Spam a prawo – próba wskazania kierunków badawczych

Piotr Waglowski

Przyjmując za podstawową definicję *spamu* definicję wynikającą z praktyki, a zaproponowaną przez *Mail Abuse Prevention System*[1], należy zastanowić się, jakie mechanizmy prawne mogą mieć zastosowanie do oceny prawnej tego zjawiska. Innymi słowy: w jaki sposób zastosować istniejące lub powstające (a czasem dopiero postulowane) regulacje prawne do opisu zjawiska nowego i wciąż narastającego – zjawiska przesyłania niezamówionej informacji drogą elektroniczną.

Piotr Waglowski
Autor serwisu VaGla.pl Prawo i Internet, Członek Zarządu Internet Society Poland. Jest słuchaczem studiów doktoranckich prowadzonych w Instytucie Nauk Prawnych Polskiej Akademii Nauk. Pełni funkcję Głównego Konsultanta Polskiej Izby Informatyki i Telekomunikacji

Z punktu widzenia rozwoju systemów prawnych zjawisko nazwane *spamem*[2] jest zjawiskiem nowym. W 1999 roku Internet obchodził trzydziestolecie swoich „narodzin", zaś w roku 2001 świętowaliśmy 10 lecie powstania Internetu w Polsce. Można przyjąć, że pierwszym przejawem zjawiska *spamu* był list Einara Stefferuda w 1978 roku z zaproszeniem na swoje urodziny[3], wysłany do wszystkich użytkowników sieci Arpanet. Zjawisko to, w wymiarze komercyjnym, zaistniało na dobre za sprawą kancelarii prawnej prowadzonej przez Lawrence'a Cantera oraz Marthę Siegel z Phoenix w stanie Arizona[4] (USA) w 1994 roku.

Porównując daty – widać wyraźnie, iż w oblicz rozwoju prawa (nawiązującego do tradycji prawa rzymskiego i tradycji wcześniejszych systemów, a więc rozwijającego się przez tysiąclecia) – potrzeba objęcia regulacjami powszechnymi zjawiska przesyłania niechcianej informacji elektronicznej dopiero się rodzi. Podobnie jak rodzi się dopiero nowe społeczeństwo nazywane informacyjnym.

Trzeba również podkreślić, że wiele informacji na temat skali oraz mechanizmów związanych ze zjawiskiem *spamu* znaleźć można wyłącznie w Internecie[5], przy jednoczesnej znikomej ilości literatury tradycyjnej – stąd konieczność odwoływania się do tych, ulotnych dla wielu, źródeł internetowych. Stąd również wynika potrzeba prowadzenia systematycznych badań i publikacji tradycyjnych dotyczących opisywanego zjawiska. Nieocenionym źródłem są tu wyniki prowadzonych stale badań amerykańskiejFederalną Komisj i Handlu[6].

Spam dotyka coraz liczniejszych technik przesyłania informacji w Internecie. Rozwój technik komunikacyjnych powoduje pojawienie się *spamu* na innych niż tradycyjne (a więc poczta elektroniczna) platformach - w szczególności takich jak telefony komórkowe oraz płaszczyzny wymiany komunikatów (ICQ, polskie Gadu Gadu) i tzw. czatów (IRC). Można również mówić o *spamie* w serwisach www (ze względu na niezamawiane komunikaty otwierające się w „nowych oknach": *pop-up window*).

[1] Mail Abuse Prevention System, http://mail-abuse.org
[2] Spam - ang. konserwa mięsna, mielonka, a w żargonie internetowym: niechciana korespondencja, list wysłany wiele razy
[3] Jest dyskusyjne, która z niezamówionych wysyłek była pierwsza. W Internecie można znaleźć doniesienia, że pierwszym *spamem* było wysłanie w dniu 3 maja 1978 przez Gary'ego Thuerk'a informacji dotyczącej prezentacji nowego produktu w ofercie DEC (Digital Equipment Corporation). Por. http://www.templetons.com/brad/spamterm.html
[4] Kancelaria posłużyła się *spamem*, by zareklamować w 1994 roku swoje usługi wypełniania formularzy amerykańskiej loterii wizowej.
[5] np. P. Waglowski, Niektóre prawne aspekty spamu, VaGla.pl Prawo i Internet, luty 2001. Artykuł dostępny pod adresem: http://www.vagla.pl/skrypts/spam_prawo.htm
[6] Federal Trade Commission, http://www.ftc.gov

Zgodnie z definicją przyjmuje się, że informacja przesłana drogą elektroniczną jest *spamem*, jeśli jej treść jest niezależna od tożsamości odbiorcy (ta sama treść może być skierowana do wielu innych odbiorców), gdy jednocześnie odbiorca elektronicznej przesyłki nie wyraził uprzedniej (weryfikowalnej), świadomej, wyraźnej i możliwej do odwołania w każdej chwili zgody na otrzymanie przesyłki oraz gdy treść informacji przesłanej drogą elektroniczną daje odbiorcy podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść korzyści nieproporcjonalne w stosunku do korzyści odbiorcy wynikających z jej odebrania[7]. Wiele organizacji zajmujących się tworzeniem standardów postępowania w Internecie zajmowało stanowiska w sprawie tego zjawiska, w śród których należy szczególnie podkreślić stanowisko Internet Engineering Task Force, działającego w ramach Internet Society, zawarte w dokumencie RFC o numerze 2635[8], którym wyjaśnia się dlaczego *spam* jest zjawiskiem szkodliwym i często patologicznym.

Powszechnie również dzieli się *spam* na *Unsolicited Bulk Email (UBE)*, czyli niechciane informacje o charakterze niekomercyjnym (do tej kategorii można zaliczyć wspomniany wyżej list zapraszający na urodziny z 1978 roku), oraz *Unsolicited Commercial Email (UCE)*, czyli *spam* komercyjny o charakterze promocyjnym, reklamowym[9] (reklama kancelarii prawnej z 1994 roku, o której wyżej, stała się pierwszym przykładem takiego *spamu*).

Powstające w Polsce regulacje mają związek z procesem dostosowania polskiego systemu prawnego do regulacji obowiązujących w Unii Europejskiej. Tak było w przypadku implementowania dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej nr 2000/31 z dnia 8 czerwca 2000 r. (dyrektywa o handlu elektronicznym) oraz dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej nr 2002/58 z dnia 12 lipca 2002 r. (dyrektywa w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej), w wyniku którego doszło do uchwalenia polskiej ustawy z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym i praktycznie równolegle ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz.U. nr 144, poz.1024).

Wcześniej jednak Polska przyjęła inne regulacje, w szczególności ustawę z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. Nr 22, poz. 271), w której mowa jest o posłużeniu się nowoczesną technologią do złożenia propozycji zawarcia umowy z konsumentem. Przyjęcie tej ustawy również było wynikiem procesu dostosowawczego, w szczególności do regulacji znajdujących się w Dyrektywie Parlamentu Europejskiego i Rady 97/7/ WE w sprawie ochrony konsumentów w umowach zawieranych na odległość z dnia 20 maja 1997 r.

Biorąc za punkt wyjścia powyższe, istniejące już w Polsce regulacje dotyczące omawianego zjawiska, a także zasady ogólne (w szczególności dotyczące ochrony dóbr osobistych, zasady odpowiedzialności deliktowej czy kontraktowej znajdujące się w kodeksie cywilnym i inne), należy prowadzić prace badawcze, ze szczególnym naciskiem na ich interdyscyplinarny charakter. W szczególności zwrócić należy uwagę na związki problemu *spamu* z zarządzaniem, marketingiem oraz z informatyką. Niniejszy artykuł stanowi próbę wskazania podstawowych kierunków takich prac.

Definicje, trudności w określeniu pojęć

W pierwszej kolejności prace badawcze skoncentrować powinny się na używanych przez ustawodawcę definicjach i pojęciach[10]. Jak można przeczytać w uzasadnieniu do projektu ustawy o świadczeniu usług drogą elektroniczną: p*róba ujęcia normatywnego niektórych kwestii wiążących się z zastosowaniem technologii informatycznych do celów świadczenia powszechnie dostępnych usług polegających na przetwarzaniu informacji, napotyka niejednokrotnie na trudności w ścisłym określeniu niektórych pojęć wynikające, z jednej strony, z braku utrwalonej (także w warstwie językowej) terminologii prawniczej, a z drugiej z dynamicznego i wielostronnego rozwoju środków technicznych umożliwiających świadczenie tego rodzaju zaawansowanych usług właściwych dla społeczeństwa ery*

[7] Definition of "spam", Mail Abuse Prevention System, definicja dostępna w dniu 3 października 2003 roku pod adresem: http://mail-abuse.org/standard.html

[8] Request for Comments: 2635, DON'T SPEW, A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*), Internet Society,

[9] Spam, Z Wikipedii, wolnej encyklopedii. Hasło dostępne pod adresem: http://pl.wikipedia.org/wiki/Spam

[10] W. Majewski, P. Waglowski, Produkty czy standardy?, Computerworld nr 40/596, 4 listopada 2003

postindustrialnej - społeczeństwa informacyjnego[11]. Zdaniem autorów Raportu "Polska informatyka w Unii Europejskiej[12]": opracowanie zbioru podstawowych definicji prawnych jest kluczem do ujednolicenia ustawodawstwa dotyczącego teleinformatyki.

W przypadku *spamu*, podobnie jak innych zjawisk z pogranicza nowych technologii[13], należy postulować opracowanie spójnych definicji dotyczących takich pojęć jak: adres elektroniczny[14], system informatyczny oraz system teleinformatyczny[15], informacja elektroniczna, informacja handlowa[16], odbiorca informacji – użytkownik systemu - usługobiorca[17], dokument elektroniczny i inne...

Należy również rozważyć zakresy znaczeniowe pojęć szeroko rozumianego prawa reklamy, w szczególności wzajemne relacje znaczeniowe pomiędzy pojęciami takimi jak: marketing, reklama, promocja, informacja handlowa, sponsoring, public relations, etc. Jest to istotne ze względu na brak ogólnych definicji tych pojęć w polskim ustawodawstwie i nadawanie różnych znaczeń tym pojęciom na gruncie różnych regulacji[18].

Regulacje ustrojowe

Już na gruncie ustawy zasadniczej mamy do czynienia z pewnego rodzaju kolizją wartości godnych ochrony. W pierwszej kolejności należy 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 którego postawić można wolność 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.

Problematyka prawna *spamu* oceniana powinna być na gruncie konstytucyjnego zapisu, zgodnie z którym władze publiczne chronią konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu oraz nieuczciwymi praktykami rynkowymi. Wedle zapisu art. 76 konstytucji Rzeczpospolitej Polskiej - zakres tej ochrony określa ustawa.

Do kwestii podstawowych zaliczyłbym decyzję ustawodawcy o przyjęciu jednego z możliwych modeli zamawiania informacji handlowych (*opt-in* lub *opt-out*), ze wskazaniem na model *opt-in*, jaki powinien być jasno wprowadzony do polskich regulacji. Wedle tego modelu informacja (w tym informacja handlowa) może zostać rozesłana wyłącznie do osób, które wyraźnie wyrażą na to zgodę. Konkurencyjnym rozwiązaniem jest model *opt-out*, w którym użytkownik (odbiorca), bez świadomego przyzwolenia, otrzymuje inauguracyjny list (lub inną przesyłkę drogą elektroniczną) i jeśli nie chce więcej otrzymywać podobnych informacji lub informacji z danego źródła ma możliwość zrezygnowania z dalszych przesyłek. Jednak stosowanie reguły *opt-out* może doprowadzić do tego, że aktywni użytkownicy Internetu zmuszeni byliby wyrażać swój sprzeciw kilkadziesiąt razy dziennie.

[11] Druk sejmowy nr 409 z dnia 17 kwietnia 2002 roku. Druk dostępny pod adresem: http://ks.sejm.gov.pl:8010/proc4/opisy/409.htm

[12] Raport przygotowany w związku z pracami 3. Kongresu Informatyki Polskiej. W postaci elektronicznej dostępny pod adresem: http://www.kongres.org.pl/3KIP_raport.pdf

[13] W. Majewski, P. Waglowski, Produkty czy standardy?, op. cit.

[14] P. Waglowski, Adres elektroniczny [w] J. Kisielnicki, J. K. Grabara, J. S. Nowak (red.) Informatyka w gospodarce globalnej - problemy i metody. Wydawnictwa Naukowo-Techniczne, Warszawa-Szczyrk 2003, str. 469; Artykuł dostępny jest w postaci elektronicznej pod adresem: http://www.vagla.pl/skrypts/adres_elektroniczny.htm

[15] *Ibidem*.

[16] P. Waglowski, Informacja handlowa w komunikacji elektronicznej, Prawo i ekonomia w Telekomunikacji nr 3/2003 (lipiec- wrzesień) str. 26. Artykuł dostępny w postaci elektronicznej pod adresem: http://www.vagla.pl/skrypts/informacja_handlowa.htm

[17] Por. P. Waglowski, Spam w formie niezamówionej informacji handlowej jako delikt nieuczciwej konkurencji, Artykuł przygotowany na potrzeby konferencji naukowej "3rd International Interdisciplinary Conference on Electronic Commerce - ECOM-03", odbywającej się w dniach 16 - 18 października 2003 roku. Artykuł w postaci elektronicznej dostępny jest pod adresem: http://www.vagla.pl/skrypts/spam_delikt_nieuczciwej_konkurencji.pdf

[18] por. X. Konarski, Internet i prawo w praktyce, Warszawa 2002.

Działanie sprzeczne z dobrymi obyczajami lub zasadami współżycia społecznego
Na mocy art. 5 Kodeksu cywilnego nie można czynić ze swego prawa użytku, który by był sprzeczny ze społecznogospodarczym przeznaczeniem tego prawa lub z zasadami współżycia społecznego. Takie działanie lub zaniechanie uprawnionego nie jest uważane za wykonywanie prawa i nie korzysta z ochrony.

Klauzula odwołująca się do zasad współżycia oraz przeznaczenia społecznogospodarczego powoduje zwiększenie elastyczności systemu prawa. Prawodawcy wielu państw odwołują się również do zwyczaju (odwoływanie się do zwyczajów poszerza zakres norm prawnych ustanawianych w sposób formalny).

Można stawiać pytanie: czy owe zasady współżycia społecznego albo ustalone zwyczaje, o których wyżej, obejmują również *Netykietę*[19] – a więc nieformalne dokumenty w sposób jedynie „faktyczny" funkcjonujące w Internecie? Na świecie były już przypadki orzeczeń, w których się na nią powołano. Do klasycznych przykładów należy orzeczenie Sądu Prowincji Ontario (Kanada), który rozpoznawał sprawę z powództwa użytkownika przeciwko Nexx Online, dostawcy usług internetowych z Toronto. Dostawca usług internetowych zlikwidował konto użytkownika za wysyłanie *spamu*. Użytkownik pozwał Nexx w związku z zerwaniem umowy. ISP z kolei oskarżył tegoż użytkownika o łamanie warunków ww. umowy. Sąd wydał orzeczenie datowane na 9 lipca 1999 roku, w którym stwierdził, że jeśli umowa między dostawcą usług (*Internet service provider*) a użytkownikiem nie stanowi inaczej, masowe rozsyłanie niezamawianej, komercyjnej korespondencji elektronicznej łamie zasady zawarte w*netykiecie* .

Nie jest już rzeczą nową, że środowisko użytkowników Internetu jest środowiskiem specyficznym. W środowisku istnieją przyjęte (nowe i nieznajdujące odpowiedników poza Siecią) normy zachowań, zasady współżycia.

Spam jako delikt nieuczciwej konkurencji
Na gruncie przyjętych aktów normatywnych można rozważać problem niezamówionej informacji jako czynu nieuczciwej konkurencji[20]. W sposób naturalny regulacje te dotyczą zaledwie jednego z rodzajów *spamu* – tego, który ma charakter komercyjny, handlowy (*UCE*). Poza zakresem regulacji znalazły się wszelkie przesyłki niezwiązane z prowadzeniem działalności gospodarczej, co należy uznać za istotny problem, jeśli miałoby się przyjąć za podstawowe narzędzia w walce ze *spamem* ustawę o świadczeniu usług drogą elektroniczną oraz ustawę o zwalczaniu nieuczciwej konkurencji.

W tym miejscu należy również podkreślić ograniczony zakres podmiotów, którym przysługują roszczenia z tytułu czynu nieuczciwej konkurencji (przedsiębiorca, którego interes został zagrożony lub naruszony, krajowa lub regionalna organizacja, której celem statutowym jest ochrona interesów przedsiębiorców oraz Prezes Urzędu Ochrony Konkurencji i Konsumentów, jeżeli czyn nieuczciwej konkurencji zagraża lub narusza interesy konsumentów).

Równie istotnym zagadnieniem jest precyzyjne określenie modelu zamówienia informacji handlowej. Na pierwszy rzut oka wydaje się, że ustawodawca przyjął w przypadku informacji handlowej model opt-in (w którym odbiorca wyraźnie wyraża zgodę), jednak szczegółowa analiza[21] regulacji może doprowadzić do wniosku, że w niektórych przypadkach dopuszczalne jest uznanie milczenia za wyrażenie zgody – a więc w efekcie można by mówić o modelu *opt-out* (umożliwiającym zrezygnowanie z otrzymywania) jako tego, który udało się w ustawie o świadczeniu usług drogą elektroniczną przyjąć.

Zakazy reklamy
Mówiąc o informacji handlowej należy podkreślić, że szereg przepisów szczególnych wprowadza zakazy lub ograniczenia dotyczące reklamowania lub promowania w inny sposób określonych produktów lub usług. W polskim systemie prawnym brak jest jednolitej definicji pojęcia reklamy[22],

[19] Por. R. Chmura, Kodeks Internetu [w] R. Skubisz (red.) Internet 2000, prawo – ekonomia – kultura, Lublin 2000, str. 460.
[20] Por. P. Waglowski, Spam w formie niezamówionej informacji handlowej... *op. cit*.
[21] *Ibidem*
[22] X. Konarski, Internet i prawo w praktyce, op. cit. Str. 135

promocji czy sponsoringu. Poszczególne ustawy operują, co prawda, tymi pojęciami, jednak pojęcia te można stosować tylko na gruncie konkretnej ustawy.

Polskie prawo reklamy zna szereg zakazów i ograniczeń reklamy, które w szczególności dotyczą leków[23], alkoholu[24], produktów tytoniowych[25] czy działalności osób wykonujących zawody takie, jak adwokat czy radca prawny. Do działalności reklamowej czy promocyjnej prowadzonej w Internecie można stosować przepisy ustawy o radiofonii i telewizji w takim zakresie, w jakim program radiowy czy telewizyjny rozpowszechniany jest za pomocą Internetu[26].

Biorąc pod uwagę potencjalnie międzynarodowy charakter prowadzenia omawianej działalności (wysyłanie niezamówionej informacji drogą elektroniczną) należy zbadać istniejące w innych krajach zakazy lub ograniczenia reklamy, również te, które wynikają z umów międzynarodowych. Należy również rozważyć wzajemne relacje pomiędzy takimi pojęciami jak reklama, promocja czy sponsoring definiowanymi na gruncie różnych ustaw.

Spam jako naruszenie dóbr osobistych

Mówiąc o naruszeniu dóbr osobistych przez *spaming* należy rozważyć przynajmniej dwa rodzaje sytuacji: zakładające ujęcie *spamu* w makroskali i w z perspektywy pojedynczego odbiorcy. W skali *makro* może naruszać szereg dóbr osobistych - zarówno osób fizycznych jak i osób prawnych.

Dobra osobiste osób prawnych *spam* naruszać może w ten sposób, że blokuje ich systemy informatyczne uniemożliwiając komunikowanie się ich pracowników lub klientów (niemożność przyjmowania jakiejkolwiek poczty elektronicznej, a nawet niemożność zalogowania - dostania się - na konto). Wedle orzecznictwa dobra osobiste osób prawnych to wartości niemajątkowe, dzięki którym osoba prawna może funkcjonować zgodnie ze swym zakresem działań[27]. Otrzymanie dużej porcji *spamu* może powodować sytuacje, w których utrudniona będzie możliwość funkcjonowania osoby prawnej. Sam fakt, że poprzez otwarty *„relay"* (serwer przekazujący pocztę) przeszła duża porcja *spamu* może naruszać dobra osobiste dostawcy usług internetowych, gdyż może tu być zagrożone jego dobre imię, reputacja czy renoma. Nieumiejętne skonfigurowanie serwera pocztowego można jednak oceniać w kategoriach paremii: chcącemu nie dzieje się krzywda.

Spam (zarówno komercyjny jak i niekomercyjny) z punktu widzenia pojedynczego użytkownika, posiadacza skrzynki pocztowej, jest znaczącym utrudnieniem funkcjonowania[28], zwłaszcza w przypadku osób aktywnie wykorzystujących Internet. Można tu mówić o naruszeniu dóbr osobistych takich jak prawo do rozpowszechniania i pozyskiwania informacji (naruszone przez zablokowanie możliwości korzystania ze skrzynki pocztowej), poszanowanie prywatności czy zdrowie psychiczne[29]. Ostanie badania nad *spamem* wykazują coraz częstszą praktykę wykorzystywania tzw. kradzieży tożsamości (*identity theft),* lub podawania nieprawdziwych i nieistniejących danych. Przesyłanie niezamówionej elektronicznej korespondencji w „cudzym imieniu", lub tylko z wykorzystaniem „cudzej nazwy"[30] ma na celu bądź zdyskredytowanie adresu prawowitego dysponenta[31], bądź ominięcie filtrów antyspamowych ze względu na to, że dana domena (adres) dotychczasowo w nich „nie funkcjonowała". W takich przypadkach można mówić o naruszeniu dobra osobistego w postaci prawa

[23] Ustawa z dnia 6 września 2001 r. Prawo farmaceutyczne (Dz. U. Z 2001 r. Nr 126, poz. 1381)

[24] Ustawa z dnia 26 października 1982 roku o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (tj. Dz. U. z 2002 r. Nr 147, poz. 1231 z póz. zm.)

[25] Ustawa z dnia 9 listopada 1995 roku o ochronie zdrowia przed następstwami używania tytoniu i wyrobów tytoniowych (Dz. U. z 1996 r. Nr 10, poz. 55 z póz. zm.)

[26] X. Konarski, Internet i prawo w praktyce, op. cit.

[27] 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

[28] Z racji prowadzenia serwisu internetowego oraz aktywnego uczestnictwa w dyskusjach na grupach Usenetu, przed zastosowaniem restrykcyjnych filtrów blokujących autor otrzymywał ponad 400 niezamawianych przesyłek dziennie.

[29] Prawo do poszanowania spokoju, zakaz immisji, etc...

[30] W przypadku fałszowania prawdziwego nadawcy nie koniecznie musi nastąpić *„kradzież tożsamości*", np. w przypadku, gdy przesyłka wykorzystuje dane nieistniejącego nadawcy.

[31] J*oe-Job - spam* sfałszowany w taki sposób, by wyglądał na wysyłany przez niewinnego w rzeczywistości nadawcę, który zazwyczaj jest „zasypywany" zwrotami niedoręczonych wiadomości; akt rozsyłania tego typu przesyłek. Por. http://nospam-pl.net/joe-job.php

do nazwiska czy pseudonimu (w przypadku osób fizycznych) lub do nazwy (w przypadku osób prawnych). Dodatkowo naraża to prawowitego dysponenta danego adresu na wpis w listach antyspamowych, a co za tym idzie – utrudnienia w komunikowaniu się.

W kontekście *spamu* można pokusić się o stworzenie nowego dobra osobistego opartego na koncepcji nietykalności mieszkania - analogia mogłaby polegać na objęciu ochroną serwerów internetowych jako swoistego "miejsca" w Sieci (mir serwera)[32].

Procesy dotyczące ochrony dóbr osobistych toczą się latami. Wobec skali zjawiska i szybkości z jaką zmieniają się sytuacje faktyczne w Internecie, konieczne jest poszukiwanie mechanizmów pozwalających na szybszą i skuteczną reakcję na zaistniałe zdarzenia.

Odpowiedzialność deliktowa

W 2003 roku firma Ferris Research[33] opublikowała raport zatytułowany „Spam Control: Problems and Opportunities"[34], wedle którego, przez zjawisko *spamu* firmy amerykańskie ponoszą straty w wysokości 8.9 miliarda dolarów rocznie. Wedle tego samego raportu – firmy europejskie ponoszą rocznie straty w wysokości 2,5 miliarda dolarów[35]. Firma Ferris Research szacowała, że 4,4 miliarda dolarów rocznie kosztuje użytkowników Internetu czas tracony na kasowanie *spamu*, a 3,7 miliarda dolarów rocznie wynoszą koszty dodatkowej mocy serwerów, koniecznej do obsługi niezamówionych, masowych przesyłek oraz koszty ponoszone dodatkowo na dzierżawę łącz internetowych.

Widać z tego, że można mówić o odpowiedzialności za realną szkodę wyrządzoną przez wysyłanie *spamu*. Ze względu na generalną klauzulę znajdującą się w art. 415 kodeksu cywilnego można oceniać *spam* na gruncie ogólnych zasad odpowiedzialności odszkodowawczej. Powstaje jednak problem z określeniem wysokości szkody w konkretnym przypadku, a także często ze wskazaniem podmiotu odpowiedzialnego (podmiotu wysyłającego – ze względu na np. praktykę „kradzieży tożsamości", o której wyżej), a także związku przyczynowego pomiędzy wysłaniem konkretnej przesyłki i zaistniałą szkodą. Przewidziana w art. 415 kc odpowiedzialność za czyn własny oparta jest na zasadzie winy.

Należy rozważyć, czy dostawca usług lub użytkownik, który nie zabezpieczył w sposób odpowiedni systemu przed otrzymywaniem lub wysyłaniem (np. komputery *zombie*[36]) niezamówionych przesyłek, może odpowiadać na zasadach ogólnych, na przykład za niewłaściwe (niedbałe) "administrowanie" daną usługą (niezastosowanie standardowych w danej dziedzinie zabezpieczeń sprzętowych lub oprogramowania), w tym nieumiejętną konfigurację (*open relay*) lub za zastosowanie niewłaściwego systemu zmiany haseł, udostępnienie haseł pozwalających na wniknięcie do systemu informatycznego przez osoby nieupoważnione, etc., dzięki czemu ktoś (osoba „anonimowa") dopuściła się deliktu.

Odrębnego opracowania wymagają sytuacje, w których dostawca lub użytkownik powierzył wykonanie pewnych czynności innym podmiotom. Może to polegać w szczególności na powierzeniu administracji daną usługą osobie trzeciej (np. przekazanie hasła *roota*). Jak się wydaje użytkownik będzie ponosił odpowiedzialność w takim przypadku, 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 kc). Anonimowość bezpośredniego sprawcy szkody wyłącza możliwość skutecznej ekskulpacji[37] .

[32] P. Waglowski, Niektóre prawne aspekty spamu, op. cit.
[33] Ferris Research, http://www.ferris.com
[34] Spam Control: Problems and Opportunities, Ferris Research, Raport w dniu 3 października 2003 roku dostępny dla subskrybentów pod adresem: http://www.ferris.com/rep/200301/SM.html; Przytoczone dane za serwisem abcNews.com: http://abcnews.go.com/wire/Business/ap20030104_1508.html
[35] Podobne dane wynikają z raportu przedstawionego przez Erkki Liikanena, Europejskiego Komisarza ds. Rozwoju Społeczeństwa Informacyjnego w dniu 15 lipca 2003 roku. Z raportu wynika również, że szacowano, iż do końca roku ponad 50% wszystkich przesyłek poczty elektronicznej stanowić będzie spam. Komisarz uznawał w swoim raporcie za spam wyłącznie przesyłki o charakterze komercyjnym (*unsolicited commercial e-mail*).
[36] Komputer, nad którym ktoś w sposób nieuprawniony przejął kontrolę i wykorzystuje go bez zgody i wiedzy użytkownika.
[37] M. Safjan: art. 429, Nb. 13 [w:] K. Pietrzykowski (red.), KC. Komentarz, Warszawa 1999.

Wydając jedną z decyzji Urząd Ochrony Konkurencji i Konsumentów[38] stwierdził, że bez znaczenia jest fakt, że nadawcą oferty przesłanej drogą elektroniczną jest inny podmiot skoro działał na zlecenie przedsiębiorcy. UOKiK zauważył, że wobec braku klauzuli umownej, wedle której przyjmujący zlecenie działałby we własnym imieniu (taką możliwość przewiduje art. 734 § 2 kc) – obowiązuje domniemanie, że czynność prawna dokonywana jest w imieniu dającego zlecenie.

Odpowiedzialność kontraktowa
Niezwykle istotnym problemem jest określenie wzajemnych relacji umownych pomiędzy przedsiębiorcą oferującym usługi internetowe (*ISP*[39]) a jego klientem. Tego typu umowy, w szczególności zawierające klauzule związane z warunkami korzystania z kont poczty elektronicznej, będą miały istotne znaczenie dla określenia odpowiedzialności stron w przypadku np. wysłania niezamówionej informacji elektronicznej lub w przypadku niedopuszczenia przesyłek nadchodzących do adresata, lub nawet utracie przesyłek w wyniku działań wynikających z administrowania serwerem pocztowym.

W przypadku takich umów odpowiedzialność wzajemną stron należy oceniać na gruncie odpowiedzialności kontraktowej (art. 471 kc i następne). W szczególności strona będzie zobowiązana do naprawienia szkody, która wynikła z niewykonania lub nienależytego wykonania zobowiązania, chyba że wykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi.

Jeśli chodzi o relacje pomiędzy użytkownikiem a firmą oferującą konta poczty elektronicznej warto wspomnieć, że szwedzki operator TeliaSonera zapowiedział blokowanie dostępu do Internetu klientom, którzy rozsyłają *spam*. Szwedzka firma jest pierwszym europejskim dostawcą Internetu, który zdecydował się na podobny krok[40].

Możliwość blokowania przesyłek elektronicznych
Sposoby korzystania z poczty elektronicznej zmieniają się wraz z rozwojem Internetu. Obecnie coraz powszechniejsze staje się blokowanie przesyłek kierowanych na dany adres poczty elektronicznej, jeśli pochodzą z określonych adresów lub zostały przesłane z określonej maszyny lub określonej klasy numerów IP. Coraz częściej stosuje się tzw. *whitelist* – listy adresów, z których korespondencja jest odbierana, przy jednoczesnym uniemożliwieniu odebrania korespondencji innej.

Biorąc pod uwagę zapisy konstytucyjne - każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji – należy stwierdzić, że blokowanie otrzymywania poczty elektronicznej można uznać za wykonywanie prawa podmiotowego dysponenta skrzynki pocztowej[41]. Jak na razie nie istnieje normatywny obowiązek posiadania prywatnego adresu poczty elektronicznej, a tym samym nie ma podstaw by twierdzić, że świadome blokowanie otrzymywania listów elektronicznych jest naruszeniem obowiązującego prawa.

Wątpliwości pojawiają się w przypadku poczty elektronicznej, która nie jest pocztą prywatną. Art. 63. Konstytucji Rzeczpospolitej Polskiej przewiduje, ze każdy ma prawo składać petycje, wnioski i skargi w interesie publicznym, własnym lub innej osoby za jej zgodą do organów władzy publicznej oraz do organizacji i instytucji społecznych w związku z wykonywanymi przez nie zadaniami zleconymi z zakresu administracji publicznej. Petycje, wnioski i skargi można składać za pomocą elektronicznych środków komunikacji, zatem organy, o których mowa w cytowanym przepisie nawet nie mogą stosować (co do zasady) narzędzi blokujących taką korespondencję kierowaną na określone adresy.

Problem rozwoju technologicznego i wynikające z niego możliwości naruszenia prywatności doprowadził w USA do powstania listy numerów telefonicznych Do-Not-Call[42]. Powstanie listy

[38] W dniu 30 września 2003 roku Delegatura Urzędu Ochrony Konsumentów i Konkurencji w Lublinie wydała decyzję o sygnaturze: RLU Nr 29/03
[39] ISP – ang. skrót od *Internet Service Provider*
[40] Szwecja: Rozsyłacze spamu będą odcinani od Internetu, Serwis Gazety Wyborczej, artykuł dostępny pod adresem: http://www1.gazeta.pl/gospodarka/1,33181,1760752.html
[41] P. Waglowski, Pozyskiwanie vs. rozpowszechnianie, VaGla.pl Prawo i Interent. Felieton dostępny pod adresem http://www.vagla.pl/felietony/felieton_003.htm
[42] National Do Not Call Registry: http://www.ftc.gov/bcp/conline/edcams/donotcall/

uzasadnione jest coraz bardziej natarczywymi praktykami telemarketerów. Umieszczenie numeru w tym rejestrze jest bezpłatne. Jeśli po umieszczeniu numeru telefonu w rejestrze będzie on wykorzystany w działalności marketingu bezpośredniego, grozi za to grzywna do 11 tysięcy dolarów za jeden telefon. Być może warto postulować stworzenie podobnych list zawierających adresy poczty elektronicznej? Niebezpieczeństwo jednak polega na tym, że nieuczciwi marketerzy otrzymaliby listę prawdziwych adresów poczty elektronicznej „gotową do użycia".

Prowadzenie systemów listujących

Wobec narastającego problemu *spamu* powstają liczne serwisy[43] oferujące bądź listę adresów poczty elektronicznej, z której nastąpiła wysyłka niezamówionej elektronicznej korespondencji, bądź tzw. RBL'e[44] – wskazujące numery IP komputerów, o których wiadomo, że służyły do wysłania *spamu*, bądź numery komputerów, które potencjalnie mogą służyć do wysyłania *spamu* (np. ze względu na konfigurację[45]). Istnieją również metody, które wykorzystując adresy poczty elektronicznej szyfrują je w sposób trudny do odszyfrowania. Ten mechanizm może być wykorzystany do porównywania pewnych wpisów: inny tekst należy zakodować tą samą metodą i sprawdzić występowanie tak powstałego skrótu we wcześniej posiadanej liście[46]. Inna metoda może polegać na wpisaniu na listę nazw domen internetowych. Metody blokowania przesyłek wciąż się rozwijają, zaś niektóre metody obejścia blokowania zostały już opatentowane[47].

Powstaje problem, czy prowadzenie takich list nie stanowi naruszenia ustawy o ochronie danych osobowych. Wątpliwość wynika z możliwości uznania adresu poczty elektronicznej za dane osobowe i w związku z tym przetwarzanie takich danych (adresów poczty elektronicznej) w zbiorach – udostępnionych w różnych postaciach w Internecie. Nie będzie tak w przypadku, gdy na liście nie występują w ogóle dane osobowe (np. przypadku listowania nazw domen internetowych czy numerów IP konkretnych maszyn lub całych klas).

Wysyłanie niezamówionej informacji handlowej drogą elektroniczną jest wykroczeniem na mocy art. 24 ustawy o świadczeniu usług drogą elektroniczną. Rozważyć zatem należy, czy w określonych przypadkach nie będzie miał zastosowania art. 13 ust. 2 prawa prasowego, który wprowadza zakaz publikowania w prasie danych osobowych i wizerunku osób, przeciwko którym toczy się postępowanie przygotowawcze lub sądowe, jak również danych osobowych i wizerunku świadków, pokrzywdzonych i poszkodowanych, chyba że osoby te wyrażą na to zgodę. W pierwszej kolejności jednak należy wskazać czy i w jakich przypadkach Internet można uznać za prasę w rozumieniu prawa prasowego.

Jak się wydaje umieszczenie w systemie umożliwiającym „blokowanie" niezamówionej korespondencji z danego adresu poczty elektronicznej czy określonych numerów IP czy domen może stanowić naruszenie lub zagrożenie dóbr osobistych określonych podmiotów. Należy rozważyć, czy nie zachodzi w niektórych przypadkach brak bezprawności działania, w szczególności ze względu na ochronę godnego do ochrony interesu publicznego?

Ochrona publicznoprawna

Mimo istnienia odpowiednich unormowań dotyczących prywatnoprawnej ochrony przed *spamem* mogą okazać się one niewystarczające. Być może konieczne jest położenie większego nacisku na niedopuszczenie do naruszeń godnych ochrony Internetów poszczególnych podmiotów (zarówno osób fizycznych jak i prawnych a także takich jak organy władzy publicznej, organizacje nie posiadające osobowości prawnej) w Internecie, a mniejszego na usunięcie jego skutków. Dlatego należy rozważyć, czy środki publicznoprawne (administracyjnoprawne) nie byłyby lepszymi jako podstawowy oręż ochrony tych interesów w nowym społeczeństwie, w społeczeństwie informacyjnym.

[43] Spamhaus (http://spamhaus.org/), Spamcop (http://spamcop.net/), czy SPEWS (http://spews.org/). Polskie serwisy reprezentowane są przez http://spam.wytnij.to czy zamknięty ostatnio serwis PolSpam.

[44] RBL – ang. skrót od *Realtime Block List*

[45] *Open relay*, *Open proxy*

[46] Ł. Kozicki, Baza do blokowania spamu bez "danych osobowych", Serwis Nospam-pl.net. Artykuł dostępny pod adresem: http://nospam-pl.net/baza-adresow.php

[47] US Patent No. 6,643,686, „*A system and method for circumventing schemes that use duplication detection to detect and block unsolicited e-mail (spam.)*"

Istnieje jednak pewne niebezpieczeństwo, gdyż w takiej sytuacji, to nie jednostka będzie decydować o zakresie ochrony jej dóbr, a twórcy prawa, którzy za nią podejmą wyprzedzające decyzje[48].

Ochrona konsumentów

Jak powiedziano wyżej prywatnoprawna ochrona przed *spamem* może okazać się niewystarczająca. Na uwagę zasługuje, wydana w dniu 30 września 2003 roku decyzja Delegatury Urzędu Ochrony Konsumentów i Konkurencji w Lublinie o sygnaturze: RLU Nr 29/03, w której stwierdza się, że po przeprowadzeniu postępowania antymonopolowego wszczętego z urzędu, działając w imieniu Prezesa Urzędu Ochrony Konkurencji i Konsumentów: uznaje się za praktykę naruszającą zbiorowe interesy konsumentów, godzące w nie bezprawne działania przedsiębiorcy prowadzącego określoną firmę (a więc działania, o których mowa w art. 23 a ust. 1 ustawy z dnia 15 grudnia 2000 roku o ochronie konkurencji i konsumentów) polegające na "*nadsyłaniu na e-mailowe adresy użytkowników skrzynek elektronicznych wykupionych w płatnych sieciach niezamówionych ofert - reklam handlowych*".

Na gruncie art. 23a ust. 2 ustawy z dnia 15 grudnia 2000 roku o ochronie konkurencji i konsumentów za praktykę naruszającą zbiorowe interesy konsumentów uważa się w szczególności stosowanie postanowień wzorców umów, które zostały wpisane do rejestru postanowień wzorców umowy uznanych za niedozwolone (o którym mowa w art. 47945 Kodeksu postępowania cywilnego), naruszanie obowiązku udzielania konsumentom rzetelnej, prawdziwej i pełnej informacji, nieuczciwą lub wprowadzającą w błąd reklamę i inne czyny nieuczciwej konkurencji godzące w zbiorowe interesy konsumentów.

Ochrona zbiorowych interesów konsumentów przewidziana w powyższej ustawie nie wyłącza ochrony wynikającej z innych ustaw, w szczególności z przepisów o zwalczaniu nieuczciwej konkurencji. Stanowić może zatem ich istotne uzupełnienie, jednak w tym przypadku również ochrona dotyczy jedynie niewielkiego wycinka *spamu*, gdyż pod pojęciem praktyki naruszającej zbiorowe interesy konsumentów rozumie się godzące w nie bezprawne działanie przedsiębiorcy. Znów możemy więc mówić o narzędziu prawnym chroniącym w pewien sposób przed spamem typu *UCE*.

Dla interpretacji zjawiska *spamu* nie bez znaczenie jest regulacja znajdująca się we wspomnianej wyżej, ustawie z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. Nr 22, poz. 271), która wprowadza wymóg, by posłużenie się telefonem, wizjofonem, telefaksem, pocztą elektroniczną, automatycznym urządzeniem wywołującym lub innym środkiem komunikacji elektronicznej w celu złożenia propozycji zawarcia umowy mogło nastąpić wyłącznie za uprzednią zgodą konsumenta.

Ochrona danych osobowych

Co już zasygnalizowano wyżej - poszukując możliwości publicznoprawnej ochrony przed *spamem* należy rozważyć jakie narzędzia tej ochrony przewidziane są w ustawie o ochronie danych osobowych. W pierwszej kolejności należy rozważyć czy i w jakich okolicznościach adres poczty elektronicznej będzie mógł zostać uznany za dane osobowe.

Istnieje w tej sprawie stanowisko Dyrektora Departamentu Prawnego GIODO[49], w którym powołując się na art. 18 ust. 1 ustawy o świadczeniu usług drogą elektroniczną dochodzi on do wniosku, że wolą ustawodawcy było zaliczenie takich informacji jak adres e-mail, w poczet danych osobowych. Przedstawiciel GIODO zauważa, że adres elektroniczny został wymieniony w katalogu, w którym wskazano dane osobowe, jakie mogą być przetwarzane przez usługodawcę w związku ze świadczeniem usług drogą elektroniczną. Biorąc powyższe pod uwagę Dyrektor Departamentu Prawnego GIODO stwierdza, iż adres e-mail stanowi daną osobową i podlega ochronie przewidzianej w przepisach o ochronie danych osobowych.

Z tak przedstawionym stanowiskiem warto się nie zgodzić. Otóż wedle definicji znajdującej się w ustawie o świadczeniu usług drogą elektroniczną adres elektroniczny to oznaczenie systemu teleinformatycznego, zatem nie może bezpośrednio identyfikować określonej osoby. Można pośrednio (ale nie w każdym przypadku) określić krąg osób fizycznych, które korzystają z danego adresu poczty

[48] M. Safjan: Ochrona danych osobowych - granice autonomii informacyjnej, [w:] M. Wyrzykowski (red.): Ochrona danych osobowych, Warszawa 1999.
[49] Pismo z GIODO dostępne jest pod adresem: http://nospam-pl.net/pub/giodo_email.pdf

elektronicznej. Jednak wobec faktu, że z jednego adresu poczty elektronicznej może korzystać więcej niż jedna osoba (np. jak to bywa w praktyce np. z adresem redakcja@nazwa.gazety) oraz wskazując niektóre adresy poczty elektronicznej, służące do wydawania poleceń systemowi teleinformatycznemu (np. adres poczty elektronicznej obsługujący listę dyskusyjną) należy zrewidować stanowcze stwierdzenie, iż każdy adres poczty elektronicznej jest daną osobową. Jednocześnie należy zauważyć, że jeśli na tle całokształtu zebranych informacji (w tym dotyczących adresu poczty elektronicznej) „wiadomo o kogo chodzi" – to wówczas należałoby uznać adres poczty elektronicznej za jedną z danych osobowych[50]. Problem ten jest kluczowy i powinien być przedmiotem odrębnego opracowania[51].

Praktyka zbierania, przetwarzania i sprzedaży baz danych zawierających adresy poczty elektronicznej, wykorzystywanych następnie do rozsyłania niezamówionych przesyłek elektronicznych (w tym handlowych) może być uznana za naruszenie ww. ustawy.

Marketing polityczny
Internet stał się wygodnym narzędziem do prowadzenia marketingu politycznego, wykorzystywanego np. w celu promocji kandydata, lub w celu zdobywania poparcia dla partii politycznej lub sprawy[52].

Przy okazji tego tematu warto odnotować wyrok Europejskiego Trybunału Praw Człowieka w sprawie "VGT kontra Szwajcaria", w którym Trybunał uznał, że obowiązujący w Szwajcarii zakaz reklamy politycznej należy uznać za pogwałcenie art. 10 Europejskiej Konwencji Praw Człowieka, gdyż zakaz taki nie jest "konieczny w społeczeństwie demokratycznym". Trybunał nie wykluczył, że w pewnych okolicznościach zakaz taki może być zgodny z art. 10. W kilku krajach obowiązuje zakaz płatnej reklamy politycznej, ponieważ jednak Konwencja nie odnosi się do sprawy reklamy politycznej, Trybunał nie zajął się tą sprawą, uznając, że powinna ona być rozstrzygana na poziomie krajowym.

Odrębnym polem badawczym będzie możliwość wykorzystania Internetu do promocji kandydatów lub określonych spraw w kampanii wyborczej oraz w czasie ciszy przedwyborczej[53].

Transgraniczność internetu
Internet jest medium międzynarodowym, transgranicznym. Ważne jest zatem badanie działalności polegających na wysyłaniu *spamu* z poza granic Polski, w szczególności rozważając sytuacje w których, dla przykładu, osoba wysyłająca znajdować się będzie poza granicami kraju podobnie jak system teleinformatyczny, dzięki któremu *spam* mógł zostać rozesłany,

Wskazówkę jak należy traktować spam prowadzony z zagranicy daje ustawa z dnia 12 listopada 1965 r. Prawo prywatne międzynarodowe, którego art. 31. § 1. stwierdza, iż zobowiązanie nie wynikające z czynności prawnej podlega prawu państwa, w którym nastąpiło zdarzenie będące źródłem zobowiązania.

Rozważania należy prowadzić zarówno na podstawie obowiązujących przepisów polskiej ustawy Prawo międzynarodowe prywatne, jak i ustawy o języku polskim i innych. Należy również przeprowadzić badania regulacji dotyczących omawianej problematyki obowiązujących w innych krajach[54].

Wykroczenie (spam komercyjny)
Na podstawie art. 24 ust. 1 ustawy o świadczeniu usług drogą elektroniczną ten kto przesyła za pomocą środków komunikacji elektronicznej niezamówione informacje handlowe, podlega karze

[50] por. P. Fajgielski, Ochrona danych osobowych w telekomunikacji – aspekty prawne, Lublin 2003, str. 223
[51] Odnośnie problematyki dotyczącej procedury związanej z ochroną danych osobowych: por. G. Sibiga, Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003.
[52] W. Cwalina, Marketing polityczny w Internecie, [w] R. Skubisz (red.) Internet 2000. Prawo - ekonomia - kultura. Lublin 2000.
[53] por. P. Waglowski, Twój wybór z internetowej perspektywy, sierpień 2000. Artykuł w postaci elektronicznej dostępny jest pod adresem: http://www.vagla.pl/skrypts/wybory.htm
[54] Omówienie regulacji dotyczących tej problematyki w krajach europejskich można znaleźć pod adresem http://www.euro.cauce.org/en/countries/, omówienie prawa dotyczącego *spamu* w USA i w innych krajach dostępne jest pod adresem http://www.spamlaws.com/

grzywny. Ściganie tego wykroczenia następuje na wniosek pokrzywdzonego. Ten sposób ochrony może mieć zastosowanie jedynie w stosunku do przesyłek o charakterze handlowym.

Przy wielu wątpliwościach dotyczących regulacji ustawowej (m.in. kłopoty z interpretacją podstawowych definicji i pojęć) – trzeba pamiętać, że za przesłanie niezamówionej informacji handlowej grozi grzywna w wysokości do 5 tys. złotych. Z podstawowych zasad polskiego prawa karnego wynika, że za jeden czyn grozi jedna kara. A zatem za jednorazowe wysłanie *spamu* (nawet jeśli kierowany był na kilka milionów adresów elektronicznych) grozi jedna grzywna.

Dla porównania – ze względu na możliwość uzależnienia orzekanej grzywny od ilości przesyłek - można przytoczyć orzeczenie sądu w Kalifornii (USA) który ukarał dwoje właścicieli firmy marketingowej PW Marketing z Los Angeles County grzywną w wysokości dwóch mln dolarów za wysyłanie niezamówionej informacji elektronicznej. Wyrok został wydany na podstawie prawa stanowego z 1998 roku. Sąd wydał wyrok, gdyż w przysyłanych listach nie znalazł numeru bezpłatego telefonu, pod który można zadzwonić i zrezygnować z dalszych reklam. Sąd nie znalazł również prawidłowego adresu zwrotnego do firmy.

Szóstego listopada 2003 roku przed Sądem Rejonowym w Białej Podlaskiej, Wydział VII Grodzki odbyła się pierwsza rozprawa sądowa przeciwko Andrzejowi J., obwinionemu przez Komendę Miejską Policji w Białej Podlaskiej o to, że w dniu 27 maja 2003 roku nadesłał w imieniu Centrum Promocji Informatyki spółki z ograniczoną odpowiedzialnością z siedzibą w Warszawie na adres poczty elektronicznej pokrzywdzonego niezamówioną informacje handlową[55]. Sąd uniewinnił obwinionego od zarzucanego mu czynu, gdyż sankcja przewidziana za wykroczenie z art. 24 ust. 1 ustawy dotyczy jedynie tej osoby, która niezamówioną informację przesyła. W tym przypadku osobą tą była pracująca na zlecenie obwinionego studentka. W konsekwencji wyroku sądu - pokrzywdzony złożył wniosek o ukaranie wspomnianej studentki.

Przestępstwo wyłączenia usługi (DDoS[56])
Jedną z form ataku na system informatyczny może być atak typu DDoS, polegający na uniemożliwieniu pracy systemu lub jego części. Bez wątpienia przesłanie olbrzymiej ilości przesyłek elektronicznych można rozpatrywać w kontekście tego rodzaju ataku. Należy zatem badać *spam* w kontekście przestępstw przeciwko systemom komputerowym.

Problem jest realny i aktualny również w Polsce: niedawno, przy okazji dyskusji na temat stawki VAT na usługi świadczenia dostępu do Internetu, grupa polityków lansowała osobliwą formę protestu, polegającą na „zalaniu" skrzynek poczty elektronicznej niektórych urzędników państwowych specjalnie przygotowanymi listami[57].

To zagadnienie należy również rozważyć w kontekście działania wszelkiego rodzaju wirusów i robaków komputerowych, które przesyłają swoje kopie za pomocą poczty elektronicznej, a które mogą doprowadzić do uniemożliwienia korzystania z zaatakowanego systemu komputerowego[58].

Rozpowszechnianie wirusów
Wirusy komputerowe, robaki internetowe czy konie trojańskie[59] rozsyłające swoje kopie za pomocą poczty elektronicznej są coraz poważniejszym problemem. Przyjęło się by rozważać ich tworzenie i działanie na gruncie prawa karnego[60]. Poza regulacjami prawnokarnymi (takimi jak polski kodeks

[55] Relacja z rozprawy dostępna jest pod adresem: http://polspam.com/cpi-relacja.html
[56] *Distributed Denial of Service* – jedna z form przeprowadzenia ataku na system komputerowy polegająca na uniemożliwieniu jego dalszej, poprawnej pracy. Zobacz również: P. Chytla, Metody detekcji, śledzenia i zapobiegania ataków rozproszonych w sieciach IP, praca dyplomowa dostępna pod adresem: http://isec.pl/papers/ddos-v2.pdf
[57] Strona domowa posła Tadeusza Jarmuziewicza, http://www.jarmuziewicz.platforma.org/protest.php
[58] Przykładem robaka internetowego, który może być wykorzystany do ataku typu DDoS jest Worm.Blaster, który po 16 sierpnia - wykorzystując do tego zainfekowane maszyny - aktywizował procedurę ataku typu Denial of Service na stronę www.windowsupdate.com.
[59] Koń trojański - program, który wykonuje bez wiedzy użytkownika dodatkowe, niezamierzone przez niego, często szkodliwe, czynności.
[60] M. Świtała, Wirusy Komputerowe - analiza prawnokarna, Poznań 2001. Praca magisterska dostępna jest pod adresem http://www.vagla.pl/skrypts/wirusy_komputerowe_karne.htm

karny czy konwencja o cyberprzestępczości[61]) warto rozważyć aspekt cywilnoprawny rozpowszechniania wirusów i internetowych robaków.

Ruch generowany poprzez rozsyłające się robaki można włączyć do ogólnej puli ruchu generowanego przez *spam*. Podobnie jeśli chodzi o komunikaty generowane przez filtry antywirusowe, jeśli przychodzą na adresy poczty elektronicznej pod które się podszyto. Można mówić o szkodach wyrządzonych przez wirusy i robaki komputerowe. Można również mówić o „kradzieży czasu pracy komputera", kradzieży tożsamości, etc.

Coraz częściej pojawiają się takie "robaki internetowe" jak np. Klez. Ma on tę cechę, że zarówno adres nadawcy jak i odbiorcy wysyłanego przez robaka listu pochodzi bądź z książki adresowej systemu MS Windows, bądź z takich źródeł jak: ICQ, lokalne pliki z adresami poczty elektronicznej (w tym z plików zawierających oglądane strony internetowe) oraz odczytane adresy z plików o różnych rozszerzeniach. Zarówno w polu *From*: (adres nadawcy), *To*: (adres odbiorcy) jak i *Return-Path*: (adres zwrotny) nie znajdziemy prawdziwego adresu poczty elektronicznej, z którego wysłany został list zawierający kod robaka.

Wysyłający niechciane przesyłki elektroniczne są coraz bardziej zdeterminowani i pewnie dlatego tworzone są specjalne wirusy czy robaki komputerowe, które mają pomagać w przeprowadzeniu ataku DDoS na serwisy blokujące *spam*. Zaatakowane maszyny mogą również służyć do wysyłania niezamówionych informacji elektronicznych. Jak widać problem jest bardzo złożony.

Problem dowodowy
To zagadnienie ma zdecydowanie szerszy kontekst i nie jest związany jedynie z pojęciem *spamu*. Należy prowadzić badania dotyczące możliwości dowodzenia pewnych faktów mających miejsce jedynie w przestrzeni wirtualnej, jedynie z wykorzystaniem elektronicznych nośników informacji i automatycznego przetwarzania danych. Jest to zagadnienie wykraczające poza problematykę oświadczeń woli oraz podpisu elektronicznego, gdyż trudno wymagać, by wysyłający *spam* w złej wierze za każdym razem podpisywał się w sposób elektroniczny, lub by narzędzia służące do odbierania elektronicznych przesyłek stosowały niebudzący wątpliwości oznaczenie faktu przyjęcia przesyłki i oznaczenie jej datą pewną[62].

Prowadzone prace prawodawcze doprowadziły do przyjęcia w Polsce rozporządzeń wykonawczych, m.in. rozporządzenia do art. 40 ust. 3 ustawy prawo telekomunikacyjne z dnia 24 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego oraz rozporządzenia do art. 242 kodeksu postępowania karnego z dnia 24 czerwca 2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobu dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów. Omawiane rozporządzenia wprowadzają szereg trudnych do egzekwowania obowiązków na operatorów i inne podmioty uczestniczące w utrzymaniu sieci komputerowych w Polsce.

Zapis art. 40 ust. 3 ustawy Prawo telekomunikacyjne stał się przedmiotem skargi Polskiej Konfederacji Pracodawców Prywatnych do Trybunału Konstytucyjnego. Zdaniem PKPP przepisy nakazujące operatorom instalowanie kosztownych urządzeń do podsłuchu rozmów telefonicznych i podglądu np. e-maili są sprzeczne z konstytucją. W tym kontekście warto przytoczyć orzeczenie austriackiego federalnego Trybunału Konstytucyjnego z 27 lutego 2003 roku[63], który uznając wniosek sześciu podmiotów, zdecydował, iż obowiązek instalowania na własny koszt systemu do kontroli przekazów informacji jest niezgodny z konstytucją oraz ustawą dot. nadzoru BGB1 II 418/2001 i winien ulec odwołaniu ze względu na sprzeczność z prawem. Wnioskodawcy poczytywali w szczególności niemożność zwrotu kosztów jako uchybienie prawu do równości, nietykalności własności, wolności

[61] por. krytyczne uwagi odnośnie nowelizacji polskiej ustawy karnej w kontekście dostosowania jej do konwencji o cyberprzestępczości: A. Adamski, Buszujący w sieci, Rzeczpospolita z dnia 27 października 2003.
[62] por. M. Kliś, A. Stella - Sawicki, Dowody cyfrowe w postępowaniu karnym - wybrane zagadnienia. Możliwość identyfikacji użytkownika komputera, czerwiec 2001. Artykuł dostępny pod adresem http://www.vagla.pl/skrypts/dowody_cyfrowe.htm
[63] Orzeczenie dostępne jest w Internecie pod adresem: http://www.vfgh.gv.at/vfgh/presse/G37-16-02.pdf

wykonywania zawodu. § 89 kwestionowanej ustawy TKG zobowiązuje operatorów m. in. do przygotowania na własny koszt zgodnie z ustawą wszystkich obiektów, jakie są potrzebne do nadzorowania komunikacji.

Zagadnienie jest wielce kontrowersyjne i wymaga gruntowych badań.

Postęp wyprzedza prawo

W niniejszym artykule wskazałem jedynie główne kierunki badań, jakie należy prowadzić by przybliżyć problematykę *spamu* nauce prawa. Z pewnością w trakcie prac pojawią się kolejne kwestie warte omówienia i zbadania.

Na zakończenie warto wskazać pewne doniesienie internetowe[64]: niezidentyfikowana nieformalna grupa z Polski zaoferowała w Internecie swoje usługi polegające na „*niewidzialnym hostingu*[65]". Gdyby potwierdzono takie możliwości, oznaczałoby to, że nie będzie możliwe ustalenie rzeczywistego adresu IP serwera przechowującego strony internetowe. Według przedstawiciela grupy, efekt ten został uzyskany dzięki wykorzystaniu sieci niemal pół miliona centralnie sterowanych komputerów z systemem operacyjnym Windows, które wcześniej zostały zaatakowane i w których zainstalowano konie trojańskie. Właściciele maszyn nie są nawet świadomi, że ich komputery i oprogramowanie służy jako system szybko zmieniających się serwerów nazw domen internetowych (tzw. serwerów DNS) dla konkretnej, ,,niewidzialnej'' domeny. Jeśli takie doniesienia okażą się prawdziwe – byłoby to idealne narzędzie dla osób pragnących wysyłać niezamówioną informację elektroniczną, bez obawy sprawdzenia prawdziwej tożsamości.

Badania nad zjawiskiem spamu w ujęciu prawnym trwają...

...I nie tylko nad spamem:

...sprawdź co się dzieje na VaGla.pl Prawo i Internet

http://www.vagla.pl

Artykuł został opublikowany w kwartalniku „Prawo i ekonomia w telekomunikacji" nr 4/2003 str. 61.

[64] B. McWilliams, Cloaking Device Made for Spammers, Wired.com, artykuł dostępny pod adresem: http://www.wired.com/news/print/0,1294,60747,00.html

[65] *host* – ang. gospodarz. Udostępnienie zasobów internetowych np. dla potrzeb działania strony internetowej przedsiębiorstwa.