. Grzybowski: op. cit., s. 15.
[30] Z Radwański: op. cit., s. 123.

koncepcja pozostaje w zgodzie z zasadą ogólną, w myśl której katalog bezwzględnych praw podmiotowych jest zamknięty i określony ustawą[31].

Samo pojęcie praw podmiotowych służy do opisu sytuacji prawnej jednego podmiotu wobec innych podmiotów. Jest to zawsze element stosunku prawnego, jego korelatem są obowiązki innych podmiotów. Wyznacznikiem prawa podmiotowego są normy prawne, będące źródłem stosunku cywilnoprawnego. Prawo podmiotowe służy ochronie uznanych przez prawo i społecznie akceptowanych interesów podmiotów prawa. S. Grzybowski, cytując za A. Wolterem, definiuje prawo podmiotowe jako „przyznaną i zabezpieczoną przez normę prawną oraz wynikającą z konkretnego stosunku prawnego sferę możności postępowania w określony sposób[32].”

Dominujący w doktrynie pogląd głosi iż konstrukcja instytucji ochrony dóbr osobistych opiera się na istnieniu praw podmiotowych osobistych. Prawa te są prawami bezwzględnymi, a więc skutecznymi przeciw wszystkim innym osobom (*erga omnes*), na których ciąży obowiązek powstrzymania się od wszelkich działań naruszających prawa podmiotowe, niemajątkowymi, niezbywalnymi i nie podlegającymi dziedziczeniu[33]. Nikt też nie może naruszać lub tylko zagrażać dobrom osobistym podmiotu uprawnionego. A. Szpunar stwierdza, że z faktem ścisłego związku tych praw z podmiotem któremu służą, łączy się ich niezbywalność[34]. Prawo podmiotowe daje możliwość (kompetencję) wystąpienia do odpowiedniego organu państwowego i zażądania udzielenia ochrony, czyli wymuszenia powinnego zachowania[35].

3.3 Inne gałęzie prawa

W polskim prawie funkcjonuje dość rozbudowanym systemem ochrony dóbr osobistych. Poza artykułami 23 i 24 oraz art. 43 kodeksu cywilnego i przepisami zawartymi w innych gałęziach prawa (prawo karne, prawo autorskie, przepisy

[31] A. Kopff: Koncepcja praw do intymności i do prywatności życia osobistego, zagadnienia konstrukcyjne, „Studia Cywilistyczne”, vol. XX Kraków 1972, s. 4 i nast.
[32] S. Grzybowski: op. cit., .s. 16.
[33] Por. Ibidem, s. 19., Por.: M. Pazdan: Art. 24, Nb 18, [w:] K. Pietrzykowski (red.): KC. Komentarz, Warszawa. 1999.
[34] A. Szpunar: op. cit., s. 97-98.
[35] A. Cisek: op. cit., s. 51-52.

regulujące konkurencję, dane osobowe etc.) ochroną dóbr osobistych zajmuje się także (a może przede wszystkim) Konstytucja Rzeczypospolitej Polskiej. Konstytucji RP w art. 47 stanowi, iż każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowaniu o swoim życiu osobistym. Art. 23 k.c. *in fine* stanowi, że dobra osobiste pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Unormowanie to stanowi o niezależności ochrony cywilnoprawnej w przypadku naruszenia dóbr osobistych. W przypadku prawa karnego i cywilnego mamy do czynienia z pewną różnicą w ochronie podobnych, ale inaczej nazwanych wartości. W sądzie karnym ograniczenie wynika z zasady *nullum crimen sine lege poenali anteriori* (art. 1 k.k.). Sąd cywilny działa w ramach szerokiego luzu decyzyjnego zapewnionego przede wszystkim przez art. 23 k.c. i otwarty katalog dóbr. Swoboda sądu cywilnego jest zatem znacznie większa[36]. Dodatkowo, jak podkreślają autorzy: gdy ochrona karna ma na celu represję za doznane naruszenie czci, ochrona cywilna spełnia również funkcje prewencyjną, gdyż może zmierzać do zapobieżenia dalszym naruszeniom i nie wymaga winy[37]. Jednocześnie art. 24 § 3 wprost mówi o tym, że przepisy kodeksu z zakresu ochrony dóbr osobistych nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym.

Koncepcja zbiegu norm jest przyjęta w doktrynie, czego wyrazem jest "System prawa cywilnego T.I". Kodeksowi cywilnemu przyznano rolę integrującą ochronę dóbr osobistych. B. Kordasiewicz[38] nazywa ten nurt koncepcjami dośrodkowymi - przenoszącymi rozwiązania innych przepisów na grunt prawa cywilnego.

3.4 Otwarty katalog dóbr osobistych

Kodeks cywilny w art. 23 zawiera niepełny i niezamknięty wykaz dóbr osobistych. Znajdują się tam takie dobra jak: zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i

[36] P. Sut: op.cit., s. 27.
[37] Z. Bidziński, J. Sereda: Cywilnoprawna ochrona dóbr osobistych w praktyce sądowej, [w:] Dobra osobiste i ich ochrona w polskim prawie cywilnym, Ossolineum 1986, s.11; Wyrok SN z dnia 5 maja 1977 r. IV CR 82/78.

racjonalizatorska. Sens tych terminów w istotnej mierze ustalają nie tylko powszechne reguły znaczeniowe języka, ale i całe systemy szczególnych reguł prawnych dotyczących wspomnianych wartości. Są one także dookreślane przez judykaturę sądową, opierającą się m. in. na funkcjonujących ocenach społecznych[39]. Należy również mieć na względzie iż przepisy konstytucji mają niezmiernie doniosłe znaczenie przy wykładni prawa cywilnego. Dlatego należy dążyć do tego, żeby wykładnia przepisów prawa cywilnego była zgodna z duchem i literą konstytucji[40].

A. Szpunar podkreśla, że częstym wypadkiem jest krzyżowanie się wzajemnie zakresów poszczególnych dóbr osobistych. Tego zdania jest również S. Grzybowski.[41] Wynika to z treści art. 23 k.c., w którym ustawodawca użył sformułowania „w szczególności". Sugeruje to wyraźnie iż wymienione tam dobra osobiste nie są jedynymi chronionymi przez prawo, można raczej powiedzieć, że zostały wskazane, jako szczególnie charakterystyczne, czy też wyjątkowo często ulegające naruszeniu.

Judykatura i doktryna nieustannie powiększa katalog dóbr osobistych. Otwarty katalog dóbr osobistych obejmuje także dobra osobiste związane ze sferą życia prywatnego, rodzinnego, ze strefą intymności. Ochrona w tym zakresie może odnosić się do wypadków ujawnienia faktów z życia osobistego i rodzinnego, nadużywania uzyskanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać[42]. Jednocześnie sfera uczuciowa związana z kultem pamięci osoby najbliższej, może stanowić przedmiot ochrony prawnej na podstawie art. 23 i 24 k.c.[43]. Nowym, nie zamieszczonym w Kodeksie cywilnym dobrem osobistym (choć jest to sporne) może być nazwa (firma) przedsiębiorstwa prowadzonego w formie spółki prawa cywilnego. Wedle SN stanowi ona dobro osobiste wspólników, podlegające ochronie stosownie

[38] B. Kordasiewicz: Jednostka wobec środków masowego przekazu, Ossolineum 1991, s. 10.
[39] Z. Radwański; op. cit., s. 122.
[40] A. Szpunar: Zadośćuczynienie za szkodę niemajątkową, Bydgoszcz 1999, s. 142
[41] A. Szpunar: Ochrona dóbr osobistych, Warszawa 1979, s. 121 i S. Grzybowski: op. cit., s. 81
[42] Wyrok SN z dnia 18 stycznia 1984 r, I CR 400/83 OSNC 1984/11/195.
[43] Wyrok SN z dnia 12 lipca 1968 r. I CR 252/68 OSNC 1970/1/18 - z uzasadnieniem.

do art. 24 k.c.[44]. Poczucie przynależności do danej płci może być uznane za dobro osobiste i jako takie podlega ochronie[45]. Orzecznictwo wskazało również takie dobra osobiste, jak: nietykalność cielesna naruszona w następstwie zabiegu lekarskiego, prawo wstępu do publicznych miejsc wypoczynku, prawo widywania się z członkami najbliższej rodziny, poczucie bycia pełnoprawnym członkiem społeczności, naruszenie dobra osobistego przez wydanie o pracowniku krzywdzącej opinii, używanie nazwy zespołu artystycznego, naturalne środowisko człowieka, jeżeli nastąpiło zakłócenie lub zagrożenie sfery osobistej powoda w sposób bezpośredni[46].

Zdrowie. Art. 23 k.c. wymienia wyraźnie jedynie zdrowie, jednakże na równi z nim traktować należy życie i nietykalność fizyczną (cielesną). Jak podaje A. Szpunar najprostszym przykładem naruszenia nietykalności cielesnej będzie uderzenie[47]. Przy czym, jak wskazuje SN naruszenie nietykalności cielesnej godzi również w godność człowieka[48]. W innej pracy cytowany autor zauważa iż w orzeczeniach sądowych znajdujemy takie określenia, jak „cisza domowa", spokój psychiczny". Tymczasem w wymienionych orzeczeniach chodziło w rzeczywistości o ochronę dobra osobistego jakim jest zdrowie człowieka. Według autora w pojęciu tym mieści się także spokój psychiczny[49].

Wolność. A. Szpunara rozumie pojęcie „wolność" szeroko, jako „wolność od czegoś", a więc wolność nie tylko od przemocy fizycznej ale także od „obawy i strachu, od użycia przemocy lub zrealizowania groźby przez inną osobę." Tak więc ochronę wolności rozumie się także jako ochronę przed bezprawnymi naciskami, krępującymi swobodne dysponowanie wartościami osobistymi[50]. Nieco inaczej i węziej S. Grzybowski uznając wolność za „wolność osobistą, swobodę poruszania

[44] Wyrok SN z dnia 14 grudnia 1990 r. I CR 529/90 OSNC 1992/7-8/136 - z uzasadnieniem. Komentarz do wyroku W. Tabor: OG 1992/2 str. 8-11. Glosy: J Krauss, M. Modrzejewska, PUG 1991, nr 7, poz. 1 str. 122, R. Skubisz, PS 1992/11-12 str. 107-116.
[45] Postan. SN z dnia 22 marca 1991 r. III CRN 28/91 niepublikowane.
[46] Z. Bidziński, J. Sereda: op. cit. s. 50.
[47] A. Szpunar: op. cit., s. 122.
[48] Uchwała SN z 30 grudnia 1971, III CZP 87/71, OSNC 1972/6/104.
[49] A. Szpunar: Zadośćuczynienie za szkodę niemajątkową, Bydgoszcz 1999.
[50] A. Szpunar: Ochrona dóbr osobistych, Warszawa 1979, s. 126

się". Z wolności rozumianej jako swoboda poruszania się wyprowadzane bywa prawo do niezakłóconego komunikowania (komunikacji)[51].

Cześć. Kolejnym z dóbr osobistych, wymienionych w kodeksie cywilnym jest cześć. Według Z. Bidzińskiego i J. Seredy – spośród dóbr osobistych cześć jest najczęściej przedmiotem ochrony[52]. Cześć można rozumieć jako „część zewnętrzną", czyli dobre imię oraz jako „cześć wewnętrzną", czyli godność osobistą. Dobre imię zostaje naruszone poprzez pomawianie innej osoby o takie postępowanie lub właściwości, które mogą ją poniżyć w opinii publicznej albo narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu, lub rodzaju działalności. Naruszenie czci może nastąpić zarówno poprzez krzywdzące pomówienie, dotyczące życia osobistego i rodzinnego, jak i przez zarzucenie niewłaściwego postępowania w życiu zawodowym.[53] Natomiast godność zostaje naruszona poprzez zniewagę, czy też obrazę, przy czym, aby można było mówić o znieważeniu, nie jest konieczna obecność znieważanego.[54] Przy ocenie naruszenia czci należy mieć na uwadze nie tylko subiektywne odczucie osoby żądającej ochrony prawnej, ale także obiektywną reakcję w opinii społeczeństwa. Nie można też przy tej ocenie ograniczać się do analizy pewnego zwrotu w abstrakcji, ale wykładać go na tle całej wypowiedzi[55].

Swoboda sumienia. Literatura wymienia głównie swobodę wyznawania bądź niewyznawania religii a także wykonywania lub nie praktyk religijnych. Do zakresu pojęcia będzie również należała ochrona pojęć, wyobrażeń i przekonań jednostki, także ochrona człowieka przed dyskryminacją ze względu na rasę, narodowość czy światopogląd.

Nazwisko lub pseudonim. Prawo do nazwiska i jego ochrona łączą się nierozerwalnie z ochroną innych dóbr osobistych, a w szczególności czci i godności osobistej. Przykładem mogą być sprawy dotyczące publikacji w prasie i książkach, w filmach i telewizji nazwisk osób, z podaniem bliższych danych personalnych, w

[51] J.Barta, R. Markiewicz: Internet a prawo, Kraków 1998, s.27
[52] Z. Bidziński, J. Sereda: op. cit., s.49
[53] Wyrok SN z 29 października 1971, II CR 455/71, OSNC 1972/4/77
[54] Ibidem
[55] Wyrok SN z 16 stycznia 1976 r. II CR 692/75 OSNC 1976/11/251 - z uzasadnieniem

sposób pozwalający na utożsamienie tych osób lub też – jeżeli chodzi o osoby powszechnie znane – podanie takich okoliczności, które z łatwością pozwalają na ich identyfikację[56]. Osobie, której prawo do nazwiska zostało w jakiś sposób naruszone, przysługuje ochrona na podstawie przepisów art. 23 i 24 k.c.[57] Typową sprawą o ochronę nazwiska jest sprawa o zaniechanie używania bezprawnie cudzego nazwiska, a ściślej rzecz ujmując podawanie się za kogoś innego, niż się jest w rzeczywistości, najczęściej w celu uniknięcia ewentualnych ujemnych konsekwencji lub też, w celu wykorzystania cudzego stanowiska lub statusu prawnego[58]. Według D. Kota pseudonimem musi sprawiać wrażenie nazwiska. Pseudonimem będzie przybrane sobie dowolnie nazwisko zazwyczaj z imieniem, przy czym sam sposób obrania tego nazwiska jest nieistotny. Ważny jest skutek – a więc upozorowanie autentyczności nazwiska. Według autora pseudonimami nie będą m.in. kryptogramy ani kryptonimy[59].

Wizerunek. Wizerunek pozostaje w pewnym związku z prawem do nazwiska i pseudonimu, jako elementu identyfikującego określoną postać, chociaż wymienionego w art. 23 k.c. jako odrębne dobro osobiste. Przepisy prawa autorskiego dodatkowo wspierają ochronę wizerunku. Wedle tych przepisów - rozpowszechnianie wizerunku wymaga zgody osoby na nim przedstawionej. Nie dotyczy to jednakże osób powszechnie znanych, lub stanowiących jedynie szczegół całości, takiej jak np. zgromadzenie. Zgodnie z art. 43 k.c. przepisy o ochronie dóbr osób fizycznych stosuje się odpowiednio do osób prawnych. Odpowiednie stosowanie art. 23 k.c. wyłącza z zakresu tej ochrony takie jednak dobra osobiste człowieka, które w przypadku osoby prawnej w ogóle nie mogą być brane pod uwagę, jak np. zdrowie lub wizerunek. Nie jest bowiem wizerunkiem osoby prawnej ani wizerunek miejsca jej siedziby ani osób, wchodzących w skład jej organów, lub nawet całego zespołu itp., jej elementów (z osobna lub łącznie wziętych)[60].

[56] Z. Bidziński, J. Sereda: op. cit., s. 59.
[57] Wyrok SN z 17 marca 1988 r., IV CR 60/88, OSNC 1989/5/83.
[58] Z. Bidziński, J. Sereda: op. cit., s. 60.
[59] D. Kot: Użycie cudzego nazwiska w prasie a autorstwo dzieła, ZNUJ z.68, 1997, s. 116.
[60] Wyrok SN z 25 maja 1977 r., I CR 159/77.

Tajemnica korespondencji. Określenie „korespondencja" nie jest dokładnie zdefiniowane w jakiejkolwiek dziedzinie prawa. Nie odpowiada ono również potocznemu rozumieniu. Jak stwierdza I. Dobosz[61]: Pojawienie się nowych środków rejestrowania wypowiedzi stwarza dodatkowe możliwości poszerzenia pojęcia „listu", będącego składnikiem korespondencji, oraz burzy uporządkowane dotychczas pojęcie korespondencji w tradycyjnym znaczeniu – jako korespondencji pisemnej. W cytowanej publikacji autorka wskazuje na istnienie kolejnych pozakodeksowych dóbr osobistych, zasługujących na ochronę: wolność komunikacji oraz tajemnica komunikacji.

Nietykalność mieszkania. Sprawy o ochronę prawa do mieszkania, nazywane również roszczeniem o ochronę miru domowego, pozostają najczęściej w związku z naruszeniem innych dóbr osobistych, takich jak prawo do nieskażonego środowiska naturalnego, prawo do czci i spokoju psychicznego[62]. Naruszenie nietykalności mieszkania może polegać na wdarciu się do cudzego domu, mieszkania czy też działki gruntu związanej z ich używaniem. Definicja nietykalności mieszkania jest ujmowana szeroko i zalicza się do niej, oprócz wdarcia się, inne przypadki niepokojenia kogoś w obrębie mieszkania, np. utrudnianie korzystania z niego[63].

Twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska. Termin „twórczość" jest zbiorczym określeniem wszelkich dóbr osobistych, przysługujących twórcy. Prawa przysługujące twórcy mają za zadanie chronić „osobisty jego stosunek do stworzonego przez niego dzieła"[64] Naruszenie tych dóbr może nastąpić poprzez np. niedopuszczalne wprowadzanie w dziele zmian, dodatków, skrótów itp. Ochrona winna przysługiwać autorowi niezależnie od tego, czy odczuł on ujemnie fakt naruszenia, co jest wyrazem podejścia obiektywnego do naruszeń tego dobra[65].

Zdaniem autorów – „na gruncie Kodeksu cywilnego dopuszczalne jest rekonstruowanie dobra osobistego w postaci prawa decydowania o dopuszczalności

[61] I. Dobosz: Przesłanki cywilnoprawnej ochrony przed podsłuchem, ZNUJ z.58 1992, s. 89.
[62] Z. Bidziński, J. Sereda: op. cit., s. 66.
[63] Por: Sprawa I C 1783/77 SW w Warszawie. Sprawa o wycofanie ze wszystkich punktów informacji, reklamy i zawiadomień informacji z numerem telefonu powoda.
[64] A. Szpunar: op. cit., s. 149
[65] Ibidem.

gromadzenia i udostępniania danych osobowych dotyczących osoby fizycznej (prawo do dysponowania swoimi danymi osobowymi)"[66]. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych uzupełnia i rozszerza przewidzianą w art. 23 k.c. ochronę dóbr osobistych. W szczególności znacznie rozszerza prawa osoby, której dane dotyczą. Danymi osobowymi jest każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby. Przetwarzanie danych - to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Przetwarzanie danych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą. Zgoda na przetwarzanie danych nie może być dorozumiana. Jednocześnie istnieją dane, które nie mogą być przetwarzane: pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, filozoficzne, przynależność wyznaniowa, partyjna, związkowa, dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym. Nie jest to jednak wyłączenie bezwzględne[67].

3.5 Ewentualna kolizja wartości

Może się zdarzyć, że chcąc chronić jedno dobro należy poświęcić inne. Taka kolizja będzie miała miejsce w przypadku przynajmniej dwóch grup, godnych ochrony z punktu widzenia systemu prawnego, dóbr. Należy w pierwszej kolejności wskazać prawo do ochrony prawnej życia prywatnego, rodzinnego czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (art. 47 Konstytucji RP). W opozycji do wolności wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji (art. 54 ust. 1 Konstytucji RP). W przypadku kolizji wybór dobra, które ma być poświęcone oparty być musi na rachunku zysków i strat. Wybór oparty jest na przyjętej hierarchii dóbr stanowiących wartość społeczną. Szczególnie trudno jest ustalić tę hierarchię, gdy mamy do czynienia z dobrami różnorodzajowymi i gdy

[66] J. Barta, R. Markiewicz: op. cit., s. 32
[67] szerzej na ten temat: B. Banaszak, K. Wygoda: Regulacja prawna ochrony danych osobowych w Polsce w świetle ustawy z 29 sierpnia 1997 r. i standardów europejskich, [w:] M. Wyrzykowski (red): Ochrona danych osobowych, Warszawa 1999.

kolidują ze sobą dobra stanowiące w pierwszym rzędzie wartość dla indywidualnej osoby z mającymi wartość ogólnospołeczną[68]. Należy mieć na uwadze, że wolność słowa stanowi jedną z najważniejszych zdobyczy nowoczesnego społeczeństwa, ale niesie również z sobą zagrożenie jej nadużywania. Jednostka nie może korzystać z praw z uszczerbkiem dla praw innych. Jest to zasada ogólna, która jest fundamentem każdego racjonalnego systemu prawa[69]. Jednak pozostaje otwarta kwestia hierarchii wartości. W przypadku Internetu problem jest jeszcze trudniejszy. 11 czerwca 1996 roku Sąd Apelacyjny stanu Pensylwania wydał ostateczny wyrok w sprawie tzw. Communication Decency Act (Prawo o przyzwoitości telekomunikacji), Sąd uznał, że DCA sprzeczny jest z I i V poprawką do konstytucji USA i tym samym został unieważniony. Z punktu widzenia naszych rozważań istotne jest uzasadnienie sądu. Otóż można w nim przeczytać, że z uwagi na unikalny charakter Internetu, jako jedynego medium, któremu w rzeczywistości udaje się realizować ideę wolnego rynku informacji w sposób dostępny dla każdego obywatela, należy uznać za niedopuszczalne jakiekolwiek ograniczenia wolności wypowiedzi w Internecie ze strony władz, zarówno teraz jak i w przyszłości. Regulacja treści wypowiedzi w Internecie, choćby dokonywana w najlepszym celu, równa się „spaleniu globalnej wioski po to, aby upiec prosiaka”[70].

Względy gwarancyjne wymagają, by możliwość poświęcenia dobra indywidualnego na rzecz ogólnospołecznego określona została w akcie prawnym wysokiej rangi[71]. Ilustracją omawianego problemu niech będzie następujące wydarzenie. Turecki sąd skazał na 10 miesięcy więzienia w zawieszeniu 18-to letniego Emre Ersoza za publikacje na łamach internetu krytyki postępowania miejscowej policji, która - zdaniem skazanego - brutalnie obchodziła się z grupą niewidomych demonstrantów. Nastolatek został oskarżony o „publiczną obrazę narodowych sił bezpieczeństwa”, po tym jak wziął udział w Internetowej debacie na temat zachowania

[68] A. Zoll: Prawo do krytyki a ochrona dóbr osobistych w prawie karnym [w:]Księga pamiątkowa ku czci prof. Natalii Gail, Trybunał Konstytucyjny Wydawnictwa 1999, s.236.
[69] J. Błeszyński: Aspekty prawne wolności słowa: http://www.krrtv.gov.pl/z4a7ble.htm
[70] J. Rafa: Amerykański zamach na Internet, Internet 3/96; J. Rafa: Wolność słowa zwycięża w Internecie, Internet 8/96.
[71] A. Zoll: ibidem.

policjantów, podając swoje imię, nazwisko i e-mail. Doniósł na niego inny Internauta[72]. Mamy tu do czynienia z kolizją wartości w postaci wolności słowa (krytyki) oraz ochronę czci (dobrego imienia), w tym konkretnym przypadku organów państwa, które dysponuje środkami przymusu państwowego.

3.6 Dobra osobiste osób prawnych

Na mocy art. 43 k.c. przepisy o ochronie dóbr osobistych osób fizycznych stosuje się odpowiednio do osób prawnych. Dobra osobiste osób prawnych - to wartości niemajątkowe, dzięki którym osoba prawna może funkcjonować zgodnie ze swym zakresem działań[73]. Dobrem osobistym przedsiębiorstwa będzie renoma, rozumiana jako ogół pozytywnych wyobrażeń i ocen konsumentów o wyrobach tego przedsiębiorstwa. Jak stwierdza SN: szkoła wyższa może należycie wypełniać powierzone jej zadania dydaktyczno-wychowawcze, polegające na kształceniu i wychowywaniu młodzieży tylko wówczas, gdy dysponuje odpowiednio wysokim autorytetem wychowawczym i moralnym[74]. Jak twierdzą autorzy Komentarza do KC – liczyć się trzeba nadto z ochroną swobody prowadzenia działalności statutowej przez osobę prawna na wypadek działań paraliżujących tę działalność[75].

Jak zostało powiedziane wyżej – odpowiednie stosowanie przepisów o ochronie dóbr osób fizycznych do osób prawnych wyłącza z zakresu tej ochrony takie dobra osobiste człowieka, które w przypadku osoby prawnej w ogóle nie mogą być brane pod uwagę.

[72] magazyn internetowy „//WWW." nr 7/98
[73] Wyrok Sądu Apelacyjnego w Warszawie z 19 grudnia 1995 r. I ACR 1013/95; Orzecznictwo Sądów w sprawach Gospodarczych 1997/4 poz. 44 str. 59.
[74] Wyrok SN z 14 listopada 1986 II CR 295/86 OSNC 1988/2-3/40
[75] M. Pazdan: art. 43 NB 12, [w:] K. Pietrzykowski (red.), KC. Komentarz, Warszawa 1999.

4 PRZESŁANKI OCHRONY

4.1 Zagrożenie i naruszenie dóbr osobistych

Ochrony może żądać nie tylko ten, czyje dobro zostało naruszone działaniem, ale także osoba, której dobra osobiste zostały zagrożone naruszeniem. Działanie o którym mowa może także polegać na zaniechaniu, o czym świadczy orzeczenie SN: „Wynikające z art. 24 § 1 k.c. działanie może polegać na zaniedbaniu w wykonywaniu obowiązku usuwania skutków zdarzeń naruszających cudze dobro osobiste”[76]. Szczególna sytuacja, do której odnosi się pierwsze zdanie art. 24 k.c., może przysporzyć pewnych trudności, ponieważ określenie, czy dobro jest zagrożone nie jest tak proste, jak stwierdzenie, czy i w jakiej formie naruszenie już nastąpiło[77]. Osoba, której dobra osobiste zostały zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W przypadku gdy naruszenie już nastąpiło – ten, czyje dobro zostało naruszone, może żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków. W praktyce najczęściej zdarzają się sprawy sądowe o naruszenie dóbr, rzadko o zagrożenie[78].

4.2 Bezprawność

Przepis art. 24 k.c. chroni przed bezprawnym naruszeniem lub zagrożeniem dóbr osobistych. Według orzecznictwa bezprawne jest zachowanie sprzeczne z normami prawa lub zasadami współżycia społecznego, bez względu na winę a nawet świadomość sprawcy[79]. Dodatkowo A. Szpunar działanie bezprawne definiuje jako sprzeciwiające się prawu podmiotowemu. Stwierdza iż do uznania działania za bezprawne wystarczy, aby sprzeczne było z „dobrymi obyczajami”[80]

[76] Wyrok SN z 16 lipca 1984r., I PR 64/84, OSNC 1985/2-3/41
[77] Por. S. Rudnicki: Ochrona dóbr osobistych na podstawie art. 23 i 24 k.c. w orzecznictwie Sądu Najwyższego w latach 1985 – 1991, "Przegląd Sądowy" nr 1/1992, s. 33
[78] Z. Bidziński, J. Sereda: op. cit., s. 12.
[79] Wyrok SN z 25 października 1982 r., I CR 239/82, niepublikowane
[80] A. Szpunar: Nadużycie prawa podmiotowego, Polska Akademia Umiejętności, Kraków 1947, s. 113

Z. Bidziński oraz J. Sereda analizując praktykę sądową pod kątem cywilnoprawnej ochrony dóbr osobistych stwierdzają iż w nauce przyjmuje się istnienie dwóch teorii bezprawności: subiektywnej i obiektywnej[81]. Wedle subiektywnej nie jest bezprawne wykonywanie prawa podmiotowego lub naturalnej wolności przez naruszyciela. Bezprawność uważa za przekroczenie własnego kręgu prawnego bez upoważnienia przez tę wolność czy też prawo podmiotowe. Teoria obiektywna natomiast ujmuje bezprawność jako naruszenie cudzego prawa podmiotowego, bądź cudzego dobra prawnego, bądź prawnie chronionego interesu. Wedle cytowanych autorów w praktyce sądowej obie teorie nadają się do stosowania czy to przy badaniu czy pokrzywdzony może powołać się na prawnie chronione dobro osobiste, czy to przy badaniu czy sprawca może powołać się na okoliczności usprawiedliwiające wkroczenie przez niego w zakres cudzego prawa[82]. Również zaniechanie może być uznane za bezprawne i uzasadniające odpowiedzialność z tytułu ochrony dóbr osobistych, jeżeli istniał obowiązek działania oparty na przepisie prawa lub zasadach współżycia społecznego[83]. Bezprawność czynu naruszającego dobro osobiste domniemywa się. Wynika stąd, że ten, kto naruszył wspomniane dobro, broniąc się przed roszczeniami uprawnionego, musi wykazać, iż działanie jego nie było bezprawne.

Kodeks cywilny nie wymaga by naruszenie lub zagrożenie było zawinione. Jak stwierdza Z. Radwański – jest to cecha znamionująca wszystkie konstrukcje ochronne oparte na prawach podmiotowych bezwzględnych – w przeciwieństwie do ochrony deliktowej[84]. A. Szpunar podaje, iż każde naruszenie dobra osobistego powinno być zasadniczo uznane za bezprawne, jako że sprawca narusza prawo podmiotowe innej osoby[85]. W kontekście bezprawności należy jednak rozróżnić naruszenie dóbr

[81] Z. Bidziński, J. Sereda: op. cit., s. 15.
[82] ibidem.
[83] Por. M. Sośniak, Bezprawność zachowania jako przesłanka odpowiedzialności cywilnej za czyny niedozwolone, Kraków 1959 s. 134, i n.
[84] Z. Radwański: op. cit., s. 123.
[85] A. Szpunar: Ochrona dóbr osobistych, PAN, Warszawa 1979, s.

osobistych i naruszenie praw osobistych. Dopiero naruszenie prawa osobistego uzasadnia zastosowanie środków ochronnych[86].

4.3 Wyłączenie bezprawności

A. **Zgoda uprawnionego**. Zgoda uprawnionego (zasada *volenti non fit iniuria* - chcącemu nie dzieje się krzywda) ma uzasadnienie w konstrukcji praw podmiotowych, która zakłada swobodę z korzystania z niego. Nie może być skutecznie udzielona, gdy jest to sprzeczne z normami prawnymi bezwzględnie obowiązującymi lub zasadami współżycia społecznego, co wynika z art. 58 k.c[87]. Zgoda może być w każdej chwili odwołana, co wynika z nieodłącznością dóbr osobistych od ich podmiotu[88]. Do udzielenia zgody wystarczy rozeznanie, nie jest konieczna zdolność do czynności prawnych.

B. **Działanie w ramach porządku prawnego**. Działanie w ramach porządku prawnego będzie wprawdzie naruszać dobra osobiste, ale jest działaniem władzy państwowej lub jednostek, które w ramach porządku prawnego zmierzają do uzyskania decyzji władzy państwowej[89]. Mimo, że generalnie działanie takie wyłącza bezprawność – może się zdarzyć, że działanie organów władzy (w szczególności władzy administracyjnej, podjęte przez organ kompetentny) może być uznane za bezprawne naruszenie dóbr osobistych[90]. W literaturze zwraca się również uwagę, że działanie podjęte w ramach porządku prawnego powinno być – jeśli chodzi o oceny innych osób – rzeczowe, obiektywne i ostrożne. Użyte sformułowania nie mogą (bez istotnej potrzeby) poniżać godności osobistej ocenianej osoby, oraz powinny przybierać odpowiednią formę[91].

C. **Działanie realizujące prawo podmiotowe**. Taką sytuację można uznać za podgrupę uchylenia bezprawności naruszenia dobra osobistego ze względu na

[86] Z. Radwański: op. cit., s. 124., S. Grzybowski: Ochrona dóbr osobistych, Wydawnictwo Prawnicze, Warszawa 1957, s. 114.
[87] Z. Radwański: op. cit., s. 124.
[88] Por.: A. Szpunar: Zgoda uprawnionego w zakresie ochrony dóbr osobistych, Ruch PES 1990/1, str. 41-57. Por. M. Sośniak: Funkcje i skuteczność zgody osoby uprawnionej w zakresie ochrony dóbr osobistych, [w:] Prace z prawa cywilnego, Ossolineum 1985, s. 67 i nast.
[89] S. Grzybowski: Ibidem.
[90] Por: Ibidem s. 116, Z. Bidziński, J. Sereda: op. cit., s.19.
[91] Z. Bidziński, J. Sereda: Ibidem., s.30.

działanie w ramach obowiązującego porządku prawnego. Nie można powoływać się na swoje prawo podmiotowe, jeżeli działanie naruszające cudze dobro osobiste byłoby sprzeczne z zasadami współżycia społecznego (nadużycie).

D. **Działanie w obronie uzasadnionego interesu**. Zaliczenie takiego działania w poczet sytuacji wyłączających bezprawność naruszenia dóbr osobistych jest kontrowersyjne. Wedle SN podawanie faktów prawdziwych nie może być zakazane, zwłaszcza w sytuacji gdy rozpowszechnienie ich leży w interesie społecznym[92]. Ale zawsze krytyka czyjegoś postępowania, zapatrywań czy działalności nie powinna przekraczać granic potrzebnych do osiągnięcia społecznego celu krytyki[93]. Krytyka jest dopuszczalna, o ile zmierza do ochrony określonego interesu społecznego i jeżeli ma cechy rzetelności i rzeczowości[94]. Z. Radwański nie przychyla się do koncepcji dopuszczającej egzoneracją z powołaniem się na działanie w obronie uzasadnionego interesu społecznego. Stwierdza mianowicie, że wszelkie koncepcje dopuszczające uchylenie bezprawności naruszenia na podstawie „ważenia" kolidujących interesów społecznych nie znajdują uzasadnienia normatywnego, a prowadzą do istotnego osłabienia ochrony dóbr osobistych[95]. Z drugiej jednak strony prawo karne wyłącza odpowiedzialność za pomówienie dokonane publicznie (także w środkach masowego komunikowania) w przypadku, gdy podniesiony lub rozpowszechniany zarzut jest prawdziwy oraz gdy zarzut ten służy społecznie uzasadnionemu interesowi.

[92] Wyrok SN z 28 grudnia 1978 I CR 424/78.
[93] Wyrok SN z 19 września 1968 II CR 291/68. OSNCP 1969, poz. 200.
[94] Wyrok SN z 23 października 1973 II CR 557/73.
[95] Z. Radwański: op. cit., s. 125.

5 NARUSZENIA DÓBR OSOBISTYCH W INTERNECIE

5.1 Zagadnienia wstępne

W niniejszym rozdziale przedstawię najczęstsze, moim zdaniem, formy naruszania dóbr osobistych za pośrednictwem Internetu. Przesyłanie informacji za pośrednictwem sieci jest bardzo proste – wystarczy dysponować bardzo łatwo osiągalnym i darmowym oprogramowaniem oraz oczywiście być podłączonym do sieci. Jednocześnie istnieje (potencjalna) możliwość ukrycia w sieci swojej prawdziwej tożsamości, albo idąc dalej – stworzenia sobie tożsamości. W dziedzinie teleinformatyki postęp jest bardzo szybki i prawdopodobnie w niedługim czasie będzie można obserwować nowe formy naruszeń dóbr osobistych. Już w tej chwili naruszenia mogą przybierać bardzo różną postać. 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 zaliczyłbym np. przyjęcie istnienia dobra osobistego, polegającego na wolności komunikacji. Konstytucja Rzeczpospolitej Polskiej wyraźnie mówi 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 i swoistą bezkarność naruszycieli, będą łamane w sieci. Do drugiej sytuacji zaliczyłbym nową formę naruszenia np. czci przez wypowiedź za pośrednictwem IRC[96]. Cześć, dobre imię były naruszane w środkach masowego przekazu i orzecznictwo zwracało uwagę na fakt dużej liczby odbiorców tych mediów. Internet stwarza możliwość dotarcia do z jednostkową informacją do najszerszego grona ludzi. Chciałbym zwrócić uwagę na pewne dodatkowe aspekty. Po

[96] Internet Relay Chat. Usługa oferująca możliwość komunikowaniu się wielu użytkownikom w trybie rzeczywistym. Bardzo upraszczając: komunikacja następuje z wykorzystaniem tzw. kanałów, na których jednocześnie może przebywać kilka tysięcy ludzi. Jeden użytkownik może przebywać na kilku kanałach jednocześnie. Użytkownik przesyła „na kanał" lub do poszczególnych współużytkowników komunikaty tekstowe.

pierwsze można dotrzeć do specyficznie wyselekcjonowanej grupy ludzi, którzy tworzą np. środowisko związane tematycznie z jakąś dziedziną życia. Tacy ludzie będą prawdopodobnie dobrze się znali na stopie np. zawodowej. 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. Tu również widzę dwa aspekty: pierwszy to kwestia udowodnienia, że nastąpiło naruszenie jakiegoś dobra, drugi to kwestia dowodowa związana z osobą, tożsamością naruszyciela. Należy pamiętać, że komunikacja w sieci polega na przesyłaniu między komputerami pakietów danych, które może przybierać postać pliku komputerowego, a taki plik ze względu na łatwość modyfikacji nie może być dowodem w sprawie. 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[97]). Karty *mikrochipowe* na pewno przyczynią się do wyselekcjonowania kolejnych dóbr osobistych i kolejnych form naruszeń.

Interesujące jest również przyjrzenie się bliżej motywom, które mogą leżeć u podstaw niektórych naruszeń. Otóż część naruszeń powstanie tylko dlatego że są one w sieci możliwe oraz ze względu na możliwość ukrycia swojej tożsamości – a więc w konsekwencji ze względu na bezkarność naruszycieli. Obrazuje to przeprowadzony eksperyment. Serwer, na którym zakładano użytkownikom konta z pełnymi uprawnieniami *roota.* Serwer działał tylko 50 minut, do momentu, aż nastąpiło jego

wyłączenie spowodowane przeciążeniem. Przeciążenie to było następstwem świadomych działań jednego z użytkowników serwera[98].

Część z przedstawionych poniżej działań wyczerpuje znamiona czynów penalizowanych w kodeksie karnym, a które pojawiły się tam po zmianach z 1997 roku. Mam tu na myśli przepisy z XXXIII rozdziału, które przewidują karalność zamachów na bezpieczeństwo elektronicznie przetwarzanej informacji. Ramy niniejszej pracy nie pozwalają na bliższą analizę zasygnalizowanego problemu. W poniższych rozważaniach będę się jedynie koncentrował na naruszenia dóbr osobistych w ich aspekcie cywilnoprawnym.

5.2 World Wide Web

W niniejszej części postaram się przybliżyć tematykę naruszeń dóbr osobistych za pośrednictwem WWW (*World Wide Web*). Jak zostało napisane w rozdziale poświęconym Internetowi: WWW zaczęło robić prawdziwą rewolucję jeśli chodzi o usługi internetowe. Jest to usługa umożliwiająca 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

[97] 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.

5.2.1 Negatywne kampanie

Jest bardzo łatwo udostępnić stronę WWW w sieci Internet. Wystarczy przygotowane pliki umieścić na serwerze WWW, który jest z siecią połączony. Coraz więcej osób dysponuje takimi możliwościami. Tematyka stron jest bardzo różna i zależy od fantazji autorów. Czasem się zdarza, że swoje emocje i uczucia przedstawiają w postaci ANTY stron. Aby zapoznać się z tego typu stronami WWW wystarczy w jakiejkolwiek wyszukiwarce internetowej (*sercher*) jako hasło wyszukiwawcze wpisać „ANTY".

„Antystrony" powstają na różne tematy. Spotkałem się ze stronami wyśmiewającymi muzykę danego wykonawcy, ze stronami antyfaszystowskimi, antykomunistycznymi. W sieci znalazłem również antystronę nauczycielki z Podbeskidzia zrobioną przez jej uczniów. Strony takie nie muszą być napisane językiem obraźliwym, co więcej mogą zawierać treści napisane w ramach wolności słowa i prawa do krytyki, nie naruszając żadnych dóbr osobistych. Jednakże czasem strony te zawierają treści obraźliwe, nieprawdziwe lub krzywdzące, 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. Może się zdarzyć, że strony takie przybierają postać negatywnej kampanii wymierzonej przeciwko danej osobie fizycznej czy prawnej.

Przykładem negatywnej kampanii może być kampania „Internetem w Warte" - negatywna kampania przeciwko jednej z ogólnopolskich firm ubezpieczeniowych. Swój prywatny spór z jednym z dwóch, ówcześnie największych, polskich towarzystw ubezpieczeniowych "Warta" S.A. prowadził Christopher Krokos z USA.

[98] Adres serwera na którym dokonano eksperymentu: http://outlaw.cavadera.com

Niechęć Krokosa do "Warty" wzięła się stąd, że podczas pobytu w USA poważnie zachorowała jego teściowa. Krokos twierdził, że firma ubezpieczeniowa nie wywiązała się z umowy i musiał zapłacić za leczenie teściowej. Ponieważ uważa, że został przez "Wartę" oszukany, stracił do firmy zaufanie i zaczął wszystkich informować o tym fakcie. Apelował również, aby nie korzystać z usług tego towarzystwa ubezpieczeniowego. Krokos realizował w ten sposób ideę wolności słowa. Oprócz wysyłania listów do centrali "Warty" zaczął wysyłać sprawozdania ze swej prywatnej kampanii przeciwko niej do użytkowników Internetu. Do milionów użytkowników sieci zaczęły trafiać listy wysyłane w ramach "*Anti-WARTA SA Campaign by Christopher Krokos*"[99]. Warto nadmienić, że jak twierdziły władze Warty – to, co się stało teściowej Ch. Krokosa nie było objęte jej polisą.

Na stronach WWW (na dwóch serwerach komputerowych poza granicami Polski: w Szwecji i Stanach Zjednoczonych) pojawiły się publikacje ostrzegające przed ubezpieczaniem się w "Warcie". Krokos pisał o firmie jako "nierzetelnej i oszukańczej". Wydaje się, że dla towarzystwa ubezpieczeniowego największym kapitałem jest jego dobre imię i renoma. Władze spółki nie wiedzą jakie poniosły straty związane z tą negatywną kampanią, jednakże nie zaprzeczają, że straty poniosły

Kolejnym Przykładem Kampanii negatywnej jest strona WWW o nazwie „Akta Norynberskie”. Na stronie tej znajdowały się zdjęcia i dokładne dane o kilkuset lekarzach przeprowadzających w USA zabiegi usuwania ciąży[100]. 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 100 mln dolarów odszkodowania od właścicieli strony, gdyż - jak argumentował – nakłania ona do przemocy przeciw lekarzom dokonującym aborcji. Jak podkreślił sędzia – właścicieli stron „Akta Norynberskie” nie chroni amerykańska konstytucja, bowiem nakłanianie do przemocy

[99] http://members.tripod.com./~krokos/warta.htm (strona usunięta z tego serwera)
[100] http://www.lancasterlife.com/nazizm_planned_parenthood.html (strona została usunięta)

w stosunku do innych wykracza poza granice wolności słowa[101]. Jak się wydaje podobne orzeczenie w sferze merytorycznej byłoby uzasadnione z punktu widzenia polskiego prawa, gdyż zostały tu naruszone takie dobra osobiste wspomnianych lekarzy jak wizerunek, prawo do prywatności, nazwisko, w konsekwencji istnienia strony było zagrożone ich zdrowie a nawet życie.

Za pośrednictwem Internetu (chodź prezentowane dalej zagadnienie jest bardzo kontrowersyjne) można naruszyć dobro osobiste w postaci zdrowia. "Pornografia, ale również jakiekolwiek opisywanie, rozmowy, prezentowanie dzieciom treści lub obrazów o charakterze seksualnym jest dokonywaniem wobec nich przemocy. Myślę, że 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[102]." W myśl tego co zostało powiedziane – treści prezentowane w środkach masowego przekazu (a tym bardziej w Internecie jako środowisku pozwalającym na swoistą interakcję z użytkownikiem) mogą mieć wpływ na psychikę użytkowników. Problem ten dotyczy raczej rozważań aksjologicznych, gdyż trudno sobie wyobrazić powództwa o naruszenie dóbr osobistych w postaci zdrowia wytoczonego przeciwko autorowi serwisu prezentującego pornografię. Po pierwsze – odwiedzający strony pornograficzne najprawdopodobniej zrobił to z własnej woli (zgoda uprawnionego), po drugie powstaje problem dowodowy, polegający chociażby na wykazaniu, iż ewentualne naruszenie zdrowia wywołane było zapoznaniem się z pornograficzną treścią konkretnych stron WWW (przy olbrzymiej ilości serwisów oferujących treści pornograficzne w Internecie).

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

5.2.2 Podmiany stron WWW

Poniżej przedstawię kilka przypadków podmiany stron WWW na serwerach. Podmiany takie nastąpiły w wyniku nielegalnych i penalizowanych w kodeksie karnym działań. Pragnę zwrócić w tym podrozdziale uwagę na cywilnoprawne naruszenie dóbr osobistych osób prawnych lub fizycznych przez takie działania. Często, w wyniku podmiany stron na serwerze danej firmy, znajdują się tam treści godzące w dobre imię, sławę czy wizerunek konkretnych osób, mogą również godzić w ich renomę (osoby prawne). Powoduje to, że tego typu działania stanowią, w pewien sposób, kwalifikowaną postać negatywnych kampanii. Archiwum włamań na serwery w Polsce dostępne jest pod adresem: http://nt.security.net.pl/default.asp, jednakże gdyby przyjąć, że podmienione strony naruszają dobra osobiste poszczególnych osób (fizycznych czy prawnych) – należałoby uznać, że udostępnianie pełnych tzw. *mirrorów* stron po włamaniu – narusza również te dobra osobiste, niezależnie czy udostępni się je z klauzulą, iż jest to tylko materiał informacyjny i że udostępniająca *mirrory* firma odcina się całkowicie od prezentowanych treści.

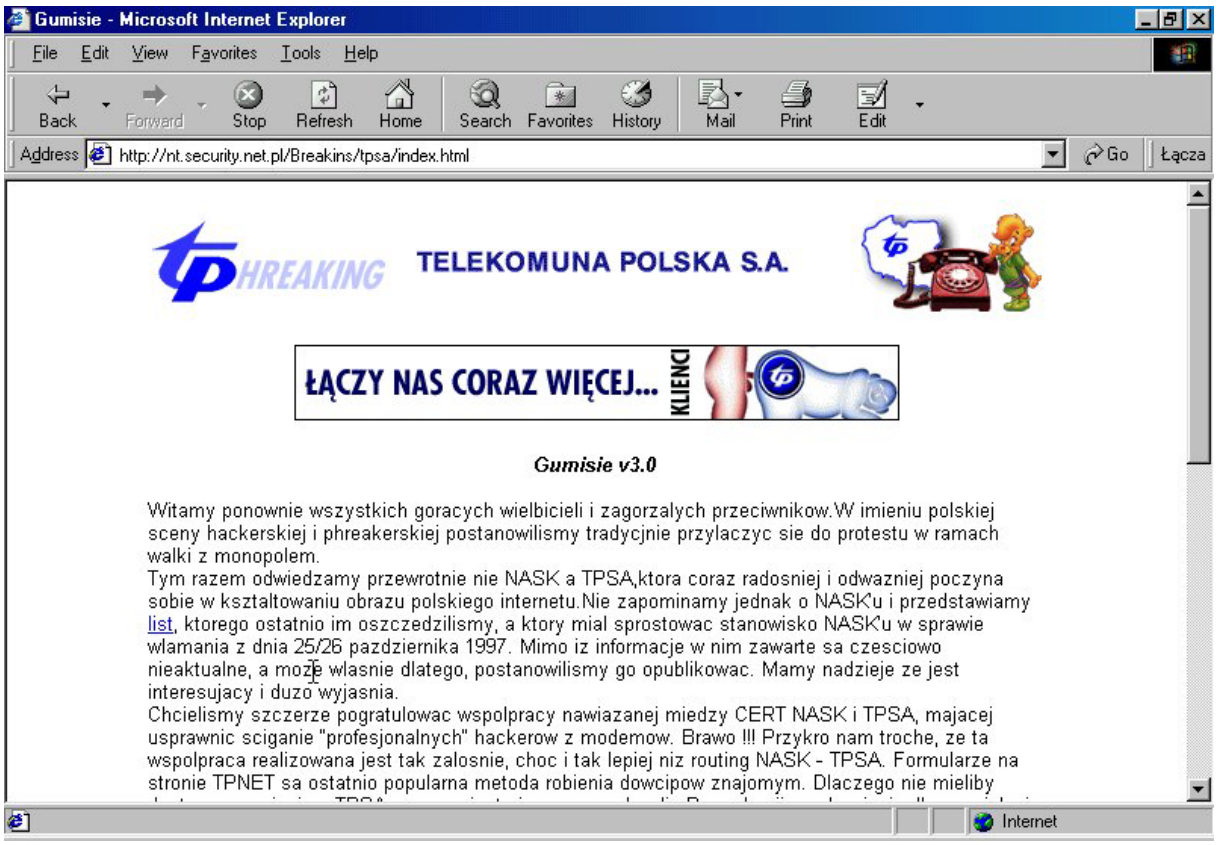
Sam fakt podmiany powoduje zwiększenie liczby odwiedzin na danej stronie przez co zwiększa się liczba odbiorców i świadków naruszenia. Ma na to również wpływ późniejsze, lub jednoczesne ogłoszenie tego za pośrednictwem grup dyskusyjnych *Usenetu*. Dodatkową okoliczność stanowi to, że osoby nie wiedzące o podmianie strony WWW łącząc się z danym adresem na przykład: http://www.firma.com.pl oczekują znalezienia tam oficjalnego serwisu informacyjnego tej właśnie firmy. Osoby podmieniające strony wykorzystują czasem elementy graficzne stron które podmieniają, przez co część osób odwiedzających podmienioną stronę WWW może być przekonana, że prezentowane na niej treści pochodzą od tej właśnie firmy (osoby fizycznej lub prawnej).

Włamanie, a raczej podmienienie strony *European Network Security Instytut* (ENSI) nastąpiło 4. marca 1999. ENSI jest jedna z najpoważniejszych firm zajmujących się zabezpieczeniami w Polsce. Poniżej prezentuje komunikat oficjalny ogłoszony przez ENSI. „W piątek (5.03.99) wieczorem nieznani sprawcy przy pomocy

techniki ARP[103] *spoofing*[104] przekierowali zapytania do serwera www.ensi.net na inny nie chroniony serwer WWW ze spreparowanymi danymi. Jest to kolejny dowód na to, że bezpieczeństwo firmy nie kończy się na *firewallu*. Przekierowanie usług takich jak WWW czy poczta można wykonać praktycznie w dowolnym miejscu sieci pomiędzy odbiorcą a serwerem. Możliwe są również ataki na usługi DNS, *routery* i wiele innych. W praktyce bezpieczeństwo usług w Internecie w dużym stopniu zależy od zabezpieczeń wszystkich dostawców po drodze." Na podmienionej stronie - zatytułowanej „Zostań kowbojem" - można było m. in. przeczytać: „Zadzwoń już dziś pod numer 0602XXXXXX (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." Numer telefonu zakryty X'ami to najprawdopodobniej numer szefa ENSI. Przekierowanie stron WWW jednej z najbardziej liczących się w dziedzinie bezpieczeństwa sieciowego firm w Polsce było szeroko komentowane w ramach grupy dyskusyjnej *Usenetu* pl.comp.security. Wielu dyskutantów poddawało w wątpliwość stopień fachowości ENSI. Ogólny oddźwięk był taki, że jeśli firma nie potrafi zadbać o bezpieczeństwo swoich własnych serwerów nie powinna tego oferować innym podmiotom. Następnie kilka osób zabierających głos w tej dyskusji wysłało listy z przeproszeniami ENSI i ze stwierdzeniami, że wypowiadały się na temat tego przekierowania nie mając pełnych danych na ten temat. Przypuszczam, iż nastąpiło to w wyniku nieformalnych działań ENSI. Na powyższym przykładzie widać, jak bardzo może nadszarpnąć renomę podmiana stron firmy zajmującej się bezpieczeństwem w sieci. Widać również, że władze ENSI doskonale zdają sobie sprawę z tego, że późniejsza dyskusja na forum grupy newsowej (która sugerowała innym dyskutantom, że nastąpiło włamanie na serwer ENSI) mogła dodatkowo nadszarpnąć jej renomę. Istotne znaczenie ma również fakt, że we

[103] ARP – Address Resolution Protocol Jest częścią Ethernetu, a także innych podobnych protokołów odpowiedzialną za konwersje adresu IP do adresu sprzetowego. Nie jest częścią protokołu IP, a jedynie obsługuje go. Więcej na ten temat: D. Atkins, P. Buis eds.: op. cit., s. 280.
[104] Spoofing – podszywanie się pod inną maszynę w sieci. Może wystąpić na każdej z warstw protokołu IP. Więcej na ten temat: D. Atkins, P. Buis eds.: op. cit., s. 278

wspomnianej dyskusji zabierały głos osoby znające się w powszechnym odczuciu na bezpieczeństwie sieciowym. Podmienione strony sugerowały, że osoby współpracujące z ENSI nie są osobami kompetentnymi w danej dziedzinie i w ten sposób zostało naruszone ich dobro osobiste w postaci czci. Dodatkowo podając numer telefonu osoby prywatnej zostały zagrożone dobra osobiste właściciela telefonu. Może być dyskusyjne jakie dobra zostały naruszone, jednakże można chyba przyjąć że uszczerbku dostąpiła sfera życia prywatnego tej osoby. Wydaje mi się, że nastąpiło również zagrożenie dobra osobistego w postaci wolności komunikacji tej osoby, gdyż posiadając numer telefonu można utrudnić lub uniemożliwić korzystanie z niego, ale o tym chciałbym napisać w dalszej części tego rozdziału.

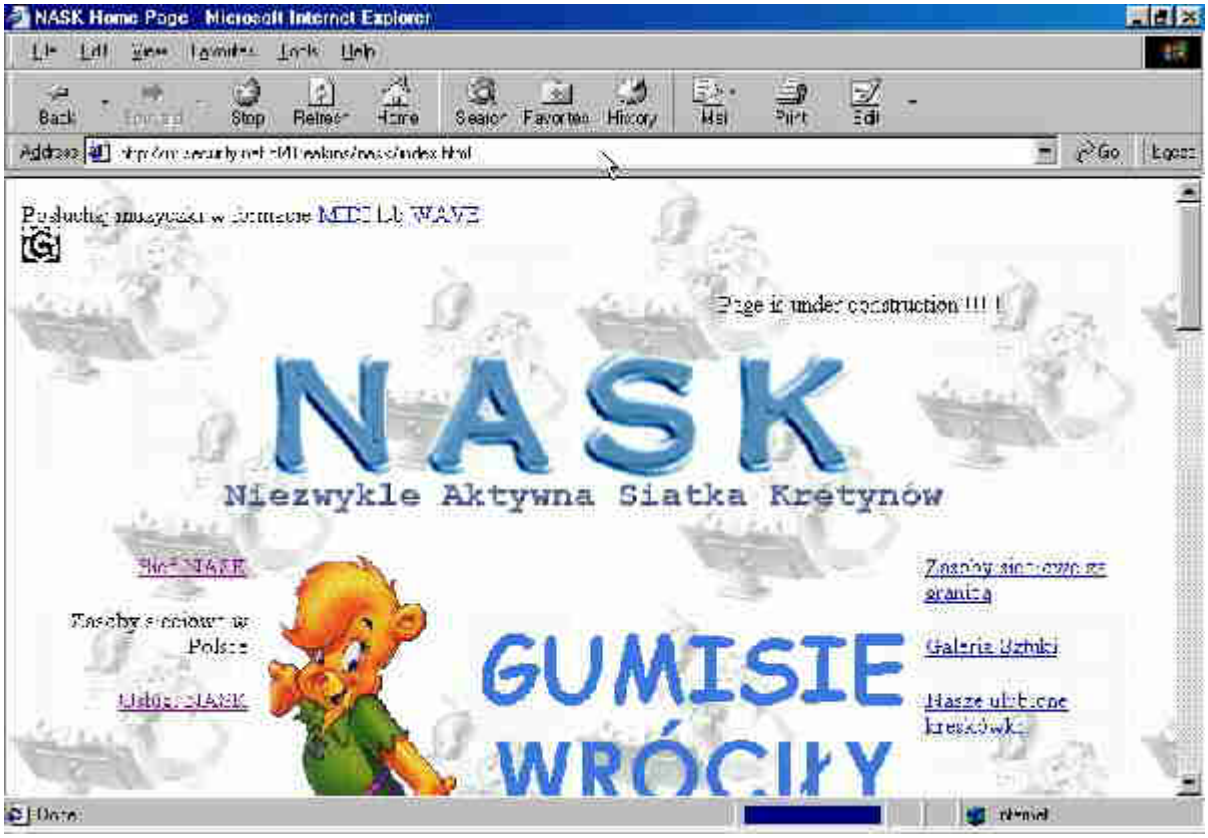


Rysunek 4: Podmieniona strona WWW Telekomunikacji Polskiej S.A.

Inną ofiarą *hackerów* była firma ICS. Włamanie nastąpiło 14. marca 1999. ICS również zajmuje się bezpieczeństwem sieci. Na podmienionych stronach ICS można było przeczytać, iż jest ona jedną z najgorzej zabezpieczonych firm w Polsce, zajmujących się zagadnieniami ochrony informacji i systemów informatycznych. „Jej dyrektor, [tu pada nazwisko] jest totalnym idiotą, potwierdza to fakt, iż jest on

profesorem Politechniki Wrocławskiej i prowadzi dla studentów cykl wykładów z dziedziny kryptografii, ochrony systemów informatycznych i sieci, technik kodowania i innych. Utworzył nowy kierunek w technice zabezpieczeń - Inżynieria Anty-Ochrony Informacji. Od wielu lat uczestniczy w pracach normalizacyjnych Polskiego Komitetu Normalizacyjnego". W cytowanym tekście wyraźnie padało nazwisko dyrektora firmy oraz określenia powszechnie uważane za pejoratywne. Ogólnie ton wypowiedzi sugeruje niefachowość osób pracujących w firmie. Dodatkowo przez samo włamanie zostały naruszone dobra osobiste firmy zajmującej się przecież bezpieczeństwem sieciowym.

Włamanie na serwer Telekomunikacji Polskiej SA nastąpiło 1 grudnia 1998. Do TPSA należy większość infrastruktury teleinformatycznej w Polsce i jednocześnie ma ona pozycję dominującą na polskim rynku *providerów* (ISP – *Internet Service Provider*). Przy okazji włamania nastąpiło podmienienie strony głównej serwisu spółki. Pod podmienioną stroną WWW podpisała się grupa *hackerska* „Gumisie". Podmiana nastąpiła w dniu protestu polskich Internautów przeciwko monopolowi Telekomunikacji Polskiej. Znamienne jest to, że następnego dnia odbywała się konferencja naukowa „Internet – problemy prawne" na Katolickim Uniwersytecie Lubelskim, gdzie wśród sponsorów występowała m.in. TPSA. W kuluarach tej konferencji dostępne były wydruki podmienionej strony WWW. Na podmienionej stronie (na jednej z podstron) znaleźć można było hasła dostępu do różnych serwerów, uzyskane z poprzedniego włamania tej grupy *hackerskiej* na serwer NASK'u (NASK - Naukowa Akademicka Sieć Komputerowa. Podczas tego włamania rozszyfrowano na podmienionych stronach ten skrót jako Niezwykle Aktywna Siatka Kretynów, włamanie nastąpiło najprawdopodobniej około 30 grudnia 1995). Na stronie „Telekomuny Polskiej S.A." (jak przekręcono nazwę spółki) zamieszczono obraźliwe animacje komputerowe.



Rysunek 5: Podmieniona strona NASK'u

Podczas włamania na strony WWW tygodnika Wprost, które nastąpiło 25/26 lipca 1999, można tam było przeczytać m. in.: „Jeśli czytacie Państwo te słowa dzisiaj, to jest to najlepszy dowód, że koniec świata zdarzył się właśnie (...) lamie administratorowi www.wprost.pl, który z trudem przebija się przez tajemnice instalacji gier na serwerze (*Heroes of Might & Magic* - nabiliśmy parę nowych rekordów, nie ??) i korzysta w czasie pracy z zasobów Internetu (strasznie paskudny ma gust w wyborze pornosów) w celu uatrakcyjnienia swojego życia płciowego (nie dziw, w końcu z taką ofermą to nawet krowy u nas na gospodarstwie by nie chciały).” Pod podmienioną stroną podpisał się Komitet Obrony Wsi Polskiej przed Lepperszczyzną i Zalewem Tandety z Europy oraz niejaki Maniek. Maniek (lub osoby tak się podpisujące) włamał się również na serwer Unimilu – producenta prezerwatyw. Włamanie nastąpiło w tym samym czasie, w którym włamał się on na strony tygodnika Wprost. Na podmienionej stronie przedstawiono certyfikat napisany cyrylicą, który wedle Mańka jest gwarancją bezpieczeństwa. Na podmienionej stronie WWW można było również przeczytać: „dzięki wprowadzonej nowej technologii produkcji gumy osiągnęliśmy niespotykany poziom skutecznych użyć naszych

produktów - 23%. W związku z tym chcielibyśmy poinformować o zapoczątkowaniu przez Mańka nowej akcji - Kinder Sjurpryza".

W pierwszym z powyższych przypadków zostały naruszone dobra osobiste administratora serwera Wprost przez sugerowanie na podmienionych stronach, iż zamiast pracy gra on w gry komputerowe oraz że wykorzystuje serwer Wprost do gromadzenia materiałów pornograficznych zgromadzonych wcześniej za pośrednictwem sieci. Użyte w treści strony WWW określenie „lama" pochodzi od angielskiego „lame" – kulawy, chromy, niedokładny, a w internetowym slangu oznacza osobę, która zupełnie nie zna się na obsłudze komputera czy poszczególnych narzędzi informatycznych. Określenie to ma zabarwienie pejoratywne.

Chociaż autorów podmienionej strony nie można w żaden sposób nazwać dziennikarzami, a dyskusyjne jest również czy publikacje WWW można nazwać prasą - chyba celowe wydaje się przytoczenie Wyroku Sądu Apelacyjnego w Warszawie, w którym stwierdza on: na opublikowanie informacji, chociażby obiektywnie prawdziwych, niezbędne jest uzyskanie wprost zgody zainteresowanej osoby. (...) staranność obejmuje nie tylko powinność uzyskania zgody dotyczącej publikacji faktów ze strony sfery życia prywatnego, ale także potrzebę rozważenia celowości ujawnienia informacji o bardzo znacznym ciężarze gatunkowym w sposób umożliwiający identyfikację danej osoby (zdjęcie, prawdziwe imię i pierwsza litera nazwiska, wskazanie miejsca jej pobytu) oraz uwzględnienia niekorzystnych je skutków[105]. A dodatkowo: Art. 24 k.c. określający przesłanki ochrony dóbr osobistych, wymienia m.in. przesłankę bezprawności działania. Bezprawność w rozumieniu tego przepisu nie jest równoznaczna z winą. Dlatego też samo przeświadczenie sprawcy o prawdziwości zarzutów nie uchyla odpowiedzialności z art. 24 k.c.[106]. Czyli możemy założyć, że nastąpiło naruszenie prawa do prywatności (a być może również intymności) administratora oraz naruszenie jego czci (dobrego imienia) poprzez sugerowanie że nie wywiązuje się z obowiązków pracowniczych

[105] Wyrok SA z 3 kwietnia 1997 r., I ACa 148/97, Wokanda 1998/4 s. 40.
[106] Wyrok S.A. z 24 września 1992 r., I ACr 340/92, OSAiSN 1993/6 poz. 39 s 32.

oraz przez powiązanie go z dystrybucją pornografii, nawet gdyby okazało się to prawdą.

W drugim przypadku nastąpiło, moim zdaniem, naruszenie dóbr osobistych w postaci renomy przedsiębiorstwa produkującego prezerwatywy. Również dla tego typu firmy ważne jest postrzeganie jej jako firmy bezpiecznej i rzetelnej. Hasło: „Unimil sobie serwer" oraz ogólnie treść strony sugeruje, że produkty Unimilu są niepewne i nie należy z nich korzystać, zwłaszcza, że właśnie nastąpiło włamanie na firmowy serwer.

Jak widać z powyższych przykładów nie tylko strony WWW należące do firm komputerowych zajmujących się bezpieczeństwem są narażone na ataki. Również firmy innego rodzaju, nieopisane tutaj – jak np. Pizza Hut, na serwery której również się włamano podmieniając strony WWW. Osoby prywatne posiadające swój prywatny „home page" również są narażone na tego typu podmiany, a w ich konsekwencji na naruszenie dóbr osobistych (takie podmiany miały już miejsce w polskiej sieci). Każde zamienienie strony WWW można również chyba traktować jako naruszenie wolności wypowiedzi osób uprawnionych z tytułu posiadania kont czy serwerów WWW za ich pośrednictwem. Bardzo łatwo można sobie wyobrazić naruszenie dóbr osobistych w postaci twórczości naukowej lub artystycznej poprzez podmienienie stron WWW, na których znajduje się dany utwór. A wydaje się również słuszne uznanie samej strony WWW za utwór i objęcie ochroną jej autora. Problem z podmianą strony polega na tym, że (nieco inaczej niż w przypadku kampanii negatywnych opisanych w poprzedniej części), tu często nie wykrywa się sprawcy naruszenia dóbr osobistych.

5.2.3 Złośliwe *aplety*[107]

Jak to zostało już wcześniej powiedziane – z poziomu stron WWW można uruchomić różne aplikację, które będą działały na lokalnym komputerze (u oglądającego), albo będą komunikowały się z jego zasobami. Programy tego typu mogą uruchamiać się również bez wiedzy i zgody osoby oglądającej z pozoru niewinnie wyglądającą stronę WWW. Po uruchomieniu mogą modyfikować system

[107] Aplet – niewielki program wbudowany w inną aplikację. Leksykon Internetu http://leksykon.koti.com.pl

oglądającego, mogą stwarzać dostęp osobom postronnym (autorom *apletu*) do danych zastrzeżonych na komputerze oglądającego, mogą powodować zablokowanie komputera (atak typu DOS – *Denial of service*[108]), który może wymagać jego ponownego uruchomienia. Najsłabszą klasą ataku przeprowadzonego przez aplet jest przeszkadzanie w pracy przez wykonywanie czynności uciążliwych dla użytkownika. W konsekwencji użytkownik jest zmuszony do restartu przeglądarki.

Poniżej przedstawię kilka atakujących *apletów* w języku Java. Osoba umieszczające je na swojej stronie WWW mogła wykorzystać je do całkowitej penetracji komputera osoby oglądającej daną stronę a w konsekwencji narazić lub wręcz naruszyć 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[109]. Atak polegający na obejściu reguły zezwalającej na otwarcie połączenia sieciowego tylko do serwera, z którego pobrano *aplet*. Taką lukę można wykorzystać do penetracji „zapory ogniowej" (*firewall*) – komputera oddzielającego sieć wewnętrzną użytkownika od Internetu. Pobrany *aplet* przejdzie przez firewalla jako normalny pakiet danych WWW a następnie uruchomiony lokalnie zacznie atakować komputery w sieci lokalnej. Kolejny przykład to *aplet*, który oszuka przeglądarkę WWW i spowoduje, że będzie ona traktować kod *apletu* jako swój własny. Kod Javy, dostarczony z przeglądarką uznawany jest za „bezpieczny". Powyższe oszustwo sprawi, że *aplet* zyska nieograniczony dostęp do plików na lokalnym dysku. Za pośrednictwem *apletu*, który uruchamia szereg procesów jednocześnie można pośrednio uniemożliwić użytkownikowi kontrolę nad komputerem. Przykładem może być *aplet*, który bardzo szybko otwiera bardzo duże okna, co uniemożliwia sprawne operowanie myszą, a efektem ubocznym może być

[108] 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. Taki atak może być także częścia większego, zwanego IP Spoofingiem, który ma na celu podszycie się pod jeden z serwerów w sieci lokalnej. Bardzo trudno się przed nim obronić. http://www.software.com.pl/Security_News/news/atak.asp

takie spowolnienie komputera, że zablokowana zostanie również klawiatura. *Aplet* „podpięty" pod stronę WWW może wysyłać e-maile w imieniu osoby, która ogląda stronę. Nastąpi to w ten sposób, że *aplet* połączy się bezpośrednio z demonem sendmail przez port 25 (co jest powszechnie znaną sztuczką na wysłanie „anonimowego" maila). Odbiorca listu będzie myślał, że wiadomość wysłano z komputera, na którym niewinny użytkownik uruchomił *aplet*. Co więcej – można tak napisać *aplet*, że będzie to wyglądało, jakby sam użytkownik napisał i wysłał list. Interesujące jest to, że nie będzie możliwości powiązania serwera, z którego pobrano *aplet* (strony WWW), z wysłana wiadomością. Łatwo sobie wyobrazić naruszenia dóbr osobistych dokonane przez takie działanie (umieszczanie na kontrolowanych przez siebie stronach WWW takich złośliwych *apletów*).

5.2.4 Cytaty publikacji oraz publikacje własne autorów

Autorzy stron WWW często umieszczają na nich informacje, które pojawiły się w innych mediach – czy to artykuł opublikowany w prasie, czy też cytaty z audycji telewizyjnych. Oczywiście część z takich działań będzie naruszało prawa osobiste autorów tych materiałów, oraz ich dobra osobiste. Gdyby artykuły takie naruszały dobra osobiste innych osób wówczas należałoby uznać, że do takiej sytuacji należy odnieść poniższe orzeczenie SN. „Gdyby nawet audycje telewizyjne stanowiły powtórzenie artykułów prasowych, to i tak nie można by podzielić poglądu rewidującego, by nie miał obowiązku sprawdzenia prawidłowości stawianych powodom w tych artykułach zarzutów godzących w ich części i dobre imię. Jak to wyjaśnił Sąd Najwyższy w orzeczeniu z dnia 7.IX.1972 r. I CR 374/72 OSPiKA 1974 r., poz. 28 zasięg przekazu telewizyjnego i masowość jego odbioru wymagają szczególnej ostrożności i wystrzegania się bezprawnego naruszenia czyjejś czci"[110]. Podobnie, a nawet z większą uwagą należy podchodzić do publikowania w Internecie opublikowanych wcześniej artykułów prasowych, czy też cytatów z audycji telewizyjnych. Wydaję się również właściwe, by generalnie przyjąć (na podstawie cytowanego orzeczenia), że zasięg przekazu Internetowego i masowość jego odbioru

[109] D. Miodunka, P. Nowakowski: Świat Javy (2), PCkurier, 19 sierpnia 1999, s.19.
[110] Wyrok SN z 29 czerwca 1983 r., II CR 160/83, niepublikowane.

wymagają szczególnej ostrożności i wystrzegania się bezprawnego naruszenia czyjejś czci, nie tylko przy cytowaniu innych materiałów, ale również przy umieszczaniu materiałów własnych na stronach WWW. Myślę że dotyczy to większości dóbr osobistych również prawa do prywatności, wizerunku, nazwiska etc.

5.3 E-mail i Usenet

Większość elektronicznej poczty przesyłana jest w Internecie z wykorzystaniem protokołu TCP/IP SMTP (*Simple Mail Transport Protocol*[111] - specyfikacja ptotokołu znajduje się w RFC[112]). Został on opracowany w roku 1982 z myślą o instytucjach rządowych i uniwersyteckich. W chwili obecnej można go uznać za standard dla globalnego systemu poczty elektronicznej. W 1992 roku grupa IETF (*Internet Engineering Task Force*) opracowała nowy standard MIME (*Multipurpose Internet Messaging Extensions*[113]). MIME poszerzył SMTP o kilka funkcji, które dotychczas nie były obsługiwane przez ten standard: z jego wykorzystaniem można przesyłać w jednej przesyłce wiele obiektów, tekst może posiadać nieograniczoną długość z nieograniczoną długością linii tekstu, list może zawierać zbiory znaków inne niż ASCII, umożliwia przesyłanie plików binarnych lub specyficznych dla danej aplikacji (w związku z tym umożliwia przesyłanie grafiki, dźwięku, video i innych danych multimedialnych). W związku z integracją wielu platform systemowych w ramach sieci Internet konieczne było stworzenie kolejnego protokołu TCP/IP związanego z przesyłaniem poczty – POP2 (*Post Office Protocol*[114]), a w późniejszym okresie kolejną wersję POP3[115]. POP służy do odbierania przesyłek z serwera poczty. Umieszczony na tym serwerze, przy kontakcie z klientem POP, realizuje kilka funkcji. Sprawdza poprawność pary identyfikator/hasło użytkownika (w UNIX-ie jest to dokładnie ta sama kombinacja, co podczas logowania do systemu), sprawdza istniejące

[111] RFC 822.
[112] RFC (Request For Comments, czyli "prośba o komentarze") to poddawane pod szeroką dyskusję propozycje różnych standardów sieciowych, bardziej niezawodnych protokołów bądź wydajniejszych algorytmów lub analizy już istniejących realizacji. Wspólnym mianem RFC określa się powstające od roku 1969 (czyli początków ARPANET-u) raporty dotyczące rozmaitych aspektów komunikacji między komputerami. http://www.www-mag.com.pl/porady/podlupa/l002/index.shtml
[113] RFC 1521.
[114] RFC 937.
[115] RFC 1225.

przesyłki dla użytkownika, a jeśli list istnieje - jest on przekazywany do komputera klienta. List na serwerze może zostać skasowany lub przekazany do archiwum. Po przekazaniu wszystkich przesyłek POP automatycznie kończy pracę danego użytkownika z serwerem. Zaimplementowany we współczesnych aplikacjach jest on aktualizowany w tle co pewien czas, co powoduje, że użytkownik podłączony do internetu może być informowany o nadejściu nowej przesyłki z niewielkim jedynie opóźnieniem.

Należy jeszcze we wstępie wspomnieć o *demonie sendmail*. Demon jest procesem, który nie jest skojarzony z żadnym użytkownikiem, lecz wykonuje funkcje systemowe, takie jak administracja i nadzór, usługi sieciowe, wykonywanie czynności o ściśle oznaczonych porach czy obsługa drukarki[116]. *Sendmail* jest popularnym agentem pocztowym. Jako *demon* oczekuje on nadchodzących od systemów zewnętrznych sesji e-mail. Odbiera on a następnie wysyła dalej wiadomości dla użytkowników lokalnych i zdalnych. Nie jest on zaprojektowany jako program użytkownika, lecz raczej jako narzędzie, wykonujące część zadań za programy pocztowe[117].

Przesyłanie poczty elektronicznej (e-mail) do niedawna było najpopularniejszą z usług w Internecie (aktualnie najprawdopodobniej jest nią WWW). Umożliwia ona komunikowanie się ludzi z niespotykaną jak dotąd skutecznością i szybkością, umożliwia prowadzenie prywatnych archiwów korespondencji, umożliwia przesyłanie otrzymanych listów do innych osób w postaci praktycznie niezmienionej. Adres e-mail w powiązaniu z imieniem i nazwiskiem można uznać za dane osobowe w myśl przepisów ustawy o ochronie danych osobowych (w dalszej części pracy przedstawiam jednak pewne zastrzeżenia). Adres e-mail w ograniczonym zakresie identyfikuje daną osobę, a raczej – można domniemywać, że list pochodzący z danego adresu pochodzi od konkretnej osoby (można jednak posiadać kilka adresów e-mail).

Poniżej przedstawię naruszenia dóbr osobistych z wykorzystaniem listu elektronicznego. Naruszenia te mogą przybierać formę wypowiedzi godzących w

[116] D. Atkins, P. Buis eds.: op. cit., s. 50.
[117] Ibidem, s. 58.

dobre imię lub cześć jakiejś osoby, mogą przybierać formę rozsyłania do osób trzecich zdigitalizowanej podobizny konkretnej osoby (komputerowa technika fotomontażu może prowadzić do powstania grafiki komputerowej, przedstawiającej daną osobę w niekorzystnym świetle, w sytuacji w jakiej ta mogła się nigdy nie znaleźć). Może to naruszać jej wizerunek (to dotyczy również przedstawionych wcześniej naruszeń na stronach WWW). Poprzez „proste" 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.", również: „Bądź ostrożny pisząc z humorem lub sarkazmem. Bez osobistego kontaktu Twój żart może być odebrany jako złośliwa krytyka"[118]. Te formy naruszeń nie różnią się praktycznie od podobnych, które można spotkać poza Internetem przy wykorzystaniu „klasycznej" poczty. Nie będę opisywał zagadnienia negatywnych kampanii, które zostało opisane we wcześniejszej części tej pracy. Również przy okazji *apletów* została opisana jedna z form naruszeń dóbr osobistych poprzez wymuszenie wysłania poczty przez program pocztowy osoby oglądającej stronę WWW w taki sposób, że dokonało się to bez jej wiedzy, a dodatkowo że list dla osób trzecich pochodził od osoby oglądającej internetową stronę.

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 potrzeby można podejść i zapoznać się z wiadomościami tam zawartymi i nie wiąże się to ze zgodą innych uczestników dyskusji. Zarówno listy dyskusyjne jak i grupy newsowe posiadają często swoje archiwa. Archiwa te przybierać mogą formę stron WWW.

[118] Netykieta, http://urethan.chem.pg.gda.pl/docs/S_S_vivre.txt

Wydaje się, że charakter publikacji artykułu na publicznej (niezamkniętej dla innych użytkowników internetu) liście dyskusyjnej czy w grupie newsowej jest zbliżony do publikacji na stronach WWW. Wydaje mi się również, że do większości przypadków spotykanych w trakcie dyskusji na forum wspomnianych list będą miały zastosowanie uwagi Z. Bidzińskiego i J. Seredy[119] dotyczące sprawy dwu krytyków muzycznych, co do których wypowiedział się SN w wyroku z dnia 19 września 1968 r. II CR 291/68[120]. SW oddalił powództwo, a SN 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 SN nie dopatrzył się w sformułowaniach pozwanego przekroczenia granic krytyki „akceptowanych w środowisku, dla którego jest przeznaczona" i uznał, ze nie nastąpiło naruszenie dóbr osobistych powoda. Stanowisko to spotkało się z krytyka A. Kopffa i A. Szpunara, gdyż wg 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. Sereda: 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[121]. Opisana sytuacja przypomina „*flame war*" (wojna ogniowa) czyli bardzo szybką wymianę listów (w slangu internetowym: *postów*), nie przemyślaną, niosącą w sobie bardzo duży ładunek emocjonalny, wykorzystującą niewyszukane słowa i zwroty. Należy pamiętać, że list (artykuł) w Internecie można opublikować bardzo łatwo. Na marginesie tych rozważań należy zwrócić uwagę na przyjętą w

[119] Z. Bidziński, J. Sereda: op. cit., s. 37 – 38.
[120] 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.

komunikacji poprzez internet formę wyrażania emocji. 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 symbolizować dobry humor „:-)", śmiech ":-D", smutek „:-(", pokazanie języka ":-P" czy też żart z przymrużeniem oka „;-)". Środowisko Internautów wypracowało również szereg angielsko- i polskojęzycznych skrótów dość powszechnie używanych w listach i w innych formach komunikacji. Prawidłowe odczytanie przekazu 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.

5.3.1 Spaming

Spam – (ang. konserwa mięsna, mielonka, a w żargonie internetowym – niechciana korespondencja) to zjawisko, które moim zdaniem może zagrażać, lub naruszać dobra osobiste w postaci wolności. Może również powodować sytuacje, w których utrudniona będzie możliwość funkcjonowania osoby prawnej. Zgodnie z polską konstytucją – każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. Konstytucja zapewnia również wolność i ochronę tajemnicy komunikowania się.

Spam może mieć kilka postaci. Pierwsza z nich to *Excessive Multi-Posting,* czyli zbyt wiele kopii tej samej wiadomości. Do kategorii tej zalicza się przesyłki, 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. Drugą odmianą *spamu* jest *Excessive Crossposting*, czyli dużo postów do więcej niż jednej grupy newsowej lub więcej niż jednego użytkownika. Istnieją specjalne algorytmy matematyczne, które administratorom serwerów pocztowych i newsowych potrafią pomóc określić stopień „agresywności" takiej partii przesyłek.

[121] Z. Bidziński, J. Sereda: Ibidem.

Najbardziej uciążliwe są przesyłki, które reklamują jakiś serwis WWW (często o charakterze pornograficznym), 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. Najbardziej narażoną na *spam* grupą użytkowników Internetu są uczestnicy grup dyskusyjnych. Podmioty „trudniące" się takim *spamingiem* dzięki specjalnemu oprogramowaniu zbierają adresy dyskutantów. Zbiory tak pozyskanych adresów kont mailowych są często przedmiotem dalszej odsprzedaży, co powoduje, że kolejny podmiot będzie wysyłał na dany adres przesyłki. Dodatkowym kłopotem w przypadku, gdybyśmy chcieli odpowiedzieć na dany list z prośba o nieprzesyłanie już więcej podobnej korespondencji, jest to, że adresy z których przesyłka pochodzi tak naprawdę, najczęściej nie istnieją. *Spam* wiąże się z innym zagadnieniem a mianowicie z *fake mailem* (ang. udawany, podrobiony list elektroniczny), o którym napiszę w dalszej części pracy.

W skrajnych przypadkach *spam* może doprowadzić do zapełnienia skrzynki pocztowej (konta) niechcianą korespondencją. Konsekwencją tego może być i często się tak zdarza, niemożność przyjmowania już jakiejkolwiek innej poczty elektronicznej, a nawet niemożność zalogowania (dostania się) na konto, co niewątpliwie narusza wolność komunikacji, a pamiętajmy, że konto (przestrzeń dyskowa na serwerze wraz z uprawnieniami do pewnych jego zasobów) nie służy wyłącznie do korespondencji e-mailowej. *Spam* z punktu widzenia pojedynczego użytkownika, posiadacza skrzynki pocztowej, jest co prawda utrudnieniem, jednakże przypuszczam, że nikt w przypadku unieruchomienia konta niechcianą pocztą nie będzie szukał ochrony prawnej w sądzie. Nie będzie szukał takiej ochrony, chociaż nastąpi prawdopodobnie przeżycie wewnętrzne polegające na ograniczeniu swobody, naruszeniu dobra i będzie to przeżycie obiektywne. Należy chyba jednak podchodzić do tego zagadnienia w makro skali.

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[122]. 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 makro 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"[123]. 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

[122] DoG: Kara śmierci odwołana, Biuro i Komputer, dodatek do Gazety.
[123] Wyrok s.apel. z 15 marca 1996 r. I ACr 33/96, OSA 1996/7-8/31 - z uzasadnieniem

niezgodnie z regułami społecznymi oraz z obowiązującym prawem (ustawa o ochronie danych osobowych).

Na zakończenie rozważań na temat *spamu* pragnąłbym zasygnalizować tendencję w światowej legislacji dotyczącej tego zagadnienia. W tym roku Austriacki parlament przyjął poprawkę do tamtejszej Ustawy Telekomunikacyjnej, na mocy której nadawcy niechcianych listów (*spamów*) będą podlegali karze grzywny. Po naleganiach licznych grup austriackich użytkowników Internetu, wniosek o wprowadzenie tej poprawki został przedstawiony przez sejmową Komisję Sprawiedliwości. Dotychczas ustawa zakazywała jedynie wysyłania reklamowych faxów i wykonywania rozmów telefonicznych bez uprzedniej zgody, środowisko Internetu domagało się rozszerzenia tej ustawy o wysyłanie e-mail'i. Omawiane zjawisko leży w sferze prawno-karnej, jednakże moim zdaniem może w sposób obiektywny naruszać dobra osobiste osób fizycznych i prawnych.

5.3.2 Fake mail

Poczty elektroniczna jest drugą co do popularności usługą wykorzystywaną w sieci[124]. We wstępie do tego rozdziału opisałem historię powstania standardów przesyłania e-maili w Internecie. Jak wspomniano – służy do tego specjalne oprogramowanie zarówno klienckie (umożliwiające redagowanie przesyłki, podanie adresata i autora, tematu), 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.

Można wpisać nieprawdziwe dane. W przypadku imienia i nazwiska – można podawać się za kogoś innego bez zbytniego wpływu na doręczenie przesyłki. Stworzy

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

to wrażenie, że osoba podająca się za osobę trzecią dysponuje danym adresem pocztowym. Gdyby podane nazwisko należało do konkretnej osoby trzeciej – przysługiwałaby jej ochrona tego nazwiska. Wpisanie przy pomocy oprogramowania klienckiego fałszywego adresu pocztowego, spowoduje, że wysyłając pocztę nie otrzymamy na adres naszej prawdziwej skrzynki pocztowej odpowiedzi. Przesyłka jednak dojdzie. Można w ten sposób uprawdopodobnić, że wysłana wiadomość pochodzi od konkretnej osoby trzeciej w ten sposób, że dysponuje ona poza danym imieniem i nazwiskiem dodatkowo konkretna adresem poczty elektronicznej. Przykładowo autor niniejszego opracowania posiada skrzynkę pocztową o adresie vagla@irc.pl. Ktoś próbujący się pod niego podszyć może wykorzystać znane mu imię i nazwisko i spróbować wysłać list, podając jako adres zwrotny właśnie vagla@irc.pl. Mamy tu już do czynienia z tzw. *fake mailem* (ang. udawany, podrobiony list elektroniczny). Spreparowany w ten sposób list będzie zawierał w swym nagłówku jak gdyby całą drogę, którą przebył przez poszczególne serwery pocztowe, jednakże zasadniczo będzie zawierał również „nazwę" maszyny, z której został wysłany. Na te informacje przeciętny użytkownik często nie zwraca w ogóle uwagi.

Możliwe jest też inne rozwiązanie. Korzystając z *telnetu* – usługi pozwalającej na zdalną pracę na innym komputerze w sieci – użytkownik posiadający podstawową wiedzę na temat mechanizmów przekazywania elektronicznej poczty jest w stanie połączyć się z demonem *sendmail* przez port 25, przez który to port przekazuje się m.in. pocztę. Użytkownik taki może całkowicie anonimowo, z poziomu klawiatury, wygenerować list elektroniczny, podając dane potrzebne do doręczenia przesyłki. W takim liście również mogą się znaleźć dane nieprawdziwe. I tak może się zdarzyć, że otrzymamy list np. z adresu: god@heaven.org, albo zupełnie bez adresu. Tu również w nagłówku będą się znajdowały informacje dotyczące serwera poczty, z którego nastąpiło wysłanie listu, i nazwy maszyny, która go wysłała. W przypadku, gdy wysyłamy list przykładowo z kawiarni internetowej lub z campusu uczelni – jesteśmy w stanie wysłać praktycznie całkowicie anonimowy list (ze względu na łatwość dostępu do terminali i dużą potencjalną liczbę użytkowników). Możemy również posłużyć się specjalnymi usługami istniejącymi w sieci, których przykładem jest Remailer. Jest to specjalne oprogramowanie, które korzystając ze specjalnego adresu

pocztowego – przykładowo remailer@reply.com przesyła dalej otrzymaną z tego adresu pocztę. W treści listu do remailera można zamieścić kilka komend, w szczególności podać do kogo ma być przesłany dany list oraz po jakim czasie od otrzymania przez remailera przesyłki ma ona być przekazana dalej. Remailer odcina cały nagłówek listu pochodzącego od nadawcy i wysyła list do odbiorcy niejako anonimowo. Remailer pozwala również dzięki specjalnym komendom umieszczonym w wysyłanym liście przekazać informację o dostarczeniu przesyłki na przykład poprzez publiczną grupę dyskusyjną *Usenetu* (np. pl.misc.test).

Dzięki przedstawionym wyżej mechanizmom istnieje możliwość naruszenia lub zagrożenia dóbr osobistych osób fizycznych i prawnych. Bo przecież nietrudno wyobrazić sobie sytuację, w której ktoś anonimowo 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 osoby pod którą się podszywa. Osoba podszywająca się potencjalnie ma możliwość obrażenia innych osób np. poprzez używanie określeń, sformułowań powszechnie uznanych za wulgarne lub obraźliwe 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 niegrzeczną, ordynarną etc. Osoba pod którą się podszyto nie koniecznie musi być równocześnie dyskutantem na tej grupie. Podszywający się może każdocześnie „podpisywać się" prawdziwym adresem poczty elektronicznej ofiary i w ten sposób kierować do niej potencjalne odpowiedzi dyskutantów (*reposty*). Adres ten może przyciągnąć bardziej pomysłowych Internautów, którzy dokonać mogą różnych ataków na posiadacza danej skrzynki. Kolejne *reposty* mogą powodować negatywne odczucia właściciela danego adresu skrzynki pocztowej (poprzez sam fakt, że się pojawią lub przykładowo przez obraźliwe treści niosące w sobie w ramach „rewanżu"). Można również wyobrazić sobie podszycie się pod pracowników danej firmy. Może to analogicznie rodzić konsekwencje w postaci utraty renomy tej firmy u części Internautów, a w dalszej kolejności u innych osób (Internet wywiera coraz większy wpływ na osoby z niego nie korzystające). 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 korzystanie ze swojej skrzynki pocztowej. Sposób ten polega na podszyciu się pod daną osobę w momencie wysłania prośby o zapisanie na listę dyskusyjną. Jeśli zasubskrybuje się taką osobę na kilka list dyskusyjnych, na których uczestnicy generują dla przykładu 20 listów dziennie – sumarycznie osoba atakowana dostaje bardzo dużą ich liczbę. Może dojść do zablokowania konta pocztowego tej osoby (analogicznie jak przy *spamie*) i w konsekwencji naruszenia dobra osobistego w postaci wolności komunikacji (oczywiście poza samym podszyciem się, gdzie być może naruszono prawo do nazwiska, pseudonimu). Zapisanie takie będzie skuteczne tylko wtedy, gdy serwery obsługujące daną listę dyskusyjną nie wysyłają prośby o potwierdzenie subskrybcji na daną listę do nadawcy pierwszej prośby. Potwierdzenie taki oczywiście w omawianym przypadku przyjdzie na konto pocztowe atakowanej osoby i będzie mogło być przeczytane (co do zasady) tylko przez nią. Nie spowoduje to zalania jej skrzynki dużą ilością korespondencji (*flood*). Bardzo podobne utrudnienia mogą się wiązać z *fake mailem* wysłanym na grupę *Usenetu* z jakąś atrakcyjną ofertą, np. sprzedaży telefonu komórkowego, wynajęcia mieszkania. Osoby zainteresowane kupnem takiego telefonu (przykładowo) po bardzo atrakcyjnej cenie będą niepokoiły ofiarę ataku przesyłając jej (na podany w liście adres e-mail) oferty kupna. Przedstawione stanowisko może być kontrowersyjne, gdyż jak wspomniano wyżej – wolność może jest rozumiana przez niektórych autorów jako wolność poruszania się.

5.4 Sniffing

Sniffing jest najczęściej spotykaną metodą ataków internetowych[125]. Jeśli włamywaczowi uda się zainstalować specjalne oprogramowanie do przechwytywania

[125] D. Atkins, P. Buis eds.: op. cit., s. 461.

pakietów w sieci (*sniffer*), to za pomocą specjalnych filtrów może obserwować połączenia z i do konkretnej domeny – celu ataku. Każde połączenie protokołu FTP, telnet, rlogin czy SMTP może pozwolić 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 rozprowadzony i po uruchomieniu w systemie ofiary, która 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 opisane przez I. Dobosz – tajemnicę komunikacji[126]. Przytacza ona twierdzenia 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"[127]. Autorka w dalszej części swojego wywodu stwierdza, że już samo przygotowanie urządzeń podsłuchowych stanowi już zagrożenie dobra osobistego. W świetle powyższych stwierdzeń należy przyjąć, że takim zagrożeniem będzie również zainstalowanie *sniffera* na którejś z tras internetowych, lub wygenerowanie odpowiedniego wirusa, który spełniałby podobne funkcje i działał w systemie informatycznym ofiary ataku.

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[128]. Użytkownik 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)

[126] I. Dobosz: op. cit., passim.
[127] Ibidem, s. 94

telefonu komórkowego. Jeśli przyjąć za A. Szpunarem iż przedmiotem odrębnej ochrony jest „wolność od złośliwego niepokojenia”[129] 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.

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 bowiem: „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”[130]. 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 i 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 niniejszej pracy[131].

---

[128] SMS - Short Message Service jest usługą polegającą na przesyłaniu krótkich (do 160 znaków) wiadomości między abonentami sieci komórkowych w standardzie GSM. SMS FAQ http://www.waw.pdi.net/~pawelk/smsfaq/

[129] A. Szpunar: Zadośćuczynienie za szkodę niemajątkową, Bydgoszcz 1999. s. 100.

[130] Wyrok SA z 29 stycznia 1993 r. AG Cr 369/92, Wokanda 1993/9 s. 33.

[131] Szersze omówienie zagadnienia znajduje się w: J. Barta, R. Markiewicza, Internet a prawo, Kraków 1998.

Pragnę również jedynie zasygnalizować występowanie w Internecie różnych praktyk nieuczciwej konkurencji (np. rozpowszechnianie nieprawdziwych wiadomości, używanie oznaczenia innego przedsiębiorstwa). Przykładem może być udostępnienie użytkownikom wyszukiwarki internetowej (*sercher*), która przy prezentacji wyników pomijać będzie informacje o konkurencyjnych przedsięwzięciach lub produktach. Innym udokumentowanym przejawem nieuczciwej konkurencji jest używanie podobnych lub takich samych Secendlevel-Domain (domen internetowych). Wedle Federalnej Komisji Handlu USA australijska firma Internic Software wprowadzała w błąd użytkowników Internetu, celowo posługując się domeną www.internic.com. Podobny adres (www.internic.net) ma agencja rejestrująca internetowe domeny – InterNIC. Australijska firma również oferuje podobną usługę, lecz za dwukrotnie wyższą cenę.

Kolejnym, jedynie zasygnalizowanym w tej pracy zagadnieniem związanym z naruszeniem lub zagrożeniem dóbr osobistych jest problem bezprawnego używania znaków towarowych w adresach domenowych. Adres domenowy to słowy zapis internetowego adresu komputera. Składa się on z co najmniej dwóch wyrazów lub skrótów, które zastępują ciąg cyfr identyfikujących komputer w sieci Internet. Adresy domenowe automatycznie zamieniane są na adresy IP przez serwer DNS (*Domain Name Server*). Sygnalizuje tu sytuację, gdy jeden podmiot jest uprawnionym z rejestracji znaku towarowego, a drugi podmiot posiada przedmiotowy adres domenowy, składający się z oznaczenia identycznego lub podobnego. Istotę tego konfliktu stanowi używanie w treści adresu domenowego, przez jego posiadacza oznaczenia identycznego z oznaczeniem, które zostało zarejestrowane jako znak towarowy dla danych produktów na rzecz innego podmiotu lub oznaczenia doń podobnego[132]. Zgodnie z art. 23 k.c. dobra takie pozostają pod ochrona prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach (ustawa o zwalczaniu nieuczciwej konkurencji, ustawa o znakach towarowych). Analogicznie –

[132] R Chmura, W. Włodarczyk: Bezprawne używanie zarejestrowanych znaków towarowych w adresach domenowych... [w:] R. Skubisz (red.): Internet – problemy prawne, Lublin 1998.

w przypadku używania w adresie domenowym nazwiska lub pseudonimu – dobra te będą podlegały ochronie przewidzianej w art. 23 i 24 k.c.

Na koniec należy przedstawić problem ochrony danych osobowych. Pragnę jedynie zasygnalizować ewentualne problemy związane z ochroną danych osobowych w kontekście Internetu. Jak zostało powiedziane wcześniej - danymi osobowymi jest każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby. W wielu systemach unixowych w ogólnie dostępnym do czytania pliku /etc/passwd często znajdują się takie informacje jak imię, nazwisko i telefon posiadacza konta. Powstaje pytanie o legalność (z punktu widzenia obowiązującego w Polsce systemu prawnego) takiego sytemu operacyjnego, lub o ewentualne obowiązki administratora takiego systemu (obowiązek rejestracji zbioru danych osobowych u Generalnego Inspektora Ochrony Danych Osobowych), na którym przecież, w gruncie rzeczy, opiera się Internet? Podobnie polecenie VRFY w *sendmailu* udziela informacji o imieniu i nazwisku posiadacza konta. Internet udostępnia również różnego rodzaju programy wyszukiwawcze, które pomagają w znalezieniu odpowiednich informacji. Dzięki takim programom - wyszukiwarkom (*serchers*) przy pewnej wprawie możliwe jest zebranie szeregu informacji o osobach fizycznych, o ile zostawiły te informacje w sieci (przykładem może być wyszukiwanie listów znajdujących się w archiwach list dyskusyjnych lub *Usenetu,*a które mogą zawierać różnego rodzaju informacje o autorze listu). Często autor nie jest w stanie kontrolować występujących w Internecie informacji o sobie. Nie można tu mówić o jakimś konkretnym zbiorze danych osobowych, a jedynie o bazie danych, w której występują same odesłania do dokumentów, w którym występuje dane słowo, fraza. Oczywiście aktualna jest Internetowa zasada wyszukiwania informacji – aby coś znaleźć w Internecie należy to wcześniej tam umieścić. Większość inforamacji o użytkownikach Internetu w Internecie pochodzi od nich samych (listy, artykuły), ale może istnieć duża grupa informacji, na którą nie będą mieli wpływu. W kontekście danych osobowych interesujących problemów może dostarczyć zagadnienie identyfikacji poszczególnych użytkowników w sieci. Zazwyczaj użytkownicy Internetu posługują się „nazwą użytkownika" (*user id, ident*), która to nazwa jest swoistym kryptonimem. Powstaje pytanie czy ten kryptonim może stanowić dane osobowe czy też nie. Podobnie czy

skoro w pewien sposób identyfikuje on użytkownika można rozciągnąć na niego ochronę przysługującą nazwisku lub pseudonimowi? Wydaje mi się, że sam *ident* nie będzie podlegał ochronie jako dobro osobiste. Również w połączeniu z innymi informacjami może już identyfikować konkretną osobę jedynie w ograniczonym zakresie. Takimi informacjami mogą być na przykład nazwa domenowa maszyny na której dany użytkownik ma konto. W takim razie adres e-mail będzie mógł identyfikować konkretną osobę (prawną czy fizyczną), jednak należy przy tym pamiętać, że jedna osoba fizyczna może dysponować dużą ilością adresów e-mail, a kilka osób może korzystać z jednego adresu e-mail. Może również zdażyć się sytuacja, gdy ktoś stworzy fikcyjną postać i zaopatrzy ją w adres e-mail, stworzy dla niej stronę WWW oraz będzie wypowiadać się w jej imieniu na forum Internetu. Czasami kryptonim funkcjonuje wśród Internautów jako „przezwisko" (*nickname*), pod którym znani są oni przez innych użytkowników. Tak będzie przykładowo w przypadku użytkowników IRC, jednakże identyfikacja konkretnej osoby może nastąpić (ale też nie ze stu procentową pewnością) jedynie w połączeniu z informacjami dotyczącymi konta na konkretnej maszynie, z której dany użytkownik łączy się z Internetem. I tu również kilka osób mających dostęp do jednego konta może wspólnie go używać, a tym samym uchodzić za jedną osobę . Wydaje mi się zatem, że nie można traktować ani adresów e-mail ani *ident'ów* czy *nickname'ów* jako samodzielnych danych osobowych, czy określeń spełniających podobną rolę jak nazwisko czy pseudonim. Natomiast w połączeniu z innymi danymi będą stanowiły przedmiot ochrony. Dopiero w połączeniu z innymi danymi określającymi konkretną osobę fizyczną, zbiory danych z popularnych programów pocztowych (tzw. książki adresowe) staną się zbiorami danych osobowych w myśl przepisów o ochronie danych osobowych, bo dopiero wtedy zawarte w nich dane będą pozwalały na określenie tożsamości konkretnej osoby. Szersze omówienie tematyki ochrony danych osobowych nie mieści się w ramach niniejszej pracy[133].

[133] Więcej na ten temat: M. Wyrzykowski (red.): Ochrona danych osobowych, Warszawa 1999.

6 CYWILNOPRAWNA OCHRONA DÓBR OSOBISTYCH

Zasada zawarta w art. 23 kodeksu cywilnego ma charakter ogólny i przewiduje ochronę jaką prawo cywilne roztacza nad instytucją dóbr osobistych. Ochrona ta jest niezależna od ochrony przewidzianej w innych przepisach. Środki ochrony, a więc sankcje na wypadek naruszenia lub zagrożenia przewidziane są w art. 24 kodeksu cywilnego. Z treści art. 24 wynika, że dobra osobiste są chronione w sposób wszechstronny, a więc środki ochrony mogą mieć zarówno charakter majątkowy jak i niemajątkowy. W jednym procesie mogą być zgłoszone zarówno roszczenia mające charakter majątkowy jak i te o charakterze niemajątkowym. W praktyce najczęściej łączone jest żądanie usunięcia skutków naruszenia dóbr osobistych z żądaniem materialnego zadośćuczynienia.

Do środków o charakterze niemajątkowym zaliczamy roszczenie o zaniechanie, roszczenie o usunięcie skutków naruszenia oraz powództwo o ustalenie. Środki o charakterze majątkowym to zadośćuczynienie pieniężne za naruszenie dóbr osobistych (445 k.c., 448 k.c.), oraz naprawienie szkody majątkowej przewidziane w art. 24 §2 k.c. (na zasadach ogólnych np. art. 415 k.c.)

6.1 Niemajątkowe środki ochrony

Przez środki niemajątkowe rozumiemy głownie te przewidziane w art. 24 k.c., aczkolwiek niemożliwym byłoby pominięcie możliwości wskazywanych przez art. 142, 423 i 424 k.c. ponieważ 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.[134]

Celem roszczeń przewidzianych przez art. 24 k.c. jest zapewnienie przebiegającego bez zakłóceń korzystania z dóbr osobistych przez uprawnione podmioty (osoby fizyczne i prawne). W razie niezrealizowania obowiązku biernego (w tym wypadku polegającego na nienaruszaniu dóbr) zachowania się podmiotu powstaje

[134] A. Cisek, op. cit., *s*. 114

możliwość podniesienia roszczeń, które maja na celu zlikwidowanie okoliczności zagrażających lub naruszających sferę uprawnień.

Usunięcie skutków naruszenia może przykładowo przyjąć postać odwołania postawionych zarzutów i dodatkowego oświadczenia przepraszającego pokrzywdzonego lub złożenia wyrazów ubolewania. Może mieć miejsce wtedy, gdy naruszenie już nastąpiło. Istotne jest, by osoba uprawniona wyraźnie określiła co jest skutkiem naruszenia jej dóbr osobistych. Mogą to być dla przykładu ujemne odczucia osoby pokrzywdzonej. 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 listy dyskusyjnej (grupy dyskusyjnej) określonego listu.

Za rodzaj oświadczenia prowadzącego do usunięcia skutków naruszenia dobra osobistego traktowane jest przeproszenie pokrzywdzonego lub złożenie wyrazów ubolewania. Fakt, że to sąd w sentencji wyroku decyduje w jaki sposób i jakimi słowami pozwany ma przeprosić, skutkuje odebraniem charakteru osobistego i moralnego przeprosinom. To, że sąd w ogóle nakazuje przeprosić wcale nie znaczy, że przeprosiny będą szczere, a pozwany zmieni zdanie w stosunku do pokrzywdzonego. Takie przeprosiny niekoniecznie spowodują usunięcie skutków naruszenia. Tak więc pozornemu przeproszeniu powinien być odebrany status środka ochrony dóbr osobistych[135].

Żądanie zaniechania 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[136]. O tym środku ochrony wyraźnie mówi art. 24 KC. Roszczenie o zaniechanie określonego działania jest wzorowane na prawie negatoryjnym z zakresu prawa rzeczowego (dlatego niekiedy jest nazywane quasi-

[135] SN w orzeczeniu z dn. 19.01.1982r., IV CR 500/81, OSN 1982 nr 9-10, poz. 183, wyraził pogląd iż sentencia wyroku powinna zawierać dokładnie sformułowaną treść przeproszenia, co spotkało się z krytyką A. Szpunara w glosie OSP 1983, nr 10, poz. 220.
[136] M. Pazdan: art. 24, Nb.11. [w:] K. Pietrzykowski (red.), KC. Komentarz, Warszawa 1999.

negatoryjnym). Przesłanką takiego roszczenia jest zagrożenie dobra osobistego cudzym działaniem lub uzasadniona obawa dalszych naruszeń. Osoba uprawniona może żądać zaniechania tylko ściśle określonego działania. Roszczenie może również przybrać postać żądania kontynuacji czy też podjęcia określonych działań. Taka sytuacja będzie miała miejsce w przypadku, gdy zaniechanie odpowiednich działań prowadzi do zagrożenia dóbr osobistych.

Powództwo o ustalenie bezprawności naruszenia (oparte na ogólnym zapisie art. 189 KPC) zawsze powinno zmierzać do ustalenia stosunku prawnego lub prawa. SN stwierdził, że celem 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 sprawdzenie, które z faktów i ocen są zgodne z prawdą i mają usprawiedliwienie, a które należy potraktować odmiennie[137]. W przypadku powództwa o ustalenie bezprawności naruszenia dóbr osobistych ustala się jednak, że sporne twierdzenie, które może naruszać dobra osobiste (a które np. opublikowały środki masowego przekazu), jest prawdziwe lub fałszywe. Są to ustalenia faktyczne. Z drugiej strony powód domaga się stwierdzenia, że rozpowszechnianie pewnych informacji narusza jego prawo osobiste i w efekcie mamy do czynienia z ustaleniem stosunku prawnego między stronami jaki powstał w efekcie podniesienia i rozpowszechniania 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[138].

6.2 Majątkowe środki ochrony.

Unormowanie przyjęte w KC jest pod względem konstrukcyjnym prawie identyczne z unormowaniem przedwojennym z KZ, w którym odnośnie zadośćuczynienia pieniężnego rządziły cztery zasady: zasada zadośćuczynienia pieniężnego jako wyjątku (w przypadkach, gdy przewiduje to ustawa) od reguły, że

[137] SN z 18.01.1984r. I CR 400/83, OSN 1984, poz. 195

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 (KC przyjął rozwiązanie odmienne, polegające na współistnieniu zadośćuczynienia z oryginalną i nie mającą odpowiednika w obcych systemach prawnych sankcją z art. 448 KC), zasada ograniczająca dziedziczenie roszczenia o zadośćuczynienie.

Odnośnie zasady trzeciej: 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. Obecnie art. 448 przyjął inne brzmienie, powracając do zasady z KZ. Nowy przepis art. 448 nie mówi już o przypadku umyślnego naruszenia dóbr osobistych. Literalnie nowy art. 448 ma zastosowanie w przypadku naruszenia dobra osobistego, a więc bez względu na stopień winy sprawcy. Jednak ze względu na usytuowanie tego przepisu wśród przepisów o czynach niedozwolonych i biorąc jednocześnie pod uwagę iż wina stanowi podstawową przesłankę odpowiedzialności z tego tytułu należy przyjąć za autorami Komentarza do Kodeksu cywilnego, że podstawą zasądzenia zadośćuczynienia będzie najmniejszy nawet stopień zawinienia, a więc do granic *culpa levissima*[139]. Ta forma ochrony jest fakultatywna i zależy od decyzji Sądu, 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. Nie oznacza to jednak, że nieumyślność sprawcy będzie z góry oceniana jako uzasadniająca łagodniejsze potraktowanie sprawcy. Podstawą odmowy zadośćuczynienia z art. 448 k.c. może być nieznaczny rozmiar szkody niemajątkowej (niekoniecznie jej znikomość)[140]. W zakresie elementu obiektywnego winy może być wykorzystana

[138] A. Szpunar: op. cit., s. 253
[139] M. Safjan: art. 448, Nb.11 [w:] K. Pietrzykowski (red.), KC. Komentarz, Warszawa.1999. Tam również różne warianty interpretacyjne art. 448. Por.: A. Szpunar: Zadośćuczynienie za szkodę niemajątkową, Bydgoszcz 1999, s. 212.
[140] A. Szpunar: op.cit., s. 215.

konstrukcja domniemania prawnego z art.. 24 k.c.[141]. Sąd może przyznać temu, czyje dobro zostało naruszone odpowiednią sumę tytułem zadośćuczynienia pieniężnego za doznaną krzywdę lub na jego żądanie zasądzić odpowiednią sumę pieniężną na wskazany przez niego cel społeczny, niezależnie od innych środków potrzebnych do usunięcia skutków naruszenia. Ustawodawca zrezygnował z owej oryginalnej sankcji przewidującej zasądzenie odpowiedniej sumy pieniężnej na rzecz PCK.

W tym miejscu należy zasygnalizować spór o możliwość kumulowania roszczeń przewidzianych w art. 448 i 445 KC pod rządami KC z przed zmiany. Możliwość tę zakwestionował Radwański, gdyż 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 SN przesądziła o dopuszczalności kumulowania obu sankcji. Możliwe było więc zasądzenie odpowiedniej sumy na PCK, a obok tego, zgodnie z art. 445 § 1 sąd mógł zasądzić odpowiednią sumę tytułem zadośćuczynienia. Można więc przyjąć, że art. 448 w nowym brzmieniu realizuje postulaty Radwańskiego, gdyż obecnie będzie funkcjonować tylko jedno źródło satysfakcji albo 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.

Artykuł 445 k.c. przewiduje w wypadku naruszenia dóbr osobistych zadośćuczynienie za doznaną krzywdę. Warunkiem jest, by zaistniało zdarzenie przewidziane w tym artykule, z którym związana jest odpowiedzialność z tytułu czynów niedozwolonych i aby między tym zdarzeniem a doznaną krzywdą istniał związek przyczynowy. 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 w przypadku Internetu raczej nie będzie miało miejsca – art. 455 może być w omawianej kwestii zastosowany jedynie w przypadku pozbawienia wolności. Przyjmuje się, że

[141] M. Safjan: Ibidem.

pozbawienie wolności może dotyczyć zarówno sytuacji fizycznego zniewolenia osoby, jak i w przypadkach skrajnych, pozbawienia osoby możliwości podejmowania decyzji o samej sobie. Istnieje również inne, szersze rozumienie wolności (choć jest to kontrowersyjne) – przykładowo wolność komunikacji, ochrona prowadzenia działalności statutowej osoby prawnej, o czym była już w niniejszej pracy mowa. Jak podkreślają autorzy Komentarza do Kodeksu cywilnego – majątkowa ochrona szerzej rozumianej wolności jest obecnie możliwa na tle omawianego już art. 448 w zw. z art. 23 k.c.[142]. W związku z powyższym art. 445 ma znaczenie marginalne w przypadku naruszeń dóbr osobistych w Internecie.

6.3 Odpowiedzialność *providera*

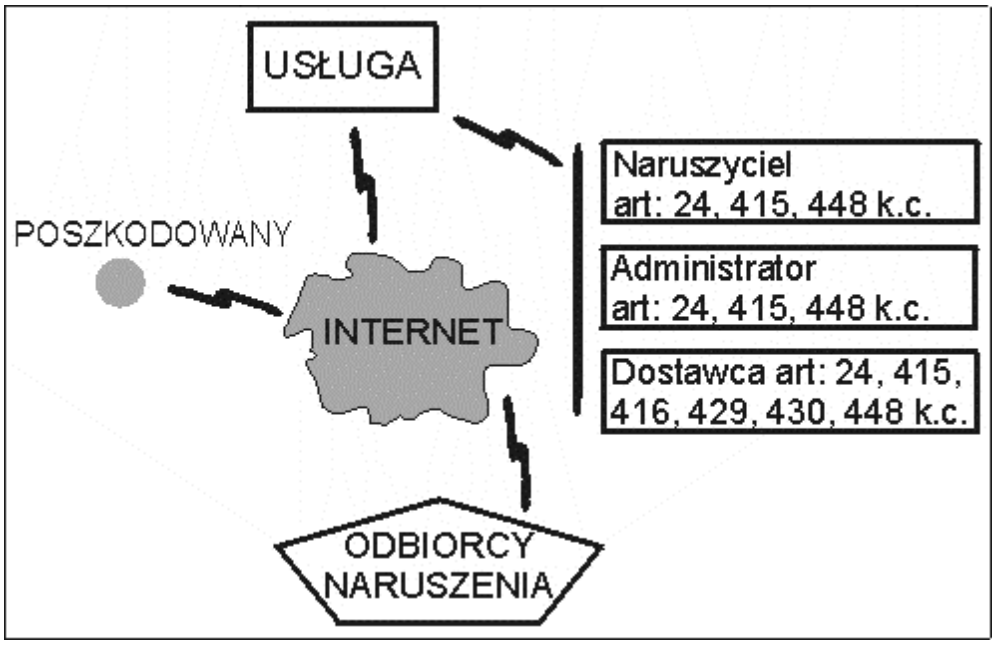
Bardzo często się zdarza, że w konkretnych sytuacjach (niektóre zostały opisane w niniejszej pracy) osoba naruszająca cudze dobra osobiste za pośrednictwem Internetu pozostaje anonimowa. Istotnym zagadnieniem jest więc określenie legitymacji biernej przy roszczeniach o ochronę dóbr osobistych. Zagrożenie lub naruszenie dóbr stanowi efekt działania podmiotu innego niż ten, którego dobro jest naruszane. Ochrona służy przeciwko „wszelkim cudzym działaniom bezprawnym, których skutkiem jest zagrożenie lub naruszenie dóbr osobistych”[143]

Rysunek nr 6 przedstawia schemat naruszenia oraz uproszczone przedstawienie zasad odpowiedzialności poszczególnych podmiotów. Internet jest przedstawiony jako chmurka, gdyż symbolizuje bardzo skomplikowane relacje między wieloma podmiotami (ISP, właściciele infrastruktury teleinformatycznej, etc.), które w ostateczności składają się na zjawisko nazwane Internetem.

Naruszenie następuje za pośrednictwem Internetu poprzez usługę. Usługą może tu być zarówno możliwość publikowania materiałów na stronach WWW, umożliwienie przesyłania e-maili lub ogłaszanie komunikatów za pośrednictwem *Usenetu*, może to być jakiekolwiek wykorzystanie znanych protokołów internetowych typu *telnet*[144], czy *ftp*[145].

[142] M. Safjan: Ibidem, art. 445, Nb11.
[143] A. Cisek, op. cit*., s*. 135.
[144] Telnet – protokół pozwalający otwierać sesje na zdalnych systemach.

Naruszycielem (naruszycielem pierwotnym) będzie tu osoba, która opublikowała dany artykuł (komunikat) *Usenecie*, umieściła na serwerze WWW strony naruszające cudze dobra osobiste etc. Osoba taka będzie odpowiadała na podstawie art. 24 oraz 448 k.c. za naruszenie dóbr osobistych oraz na zasadach ogólnych na podstawie art. 415 k.c. Jednakże, co wynika ze specyfiki Internetu może się zdarzyć, że zawiodą klasyczne metody ochrony, ze względu na anonimowość naruszenia (nie będzie znana osoba, która np. wprowadziła dane informacje do sytemu informatycznego i w konsekwencji do sieci Internet).



Rysunek 6. Schemat naruszeń, uproszczone zasady odpowiedzialności

Każda z usług internetowych ma swojego *administratora* – osobę fizyczną, która „opiekuje się" danym serwisem. W przypadku grup dyskusyjnych może nazywać się *postmasterem*, w przypadku stron WWW – *webmasterem* w innych przypadkach będzie to porostu administrator. *Administrator* może odpowiadać za własne działania naruszające lub zagrażające dobrom osobistym. Może to być np. zaniechanie podjęcia działań które prowadzą do usunięcia skutków naruszenie (a tym samym dalsze ich naruszanie), w przypadku, gdy np. dowiedział się o zaistniałym naruszeniu z wykorzystaniem danej, administrowanej przez niego (*administratora*)

[145] ftp – File Transfer Protocol. Niezależny od systemu operacyjnego protokół pozwalający na przesyłanie plików przez połączenie TCP/IP

usługi. Może się zdarzyć, że administrator będzie naruszycielem (naruszycielem pierwotnym). Poza niemajątkowymi środkami ochrony będzie tu miał zastosowanie art. 448 k.c. Może odpowiadać również na zasadach ogólnych na przykład za niewłaściwe (niedbałe) „administrowanie" daną usługą (niezastosowanie standardowych w danej dziedzinie zabezpieczeń sprzętowych lub oprogramowania np. *firewall'a* lub systemu zmiany haseł, udostępnienie haseł pozwalających na wniknięcie do systemu informatycznego przez osoby nieupoważnione) dzięki czemu ktoś (osoba anonimowa) dokonała naruszenia cudzych dóbr osobistych. Będzie to odpowiedzialność na zasadzie winy (art. 415 k.c.).

Dostawca usług może ponosić odpowiedzialność za działanie własne (na zasadzie art. 415, ew. 416 w przypadku osób prawnych) analogicznie do odpowiedzialności *administratora*. Również będą miały zastosowanie przepisy art. 24 i 448 k.c. Może również ponosić odpowiedzialność solidarną wraz z *administratorem*. *Dostawcą* usługi będzie tu osoba fizyczna lub prawna, która jest jej dysponentem (może być np. właścicielem nośników informacji, serwerów etc.). Będzie nim przykładowo przedsiębiorstwo udostępniające darmowe konta, osoba prawna prowadząca swój serwis informacyjny na stronach WWW, przedsiębiorstwo utrzymujące serwery *Usenetu,* wyższa uczelnia posiadająca strukturę teleinformatyczną.

Dostawca może powierzyć wykonanie pewnych czynności innym podmiotom, w wyniku czego może nastąpić naruszenie dóbr osobistych. Będzie to w szczególności powierzenie administracji daną usługą osobie trzeciej (np. przekazanie hasła *roota*). Odpowiadać będzie, chyba że nie ponosi winy w wyborze (*culpa in eligendo*) albo że wykonanie czynności powierzył osobie, przedsiębiorstwu lub zakładowi, które w zakresie swej działalności zawodowej trudnią się wykonywaniem takich czynności (art. 429 k.c.). Anonimowość bezpośredniego sprawcy szkody wyłącza możliwość skutecznej ekskulpacji[146]. W przypadku, gdy następuje powierzenie wykonania czynności osobie, która przy wykonywaniu tej czynności podlega kierownictwu *dostawcy* usługi, oraz gdy nastąpi zawinione zachowanie tej osoby powodujące szkodę

u osoby trzeciej będzie miała miejsce współodpowiedzialność oparta na zasadzie ryzyka (art. 430 k.c.). Przykładem może być stworzenie przez *webmastera* w ramach stosunku pracy stron WWW na podstawie wskazówek działu marketingu firmy, ale z pozostawioną pewną sferą samodzielności[147].

Za szkodę wyrządzoną przez funkcjonariusza państwowego przy wykonywaniu powierzonej mu czynności (np. prowadzeniu serwisu Internetowego organów władzy, administracji lub gospodarki państwowej) odpowiada Skarb Państwa (art. 417 k.c.). Przesłanką odpowiedzialności Skarbu Państwa jest bezprawność zachowania się funkcjonariusza[148].

Ilość informacji i jej nieustanny przepływ w Internecie jest bardzo duży. Praktycznie żaden dostawca usług nie jest w stanie w pełni kontrolować treści przesyłanych przez siebie pakietów. Nie ma możliwości dokonywania przez dostawce usług „cenzury" i weryfikacji wprowadzonego do sieci materiału pod kontem naruszenia cudzych dóbr osobistych, w tym autorskich dóbr osobistych[149]. Jednakże w przypadku w którym dostawca taki dowie się w dowolny sposób o naruszeniu za jego pośrednictwem przepisów prawa powinien w odpowiedni sposób zareagować.

Poniżej przytaczam fragment wypowiedzi J. Rychtera, podsumowujące niedawną „aferę" związaną z przesyłaniem pornograficznych, zdygitalizowanych zdjęć za pośrednictwem grup dyskusyjnych *Usenetu*. „Jak wiadomo, serwery *Usenetu* wykorzystywane bywają do różnych celów. Dostęp do nich ma wiele osób, a fałszywe poczucie anonimowości zachęca do działań na granicy prawa. Każdy administrator serwera *Usenet* stara się jednak ograniczać takie zjawiska, w miarę swoich możliwości. (...) zarówno naruszenia technicznej sprawności *Usenet*, jak i artykuły naruszające prawo, będą ścigane. Robi się to z powodzeniem, sporo instytucji

[146] M. Safjan: art. 429, Nb. 13 [w:] K. Pietrzykowski (red.), KC. Komentarz, Warszawa 1999.
[147] Por. M. Safjan: art. 430, Nb. 11 [w:] K. Pietrzykowski (red.), KC. Komentarz, Warszawa 1999.; A. Szpunar: Odpowiedzialność za szkodę wyrządzoną przez podwładnego [w:] Rozprawy z polskiego i europejskiego prawa prywatnego, Kraków 1994, s. 468; A. Rembieliński: Odpowiedzialność cywilna za szkodę wyrządzoną przez podwładnego, Warszawa 1971, s. 164.
[148] Por.: Z. Banaszczyk: art. 417, Nb. 6, 29 [w:] K. Pietrzykowski (red.), KC. Komentarz, Warszawa 1999. Postulaty odnośnie zmiany dotychczasowej wykładni art. 417 k.c., uzależniającej odpowiedzialność Skarbu Państwa od przesłanki zawinionego działania funkcjonariusza.
[149] Por: J. Maciąg, S. Stanisławska: op.cit., s. 92.

otrzymało ostrzeżenia lub straciło dostęp z tych powodów. W przypadku zgłoszenia naruszenia prawa, poza utratą dostępu powiadomimy też policję i (lub) prokuraturę i przekażemy wszystkie niezbędne dane. W takich przypadkach współpracuje też Telekomunikacja Polska S.A., pomagając w wyśledzeniu sprawcy”[150].

Przykładem działania administratora zmierzającego do zaniechania dalszych naruszeń jest uniemożliwienie korzystania z usługi osobie (osobom) korzystającej z danego (konkretnego) komputera. W skrajnych przypadkach przybiera w chwili obecnej postać odcięcia przez Telekomunikacje Polską S.A. od możliwości korzystania z numeru dostępowego do Internetu (0202122). Zwyczajowo przyjęło się, że operatorzy oraz administratorzy w Internecie udostępniają specjalny, interwencyjny adres e-mailowy. Z reguły adres ten wygląda w sposób następujący: abuse@nazwa.domeny. Na ten właśnie adres można wysłać list powiadamiający np. o naruszeniu prawa dokonanego z użyciem danego serwisu internetowego czy też danej maszyny (komputera).

[150] J. Rychter: Serwer news.icm.edu.pl – podsumowanie. pl.internet.polip.2.września.1999.

7 ZAKOŃCZENIE

Niniejsza praca miała za zadanie przybliżyć nowe formy naruszeń oraz zagrożeń dóbr osobistych wynikające z używania Internetu. Pragnąłem przedstawić specyfikę tychże naruszeń wynikającą z masowego i globalnego charakteru Internetu. W podsumowaniu pragnę syntetycznie przedstawić główne problemy które rodzą się w związku z wykorzystaniem Internetu a mające niebagatelne znaczenie dla funkcjonowania systemu ochrony dóbr osobistych.

Ze względu na wspomniany, globalny charakter, w Internecie spotykamy się masowością naruszeń, ale również z nieokreślonym kręgiem odbiorców tych naruszeń. Łatwo sobie wyobrazić sytuacje gdy powstaje jednoczesne, wielokrotne naruszenie dóbr osobowych (jeden fakt, wiele naruszeń). Co więcej następować ono może na wielu możliwych płaszczyznach komunikacji internetowej (opublikowanie listu na liście dyskusyjnej, przeniesienie tego listu do archiwum WWW a następnie skopiowanie go z danego archiwum i opublikowanie poprzez inne usługi lub te same usługi, ale używane przez inne kręgi ludzi). Jak się wydaje dzięki Internetowi (technikom teleinformatycznym) intensywność naruszeń znacząco się zwiększa[151]. Idąc dalej – w momencie gdy osoba naruszająca dobro osobiste traci kontrole nad dystrybucją informacji, i biorąc pod uwagę możliwość nieograniczonego kopiowania i przesyłania dalej różnego rodzaju pakietów zawierających dane naruszają dobra osobiste – niemożliwe staje się być może usunięcie skutków naruszenia tych dóbr w tradycyjny sposób.

Nową sytuacją jest problem dowodowy. Tu również należy brać pod uwagę niemożliwość określenia kręgu odbiorców naruszenia, ale też fakt, że współczesna technika umożliwia dość dużą anonimowość. W połączonych systemach teleinformatycznych różne informacje zbierane są i zapisywane (*logowane*) w różnych miejscach. To rozproszenie z jednej strony utrudnia wydobycie informacji dla potrzeb dowodowych (czas wejścia do systemu teleinformatycznego, czas pozostawania w tym systemie, zdalna praca na innych systemach przy wykorzystaniu tego konkretnego sytemu, etc.), z drugiej strony umożliwia osobą posiadającym odpowiednią wiedze

[151] Ilustracją wykorzystania Internetu jest afera Moniki Lewinsky i Billa Clintona. Ten skandal obyczajowy wybuchł właśnie w Internecie i nabrał takiego rozmachu i intensywności również dzięki sieci.

informatyczną na usuwanie informacji z systemów lub ich fałszowanie. Ze względu na łatwość modyfikacji plik komputerowy ma bardzo ograniczoną wartość dowodową. Może się również zdarzyć, że mimo zaistnienia w świadomości użytkowników Internetu pewnych faktów nikt nie będzie w stanie stwierdzić skąd się wzięła dana informacja, dane przedstawienie faktów. Będzie to zjawisko podobne do plotki, która nie ma jednego konkretnego źródła, a funkcjonuje w pewnym środowisku. W przypadku Internetu to środowisko ma charakter globalny. To wszystko sprawia, że wypracowane dotychczas, tradycyjne metody ochrony dóbr osobistych nie będą działać.

Starałem się wykazać istnienie specyficznego środowiska użytkowników Internetu, oraz istniejące w tym środowisku przyjęte (nowe i nieznajdujące odpowiedników poza siecią) normy zachowań, zasady współżycia. Z jednej strony wedle Sądu Najwyższego „czynność sprzeczna z prawem, w danym przypadku z treścią art. 23 k.c., nie może być jednocześnie zgodna z zasadami współżycia społecznego ani nawet z przyjętymi zwyczajami, na które zresztą tylko wówczas można się powoływać, gdy konkretny przepis prawa w dyspozycji swej zawiera odesłanie do takich zwyczajów, zaś wspomniany przepis (art. 23) w dyspozycji swej do żadnych zwyczajów się nie odwołuje”[152]. Tak więc naruszenie dóbr osobistych w Internecie będzie naruszeniem mimo, że może się zdarzyć, iż będzie takie działanie zgodne z zasadami specyficznego współżycia społeczeństwa informacyjnego. Z drugiej jednak strony owe specyficzne zasady współżycia oraz relacje między jednostkami współegzystującymi w Internecie będą miały wpływ na samą treść dóbr osobistych (wszystkie definicje powołujące się na kryteria obiektywne wskazują na relacje społeczne przy formułowaniu dóbr osobistych)

To wszystko prowadzi do konkluzji, że mimo istnienia odpowiednich unormowań dotyczących ochrony dóbr osobistych w Kodeksie cywilnym staną się one (już się stały) niewystarczające. Być może konieczne jest położenie większego nacisku na niedopuszczenie do naruszenia dóbr osobistych w Internecie, a mniejszego na usunięcie jego skutków. I być może tak jak się stało ze specyficznym problemem

[152] Wyrok SN z 10 stycznia 1997 r. II CKN 62/96, Wokanda 1997/4 s. 7

ochrony danych osobowych należałoby uznać środki publicznoprawne (administracyjnoprawne) za podstawowy „oręż" ochrony tych dóbr w tym specyficznym środowisku. W takiej sytuacji to nie jednostka będzie decydować o zakresie ochrony jej dóbr, a twórcy prawa, którzy za nią podejmą wyprzedzające decyzje[153].

W związku z globalnym charakterem Internetu należy zwrócić również uwagę na konieczność tworzenia ponad granicznych systemów ochrony, gdyż bez jednolitych, międzynarodowych standardów ochrona dóbr osobistych w Internecie nie jest możliwa[154].

W świadomości użytkowników tego medium Internet to swoista oaza wolności i anarchizmu. Bardzo duże znaczenie dla Internautów ma wolność słowa – ale pojęta w ten sposób, że można głosić każdą tezę. Należy jednak zwrócić uwagę, że w prawie cywilnym prawo do wolności słowa chronione jest przede wszystkim przepisami o ochronie dóbr osobistych. Poszanowanie praw innych przy wykonywaniu wolności słowa oznacza w szczególności respektowanie cudzej integralności, autonomii, prywatności i intymności, respektowanie cudzej godności i prawa do dobrej sławy[155]. Coraz bardziej skomplikowane techniki teleinformatyczne niosą same w sobie zagrożenie dla wspomnianych dóbr. Być może konieczne jest wprowadzenie odrębnych (dedykowanych specjalnie Internetowi) regulacji prawnych, jednakże należy w takim przypadku zwrócić szczególną uwagę na konieczność odpowiedniego wyważenia chronionych wartości, ochrony indywidualnych dóbr jednostek oraz stworzenia warunków działania Internetu jako środka masowego przekazu informacji. Jak podkreślają autorzy – niewskazane byłoby wprowadzenie takich rozwiązań, które pozbawiłyby Internet jego podstawowych atrybutów, w tym wolności słowa[156].

[153] M. Safjan: Ochrona danych osobowych – granice autonomii informacyjnej, [w:] M. Wyrzykowski (red.): Ochrona danych osobowych, Warszawa 1999.
[154] Problemy prawa prywatnego międzynarodowego oraz prawa międzynarodowego publicznego w kontekście ochrony dóbr osobistych wymagają odrębnego analitycznego opracowania. Ze względu na ramy niniejszej pracy nie mogły się znaleźć w niej rozważania na ten temat.
[155] J. Błeszyński: Aspekty prawne wolności słowa, http://www.krrtv.gov.pl/z4a7ble.htm
[156] J. Maciąg, S. Stanisławska: Internet – Prasa – Prawo, ZNUJ z. 68 1997 s. 91.

8 BIBLIOGRAFIA

1. Archiwum włamań na strony WWW: http://nt.security.net.pl/default.asp
2. D. Atkins, P. Buis eds.: Bezpieczeństwo Internetu. Profesjonalny Informator. LT&P 1997.
3. B. Banaszak, K. Wygoda: Regulacja prawna ochrony danych osobowych w Polsce w świetle ustawy z 29 sierpnia 1997 r. i standardów europejskich, [w:] M. Wyrzykowski (red.), Ochrona danych osobowych, Warszawa 1999.
4. M. Baranowska, NASK, Wyniki badania zbiorowości użytkowników Internetu w Polsce, Internet 2/97.
5. J. Barta, R. Markiewicz: Internet a prawo, Kraków 1998.
6. Z. Bidziński, J. Sereda: Cywilnoprawna ochrona dóbr osobistych w praktyce sądowej, [w:] Dobra osobiste i ich ochrona w polskim prawie cywilnym, Ossolineum 1986.
7. J. Błeszyński: Aspekty prawne wolności słowa, http://www.krrtv.gov.pl/z4a7ble.htm
8. R. Chmura, W. Włodarczyk: Bezprawne używanie zarejestrowanych znaków towarowych w adresach domenowych... [w:] R. Skubisz (red.): Internet - problemy prawne, Lublin 1998.
9. I. Dobosz: Przesłanki cywilnoprawnej ochrony przed podsłuchem. ZNUJ z.58 1992.
10. Dobra osobiste i ich ochrona w polskim prawie cywilnym (red.) J. St. Piątkowski, Ossolineum 1986.
11. S. Grzybowski: Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego, Warszawa 1957.
12. T. Hofmokl: Jacy jesteśmy? Trochę liczb!, "CHIP":
13. Internet - problemy prawne, (red.) R. Skubisz, Lublin 1998.
14. A. Kopff: Koncepcja praw do intymności i do prywatności życia osobistego, zagadnienia konstrukcyjne, „Studia Cywilistyczne", vol. XX Kraków 1972.
15. B. Kordasiewicz: Jednostka wobec środków masowego przekazu, Ossolineum 1991.
16. D. Kornas-Biela. Sejmowa Komisja Rodziny z dnia 13.03.98. Problemy zagrożeń rodziny przez przemoc i pornografię, ze szczególnym uwzględnieniem roli mediów. Materiały z posiedzenia komisji.
17. D. Kot: Użycie cudzego nazwiska w prasie a autorstwo dzieła, ZNUJ z.68, 1997.
18. Księga pamiątkowa ku czci prof. Natalii Gail, Trybunał Konstytucyjny - Wydawnictwa 1999.

19. M. Kuchciak, Geneza i rozwój Internetu, http://www.ccs.pl/~mkc/internet/genrozw.html
20. Leksykon Internetu http://leksykon.koti.com.pl
21. J. Maciąg, S. Stanisławska: Internet - Prasa – Prawo, ZNUJ z. 68, 1997.
22. Materiały z konferencji: „Integracja europejska wobec wyzwań ery informacyjnej (postindustrialnej)", http://eris.kbn.gov.pl/Pl-iso/pub/info/dep/integracja/index.html
23. D. Miodunka, P. Nowakowski: Świat Javy (2), PCkurier, 19 sierpnia 1999.
24. Netykieta: http://urethan.chem.pg.gda.pl/docs/S_S_vivre.txt
25. Ochrona danych osobowych (red.) M. Wyrzykowski, Warszawa 1999.
26. *Pretty Good Privacy*: http://www.pgpi.org
27. J. St. Piątkowski, Ewolucja ochrony dóbr osobistych [w:] E. Łętowska (red.), Tendencje rozwoju prawa cywilnego, Ossolineum 1983.
28. K. Pietrzykowski (red.), KC. Komentarz, Warszawa 1999
29. Z. Radwański: Prawo cywilne – część ogólna, Warszawa 1993.
30. J. Rafa: Amerykański zamach na Internet, Internet 3/96.
31. J. Rafa: Wolność słowa zwycięża w Internecie, Internet 8/96.
32. A. Rembieliński: Odpowiedzialność cywilna za szkodę wyrządzoną przez podwładnego, Warszawa 1971
33. S. Rudnicki: Ochrona dóbr osobistych na podstawie art. 23 i 24 k.c. w orzecznictwie Sądu Najwyższego w latach 1985 – 1991, "Przegląd Sądowy" nr 1/1992.
34. M. Safjan: Ochrona danych osobowych – granice autonomii informacyjnej, [w:] M. Wyrzykowski (red.): Ochrona danych osobowych, Warszawa 1999.
35. M. Sośniak, Bezprawność zachowania jako przesłanka odpowiedzialności cywilnej za czyny niedozwolone, Kraków 1959.
36. M. Sośniak: Funkcje i skuteczność zgody osoby uprawnionej w zakresie ochrony dóbr osobistych, [w:] Prace z prawa cywilnego, Ossolineum 1985
37. SMS FAQ: http://www.waw.pdi.net/~pawelk/smsfaq/
38. A. Szpunar: Nadużycie prawa podmiotowego, Polska Akademia Umiejętności, Kraków 1947.
39. A. Szpunar: Ochrona dóbr osobistych, Warszawa 1979.
40. A. Szpunar: Odpowiedzialność za szkodę wyrządzoną przez podwładnego [w:] Rozprawy z polskiego i europejskiego prawa prywatnego, Kraków 1994
41. A. Szpunar: Zadośćuczynienie za szkodę niemajątkową, Bydgoszcz 1999.
42. Tendencje rozwoju prawa cywilnego, (red.) E. Łętowska, Ossolineum 1983.
43. B. Węglarczyk: Wolność słowa czy przemocy, Gazeta Wyborcza 4 luty 1999.

44. A. Wojciechowska: Czy autorskie dobra osobiste są dobrami osobistymi prawa cywilnego?, „Kwartalnik Prawa Prywatnego" 1994, z.3.
45. S. Zembrzuski: Milion Polaków w sieci, Teleinfo 14/97.
46. A. Zoll: Prawo do krytyki a ochrona dóbr osobistych w prawie karnym [w:] Księga pamiątkowa ku czci prof. Natalii Gail, Trybunał Konstytucyjny - Wydawnictwa 1999.

Orzecznictwo:

1. Wyrok SN z dnia 12 lipca 1968 r. I CR 252/68 OSNC 1970/1/18 - z uzasadnieniem.
2. Wyrok SN z 19 września 1968 II CR 291/68. OSNCP 1969, poz. 200.
3. Wyrok SN z 29 października 1971, II CR 455/71, OSNC 1972/4/77
4. Uchwała SN z 30 grudnia 1971, III CZP 87/71, OSNC 1972/6/104.
5. Wyrok SN z 23 października 1973 II CR 557/73.
6. Wyrok SN z 16 stycznia 1976 r. II CR 692/75 OSNC 1976/11/251 - z uzasadnieniem
7. Wyrok SN z 5 maja 1977 r. IV CR 82/78.
8. Wyrok SN z 25 maja 1977 r., I CR 159/77
9. Wyrok SN z 28 grudnia 1978 I CR 424/78.
10. Wyrok SN z 25 października 1982 r., I CR 239/82, niepublikowane
11. Wyrok SN z 29 czerwca 1983 r., II CR 160/83, niepublikowane.
12. Wyrok SN z dnia 18 stycznia 1984 r, I CR 400/83 OSNC 1984/11/195.
13. Wyrok SN z 16 lipca 1984r., I PR 64/84, OSNC 1985/2-3/41
14. Wyrok SN z 14 listopada 1986 II CR 295/86 OSNC 1988/2-3/40
15. Wyrok SN z 17 marca 1988 r., IV CR 60/88, OSNC 1989/5/83
16. Wyrok SN z dnia 14 grudnia 1990 r. I CR 529/90 OSNC 1992/7-8/136 - z uzasadnieniem. Komentarz do wyroku W. Tabor: OG 1992/2 str. 8-11. Glosy: J Krauss, M. Modrzejewska, PUG 1991, nr 7, poz. 1 str. 122, R. Skubisz, PS 1992/11-12 str. 107-116.
17. Postanowienie SN z dnia 22 marca 1991 r. III CRN 28/91 niepublikowane.
18. Wyrok S.A. z 24 września 1992 r., I ACr 340/92, OSAiSN 1993/6 poz. 39.
19. Wyrok SA z 29 stycznia 1993 r. AG Cr 369/92, Wokanda 1993/9 p. 33.
20. Wyrok Sądu Apelacyjnego w Warszawie z 19 grudnia 1995 r. I ACR 1013/95; Orzecznictwo Sądów w sprawach Gospodarczych 1997/4 poz. 44.
21. Wyrok SA. z 15 marca 1996 r. I ACr 33/96, OSA 1996/7-8/31 - z uzasadnieniem
22. Wyrok SN z 10 stycznia 1997 r. II CKN 62/96, Wokanda 1997/4

23. Wyrok SA z 3 kwietnia 1997 r., I ACa 148/97, Wokanda 1998/4.

RFC:

1. RFC 822.
2. RFC 1521.
3. RFC 937.
4. RFC 1225.

9 AUTOR

Piotr Waglowski - dyrektor marketingu 3W Internet Marketing sp. z o.o. oraz redaktor naczelny serwisu marketingowego prowadzonego przez tę firmę. Założył pierwszą w Internecie polskojęzyczną listę dyskusyjną na temat prawa: prawo@plearn.bitnet (założona w marcu 1995, obecnie lista jest zamknięta, jednak dyskusja jest możliwa na WebForum funkcjonującym w ramach serwisu „VaGla.pl - Prawo i Internet"), prowadzi internetowy serwis poświęcony związkom prawa z Internetem: "VaGla.pl - Prawo i Internet" (serwis powstał w styczniu 1997 roku). Pełnił funkcje przewodniczącego Komisji Rewizyjnej, następnie Członka Zarządu Stowarzyszenia Studentów i Absolwentów Wydziału Prawa i Administracji Uniwersytetu Warszawskiego „PROCURA" oraz redaktora naczelnego Czasopisma Wydziału Prawa i Administracji Uniwersytetu Warszawskiego "Jurysta". Członek - założyciel ISOC Polska (Internet Society Poland: http://www.isoc.org.pl/) – obecnie Członek Zarządu tej organizacji. Autor wielu publikacji dotyczących głównie prawnych aspektów internetu oraz wykorzystania go w celach marketingowych.

http://www.vagla.pl