Piotr Kucharski

Społeczne i prawne aspekty spamu

Jeśli nie wiesz, jak należy się w jakiejś sytuacji zachować,
na wszelki wypadek zachowuj się przyzwoicie.
Antoni Słonimski

Geneza

Dawno temu w Ameryce powstała sieć. Na początek ot, trzy komputery zestawione przez naukowców pracujących na zlecenie wojska. Tak im się spodobały jej możliwości, w tak dużym stopniu rozpowszechnili ją na wielu uniwersytetach, że w końcu powstał Internet, jaki znamy dziś.

Naukowcy podeszli do problemu poważnie — wymyślili setki protokołów, dzięki którym można się komunikować między różnymi maszynami, systemami operacyjnymi i programami. Każda aktywność w Internecie opiera się na protokołach.

Przeciętny użytkownik nie zdaje sobie sprawy ze złożoności i ilości protokołów, z których korzysta na co dzień. Przyjrzyjmy się pozornie prostej czynności wysłania i odebrania listu.

Wysłanie poczty to połączenie do serwera SMTP [RFC 2821] i podanie mu ustrukturalizowanego strumienia informacji (MAIL FROM, RCPT TO, DATA, potem nagłówki listu i na końcu odpowiednio zakodowana treść właściwa i załączniki); odebranie poczty to połączenie do serwera protokołem IMAP [RFC 3501] i korzystanie z wielu jego rozszerzeń. Po drodze korzysta się jeszcze z co najmniej kilku innych standardów, np. Ethernet w sieci lokalnej, TCP/IP do połączenia z serwerem zdalnym, protokołu TLS [RFC 2246] do zabezpieczenia poufności danych.

Z jednej strony niewiedza użytkownika ma dobre strony — w końcu nie trzeba być mechanikiem samochodowym, żeby jeździć — ale z drugiej ma wady. Nawet nie dlatego, że jeśli się nie wie, co to jest koło, to trudno zgłosić mechanikowi problem. Uważam, że najbardziej niebezpiecznym aspektem ignorancji technicznej jest brak świadomości zagrożeń czających się w Internecie. Dodatkowo wieloletnia propaganda na rzecz ułatwiania dostępu do sieci spowodowała, że do korzystania z sieci (w odróżnieniu od jazdy samochodem) nie są wymagane praktycznie żadne szkolenia, a dzięki „inteligentnym" programom wszystkim wydaje się to bardzo proste...

> *Progress (n.): The process through which the Internet has evolved from smart people in front of dumb terminals to dumb people in front of smart terminals. (obscurity)*

Ewolucja, a moim zdaniem raczej regres intelektualny i moralny użytkowników w Internecie to złożony problem. W początkach każdej nowej technologii istnieją różne bariery jej wykorzystania. W przypadku sieci była to bariera kosztów, którą omijało się przez korzystanie z dostępu na uczelniach oraz — a może przede wszystkim — bariera wiedzy,

której nie dało się łatwo przeskoczyć. Nie istniały przyjazne programy, konfiguracje, graficzne interfejsy, nie było tylu przykładów, nie istniało jeszcze zbyt wiele stron WWW [RFC 2616], nie wspominając o wyszukiwarkach.

Ta bariera wejścia do Internetu była niezwykle skutecznym filtrem użytkowników — w dawnych czasach z sieci korzystali ludzie raczej dobrze wykształceni, zorientowani w ówczesnym Internecie, świadomie z niego korzystający i, co bardzo ważne, dość życzliwi wobec innych użytkowników (na psychologicznej zasadzie przyciągania — w końcu ci *inni* byli bardzo podobni do nich). Takim zachowaniom sprzyjała też niewielka liczba wtajemniczonych.

Projektanci sieci mierzyli świat swoją miarą (to jeden z nielicznych ich błędów) i zaprojektowali sieć dla sobie podobnych — inteligentnych i życzliwych. Wiele protokołów nie miało zabezpieczeń, wiele spraw zostało określone podobnymi do klauzuli generalnej z Kodeksu Cywilnego[1] zasadami ogólnymi, zgodnie z którymi można robić wiele, ale świadomie się z tego prawa nie korzysta. Każdy miał więc prawo moralne w sobie. Dla przykładu: protokół SMTP [RFC 2821] pozwalał wysyłać listy każdemu przez dowolny serwer oraz nie był zabezpieczony przed podszywaniem się nadawców! Nikt tego nie nadużywał, naturalnie do pewnego momentu.

W dużym uproszczeniu Internet rozwijał się wedle następującego scenariusza. Wraz ze zwiększeniem liczby użytkowników postępowała erozja wartości moralnych, zwłaszcza odpowiedzialności za dobro wspólne; nasilały się fenomeny opisane w „Psychologii tłumu" Gustawa Le Bona: tłum bezmyślnie niszczący na swojej drodze wszystko, co szlachetne i dobre. Oczywiście zostały opracowane zasady sieciowego savoir vivre (netykieta [RFC 1855]), ale podobnie jak w przypadku zwykłej etykiety, porządni ludzie jej nie potrzebują, bo zachowują się przyzwoicie, a informacyjny lumpenproletariat, który powinien ją przeczytać, wcale nie ma zamiaru. Potem jeszcze, całkiem jak w życiu, pojawili się oszuści i naciągacze, którzy chcieli na tłumie zarobić.

I tak na polu poczty elektronicznej narodził się chwast, którego nie można wyplenić do dziś — spam. Nazwa ta ma swoją genezę w skeczu Monthy Pythona, w którym Wikingowie skutecznie zagłuszali rozmowy przez zachwalanie konserwy mięsnej głośnym skandowaniem *SPAM, SPAM, SPAM*. A przy okazji: nie należy pisać słowa „spam" wielkimi literami — taka forma jest zastrzeżona przez Hormel Foods Corp. dla ich konserwy mięsnej produkowanej od 1937 r. i ponoć bardzo popularnej w czasie wojny.

Społeczne aspekty spamu

W ogólnym ujęciu spam to nadmiar informacji zbędnych dla odbiorcy przekazu. W poczcie elektronicznej wyróżnia się co najmniej dwa typy: UCE (unsolicited commercial email, niezamawiany komercyjny email) oraz UBE (unsolicited bulk email, niezamawiany wielokrotny email) — czyli listy niezamówione przez odbiorcę, które mają charakter komercyjny (reklamy), albo są wysyłane w masowych ilościach.

Spamerzy żerują na ułomnościach protokołu i natury ludzkiej. Jak wspomniałem wcześniej, SMTP pozwala na wysyłanie wiadomości od (prawie) dowolnego nadawcy do dowolnego odbiorcy. Co gorsza, można to osiągnąć przy praktycznie zerowym koszcie nadania, co oznacza niespotykany gdzie indziej zwrot z „inwestycji" — koszt tej wątpliwej jakości

[1] *Kodeks Cywilny [KC] Art. 5. Nie można czynić ze swego prawa użytku, który by był sprzeczny ze społeczno-gospodarczym przeznaczeniem tego prawa lub* z zasadami współżycia społecznego.

kampanii reklamowej nie dość, że prawie nie zależy od wielkości akcji, to jeszcze zostaje przerzucony niemal w całości na odbiorcę!

Spamer wysyła miliony wiadomości dziennie[2], ale przecież ich nie pisze ani nie czyta... Jeden szablon, kilkaset serwerów, wysyłka automatem. Niech inni się martwią. A taki spam nie tylko trzeba przesłać po łączach internetowych (wcale nie tanich), ale także przechowywać na serwerach, dopóki nie zostanie skasowany przez użytkowników. Statystyki firmy Brightmail[3] w 2004 wskazywały na blisko 60% spamu w poczcie. Serwery Szkoły Głównej Handlowej w Warszawie przetwarzają dziennie około 100 tys. listów o łącznej objętości 2,5 gigabajta. Czyli około 1,5 gigabajta i 60 tys. listów *dziennie* to śmieci. Obsługa tej poczty to konkretne inwestycje w łącza, serwery i dyski. Odbiorcy muszą odebrać listy (czasem płacąc — i płacząc — za połączenie), przeczytać (choćby tylko zerknąć) i skasować śmieci, żeby wyłuskać te pożądane przesyłki. To strata czasu, która łatwo przekłada się na pieniądze. Dalej: konta pocztowe nie są z gumy, czasem wystarczy wyjazd na urlop, żeby cenny list wrócił do nadawcy, bo skrzynka została zapchana śmieciami. To przyczynia się do utraty zaufania do poczty elektronicznej. To są wymierne i ciągle rosnące straty; przez firmę konsultingową Radicati Group szacowane były w 2002 r. na 11 mld dolarów na całym świecie, w 2003 r. na 21 mld dolarów, w 2004 r. na 41 mld dolarów.

Najsmutniejsze w tym procederze wydaje się to, że niektórzy odbiorcy spamu kupią te podrabiane roleksy i inne reklamowane produkty — zupełnie nieświadomi, że to dzięki nim spamerzy istnieją i że to przez nich tak naprawdę cierpi reszta społeczności internetowej. Takich naiwnych użytkowników jest co prawda niewielu (spamerzy mówią, że opłacalność ich działań oscyluje wokół ułamków promila[4]), ale to tylko zachęca do zwiększania akcji spamerskich.

W dodatku jest to spirala, która może skończyć się załamaniem systemu pocztowego. Im więcej wydajemy na ochronę przeciwspamową, im więcej czasu nam to zajmuje oraz im skuteczniej radzimy sobie ze spamem automatycznie, tym więcej spamu będzie rozsyłane, żeby temu przeciwdziałać i utrzymać te ułamki promila skuteczności.

Spamowanie jest prowadzone zupełnie na ślepo. Do ludzi trafiają treści kompletnie dla nich nieodpowiednie. Kobiety otrzymują propozycje powiększenia penisa, mężczyźni — biustu, a wszyscy po równo dostają propozycje oszustw i treści pornograficzne. Być może nikt nad tym się nie zastanawia, ale *wszyscy* oznacza w przypadku posiadaczy kont pocztowych także dzieci! Według raportu firmy Symantec z 2003 roku 80% nieletnich korzystających z poczty otrzymuje treści dla nich nieodpowiednie.

W ostatnich latach zmieniają się proporcje rozsyłanych gatunków spamu. O ile oferty niepotrzebnych dóbr są na mniej więcej takim samym poziomie, to zmniejsza się ilość spamu pornograficznego, a zwiększa zawierającego oszustwa i próby wyłudzeń. Ten spam to prawdopodobnie o wiele lepszy interes niż zwykłe reklamy produktów. Mechanizmów jest kilka: słynny spam nigeryjski i jego odmiany („jestem przedstawicielem pana X., mamy na koncie 50 milionów, ale z jakiegoś powodu nie możemy ich podjąć, prosimy o pomoc, proszę przesłać 1000 dolarów, a dostanie Pan 5 milionów prowizji"), podszywanie się pod obsługę banków i instytucji finansowych („wystąpił problem z pańskim rachunkiem, proszę się zalogować i sprawdzić" i oszust już zna nasz numer konta, pin lub hasło)

[2] Scott Richter, jeden z największych spamerów, został pozwany za rozsyłanie 250 milionów sztuk spamu dziennie

[3] Zob. [ŁK], art. „Dlaczego spam jest zły", punkt 1

[4] Forrester Research na zlecenie Business Software Alliance przeprowadził w 2004 r. badanie (`http://www.theregister.co.uk/2004/12/10/spam_buyers_survey_bsa/`), w którym ponad 20% Brytyjczyków przyznaje się do kupowania produktów reklamowanych w spamie. Ciekawa rozbieżność między spamerami i użytkownikami. Mam nadzieję, że to tylko błąd w metodologii badania...

oraz rzadziej spotykane w Polsce polecanie zakupu akcji jakiejś firmy (ceny waloru rosną, gdy wielu naiwnych kupuje, wtedy oszust sprzedaje swoje akcje z krociowym zyskiem). Ludzie oszukani przez Internet jeszcze nie są problemem społecznym, ale przy takim tempie rozwoju...

Niedawno pojawił się też nowy gatunek spamu, rozsyłanego głównie przez przestępców zorganizowanych: propozycja kupna tanio (lub wręcz tylko zainstalowania) oprogramowania, które jest de facto oprogramowaniem szpiegowskim (spyware), dzięki któremu przestępcy zyskują dostęp do danych osobowych ofiary znajdujących się w komputerze, a także jego haseł i kodów dostępu.

Prawne aspekty spamu

Listę aktów prawnych wypada rozpocząć odpowiednią interpretacją Konstytucji Rzeczypospolitej Polskiej [KRP]:

> *Art. 47. Każdy ma prawo do* ochrony prawnej życia prywatnego [to i następne podkreślenie w cytowanych aktach prawnych pochodzą ode mnie — PK]*, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.*
>
> *Art. 76. Władze publiczne chronią konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu oraz przed* nieuczciwymi praktykami rynkowymi*. Zakres tej ochrony określa ustawa.*

Łatwa do obrony wydaje się teza, że spam wchodzi z butami w nasze życie prywatne (argument, że możemy nie korzystać z poczty elektronicznej, odrzucam jako niezorganizowany). Tym łatwiej obronić zdanie, że to nieuczciwa praktyka rynkowa (oczywiście, że nieuczciwa, skoro spamer nie ponosi kosztów wysłania, a odbiorca ponosi koszty odebrania i przeczytania).

Bardziej szczegółowe są ustawy. Na pierwszy ogień niezwykle pasujący do spamu punkt Ustawy o zwalczaniu nieuczciwej konkurencji [UZNK]:

> *Art. 16. 1. Czynem nieuczciwej konkurencji w zakresie reklamy jest w szczególności:*
> *[...]*
> *5) reklama, która stanowi istotną ingerencję w sferę prywatności, w szczególności przez uciążliwe dla klientów nagabywanie w miejscach publicznych,* przesyłanie na koszt klienta nie zamówionych towarów *lub* nadużywanie technicznych środków przekazu informacji*.*

Ustawa o swobodzie działalności gospodarczej [USDG] chroni nas przed podszywaniem się spamerów (niestety, spamerzy nie czytają ustaw):

> *Art. 21. 1. Jeżeli przedsiębiorca oferuje towary lub usługi w sprzedaży bezpośredniej lub sprzedaży na odległość za pośrednictwem środków masowego przekazu, sieci teleinformatycznych lub druków bezadresowych, jest on obowiązany do podania w ofercie co najmniej następujących danych: 1) firmy przedsiębiorcy; 2) numeru identyfikacji podatkowej (NIP); 3) siedziby i adresu przedsiębiorcy.*

Przed spamem chronią nas też niektóre przepisy Ustawy o ochronie praw konsumentów [UOPK],

> *Art. 6. 3. Posłużenie się [...] pocztą elektroniczną [...] w celu złożenia propozycji zawarcia umowy może nastąpić* wyłącznie za uprzednią zgodą *konsumenta.*

Należy zauważyć, że mamy tu wyraźne określenie, iż zgoda na otrzymywanie propozycji zawarcia umowy (a tak należy rozumieć większość spamów reklamowych) musi wystąpić *przed* wysłaniem takiej propozycji. Ten jeden zapis pozwala zdelegalizować większość spamów: *nie zgadzałem się, nie mieliście prawa mi wysłać tego spamu.* Jakkolwiek wydaje się, że zapis ten nie był dostatecznie wyraźny. Nowsza Ustawa o świadczeniu usług drogą elektroniczną [UŚUDE], powstała podczas dostosowywania prawa polskiego do wytycznych unijnych[5], zawiera mocniejszy zapis:

> *Art. 4. 1. Jeżeli ustawa wymaga uzyskania zgody usługobiorcy to zgoda ta:*
> *1)* nie może być domniemana *lub dorozumiana z oświadczenia woli o innej treści,*
> *2) może być odwołana w każdym czasie.*
> *2. Usługodawca wykazuje uzyskanie zgody, o której mowa w ust. 1, dla celów dowodowych.*
>
> *Art. 10. 1.* Zakazane jest przesyłanie niezamówionej informacji handlowej *skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.*
> *2. Informację handlową uważa się za zamówioną, jeżeli odbiorca* wyraził zgodę *na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny.*
> *[. . .]*

Te zapisy unieważniają wszelkie zastrzeżenia typu *Państwa adres jest publicznie znany, jeżeli Państwo nie chcą otrzymywać informacji handlowych, to proszę wysłać list o treści NIE na adres. . .* Jeżeli nie zapisaliśmy się sami do otrzymywania informacji handlowych, to nie można tego domniemywać, nie można wyprowadzić takiej zgody z naszej zgody na inne rzeczy (np. usługi), a obowiązek dowodu ciąży na usługodawcy, nie na nas.

Ponieważ niezamawiana informacja handlowa to wykroczenie ścigane na wniosek poszkodowanego, ofiara spamu powinna zgłosić je w dowolnym komisariacie. Co prawda dotychczasowa praktyka sądowa jest raczej zniechęcająca — niewielka szkodliwość społeczna i niewielkie grzywny, a zmarnowanego czasu dużo — ale miejmy przynajmniej świadomość, że jak najbardziej do sądu z tym pójść można Co ciekawe, spamerzy mają czelność podawać do sądów osoby, które publikują teksty antyspamerskie — nawet niedawno organizowaliśmy zrzutkę na adwokata dla jednego z czołowych polskich publicystów antyspamowych w Polsce, Łukasza Kozickiego[ŁK], przeciw któremu spamer złożył do sądu wniosek o zakazanie publikowania opinii oraz rzekomo nieprawdziwych informacji na temat działań, jakie spamer podejmował.

Niektórzy jako jedno ze źródeł ochrony wskazują też Ustawę o ochronie danych osobowych [UODO], a dokładnie zapis o kontroli przetwarzania danych:

> *Art. 32. 1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:*
> *[. . .]*
> *8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.*

[5] Dyrektywy 2000/31/EC i 2002/58/EC.

O ile wysyłanie spamu niewątpliwe jest przetwarzaniem danych, o tyle do dziś nie zostało jednoznacznie określone, czy i jaki adres mailowy stanowi dane osobowe w rozumieniu Ustawy [UODO]

> *Art. 6. 1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.*
> *2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.*
> *3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.*

Z tego względu musimy sami rozważyć, czy nasz adres mailowy jednoznacznie określa naszą osobę, czy nie.

Należy zauważyć, że kwestia spamu niekomercyjnego w prawie polskim w zasadzie nie jest uregulowana. Można próbować coś zdziałać na podstawie powyższych paragrafów Ustawy [UODO], ale w przypadku spamu niekomercyjnego — chyba że akurat trafi się spam wyborczy, bo na to jest paragraf — to ofiara jest w zasadzie bezradna. Rzecz jasna oprócz możliwości zgłoszenia nadużycia do administratora spamera, bo to *jest* nadużycie, choć nie objęte penalizacją.

Różnego rodzaju oszustwa przemycane w spamie podlegają Kodeksowi Karnemu [KK] i nie ma z tym problemu:

> *Art. 286.* § *1. Kto, w celu osiągnięcia korzyści majątkowej,* doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem *za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.*
> *[. . .]*
> *Art. 287.* § *1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
> *[. . .]*

Przy okazji zwracam uwagę, że często wykorzystywane przez spamerów do wysyłania listów armie komputerów-zombie również są przestępstwem przeciwko mieniu.

Kolejny problem to spam niepodlegający jurysdykcji polskich sądów. Możemy zgłaszać to odpowiednim prawnie i miejscowo instytucjom, ale nie dość, że musielibyśmy poświęcić mnóstwo czasu na poznanie prawa innych krajów (a często nawet języka!), to jeszcze prowadzenie sprawy mogłoby być utrudnione ze względu na przesłuchania poszkodowanego. Prawo, niestety, nie nadąża za globalizacją i Internetem. Dość skuteczne pozostaje zgłaszanie takiego spamu po pierwsze do administratora spamera, a po drugie do instytucji takich jak SpamCop[6], które publikują adresy nadania spamu do wykorzystania przez wszystkich internautów w celach defensywnych.

[6] `http://www.spamcop.net/`

Co dalej?

Człowiek posiada informacyjną przepustowość obecnie taką samą, jak sto tysięcy lat temu stwierdza Stanisław Lem w „Bombie megabitowej". W dobie zalewu spamem szkoda czasu i zdrowia na samodzielne odsiewanie śmieci. Polecam zainstalowanie we współpracy z administratorem oprogramowania antyspamowego działającego po stronie serwera, aby nie ściągać śmieci do domu. Niektóre z tych programów korzystają z zaawansowanych algorytmów statystycznych do określania, co jest spamem. Choć trzeba też mieć świadomość, że — niestety — nie dają stuprocentowej skuteczności i czasem potrafią przepuścić spam, ale mogą też list, którego oczekujemy, błędnie zakwalifikować i wyrzucić do kosza (a to kolejny kamyczek do ogródka braku zaufania do poczty elektronicznej).

No i najważniejsze: nie spamuj i nie daj spamować innym! To nie tylko edukacja w zakresie tego, co jest spamem, ale też tego, co spamem *nie jest*. W końcu są listy dyskusyjne, różnego rodzaju subskrypcje i powiadamiania o nowościach. To jest część Internetu i powinna działać — jednak trzeba sobie zdawać sprawę z możliwych nadużyć i tego, jak się przed nimi zabezpieczać (warto przeczytać zalecenia w sprawie masowego wysyłania poczty [RFC 2635]).

Ale co dalej? Czy da się znaleźć systemowe rozwiązanie problemu spamu? Obawiam się, że nie, że wrósł już w Internet tak, jak w życie codzienne wrosły wszędobylskie reklamy. Co prawda podnosi się różne pomysły, jak opłaty za maile (na przykład w postaci czasu procesora *nadawcy*, niekoniecznie w postaci bezpośrednio pieniężnej), ale wymagają one fundamentalnych zmian, co przy tak rozpowszechnionym protokole jest nietrywialne. Ostatnio firmy AOL i Yahoo ogłosiły, że w przyszłości nadawcy za opłatą będą mogli omijać filtry antyspamowe, co miałoby stanowić gwarancję dostarczenia. Pomysł *wydaje się* ciekawy (z założenia spamerzy nie będą płacić za wysyłane maile, nieprawdaż?), ale może okazać się niebezpieczny. Oprócz wzrostu kosztów posiadania konta pocztowego opłaty takie grożą tym, że nikt, kto nie zapłaci, nie będzie mógł skorzystać z maila (nikt nie będzie czytał tych niegwarantowanych listów, skoro to może być spam, nieprawdaż?). I wreszcie dojdzie do nieprzyjmowania nieopłaconych przesyłek, co dotknie najmocniej osoby prywatne, listy dyskusyjne i organizacje non-profit.

Jedną jednak rzecz można w prawie polskim usprawnić. W tej chwili spamera pozywa poszkodowana osoba i nie ma możliwości pozwu grupowego (można się zorganizować w grupę i mieć wspólnego adwokata, ale w dalszym ciągu będzie to kilka(dziesiąt) oddzielnych pozwów). Gdyby w przypadku spamowania (czyli na razie, niestety, tylko wysyłania niezamówionej informacji handlowej) sąd po zbadaniu sprawy stwierdził, że spamer wysyłał takie informacje nie tylko do powoda, ale do kilku(set) innych osób i zasądził karę wprost proporcjonalną do liczby wysłanych spamów... Tak, to być może mogłoby polskich spamerów powstrzymać.

Czego i sobie, i wszystkim internautom życzę.

Literatura

[ŁK] Kozicki, Ł., „Walka ze spamem - obyczaje i prawo", `http://www.nospam-pl.net/`

[KC] Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny, Dz.U. z 1964 r., Nr 16, poz. 93

[KK] Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny, Dz.U. z 1997 r., Nr 88, poz. 553

[KRP] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r., Nr 78, poz. 483

[UZNK] Ustawa z dnia 17 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 2003 r., Nr 153, poz. 1503

[UODO] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 1997 r., Nr 133, poz. 883

[UOPK] Ustawa z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny, Dz.U. z 2000 r., Nr 22, poz. 271

[USDG] Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. z 2004 r., Nr 173, poz. 1807

[UŚUDE] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r., Nr 144, poz. 1204

[RFC 1855] Hambridge, S., Netiquette Guidelines, październik 1995

[RFC 2246] Dierks, T., Allen, C., The TLS (Transport Layer Security) Protocol Version 1.0, styczeń 1999

[RFC 2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., T. Berners-Lee, Hypertext Transfer Protocol — HTTP/1.1, czerwiec 1999

[RFC 2635] Hambridge, S., Lunde, A., DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings, czerwiec 1999

[RFC 2821] Klensin, J., Simple Mail Transfer Protocol, kwiecień 2001

[RFC 3501] Crispin, M., Internet Message Access Protocol - version 4rev1, marzec 2003

[HTML] Raggett, D., et al., HyperText Markup Language Specifications, W3C Recommendation, `http://www.w3.org/MarkUp/`