Mariusz CZYŻAK
URZĄD KOMUNIKACJI ELEKTRONICZNEJ

Spamming i jego karalność w polskim systemie prawnym

Dr Mariusz CZYŻAK

Absolwent Katolickiego Uniwersytetu Lubelskiego Jana Pawła II (1997 r.). Doktor nauk prawnych (2003 r.). Autor publikacji z zakresu prawa karnego i prawa administracyjnego, poświęconych w szczególności karnoadministracyjnym i prawnokarnym aspektom odpowiedzialności podmiotów prowadzących działalność telekomunikacyjną i pocztową. Od listopada 2006 r. Dyrektor Generalny Urzędu Komunikacji Elektronicznej.

e-mail: m.czyzak@uke.gov.pl

Streszczenie

Artykuł poświęcony jest *spammingowi* (tj. przesyłaniu niezamówionej informacji handlowej) oraz środkom jego zwalczania w polskim prawie, które uznaje go za wykroczenie oraz delikt administracyjny podlegający karze pieniężnej nakładanej przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów. Przedstawiono w nim również założenia projektu nowelizacji Prawa telekomunikacyjnego z 2004 r. przyznającego Prezesowi Urzędu Komunikacji Elektronicznej kompetencje w zakresie przeciwdziałania temu zjawisku. Polskie rozwiązania w tym zakresie wydają się dolegliwe finansowo, ale istotne jest także wykorzystanie narzędzi informatycznych identyfikujących źródła *spamu* i tworzących bariery uniemożliwiające jego rozpowszechnianie.

Słowa kluczowe: *spamming*, Internet, przestępczość internetowa.

Punishablity for spam under the Polish legal system

Abstract

The paper discusses a concept of spamming and selected anti-spam remedies in the Polish legal system. Spam shall be recognized as information which is: delivered by e-mail to a defined recipient; unsolicited; predominately of commercial, but also of political, ideological or other nature; sent in order to acquire specific personal and financial benefits (Section 2). Other forms of internet crimes similar to spamming include spamindexing, spimming, phishing and pharming (Section 3). According to the Polish law spam is treated as an offence subject to a fine (the Act on providing e-services of 2002, the Act of combating unfair market practices of 2007) and as an administrative tort subject to financial penalty in the maximum amount of 10% of the undertaking's income (Act on competition and consumer protection of 2007) imposed by the President of the Office of Competition and Consumer Protection (Section 4). The study also includes some of the guidelines for the amendment of the Telecommunications law of 2004 (providing for a number of powers to be granted to the President of the Office of Electronic Communications in the scope of spam prevention, including the right to impose financial penalties in the amount from 100 to 100 000 PLN on the spam sender (Section 5). The remedies against spam available under the Polish legislation shall be regarded as burdensome, especially in the case of financial consequences of an administrative financial penalty. However, as the mentioned remedies are dispersed over a number of normative acts they are to some degree incoherent. In the battle with spam it is extremely important to use relevant information and technological tools that prevent the spread of spam and also to promote appropriate rules of conduct in the Internet network (e.g. ethical codes).

Keywords: spamming, Internet, Internet crime.

1. Wstęp

Stały rozwój technologiczny towarzyszący współczesnemu światu sprawia, że prawu, a zwłaszcza tym jego gałęziom, które zapewniają ochronę dóbr osobistych i ekonomicznych jednostki, jest coraz trudniej przeciwdziałać godzącym w nie zachowaniom związanym z wykorzystywaniem nowoczesnych rozwiązań teleinformatycznych. Wspomniana teza odnosi się w szczególności do tego obszaru łączności elektronicznej, który wykorzystywany jest jako nośnik informacji we współczesnym obrocie gospodarczym. Niekiedy przedstawiciele doktryny prawa i analitycy rynku komunikacji elektronicznej posługują się nawet pojęciem „przestępczości internetowej" lub „cyberprzestępczości" na określenie, zabronionych prawem, działań dokonywanych za pomocą komputera w sieci internetowej lub przy jej wykorzystaniu, godzących m.in. w bezpieczeństwo wykorzystania technologii informatycznych [1, 4, 15, 27]. Niemniej jednak tylko częściowo, w przypadkach najbardziej społecznie szkodliwych, czyny te stanowią przedmiot zainteresowania dziedziny prawa karnego *sensu stricte*, w wielu zaś sytuacjach zadanie przeciwdziałania tego typu zjawiskom pozostawiono sankcjom finansowym o charakterze karnoadministracyjnym.

Zagadnienie bezpieczeństwa jest jednym z najpoważniejszych wyzwań stojących przed procesem stworzenia jednolitej europejskiej przestrzeni informacyjnej *(ang. Single European Information Space*). Powszechny rozwój usług świadczonych za pomocą łączności elektronicznej zależy bowiem w dużej mierze od wiarygodności, bezpieczeństwa i niezawodności technologii teleinformatycznych, zaś coraz większa ilość *spamu*, wirusów, programów szpiegujących *(ang. spyware)* oraz innych form szkodliwego oprogramowania *(ang. malware)* przyczynia się do spadku zaufania jej użytkowników. Sam rynek szeroko rozumianej komunikacji elektronicznej nie zdołał jednakże rozwiązać kwestii bezpieczeństwa w sposób zadowalający, stąd też niezbędne stało się ustanowienie ram prawnych służących zapewnieniu odpowiedniego zakresu ochrony obywateli i przedsiębiorców, a także podniesieniu poziomu zaufania konsumentów do społeczeństwa informacyjnego. Stosowane w tym zakresie środki nie powinny przy tym ograniczać tak interoperacyjności, jak i konkurencyjności usług tego rodzaju [13].

Zasygnalizowane powyżej problemy w pełni odnoszą się do zjawiska tzw. *spammingu*, którego zdefiniowaniu i wybranym aspektom karalności poświęcone jest niniejsze opracowanie.

2. Pojęcie „spamu"

Etymologicznie pojęcie „spam" pochodzi z języka angielskiego i jest skrótem wyrażenia *„spiced pork and ham"*, co oznacza mielonkę i wskazuje na zawartość oraz charakter informacji uznawanych za *spam*. Synonimami tego pojęcia są również takie wyrażenia jak *„junk-mail"* tzn. rupiecie pocztowe, czy też, w zależności od treści informacji - UCE (*ang. Unsolicited Commercial E-mail* - niepożądany list komercyjny) lub UBE (*ang. Unsolicited Bulk E-mail* – niepożądany list niekomercyjny). Proceder wysyłania tego typu niezamówionych informacji to *spamming* [2, 7, 10, 25, 27].

Polski ustawodawca pokusił się nawet o sformułowanie legalnej definicji *„spammingu"*. Zgodnie z postanowieniami art. 10 ust. 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [19] (dalej: u.ś.u.d.e.) zakazane jest bowiem *„przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej*.".

Wspomnieć w tym miejscu jednak należy, że niekiedy jako *spam* traktowane bywają również niezamówione informacje nie mające charakteru handlowego, ale polityczny, ideologiczny lub dobroczynny. O uznaniu informacji za taką, która nie ma charakteru *spamu*, decyduje wówczas jej osobisty charakter oraz brak związku z działalnością zarobkową, wykonywaną profesją lub funkcją pełnioną przez nadawcę [5].

Reasumując, mianem *spamu* określić możemy informację, która odznacza się następującymi cechami. Po pierwsze, jest przesłana drogą elektroniczną do oznaczonego odbiorcy. Po drugie, nie jest przez niego zamówiona. Po trzecie, ma charakter handlowy *(spam*

sensu stricte), a w niektórych przypadkach również polityczny, ideologiczny lub charytatywny *(spam sensu largo)*. Po czwarte, wysłana została w celu osiągnięcia określonych korzyści osobistych lub majątkowych.

Nie sposób nie przytoczyć w tym miejscu kilku danych historycznych i statystycznych obrazujących rozmiary zjawiska *spammingu*. Uznaje się, iż pierwszym nadawcą *spamu* był Einar Stefferud, który w 1978 r. wysłał około tysiąca niezamówionych e-maili z zaproszeniem urodzinowym i zapoczątkował w ten sposób proceder wysyłania niechcianych informacji drogą elektroniczną. Podaje się również, że w 1994 r. w Phoenix w Stanach Zjednoczonych wysłano pierwszy *spam* o charakterze komercyjnym oferujący usługi prawnicze kancelarii adwokackiej prowadzonej przez Lawrence'a Cantera i Marthę Siegel [2, 10].

Obecnie, po ponad trzydziestu latach, *spamming* stał się problemem o charakterze powszechnym i masowym. Badania wskazują, że aż 78% e-maili jest *spamem*, przy czym 35,4% niezamówionej informacji pochodzi z Azji, 29,5% z Europy, 18,2% z Ameryki Północnej, a 14,8% z Ameryki Południowej [3]. Najczęściej *spam* dotyczy reklamy artykułów erotycznych, oprogramowania nielegalnego pochodzenia oraz uczestnictwa w tzw. piramidach finansowych stwarzających wrażenie możliwości szybkiego zarobku. Szkody związane z usuwaniem przesyłanych za pomocą spamu wirusów sięgają dziesiątek miliardów dolarów rocznie [2, 4].

3. Pokrewne zjawiska szkodliwe

Nadmienić należy przy tym, że w ostatnich latach pojawiło się szereg nowych odmian *spammingu* bądź pokrewnych mu szkodliwych zachowań, posługujących się coraz to nowszymi metodami nielegalnego przekazywania i pozyskiwania informacji w tzw. „cyberprzestrzeni".

Przykładem jest *spamdexing (ang. spam + index)* polegający na „spamowaniu" indeksu wyszukiwarki zmierzającym do jej oszukania i nadania określonej stronie internetowej wyższego rankingu, aniżeli ten, który w rzeczywistości posiada. Wyróżnia się przy tym dwie jego odmiany – *spam* zawartości strony *(ang. content spam)* i *spam* odesłań *(ang. link spam)*. Ta pierwsza przybiera rozmaite postaci uzależnione od wybranego przez tzw. *webspamera* elementu strony internetowej. Może polegać np. na wyświetlaniu użytkownikowi określonych wyrazów w tym samym kolorze, co tło strony internetowej, stąd nie dają się one wyłowić gołym okiem albo na wykorzystaniu stron internetowych przekierowujących *(ang. doorway pages)* użytkownika do pustej treściowo strony. W drugim przypadku *webspamer* wykorzystuje własne oraz obce strony w celu „podbijania" wyników określonej strony internetowej, na której mu zależy. Najczęstszą formę tego procederu stanowią tzw. farmy linków *(ang. link farms)* tj. grupy stron internetowych, które nie zawierają żadnej istotnej treści, ale ogromną liczbę odesłań do samych siebie. Szacuje się przy tym, że obecnie około 10-15% stron internetowych to tzw. *Webspam* [8, 25].

Środkiem przesyłania niezamówionej informacji stały się również m.in. funkcjonalne i proste w obsłudze, a przy tym bezpłatne komunikatory. Wykształciła się nowa forma *spamu* określana mianem *spimu (ang. stupid personal information)*, a polegająca na przesyłaniu za pomocą komunikatora *spamu* mającego postać krótkiego komunikatu zakończonego odsyłaczem do określonej strony internetowej [7, 25].

Postacią przestępczości internetowej, nieporównywalnie bardziej szkodliwej aniżeli *spamming*, jest tzw. *phishing,* zwany również *spoofingiem* (*ang. password harvesting fishing* – łowienie haseł) tj. oszukańcze pozyskiwanie poufnej informacji osobistej (haseł, loginu, PIN-u, numeru karty kredytowej, itp.), poprzez podszywanie się pod osobę godną zaufania, której informacje te są pilnie potrzebne np. z uwagi na konieczność weryfikacji danych bankowych. Po podaniu hasła „napastnik" uzyskuje dostęp do konta i wykorzystuje je w przestępczym celu, np. do wysyłania *spamu* lub uzyskania korzyści majątkowej [4, 7, 25, 27]. Jego odmianą jest tzw. SMiShing (*ang. SMS phishing – phishing* sms-owy) sprowadzający się do rozsyłania SMS-ów, które mają skłonić „ofiarę ataku" do podjęcia określonej czynności na stronie internetowej, skutkującej zainstalowaniem na jej komputerze szkodliwego oprogramowania [25].

Zaawansowaną formą *phishingu* jest z kolei tzw. *pharming*. Polega on na przekierowywaniu użytkownika Internetu do spreparowanej strony internetowej, która swoim wyglądem przypomina lub jest identyczna z witryną banku internetowego, serwisu aukcyjnego, sklepu internetowego lub innej instytucji tego typu, a w konsekwencji pozwala „napastnikowi" zdobyć dane i przynieść korzyści finansowe w następstwie kradzieży z konta bankowego, itp. Oszust internetowy wykonuje dodatkowo atak na serwer DNS w celu skojarzenia prawdziwego adresu URL z serwerem WWW podrobionej strony internetowej [25].

4. Środki zwalczania „*spammingu*"

Oczywistym jest, że ze względu na teleinformatyczną naturę *spammingu* oraz jego skalę, instrumenty przeciwdziałania temu zjawisku muszą mieć charakter wielopłaszczyznowy [15, 27]. Należą do nich w szczególności:

- wprowadzanie do obowiązującego porządku prawnego instytucji o charakterze represyjnym, wymierzonych przeciwko nieuczciwym działaniom w sieci internetowej;
- rozwijanie współpracy międzynarodowej w obszarze wymiany danych nt. zjawiska, prowadzenia wspólnych akcji oraz nowych procedur prawnych;
- podejmowanie działań w zakresie *softlaw* (kodeksów dobrych praktyk);
- propagowanie technologii ochronnych;
- prace badawczo-rozwojowe w dziedzinie teleinformatyki;
- edukację w zakresie upowszechnienia modelu uczciwych praktyk w działalności w obszarze *e-commerce*.

Przedmiot dalszych rozważań stanowić będą przede wszystkim prawnokarne i karnoadministracyjne środki jego zwalczania, które znalazły swoje zastosowanie w polskim systemie prawnym.

Uzasadnienia dla samej karalności zjawiska *spammingu*, o czym wspomniano już na wstępie, upatrywać trzeba w jego wielowymiarowej społeczno-technologicznej szkodliwości. Godzi on bowiem zarówno w dobra osobiste człowieka, jak i w bezpieczeństwo komunikacji za pośrednictwem środków łączności elektronicznej. Narusza prawo do prywatności i wolność przybierającą postać swobody konsumenta w zakresie dobrowolnego uczestnictwa w obrocie gospodarczym i doboru wykorzystywanych przez niego informacji handlowych, z których zamierza skorzystać. Nie bez znaczenia pozostaje również fakt blokowania przez *spam* skrzynek pocztowych użytkowników, ograniczania przepustowości sieci internetowej, a także rozpowszechniania za jego pośrednictwem wirusów komputerowych, oprogramowania złośliwego, itp. Co więcej, nie sposób pominąć również związków *spammingu* z takimi bezprawnymi działaniami jak stosowanie nieuczciwych praktyk rynkowych, rozpowszechnianie zakazanych form pornografii, naruszanie praw autorskich poprzez nielegalne udostępnianie oprogramowania, itp.

Instrumentarium służące zwalczaniu *spammingu* na gruncie polskiego porządku prawnego przybiera przede wszystkim formę środków represyjnych, aczkolwiek ustawodawca nie zdecydował się skorzystać z kary kryminalnej dla napiętnowania działania tego typu, wychodząc najprawdopodobniej z założenia, że stopień jego szkodliwości społecznej jest dalece niższy, aniżeli ma to miejsce chociażby w przypadku takiego czynu jak bezprawna ingerencja w zapis na komputerowym nośniku informacji (np. poprzez wprowadzenie wirusa do cudzego komputera), który uznał za przestępstwo (art. 268 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny [17]). Mowa tutaj bowiem o odpowiedzialności prawnej podlegającej rygorowi nie prawa karnego, ale prawa wykroczeń i prawa administracyjnego, a związanej w obydwu przypadkach z wymierzeniem określonej dolegliwości finansowej stanowiącej konsekwencję wysłania *spamu*. Podmiotem tej pierw-

szej może być wyłącznie osoba fizyczna, drugiej zaś tak osoba fizyczna, jak i podmiot o charakterze korporacyjnym, tj. osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej.

Nadmienić trzeba przy tym na wstępie, że kierunek polskiemu ustawodawstwu antyspamowemu nadaje w tym zakresie prawo unijne, które zobowiązuje kraje Unii Europejskiej do zapewnienia, aby informacje handlowe przesyłane przez usługodawcę mającego siedzibę na terytorium tych państw były, w chwili ich otrzymania przez odbiorcę, wyraźnie i jednoznacznie rozpoznawalne [11].

Zgodnie z postanowieniami art. 24 ust. 1 u.ś.u.d.e., przesyłanie za pomocą środków komunikacji elektronicznej niezamówionych informacji handlowych tj. *spamu*, stanowi wykroczenie i podlega karze grzywny (wymierzanej w wysokości od 20 do 5.000 PLN), przy czym ściganie za nie następuje na wniosek pokrzywdzonego, tj. jedynie tego, czyje dobro prawne zostało przez nie bezpośrednio naruszone lub zagrożone (art. 25 § 1 ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia [18]). Wymierzając grzywnę, sąd zobligowany jest wziąć pod uwagę dochody sprawcy, jego warunki osobiste i rodzinne, stosunki majątkowe i możliwości zarobkowe (art. 24 ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń [16]), w tym i te osiągnięte w związku z działalnością gospodarczą reklamowaną nielegalnie za pomocą poczty elektronicznej. Jak się wydaje, dolegliwość ekonomiczna towarzysząca wymierzeniu kary grzywny za popełnienie przedmiotowego wykroczenia może jednak nie stanowić wystarczającej sankcji odstraszającej od prowadzenia analizowanego procederu te podmioty, które czerpią dochody z tytułu reklamy, za pomocą nielegalnego wykorzystania Internetu jako środka jej przekazu.

Należy w tym miejscu nadmienić, że do problemu przesyłania spamu zastosowanie mają również postanowienia ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym [22] (dalej: u.p.n.p.r.) implementującej do polskiego systemu prawnego tzw. dyrektywę o nieuczciwych praktykach handlowych [9, 12]. Wprowadza ona bowiem do systemu powszechnie obowiązującego prawa instytucję tzw. nieuczciwej praktyki rynkowej, do których zalicza m.in. informację handlową (np. reklamę i marketing), bezpośrednio związaną z promocją lub nabyciem produktu przez konsumenta w sytuacji, gdy jest *„sprzeczna z dobrymi obyczajami i w istotny sposób zniekształca lub może zniekształcić zachowanie rynkowe przeciętnego konsumenta przed zawarciem umowy dotyczącej produktu, w trakcie jej zawierania lub po jej zawarciu”* (art. 2 pkt 4 i 4 ust. 1 u.p.n.p.r.). Agresywne praktyki rynkowe zagrażające lub naruszające interes konsumenta, za które przedmiotowa ustawa uznaje w szczególności także uciążliwe i nie spowodowane działaniem albo zaniechaniem konsumenta nakłanianie do nabycia produktów za pośrednictwem poczty elektronicznej (z wyłączeniem dozwolonych przepisami powszechnie obowiązującego prawa przypadków egzekwowania zobowiązań umownych), podlegają – analogicznie jak na gruncie ustawy o świadczeniu usług drogą elektroniczną – karze grzywny jako wykroczenie (art. 9 pkt 3 w zw. z art. 15 ust. 1 u.p.n.p.r.).

Spamming w przytoczonym na wstępie znaczeniu nadanym mu ustawą o świadczeniu usług drogą elektroniczną, został uznany przez ustawodawcę za czyn nieuczciwej konkurencji [26], stąd też podlega również odpowiedzialności karnoadministracyjnej na gruncie ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów [21] (dalej: u.o.k.k.). W rezultacie Prezes Urzędu Ochrony Konkurencji i Konsumentów (dalej: Prezes UOKiK) może wymierzyć przedsiębiorcy administracyjną karę pieniężną w wysokości do 10% przychodu osiągniętego przez tego przedsiębiorcę w roku rozliczeniowym poprzedzającym rok nałożenia kary, jeżeli dopuścił się on, chociażby nieumyślnie, stosowania praktyki naruszającej zbiorowe interesy konsumentów w rozumieniu art. 24 u.o.k.k., tj. godzącego w nie bezprawnego działania przedsiębiorcy, w szczególności takiego czynu nieuczciwej konkurencji, jakim jest *spamming* (art. 10 ust. 3 u.ś.u.d.e.). Przy ustalaniu wysokości przedmiotowej kary pieniężnej zobowiązany jest uwzględnić w szczególności okres, stopień oraz okoliczności naruszenia przepisów ustawy, a także uprzednie naruszenie przepisów ustawy o ochronie konkurencji i konsumentów (art. 111 u.o.k.k.), polegające chociażby na permanentnym wykorzystywaniu *spamu* jako środka reklamy. Co istotne, Prezes UOKiK może, ze względu na ważny interes przedsiębiorcy, odroczyć na jego wniosek, uiszczenie kary pieniężnej bądź rozłożyć ją na raty (art. 113 ust. 1 u.o.k.k.).

Jak zatem wynika z przedstawionych powyżej obowiązujących rozwiązań legislacyjnych, *spamming* uznawany jest na gruncie polskiego ustawodawstwa z jednej strony za wykroczenie podlegające karze grzywny, z drugiej zaś za delikt administracyjny podlegający karze pieniężnej. Jakkolwiek w myśl znanej nauce prawa karnego zasady *ne bis in idem*, wyłączona jest możliwość dwukrotnego ukarania za ten sam czyn zabroniony prawem, to kumulacja odpowiedzialności wykroczeniowej i karnoadministracyjnej w przedmiotowej sytuacji zdaje się być dopuszczalna, a to z uwagi na różnicę pomiędzy znamionami oraz ciężarem gatunkowym wykroczenia z art. 24 ust. 1 u.ś.u.d.e. i naruszenia stanowiącego czyn nieuczciwej konkurencji, o którym mowa w art. 24 u.o.k.k.

5. Projektowane zmiany legislacyjne

Warto zwrócić również uwagę na stanowiące w chwili obecnej przedmiot prac legislacyjnych projekty (rządowy i poselski) nowelizacji ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne [20], które zawierają propozycje wprowadzenia na grunt tej ustawy szeregu dodatkowych rozwiązań legislacyjnych służących zwalczaniu *spammingu* [23, 24]. W myśl założeń obydwu projektów kolejnym, obok Prezesa UOKiK, centralnym organem administracji rządowej zajmującym się zwalczaniem analizowanego zjawiska, stałby się Prezes Urzędu Komunikacji Elektronicznej (dalej: Prezes UKE). Zakładają one wprowadzenie zakazu przesyłania bez uprzedniej zgody odbiorcy:

- komunikatów, których treść i kontekst są niezależne od tożsamości odbiorcy;
- komunikatów, których zadaniem jest tworzenie baz danych teleadresowych odbiorców, w szczególności dla celów marketingowych;
- informacji handlowej tj. każdej informacji przeznaczonej *„bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niesłużącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi”* (art. 2 pkt 2 u.ś.u.d.e.).

Przesyłanie *spamu*, zlecanie jego przesyłania lub odnoszenie korzyści z jego przesłania podlegać miałoby administracyjnej karze pieniężnej, nakładanej przez Prezesa UKE. Jej wysokość, w zależności od zakresu naruszenia, dotychczasowej działalności ukaranego podmiotu oraz jego możliwości finansowych, mogłaby wynosić od 100 do 100.000 PLN [5, 23, 24].

Nie sposób pominąć jednakże rozwiązań organizacyjno-technicznych służących zarówno wykryciu źródeł niezamówionej informacji handlowej, jak i przeciwdziałaniu jej rozpowszechnianiu, których obowiązek wdrożenia spoczywać miałby na Prezesie UKE. Mowa tutaj o utworzeniu centrum zajmującego się przyjmowaniem zgłoszeń o *spamie*, którego zadaniem miałoby być gromadzenie informacji i dowodów na potrzeby prowadzonych postępowań „antyspamowych” zmierzających do wykrywania i eliminowania źródeł tego procederu. Na samych dostawcach usług telekomunikacyjnych spoczywałby zaś obowiązek utworzenia punktów przyjmowania skarg klientów na nadsyłany z ich

pośrednictwem *spam*, którego nieprzestrzeganie zagrożone byłoby karą od 100 do 5.000 PLN [5, 23, 24].

W przypadku wprowadzenia projektowanych zmian w życie, w obszarze przeciwdziałania *spamowi* właściwymi stałyby się więc dwa organy administracji – Prezes UOKiK i Prezes UKE, spośród których pierwszy jest organem generalnie właściwym we wszystkich sprawach związanych z ochroną konkurencji i konsumentów, drugi jest natomiast sektorowym telekomunikacyjnym organem regulacyjnym. Podkreślić przy tym jednak należy, że chociaż prawna dopuszczalność równoległego podejmowania przez nie działań prokonkurencyjnych nie budzi wątpliwości, to przyznane im do dyspozycji antyspamowe środki represyjne miałyby taką samą naturę i pełniłyby podobne funkcje.

6. Wnioski

Spamming i jego odmiany, podobnie jak oprogramowanie złośliwe, jest coraz częściej wykorzystywany w celu osiągnięcia nielegalnych korzyści majątkowych, stąd też - z uwagi na znaczące, tak społeczne jak i ekonomiczne skutki niedozwolonych działań w tym zakresie - konieczna jest odpowiednia reakcja na ten proceder, przybierająca postać zarówno dostosowania prawa krajowego do zachodzących przemian technologicznych, jak i zwiększona świadomość użytkowników łączności elektronicznej [14]. Rozwiązania służące jego zwalczaniu, które są znane polskiemu ustawodawstwu uznać należy z jednej strony za wystarczająco dolegliwe, zwłaszcza w przypadku konsekwencji finansowych administracyjnej kary pieniężnej, jakkolwiek w pewnej mierze niespójne z uwagi na rozproszenie w kilku aktach normatywnych rangi ustawowej. Tym niemniej niezwykle istotne jest wykorzystanie w walce ze *spamem* również odpowiedniego instrumentarium informacyjno-technologicznego, umocowanego z oczywistych względów w postanowieniach przepisów powszechnie obowiązującego prawa.

W ostatnim czasie daje się zauważyć obostrzenie reakcji karnej za przestępstwa określane mianem komputerowych, jak chociażby bezprawne ingerowanie w systemy informatyczne [6]. Wydaje się przy tym jednak, że przeciwdziałanie szkodliwym społecznie praktykom użytkowników łączności elektronicznej, w szczególności komunikujących się za pośrednictwem Internetu, wyłącznie w drodze zaostrzenia wymiaru sankcji, czy to karnych, czy to administracyjnych, nie doprowadzi do wyeliminowania tych zjawisk z życia gospodarczego w stopniu wystarczającym.

Za niezbędne uznać należy bowiem stworzenie specjalnych regulacji prawnych wprowadzających obligatoryjne standardy bezpieczeństwa systemów informatycznych, służące identyfikacji źródeł i nadawców *spamu* oraz stworzeniu skutecznych i ogólnodostępnych barier uniemożliwiających jego niczym nieskrępowane rozpowszechnianie, ale także propagowanie właściwych reguł postępowania (w tym kodeksów etycznych) wśród wszystkich uczestników wymiany informacji (tj. nadawców i odbiorców) w sieci internetowej, lecz przede wszystkim wśród przedsiębiorców prowadzących działalność gospodarczą w obszarze e-commerce i wykorzystujących nośniki elektroniczne do przekazu informacji handlowej.

7. Literatura

[1] A. Adamski: Prawo karne komputerowe. Wydawnictwo C.H. Beck, Warszawa, 2000.

[2] A. Gajowniczek: Wykorzystanie Internetu w celu reklamy - wybrane zagadnienia prawne. Warszawa, 1999, http://www.vagla.pl.

[3] Królowie spamu. Chip, 2008, Nr 10, s. 30.

[4] McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet. July 2005.

[5] M. Kosiarski: Za wysłanie spamu nawet 100 tys. zł kary. Rzeczpospolita, 19.12.2008 r.

[6] A. Łukaszewicz: Przestępstwa w sieci traktowane surowiej. Rzeczpospolita, 18.12.2008 r.

[7] International Telecommunications Union: Overall aspects of countering spam in IP-based multimedia applications. Recommendation ITU-T, X.1244 (09.2008).

[8] P. Polański: Prawne problemy spamdexingu. Prawo Nowych Technologii, 2008, Nr 3, s. 4-11.

[9] M. Sieradzka: Komentarz do ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz. Oficyna, 2008.

[10] P. Waglowski: Spam w postaci niezamówionej informacji handlowej jako delikt nieuczciwej konkurencji [w:] A. Tubielewicz (red.): Problemy Informatyki w Zarządzaniu. Wydział Zarządzania i Ekonomii Politechniki Gdańskiej, Gdańsk, 2003, s. 83-108.

[11] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U.UE.L.00.178.1).

[12] Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady (dyrektywa o nieuczciwych praktykach handlowych) (Dz.U.UE.L.05.149.22).

[13] Komunikat Komisji Europejskiej do Rady Unii Europejskiej, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów w sprawie przeglądu ram regulacyjnych sieci i usług łączności elektronicznej w Unii Europejskiej. Proponowane zmiany {COM(2006)334 końcowy}.

[14] Komunikat Komisji Europejskiej do Rady Unii Europejskiej, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów w sprawie zwalczania spamu, oprogramowania szpiegowskiego i złośliwego oprogramowania. Wersja ostateczna {COM(2006)688}.

[15] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów w kierunku ogólnej strategii zwalczania cyberprzestępczości {SEK(2007)641} {SEK(2007)642}. Wersja ostateczna {COM(2007)267}.

[16] Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (Tekst jednolity Dz. U. z 2007 r. Nr 109, poz. 756, ze zm.).

[17] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.).

[18] Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2008 r. Nr 133, poz. 848, ze zm.).

[19] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, ze zm.).

[20] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, ze zm.).

[21] Ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. Nr 50, poz. 331, ze zm.).

[22] Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (Dz. U. Nr 171, poz. 1206).

[23] Ministerstwo Infrastruktury, Projekt ustawy o zmianie ustawy Prawo telekomunikacyjne oraz niektórych innych ustaw, 25 listopada 2008 r.

[24] Poselski projekt ustawy o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw, Sejm RP VI kadencji, Druk nr 1452.

[25] http://www.i-slownik.pl.

[26] http://www.uke.gov.pl.

[27] http://www.uokik.gov.pl.

Artykuł recenzowany