

# Mariusz Czyżak

---

## Wybrane aspekty prawnej ochrony usług świadczonych drogą elektroniczną

---

Ekonomiczne Problemy Usług nr 57, 743-751

---

2010

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MARIUSZ CZYŻAK

Urząd Komunikacji Elektronicznej

m.czyzak@uke.gov.pl

## WYBRANE ASPEKTY PRAWNEJ OCHRONY USŁUG ŚWIADCZONYCH DROGĄ ELEKTRONICZNĄ

### Wprowadzenie

Towarzyszący współczesnemu społeczeństwu w dobie globalizacji stały rozwój technologiczny sprawia, że prawnu coraz trudniej przychodzi reagować na różnorodne zjawiska patologiczne związane z wykorzystywaniem nowoczesnych rozwiązań teleinformatycznych. Wspomniana teza odnosi się w znacznej mierze do tego obszaru działalności gospodarczej, który wykorzystuje łączność elektroniczną jako nośnik informacji, zwłaszcza na płaszczyźnie wymiany intelektualnej i ekonomicznej. Instrumenty służące prowadzeniu działalności gospodarczej (np. bankowość elektroniczna, sklepy internetowe), stają się często narzędziem popełnienia przestępstwa, i to takiego, które godzi w prawo własności, tajemnicę komunikowania się, porządek publiczny i bezpieczeństwo powszechne, a nawet zdrowie i życie człowieka.

Jednym z najistotniejszych problemów, które stoją obecnie przed społeczeństwem, jest zatem kwestia etycznych wyznaczników rozwoju technologicznego<sup>1</sup> i właściwy dobór środków reakcji organów ochrony prawnej na szkodliwe zachowania, naruszające prawa i wolności uczestników rynku usług komunikacji elektro-

---

<sup>1</sup> Za wysoce trafną uznać należy przy tym diagnozę zaistniałego stanu rzeczy przedstawioną na gruncie katolickiej nauki społecznej. Zdaniem Benedykta XVI, „*Rozwój technologiczny może zrodzić ideę samowystarczalności techniki [...]. Z tego też powodu technika przyjmuje dwuznaczne oblicze. Zrodzona z twórczości ludzkiej jako narzędzie wolności człowieka, może być ona pojmowana jako element wolności absolutnej, tej wolności, która chce abstrahować od ograniczeń, jakie rzeczy zawierają w sobie*”. Benedykt XVI encyklika *Caritas in veritate*, 2009, s. 70.

nicznej. Ustawodawca sięga w tym przypadku częstokroć po szczególnie dolegliwe instrumenty o charakterze prawnokarnym i karnoadministracyjnym. Nie sposób byłoby w ramach niniejszych rozważań przedstawić całości regulacji prawnych służących ochronie tego sektora gospodarki na gruncie polskiego systemu prawnego. Przedmiotem dalszych rozważań staną się zatem jedynie wybrane rozwiązania legislacyjne służące ochronie usług komunikacji elektronicznej o największym, jak się wydaje, zastosowaniu w działalności gospodarczej, które związane są z przesyłaniem drogą elektroniczną niezamówionej informacji handlowej (spammingiem), wydawaniem i używaniem elektronicznych instrumentów płatniczych oraz przestrzeganiem tajemnicy telekomunikacyjnej.

## 1. Zwalczanie spammingu

Samo określenie „spam” ma swoje źródło w języku angielskim i oznacza skrót od wyrażenia *spiced pork and ham*, co wskazuje na zawartość oraz charakter informacji za niego uznawanych. Niekiedy określany bywa także jako *junk-mail* (rupiecie pocztowe), UCE (*ang. Unsolicited Commercial E-mail* – niepożądany list komercyjny) czy też UBE (*ang. Unsolicited Bulk E-mail* – niepożądany list niekomercyjny)<sup>2</sup>.

Zgodnie z postanowieniami art. 10 ust. 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną<sup>3</sup> (dalej: u.ś.u.d.e.) zakazane jest „przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej”, jakkolwiek za *spam* uznać należy również niezamówione informacje o charakterze np. politycznym lub ideologicznym. Zgodnie z postanowieniami art. 24 ust. 1 u.ś.u.d.e., przesyłanie *spamu* stanowi wykroczenie i podlega karze grzywny od 20 do 5000 złotych. *Spamming* w przytoczonym powyżej znaczeniu ustawowym został uznany również za czyn nieuczciwej konkurencji<sup>4</sup> (art. 10 ust. 3 u.ś.u.d.e.) i jako taki podlega odpowiedzialności karnoadministracyjnej na gruncie ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów<sup>5</sup>. Prezes Urzędu Ochrony Konkurencji i Konsumentów może wymierzyć przedsiębiorcy administracyjną karę pieniężną w wysokości do 10% przychodu osiągniętego przez

---

<sup>2</sup> Zob. M. Czyżak, *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary Automatyka Kontrola” 2009, nr 7, s. 548-549.

<sup>3</sup> Dz.U. nr 144, poz. 1204, z późn. zm.

<sup>4</sup> W myśl postanowień art. 3 ust. 1 przepisu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Tekst jednolity Dz.U. z 2003 r. nr 153, poz. 1503, z późn. zm.), czynem nieuczciwej konkurencji jest „działanie sprzeczne z prawem lub dobrymi obyczajami, jeżeli zagraża lub narusza interes innego przedsiębiorcy lub klienta”.

<sup>5</sup> Dz.U. nr 50, poz. 331, z późn. zm.

niego w roku rozliczeniowym poprzedzającym rok nałożenia kary, jeżeli dopuścił się on, nawet nieumyślnie, stosowania *spammingu*.

Nadmienić należy jednakże, że skala *spammingu* okazała się na tyle duża, a jego powiązanie z niektórymi szczególnie szkodliwymi społecznie formami przestępczości internetowej na tyle powszechne, że pożądane stało się wykorzystanie nowych narzędzi zapobiegania rozprzestrzenianiu się spamu. Stały się one przedmiotem opracowanego w Ministerstwie Infrastruktury „Projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne i niektórych innych ustaw”<sup>6</sup> (dalej: n.P.t.). Zakłada on nowelizację ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne<sup>7</sup> (dalej: P.t.) i włączenie prezesa Urzędu Komunikacji Elektronicznej (dalej: prezes UKE) do grona organów ochrony prawnej zajmujących się przeciwdziałaniem temu zjawisku.

Zgodnie z analizowanym projektem nowelizacji ustawy Prawo telekomunikacyjne zakazane byłoby przesyłanie bez uprzedniej zgody odbiorcy: komunikatów o treści i kontekście niezależnym od tożsamości odbiorcy; komunikatów za pomocą automatycznych systemów wywołujących, dla celów marketingu bezpośredniego; komunikatów, których zadaniem jest tworzenie baz danych teleadresowych odbiorców, w szczególności dla celów marketingowych; informacji handlowej<sup>8</sup>.

W myśl postanowień projektu prezes UKE zobligowany byłby do wszczęcia z urzędu postępowania w sprawach o nałożenie kary pieniężnej za *spamming*, jeśli ze względu na jego charakter, częstotliwość lub ilość stanowi on „zagrożenie dla integralności lub bezpieczeństwa sieci lub świadczenia usług telekomunikacyjnych” (art. 175c n.P.t.), natomiast ciężar udowodnienia posiadania zgody odbiorcy na przesłanie tego rodzaju komunikatów i informacji spoczywałby na wysyłającym informację handlową (art. 175a ust. 3 n.P.t.). Podczas prowadzonego postępowania prezes UKE mógłby żądać od dostawców usług telekomunikacyjnych i operatorów dostarczenia, we wskazanym przez niego terminie, informacji niezbędnych dla wypełnienia jego zadań, w tym danych osobowych abonentów (art. 175e n.P.t.), zaś przy UKE funkcjonować miałyby jednostka organizacyjna zajmująca się przyjmo-

---

<sup>6</sup> Projekt ustawy o zmianie ustawy – Prawo telekomunikacyjne i niektórych innych ustaw, wersja projektu z 14 maja 2009 r., Ministerstwo Infrastruktury, Departament Telekomunikacji, <http://bip.mi.gov.pl>.

<sup>7</sup> Dz.U. 2004, nr 171, poz. 1800, z późn. zm.

<sup>8</sup> W myśl postanowień przepisu art. 2 pkt 2 ustawy o świadczeniu usług drogą elektroniczną informacją handlową jest każda informacja przeznaczona „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”.

waniem zgłoszeń o spamie (art. 175d n.P.t.). Dostawcy usług telekomunikacyjnych zobowiązani zostaliby do niezwłocznego przesyłania do wspomnianego powyżej ośrodka wszelkich informacji dotyczących zlokalizowanego w ramach świadczonych usług zakończenia sieci, z którego został wysłany spam, a także informacji o przypadkach przesyłania do ich abonentów spamu spoza terytorium Polski (art. 175g ust. 6 i 7 n.P.t.).

Projekt zakłada stosunkowo szerokie granice dolegliwości tej sankcji administracyjnej – od 100 do 100 000 złotych w przypadku przesyłania spamu i od 100 do 5000 złotych w przypadku pozostałych deliktów administracyjnych zaproponowanych w analizowanym projekcie, np. zaniechania realizacji ww. obowiązków informacyjnych (art. 209a ust. 2 i 3 n.P.t.).

## 2. Ochrona elektronicznych instrumentów płatniczych

Jedną z głównych cech, którą odznacza się współczesny obrót gospodarczy, jest wzrost znaczenia pieniądza elektronicznego. Przyczyn takiego stanu rzeczy upatrywać należy w dwojakiego rodzaju przesłankach. Z jednej strony ułatwia on bowiem wymianę handlową na odległość, z drugiej zaś strony zapewnia wbrew pozorom swoiste bezpieczeństwo, obce transakcjom gotówkowym. Sam pieniądz elektroniczny jest instytucją prawa bankowego podlegającą ścisłym regulacjom prawnym, poczynając od jego legalnej definicji, a kończąc na niezwykle restrykcyjnych zasadach obrotu nim.

W świetle przepisów art. 4 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe<sup>9</sup> (dalej: P.b.), pieniądzem elektronicznym jest zatem wartość pieniężna będąca elektronicznym odpowiednikiem znaków pieniężnych, która spełnia łącznie następujące przesłanki: jest przechowywana na informatycznych nośnikach danych, jest wydawana do dyspozycji na podstawie umowy w zamian za środki pieniężne o nominalnej wartości nie mniejszej niż ta wartość, jest przyjmowana jako środek płatniczy przez przedsiębiorców innych niż wydający ją do dyspozycji, na żądanie jest wymieniana przez wydawcę na środki pieniężne, jest wyrażona w jednostkach pieniężnych.

Ustawodawca poddał również szczegółowej reglamentacji proces wydawania i używania elektronicznych instrumentów płatniczych. W myśl postanowień przepisu art. 2 pkt ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych<sup>10</sup> (dalej: u.e.i.p.) za elektroniczne instrumenty płatnicze uznaje się *„każdy instrument płatniczy, w tym z dostępem do środków pieniężnych na odległość, umożliwiającą posiadaczowi dokonywanie operacji przy użyciu informatycz-*

<sup>9</sup> Tekst jednolity Dz.U. 2002, nr 72, poz. 665, z późn. zm.

<sup>10</sup> Dz.U. 2002, nr 169, poz. 1385, z późn. zm.

nych nośników danych lub elektroniczną identyfikację posiadacza niezbędną do dokonania operacji, w szczególności kartę płatniczą<sup>11</sup> lub instrument pieniądza elektronicznego<sup>12</sup>. Uczestnikami tego procesu są zwykle: wydawca elektronicznego instrumentu płatniczego; posiadacz elektronicznego instrumentu płatniczego, tj. podmiot, który na podstawie umowy o elektronicznym instrumencie płatniczym dokonuje w swoim imieniu i na swoją rzecz operacji określonych w tej umowie (ewentualnie użytkownik karty płatniczej będący osobą fizyczną upoważnioną przez posiadacza do dokonywania w jego imieniu i na jego rzecz operacji określonych w umowie, której dane identyfikacyjne są umieszczone na karcie płatniczej); agent rozliczeniowy, tj. bank bądź inna osoba prawna zawierająca z akceptantami umowy o przyjmowanie zapłaty przy użyciu elektronicznych instrumentów płatniczych; oraz akceptant, tj. przedsiębiorca, który zawarł z agentem rozliczeniowym umowę o przyjmowanie zapłaty przy użyciu elektronicznych instrumentów płatniczych (art. 2 pkt 1,2,11,12 u.e.i.p.).

Ustawodawca poddał penalizacji, na gruncie ustawy o elektronicznych instrumentach płatniczych, trzy kategorie zachowań, które jego zdaniem stanowią czyny o najwyższym stopniu szkodliwości społecznej, zasługujące na reakcję podlegającą rygorowi prawa karnego.

Do pierwszej grupy należą zachowania godzące we wszelkie, bez ograniczenia, wskazane w przedmiotowej ustawie zasady wydawania elektronicznych instrumentów płatniczych (art. 71 u.e.i.p.). Podlegają one karze grzywny do 5 000 000 złotych lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie, zaś w przypadku, gdy przedmiotem tego czynu zabronionego jest instrument pieniądza elektronicznego, sprawca podlega kumulatywnie grzywnie do 5 000 000 złotych i karze pozbawienia wolności do lat 3. Wspomnianym powyżej karom podlega alternatywnie sprawca czynu polegającego z kolei na wydaniu elektronicznego instrumentu płatniczego wbrew warunkom określonym w ustawie, który działa w imieniu lub w interesie osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Za przestępstwo zagrożone karą grzywny do 1 000 000 złotych uznał ustawodawca również zaniechanie udzielania Narodowemu Bankowi Polskiemu lub udzielanie niezgodnie z prawem informacji wskazanych w ustawie o elektronicznych instrumentach płatniczych (art. 72 u.e.i.p.). Mowa tutaj w szczególności o obowiązkach informacyjnych nałożonych na: banki i instytucje pieniądza elektronicz-

---

<sup>11</sup> Za kartę płatniczą uznaje się „kartę identyfikującą wydawcę i upoważnionego posiadacza, uprawniającą do wypłaty gotówki lub dokonywania zapłaty, a w przypadku karty wydanej przez bank lub instytucję ustawowo upoważnioną do udzielania kredytu – także do dokonywania wypłaty gotówki lub zapłaty z wykorzystaniem kredytu” (art. 4 ust. 1 pkt 4 P.b.)

<sup>12</sup> Za instrument pieniądza elektronicznego uznaje się „urządzenie elektroniczne, na którym jest przechowywany pieniądz elektroniczny, w szczególności karta elektroniczna zasilana do określonej wartości” (art. 2 pkt 6 u.e.i.p.).

nego, dotyczących wydawania pieniądza elektronicznego i instrumentu pieniądza elektronicznego oraz sytuacji finansowej wydawcy (art. 64 u.e.i.p.); agentów rozliczeniowych, dotyczących rozmiarów prowadzonej przez nich działalności (art. 13 u.e.i.p.); wydawców kart płatniczych, dotyczących np. liczby wydanych kart, przeprowadzanych za ich pomocą operacji oraz udostępnianych bankomatów (art. 15 u.e.i.p.). Służą one Narodowemu Bankowi Polskiemu zarówno do określenia łącznej wartości pieniądza elektronicznego w obrocie gospodarczym, jak również dostarczają danych statystycznych pozwalających określić rozmiary działalności związanej z wydawaniem i używaniem elektronicznych instrumentów płatniczych.

Trzecim typem czynu zabronionego, podlegającym karze grzywny do 1 000 000 złotych lub karze pozbawienia wolności do roku, jest sprzeczne z przepisami ustawy o elektronicznych instrumentach płatniczych prowadzenie reklamy i promocji działalności polegającej na wydawaniu elektronicznych instrumentów płatniczych i rozliczaniu operacji dokonywanych z ich użyciem (art. 73 u.e.i.p.). Ograniczenie to stanowi konsekwencję dyspozycji przepisu art. 65 u.e.i.p., w myśl którego reklamę i promocję tego rodzaju działalności mogą prowadzić jedynie podmioty uprawnione do jej wykonywania zgodnie z postanowieniami przepisów ustawy o elektronicznych instrumentach płatniczych lub podmioty działające w ich imieniu i na ich rzecz.

### 3. Ochrona tajemnicy telekomunikacyjnej

Komunikacja z wykorzystaniem techniki telekomunikacyjnej jest nieodłącznym elementem dziedziny działalności gospodarczej określanej mianem e-gospodarki. Komunikacja posiada przy tym strukturę dychotomiczną. Z jednej strony bowiem zapewnić ma niczym niezakłóconą wymianę informacji pomiędzy jej nadawcą i odbiorcą. Z drugiej strony ma być, co do zasady, niedostępna dla innych użytkowników technologii informacyjnych – w przypadku technologii telekomunikacyjnych tak klientów, jak i podmiotów prowadzących profesjonalną działalność w obszarze usług komunikacji elektronicznej. W rezultacie oczywiste jest, że tajemnica komunikowania się podlega ochronie prawnej. Dotyczy to w szczególności tych podmiotów, które z racji prowadzonej działalności gospodarczej odgrywają rolę swoistego pośrednika w procesie wymiany informacji we współczesnym świecie, a zatem przede wszystkim przedsiębiorców telekomunikacyjnych<sup>13</sup>.

<sup>13</sup> W myśl postanowień przepisu art. 2 pkt 27 P.t. za przedsiębiorcę telekomunikacyjnego uznaje się „przedsiębiorcę lub inny podmiot uprawniony do wykonywania działalności gospodarczej na podstawie odrębnych przepisów, który wykonuje działalność gospodarczą polegającą na dostarczaniu sieci telekomunikacyjnych, udogodnień towarzyszących lub świadczeniu usług telekomunikacyjnych”, przy czym ustawa wyodrębnia jednocześnie dwie kategorie tego rodzaju przedsiębiorców, tj. dostawców usług, uprawnionych do świadczenia usług telekomunikacyjnych, oraz operatorów, uprawnionych do dostarczania publicznych sieci telekomunikacyjnych lub

Tajemnica telekomunikacyjna stanowi realizację konstytucyjnej wolności komunikowania się, o której mowa w przepisie art. 49 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.<sup>14</sup>, zapewniającym wolność i ochronę tajemnicy komunikowania się, której ograniczenie może nastąpić jedynie ustawowo.

Pod pojęciem tajemnicy telekomunikacyjnej należy rozumieć tajemnicę komunikowania się w sieciach telekomunikacyjnych (art. 159 ust. 1 P.t.). Obejmuje ona w szczególności: dane dotyczące użytkownika; treść indywidualnych komunikatów; dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne; dane o lokalizacji; oraz dane o próbach uzyskania połączenia między określonymi zakończeniami sieci telekomunikacyjnej.

Zgodnie z postanowieniami przepisu art. 159 ust. 2 P.t. bezprawne jest „zapoznanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu”.

Naruszenie tajemnicy telekomunikacyjnej podlega tak odpowiedzialności karnoadministracyjnej na gruncie ustawy Prawo telekomunikacyjne, jak i prawnokarnej na gruncie ustaw karnych. W myśl postanowień przepisu art. 209 ust. 1 pkt 24 P.t. podmiot naruszający obowiązek zachowania tajemnicy telekomunikacyjnej, o którym mowa w art. 159 P.t. – podlega administracyjnej karze pieniężnej. Wymierza ją prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym, uwzględnienia ustawowe dyrektywy wymiaru kary pieniężnej, o których mowa w przepisie art. 210 ust. 2 P.t., tj. zakres naruszenia, dotychczasową działalność karanego podmiotu oraz jego możliwości finansowe<sup>15</sup>.

Tajemnica telekomunikacyjna podlega również, w pewnej mierze, ochronie prawnokarnej. W myśl postanowień przepisu art. 266 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny<sup>16</sup> (dalej: K.k.) „Kto, wbrew przepisom ustawy (w szczególności ustawy Prawo telekomunikacyjne – M.Cz.) lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z (...) wykonywaną pracą, działalnością (...) gospodarczą (...), podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”. Podkreślić przy tym należy, że obostrzonej odpowiedzialności, tj. karze pozbawienia wolności do lat 3, podlega funkcjonariusz publiczny, który „ujawnia osobie nieuprawnionej informację stanowiącą tajemnicę służbową lub informację, którą uzyskał w związku z wy-

---

udogodnień towarzyszących (S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2005, s. 82-83).

<sup>14</sup> Dz.U. 1997, nr 78, poz. 483, z późn. zm.

<sup>15</sup> M. Czyżak, *Kilka uwag o administracyjnej karze pieniężnej na gruncie ustawy Prawo telekomunikacyjne z 2004 r.*, „Studia Prawnicze KUL” 2008, nr 2, s. 12-15.

<sup>16</sup> Dz.U. 1997, nr 88, poz. 553, z późn. zm.



*konywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes*". Szczególnej ochronie prawnokarnej poddaje ustawodawca tajemnicę telekomunikacyjną także na gruncie przepisu art. 267 § 1 K.k., stanowiąc: „*Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, (...) podłączając się do sieci telekomunikacyjnej (...), podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*”.

Pokrewnym przytoczonym powyżej typom czynów zabronionych jest przestępstwo nieuprawnionego zakłócania w istotnym stopniu pracy sieci teleinformatycznej, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, które powiązane może być z naruszeniem tajemnicy telekomunikacyjnej i podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (art. 269a K.k.). Tego typu zakłóceniu pracy sieci teleinformatycznej towarzyszyć może bowiem naruszenie tajemnicy telekomunikacyjnej na skutek zapoznania się przez nieuprawnioną osobę z informacjami przesyłanymi za ich pośrednictwem.

#### **4. Uwagi końcowe**

Stopień wykorzystania handlu elektronicznego, elektronicznych instrumentów płatniczych oraz telekomunikacji do porozumiewania się, jest z pewnością poważnym wyznacznikiem poziomu rozwoju społeczeństwa informacyjnego, a zatem i kondycji tzw. e-gospodarki, będącej jego istotnym elementem.

Jednym z najpoważniejszych zadań, które stoją obecnie przed rynkiem usług komunikacji elektronicznej, jest zapewnienie ich użytkownikom odpowiedniego poziomu bezpieczeństwa, zarówno ekonomicznego, jak i teleinformatycznego. Sami dostawcy tego rodzaju usług nie zdołali jednakże jak dotąd rozwiązać przedmiotowej kwestii w sposób zadowalający. Niezbędne stało się wobec tego nie tylko wyznaczenie przez ustawodawcę ścisłych ram prawnych ich wykonywania, służących zapewnieniu odpowiedniego zakresu ochrony klientów i przedsiębiorców we wspomnianym powyżej obszarze, a tym samym podniesieniu poziomu zaufania do idei społeczeństwa informacyjnego, ale również wykorzystanie narzędzi o charakterze prawnokarnym i karnoadministracyjnym, w celu utrzymania stanu przestrzegania prawa w tej gałęzi gospodarki państwa.

Przedstawione powyżej wybrane przykłady instrumentów ochrony usług świadczonych drogą elektroniczną, jakkolwiek stanowią jedynie wycinek szerokiego spektrum środków ochrony prawnej znanych polskiemu systemowi prawnemu, pozwalają stwierdzić, jak dużą uwagę przywiązuje ustawodawca do należytego zabezpieczenia prawidłowego świadczenia i korzystania z tej kategorii usług, której znaczenie stale wzrasta wraz ze współczesnym rozwojem technologicznym i gospodarczym.

**Literatura**

1. Benedykt XVI, Encyklika *Caritas in veritate*, 2009.
2. Czyżak M., *Spamming i jego karalność w polskim systemie prawnym*, „Pomiary Automatyka Kontrola” 2009, nr 7.
3. Czyżak M., *Kilka uwag o administracyjnej karze pieniężnej na gruncie ustawy Prawo telekomunikacyjne z 2004 r.*, „Studia Prawnicze KUL” 2008, nr 2.
4. Piątek S., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2005.
5. Projekt ustawy o zmianie ustawy – Prawo telekomunikacyjne i niektórych innych ustaw, wersja projektu z 14 maja 2009 r., Ministerstwo Infrastruktury, Departament Telekomunikacji, <http://bip.mi.gov.pl>
6. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997, nr 78, poz. 483, z późn. zm.).
7. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997, nr 88, poz. 553, z późn. zm.).
8. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Tekst jednolity Dz.U. 2002, nr 72, poz. 665, z późn. zm.).
9. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002, nr 144, poz. 1204, z późn. zm.).
10. Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz.U. 2002, nr 169, poz. 1385, z późn. zm.).
11. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2004, nr 171, poz. 1800, z późn. zm.).

**SOME ASPECTS OF LEGAL PROTECTION  
OF SERVICES PROVIDED BY ELECTRONIC MEANS**

**Summary**

Technological progress requires that measures which would not only regulate the ways of providing services by electronic means but would also counteract undesirable phenomena related to the usage of ICT are applied by the legislator. The example of the latter covers in particular criminal law and penal administrative measures counteracting distribution of unsolicited commercial information (spamming), illegal issuance and usage of electronic payment means and the breach of telecommunications confidentiality.

*Translated by Mariusz Czyżak*