Anna Rogacka-Łukasik*

NARUSZENIE DÓBR OSOBISTYCH W INTERNECIE ORAZ ICH OCHRONA NA PODSTAWIE USTAWY O ŚWIADCZENIU USŁUG DROGĄ ELEKTRONICZNĄ

WSTĘP

Postęp techniczny, którego konsekwencją jest intensywny rozwój środków elektronicznego przekazu, przyczynił się do zainteresowania problematyką dóbr osobistych. W dobie współczesnej globalizacji Internetu ze szczególną uwagą należy przyjrzeć się zjawiskom w cyberprzestrzeni, które stanowią naruszenie bądź zagrożenie dóbr osobistych podmiotów uczestniczących w wymianie informacji za pomocą Internetu. W technologicznie skomplikowanym i elektronicznie zdominowanym świecie dobra osobiste zarówno osób fizycznych, jak i prawnych są systematycznie narażane[1]. Naruszeniu podlegają fundamentalne dobra osobiste osób fizycznych w postaci wolności, wizerunku, tajemnicy korespondencji, prywatności, nazwiska, pseudonimu, czy nazwy w przypadku osób prawnych.

Przedmiot rozważań niniejszej publikacji, po próbie zdefiniowania pojęcia dóbr osobistych i wskazaniu ich cech, stanowi przeanalizowanie zjawisk występujących w sieci Internet, które bezpośrednio zagrażają dobrom osobistym. Publikacja nie przedstawia wszystkich możliwych form naruszających dobra osobiste z uwagi na ich dużą ilość, jedynie te, które najczęściej występują w sieci Internet, chociażby takie jak spamming, cookies, phishing czy sniffing.

Ciągle trwający rozwój technologii elektronicznej, związanej w głównej mierze z wykorzystaniem Internetu, powoduje, iż należy analizować istniejące regulacje prawne właśnie przez pryzmat ich aktualności i oryginalności wobec panujących warunków. Dopełnieniem publikacji jest omówienie kwestii, w jaki sposób chronione są naruszone dobra osobiste na podstawie wybranej regulacji prawnej, znajdującej się poza kodeksem cywilnym[2]. Dla analizowanej problematyki ciekawą podstawę ochrony stanowi Ustawa o świadczeniu usług drogą elektroniczną[3]. Celem ustawy jest przeciwdziałanie zagrożeniom, jakie niesie ze sobą anonimowość podejmowanych w sieciach działań usługodawców.

* dr; Wyższa Szkoła Humanitas w Sosnowcu.

[1] J. Janowski, *Informatyka prawa. Zadania i znaczenie w związku z kształtowaniem się elektronicznego obrotu prawnego*, Lublin 2011, s. 423.

[2] Ustawa z dnia 23 kwietnia 1964r. – Kodeks cywilny, Dz.U. z 1964, nr 16, poz. 93 z późn. zm., określany jako k.c.

[3] Ustawa o z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2011r., nr 134, poz. 779, określana jako u.ś.u.d.e.

I. UWAGI WPROWADZAJĄCE W PROBLEMATYKĘ DÓBR OSOBISTYCH

1. POJĘCIE DÓBR OSOBISTYCH

Przymiotem każdej osoby fizycznej są jej dobra osobiste, które podlegają ochronie prawnej uregulowanej w różnych gałęziach prawa[4]. Pojęcie dóbr osobistych nie zostało zdefiniowane ani w konstytucji, ani w kodeksie cywilnym. W art. 23 k.c. ustawodawca ograniczył się tylko do wskazania przykładowego wyliczenia dóbr osobistych osób fizycznych, przy równoczesnym zapewnieniu im ochrony. Dobra osobiste stanowią rozległy, bardzo zróżnicowany charakter. Przepis artykułu 23 k.c. formułuje zasadę cywilnoprawnej ochrony dóbr osobistych, którą na podstawie art. 43 k.c. należy odnosić również do osób prawnych. Katalogu przykładowo wymienionych w art. 23 k.c. dóbr osobistych osób fizycznych nie da się wprost odnieść do osób prawnych. Jednakże wytyczne, które z niego wynikają, są pomocne przy konstruowaniu dóbr osobistych osób prawnych[5]. W związku z powyższym określenie treści i zakresu pojęcia dóbr osobistych stało się niezbędnym celem ustawodawcy, aby w ogóle móc rozstrzygnąć, kiedy mamy do czynienia z dobrem osobistym[6].

Wydaje się słusznym uprzednie zdefiniowanie samego pojęcia „dobro". W literaturze wskazuje się, iż dobro może służyć ludziom do zabezpieczenia ich potrzeb życiowych, ale traktowane w sensie normatywnym, a więc ze względu na które uregulowane są prawa i obowiązki podmiotów stosunków prawnych[7].

Przechodząc do próby zdefiniowania dóbr osobistych, należy podkreślić, iż początkowo przy objaśnianiu istoty dóbr osobistych dominowało kryterium subiektywne, które przy definiowaniu dóbr osobistych nacisk kładło na odczucia osoby żądającej ochrony prawnej[8]. Reprezentantem takiego podejścia był szczególnie S. Grzybowski, w ujęciu którego dobra osobiste to indywidualne wartości świata uczuć, stanu psychicznego człowieka[9]. Jednakże współcześnie dominuje pogląd, zgodnie z którym przy wyjaśnianiu istoty dóbr osobistych, jak i ich naruszeń, należy posługiwać się ujęciem obiektywnym, które odwołuje się do ocen przyjętych w społeczeństwie[10]. Uwzględniając tak przyjęte kryterium, wskazuje się w literaturze, iż dobra osobiste to uznane przez system prawny wartości, które obejmują fizyczną i psychiczną integralność człowieka, jego indywidualność oraz godność i pozycję w społeczeństwie, co stanowi przesłankę samorealizacji osoby ludzkiej[11].

Poza przedstawicielami nauki również w orzecznictwie podjęto próbę ustalenia definicji dóbr osobistych. Sąd Najwyższy w swoim wyroku z dnia 19 września 1968 r.[12], w którym przychylił się do panującego poglądu obiektywnego ujęcia dóbr osobistych, sprecyzował do-

[4] J. Kremis [w:] *Podstawy prawa cywilnego*, red. E. Gniewek, Warszawa 2011, s. 48.
[5] M. Pazdan [w:] *Prawo cywilne – część ogólna*, t. I, Warszawa 2007; M. Safjan [w:] *System Prawa Prywatnego. Prawo cywilne – część ogólna*, t. I, red. Z. Radwański, s. 1118.
[6] S. Grzybowski [w:] *System Prawa Cywilnego. Część ogólna*, [w:] *System Prawa Cywilnego*, t. I, red. naczelny W. Czachórski, Wrocław – Warszawa – Kraków – Gdańsk – Łódź 1985, s. 300.
[7] S. Sołtysiński, *Charakter prawny wynalazcy*, Poznań 1967, s. 119.
[8] K. Grzybczyk, *Naruszenie dobra osobistego w reklamie*, „Rejent" 1999, nr 9, s. 120.
[9] S. Grzybowski, *Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego*, Warszawa 1957, s. 78.
[10] M. Pazdan [w:] *Kodeks cywilny. Komentarz do artykułów 1-449[1o]*, t. I, red. K. Pietrzykowski, Warszawa 2011, s. 119.
[11] Z. Radwański, *Prawo cywilne – część ogólna*, Warszawa 1997, s. 148.
[12] Wyrok SN z dnia 19 września 1968 r., II CR 291/68.

bra osobiste jako wartości związane z wewnętrzną stroną życia ludzi, niejednakowo wymierzalne, podlegające ochronie cywilnej w razie ich bezprawnego naruszenia lub zagrożenia.

Konkludując, należy stwierdzić, iż dobra osobiste stanowią wyróżnik każdego człowieka jako osoby fizycznej, są w sposób nieodłączny i ścisły związane z człowiekiem[13], będąc mu przynależne. Są również cechą osób prawnych, a także jednostek organizacyjnych nieposiadających osobowości prawnej, jednakże wyposażonych w zdolność prawną[14].

2. CECHY DÓBR OSOBISTYCH

Niezaprzeczalną cechą dóbr osobistych jest ich niemajątkowy charakter, oznaczający, że ich przedmiotem są dobra niematerialne. Oznacza to, że dóbr osobistych nie można uzewnętrznić w kategoriach ekonomicznych. Niemajątkowego charakteru dóbr osobistych nie przekreśla nawet sytuacja, że ich naruszenie niesie ze sobą skutki w sferze majątkowej.

Istotną cechą dóbr osobistych jest to, iż są one ściśle związane z podmiotem podlegającym ochronie. Konsekwencją ścisłego związku dóbr osobistych z podmiotem jest to, że powstają i wygasają razem z nim. Dobra osobiste są niezbywalne, gdyż nie ma możliwości ich oddzielenia od konkretnego podmiotu, jak również są niedziedziczne, ponieważ brak jest możliwości ich przeniesienia na inne osoby. Niektóre prawa osobiste osoby zmarłej mogą być wykonywane przez jej osoby bliskie, jednakże wówczas przyjmuje się, iż są to prawa podmiotowe najbliższych członków rodziny zmarłego.

Do ochrony dóbr osobistych człowieka w prawie cywilnym służą prawa podmiotowe osobiste, które mają charakter praw podmiotowych bezwzględnych. Skutkiem powyższego jest nadanie kolejnej, niewątpliwej cechy dobrom osobistym: bezwzględny charakter praw wynikających z dóbr osobistych, oznaczający ich skuteczność *erga omnes*, a więc wobec wszystkich (osób fizycznych i prawnych)[15].

3. POSTACIE DÓBR OSOBISTYCH

Ramy niniejszej publikacji nie pozwalają na omówienie poszczególnych dóbr osobistych. Zagadnienie to nie stanowi również jej celu, ma jedynie zasygnalizować rodzaje dóbr osobistych zarówno osób fizycznych, jak i prawnych, aby można było przejść do omówienia form ich naruszenia. Katalog dóbr osobistych charakteryzuje dynamika rozwoju. Postęp cywilizacyjny, w szczególności techniczny, stał się głównym stymulatorem ich rozwoju. Judykatura i doktryna odkrywają coraz to nowe rodzaje dóbr osobistych[16].

Do dóbr osobistych osób fizycznych należy zaliczyć w pierwszej kolejności te, które zostały wskazane przez ustawodawcę w art. 23 k.c., a więc: zdrowie, wolność, swoboda sumienia, nazwisko bądź pseudonim, cześć człowieka, wizerunek[17], tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza, racjonalizatorska. Zgodnie z tym co zostało już zasygnalizowane, nie ulega wątpliwości, iż pod wpływem

[13] Z. Radwański, *Prawo cywilne – część ogólna*, Warszawa 2009, s. 156.
[14] A. Kawałko, H. Witczak, *Prawo cywilne – część ogólna*, Warszawa 2011, s. 122.
[15] S. Dmowski, S. Rudnicki, *Komentarz do Kodeksu cywilnego. Księga pierwsza. Część ogólna*, Warszawa 2011, s. 110.
[16] M. Pazdan [w:] *Kodeks cywilny...*, s. 123 i nast.
[17] A. Matlak, *Cywilnoprawna ochrona wizerunku*, „Kwartalnik Prawa Prywatnego" 2004, z. 2, s. 318 i nast.

zarówno doktryny, jak również orzecznictwa powstają coraz to nowe dobra osobiste człowieka. Najważniejszym dobrem osobistym człowieka, nieujętym w omawianym powyżej artykule, jest jego życie. Ochronę życia gwarantuje art. 38 Konstytucji RP[18], a przestrzeganiu tej zasady służą przepisy prawa karnego[19]. Do takich dóbr osobistych zalicza się także nietykalność cielesną, integralność seksualną, stan cywilny, poczucie przynależności do określonej płci, kult po zmarłej osobie bliskiej, sfera prywatności[20], jak również korzystanie z nieskażonego środowiska naturalnego, bądź tradycję rodzinną rozumianą jako dziedzictwo[21].

Przechodząc z kolei do dóbr osobistych osób prawnych, można przykładowo wskazać na dobre imię osoby prawnej, będące odpowiednikiem czci człowieka, tajemnicę korespondencji czy nazwę osoby prawnej bądź podmiotu bez osobowości prawnej[22]. Jednakże należy z całą stanowczością podkreślić, iż pomimo kilku odpowiedników dóbr osobistych osób fizycznych i osób prawnych, nie wszystkie ich postacie są takie same. Należy dojść do wniosku, iż do dóbr osobistych osób prawnych nie będą zaliczały się te dobra, które są atrybutami człowieka, nierozerwalnie z nim związane. Chodzi tutaj między innymi o życie i zdrowie, swobodę sumienia, wolność bądź integralność seksualną.

II. INTERNET JAKO ZAGROŻENIE DÓBR OSOBISTYCH

Nowoczesna technika i sposoby przekazywania informacji są przejawem intensywnego rozwoju nowoczesnych technologii[23]. Szczególnie w drugiej połowie lat dziewięćdziesiątych, kiedy to inwestowanie w spółki nowych technologii (*dotcoms*) osiągnęło apogeum, nastąpił gwałtowny rozwój medium komunikacyjnego opartego na globalnej sieci połączeń, jakim jest Internet. Internet jest globalnym systemem wymiany danych, funkcjonującym w oparciu o wzajemnie połączone sieci lokalne, rozmieszczone w wielu lokalizacjach, który umożliwia jednoczesną interakcję użytkowników z całego świata[24]. Można zaryzykować twierdzenie, iż żadne inne medium nie rozwijało się w tak szybkim tempie jak Internet, wywierając równocześnie ogromny wpływ na każdą dziedzinę życia[25]. Ten intensywny postęp techniczny, w szczególności w dziedzinie technik informatycznych i telekomunikacyjnych, prowadzi do konstatacji, iż z jednej strony jesteśmy zafascynowani czymś nowym, z drugiej rodzi się świadomość realnych zagrożeń w sferze życia prywatnego i rodzinnego jednostki. Wydaje się, iż z uwagi na globalność Internetu, można mówić o powstaniu nowego jakościowo społeczeństwa informacyjnego. Termin ten został wprowadzony w 1963 r. przez Japończyka T. Umesao w artykule o teorii ewolucji społeczeństwa opartego na technologiach informatycznych. Społeczeństwo informacyjne oznacza nowy system społeczny kształtujący się w krajach wysokiego rozwoju technologicznego, gdzie zarządzanie informacją odbywa się za pomocą nowoczesnych technik[26]. Z przedstawionej definicji społeczeństwa in-

[18] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r., nr 78 poz. 483 z późn. zm.
[19] M. Pazdan [w:] *Prawo cywilne – część ogólna*, t. I, red. M. Safjan [w:] *System Prawa Prywatnego:* s. 1119.
[20] M. Pazdan [w:] *Kodeks cywilny...*, s. 124 i nast.
[21] A. Kawałko, H. Witczak, *Prawo cywilne ...*, s. 127 i nast.
[22] M. Pazdan [w:] *Prawo cywilne–część ogólna*…, s. 1121 i nast.
[23] M. Wyrzykowski, *Ochrona danych osobowych*, Warszawa 1999, s. 9.
[24] J. Kulesza, *Ius internet. Między prawem a etyką*, Warszawa 2010, s. 23.
[25] D. Kasprzycki, *Spam, czyli niezamawiana komercyjna poczta elektroniczna: zagadnienia cywilnoprawne*, Kraków 2005, s. 21.
[26] J. Janowski, *Elektroniczny obrót prawny*, Warszawa 2008, s. 26.

formacyjnego można wywieść wniosek, iż najistotniejszymi cechami takiego społeczeństwa jest wysoko rozwinięty sektor usług nowoczesnych, jak również gospodarka uzależniona od wiedzy i na niej oparta. W tym właśnie społeczeństwie coraz częściej napotyka się silny opór użytkowników wobec pewnych zjawisk w nim występujących, i równocześnie dostrzega się, iż stosowanie nowych technologii w sferze informacji i komunikacji za pośrednictwem Internetu doprowadza do pojawiania się treści, które naruszają powszechne dobra osobiste zarówno osób fizycznych, jak również osób prawnych. Naruszenie dóbr osobistych w cyberprzestrzeni dotyczy praktycznie wszystkich form komunikacji, bowiem może być dokonane za pomocą stron www, kanałów „chat" czy przy użyciu poczty elektronicznej[27]. W rezultacie wskutek rozwoju globalnej sieci komputerowej stajemy w obliczu poważnych zagrożeń naszych dóbr osobistych. W związku z ekspansją Internetu w różne sfery aktywności ludzkiej, wkraczaniem w prawie każdą dyscyplinę prawniczą, wzrasta potrzeba poszukiwania stosownych rozwiązań prawnych, co stanowi olbrzymie wyzwanie dla prawodawcy. Ciągle powstające nowe sytuacje implikują konieczność tworzenia odpowiednich rozwiązań prawnych. Prawodawca musi rozstrzygać, czy wysyłanie informacji z danych dyscyplin prawniczych za pomocą Internetu jest legalne i jakie są tego skutki prawne.

W polskiej praktyce prawnej, na wzór zasad światowych regulacji, zrodziła się możliwość stosowania zasad pracy w Internecie. Do katalogu owych zasad – katalogu, który ma charakter wyłącznie przykładowy – można zaliczyć np. „szanuj prawa autorskie, chroń prywatność i dane osobowe, unikaj spamu", czy zasadę, iż powinna być możliwa dokładna identyfikacja nadawcy. Zespół takich zasad to tzw. netykieta, czyli kodeks zachowania się w sieci. Słowo netykieta wywodzi się ze złożenia dwóch słów pochodzących z języka angielskiego: *net* (sieć) oraz *etiquette* (etykieta) – stąd „etykieta sieciowa"[28]. Netykieta, jako zbiór zasad kultury obowiązującej w Internecie, mimo że kojarzy się z jakimś prawem, kodeksem, nie jest zbiorem zasad prawnie wiążących, nie ma mocy obowiązującego w polskim systemie prawnym aktu normatywnego, jest jedynie wyznacznikiem zachowań podejmowanych w Internecie.

III. FORMY NARUSZENIA DÓBR OSOBISTYCH W INTERNECIE

Spamming

Najpoważniejszym problemem charakterystycznym dla ery poczty elektronicznej, jak również zagrożeniem sfery prywatnej osoby fizycznej jako użytkownika Internetu jest *spamming* (spam). Spamming to notorycznie występujące i szkodliwe zjawisko, trudne do zdefiniowania. W literaturze wskazuje się, iż spamem jest informacja przesłana drogą elektroniczną, której treść jest niezależna od tożsamości odbiorcy (sama treść może być skierowana do kilku innych odbiorców), a jednocześnie odbiorca elektronicznej przesyłki nie wyraził uprzedniej, wyraźnej i świadomej, jak również możliwej do odwołania w każdym momencie zgody na otrzymanie przesyłki. Jednocześnie podkreśla się, iż treść informacji przesłanej elektronicznie daje odbiorcy podstawę do twierdzenia, iż nadawca wskutek jej wysłania może odnieść korzyści nieproporcjonalne w stosunku do korzyści odbiorcy wynikających z ich odebrania[29].

[27] A. Wojciechowska [w:] J. Barta, R. Markiewicz, *Media a dobra osobiste*, Warszawa 2009, s. 387.
[28] J. Kulesza, *Ius internet*..., s. 24 i nast.
[29] P. Waglowski, *Spam a prawo. Próba wskazania kierunków badawczych*, „Prawo i Ekonomia w Telekomunikacji" 2003, nr 4, s. 62.

Posługując się potocznym słownictwem, spam można zdefiniować jako list elektroniczny, najczęściej w postaci informacji reklamowej, zbędny dla adresata wiadomości. Jako cechy spamu można wyróżnić z jednej strony jego masowy charakter, co oznacza, że wiadomość tej treści wysyłana jest do większej liczby odbiorców, a zatem mamy do czynienia z brakiem skonkretyzowania odbiorcy, z drugiej zaś strony ma charakter komercyjny, promocyjny (reklamowy), przy pomocy którego podmioty wysyłające spam zamierzają osiągnąć korzyści majątkowe. Spamming można porównać do materiałów reklamowych (ulotek, katalogów) rozsyłanych tradycyjną pocztą. Jednakże pomiędzy tymi dwoma formami dostarczania korespondencji występuje zasadnicza różnica związana z kosztami. W przypadku spamu, o ile nadawca wiadomości, poza opłatą za dostęp do sieci, nie ponosi żadnych kosztów związanych z przesyłaniem danych, o tyle koszty po stronie odbiorcy wiadomości są niewspółmiernie wyższe. W sytuacji gdy użytkownik Internetu (odbiorca wiadomości) korzysta z Internetu za pomocą połączenia, którego koszt uzależniony jest od czasu trwania, wpływ niezamówionej korespondencji na opłaty internetowe jest ewidentny. Nie każdy komputer posiada zabezpieczenie w postaci programu antyspamowego i nie wszystkie programy pocztowe umożliwiają uprzednią identyfikację nagłówka listu, co mogłoby umożliwić podjęcie decyzji o ściągnięciu bądź nieściągnięciu wiadomości na dysk. Stały dostęp do Internetu przez użytkowników również nie zwalnia ich od niechcianego ponoszenia strat. Czas poświęcony na odebranie zbędnych informacji użytkownik mógłby przeznaczyć na inne zamierzone cele[30]. W świetle powyższych uwag należy z całą stanowczością podkreślić, iż otrzymywany w drodze elektronicznej spam narusza dobra osobiste zarówno osoby fizycznej, jako jednostki, jak również osób prawnych. Z punktu widzenia osób prawnych spam narusza ich dobra osobiste poprzez blokowanie lub przynajmniej opóźnianie oczekiwanej przez użytkownika korespondencji i poprzez uniemożliwienie dostania się do swojego konta. Naruszenie dóbr osobistych osób fizycznych przejawia się również w postaci utrudnień w swobodnym komunikowaniu się i prawidłowym funkcjonowaniu poprzez zapełnianie skrzynki pocztowej niechcianą korespondencją, co bezwzględnie stanowi naruszenie takich dóbr osobistych jak prywatność, wolność, pozyskiwanie informacji czy nawet zdrowie psychiczne[31].

Cookies

Wielu użytkowników sieci Internet pozostaje wciąż w przekonaniu, że używając Internetu pozostaje się anonimowym i zachowuje się prywatność. Twierdzenie takie jest błędne. Internet posiada mnóstwo mechanizmów pozwalających na gromadzenie danych, które umożliwiają zbieranie informacji o użytkownikach (o danych osobowych, danych bankowych, stronach, które przeglądali, zainteresowaniach)[32]. Dla gromadzenia takich danych służą *cookie,* które z całą pewnością są przejawem naruszenia dobra osobistego, jakim jest prywatność. Stanowią one krótkie pliki tekstowe, zawierające informacje, zapisywane w systemie informatycznym stosowane przez serwery w celu identyfikacji użytkowników sieci. Pliki te umożliwiają powtórny dostęp do witryn w razie ponownego połączenia z komputera, na którym zostały automatycznie zapisane. *Cookie* zawierają szereg informacji o usługobiorcy i o jego systemie, których uzyskiwanie odbywa się z re-

[30] D. Kasprzycki, *Spam...*, s. 34 i nast.
[31] P. Waglowski, *Prawo w sieci. Zarys regulacji internetu*, Gliwice 2005, s. 84.
[32] J. Kulesza, *Międzynarodowe prawo internetu*, Poznań 2010, s. 123 i nast.

guły bez jego wiedzy[33]. Wprawdzie sam plik *cookies* nie zawiera informacji, które pozwalają na identyfikację osoby, ale strona może już identyfikować użytkownika, którego przeglądarka wysyła plik *cookies*.

Usenet

Termin *Usenet* stanowi skrót pochodzący z języka angielskiego ***USE****r* ***NET****work* i oznacza sieć użytkowników. Usenet to ogólnoświatowy system serwerów oraz grup dyskusyjnych, z którego można korzystać przez Internet. Składa się on z tysięcy grup tematycznych, ułożonych w strukturę hierarchiczną[34]. Usenet to najpopularniejsze forum publicznych dyskusji w Internecie. Codziennie użytkownicy Internetu z całego świata publikują na jego grupach dyskusyjnych miliony wiadomości. Usenet charakteryzuje się kilkoma cechami, takimi jak np. ogólnoświatowa powszechność (serwery Usenetu są ze sobą w stałej łączności i stale wymieniają między sobą nadchodzące posty), czy też ścisła hierarchia grup tematycznych (grupy tworzą hierarchię, która jest jednakowa na wszystkich serwerach). Usenet, będący aktualnie usługą internetową, jest niewiele młodszy od Internetu i początkowo rozwijał się zupełnie od niego niezależnie. Pierwowzorem Usenetu była mała sieć oparta na serwerach na Uniwersytecie Duke i Uniwersytecie Północnej Karoliny połączonych razem zwykłą linią modemową. Sieć zapoczątkowana na Uniwersytecie Duke rozrastała się w szybkim tempie. W 1981 roku było już ponad 150 serwerów i kilka tysięcy użytkowników rozsianych po całych Stanach Zjednoczonych. Po wejściu w 1982 roku Uniwersytetu Duke do programu Arpanet (Advanced Research Project Agency), będącego początkiem rozwoju Internetu, serwer news tego uniwersytetu został podłączony do sieci opartej na protokołach TCP[35]/IP[36]. Oznaczało to, iż dowolne dwa komputery używające TCP/IP mogą być połączone ze sobą. Jeżeli w części sieci wystąpi usterka, informacja ominie ten fragment i inną drogą trafi do celu. Wszyscy użytkownicy Arpanetu mogli zacząć z niego korzystać. Serwer ten był jednocześnie nadal podłączony zwykłymi liniami modemowymi do tych serwerów, które jeszcze nie zostały podłączone do Arpanetu. Od tego momentu datuje się intensywny rozwój Usenetu[37]. Usenet umożliwia zatem wymianę poglądów z grupą osób zainteresowanych danym tematem, niezależnie od ich miejsca przebywania. Wiadomości są przechowywane na serwerach i nie są bezpośrednio wysyłane do zainteresowanych osób, ponieważ osoby te muszą je z serwera pobrać za pomocą odpowiedniego programu. Nie istnieje potrzeba zapisywania się do grup dyskusyjnych, a posty nie zapełniają skrzynek pocztowych uczestników dyskusji. Żeby dostać się do Usenetu, potrzebny jest specjalny program, tzw. czytnik newsów. Rolę taką spełnia np. Outlook Express. Choć niektóre grupy mają zasięg lokalny, to większość (a na pewno najpopularniejsze) znajduje się na wszystkich serwerach obsługujących Usenet. I co ważne – są na nich te same wiadomości. Działające w systemie komputery nieustannie komunikują się. Gdy połączą się dwa z nich, porównują to, co się na nich znajduje, po czym każdy „uzupełnia" braki drugiego. Dzięki temu wiadomości te można odczytać na serwerach znajdujących się w różnych częściach świata.

[33] J. Janowski, *Elektroniczny obrót*..., s. 26.
[34] P. Waglowski, *Prawo w sieci*..., s. 131.
[35] Transmission Control Protocol. TCP to protokół kontroli transmisji, według którego dane przesyłane w Internecie rozbijane są u nadawcy na tzw. pakiety i z powrotem składane w jedną całość u odbiorcy.
[36] Internet Protocol. IP to protokół definiujący sposób adresowania.
[37] P. Waglowski, *Prawo w sieci*..., s. 132 i nast.

Prowadzonym przez użytkowników Internetu na publicznym forum dyskusjom częstokroć towarzyszy łatwość formułowania ocen, gróźb skierowanych do danej osoby oraz umieszczania pewnych danych innych osób. Jeżeli na forum umieszczone jest bezprawnie (bez wiedzy osoby zainteresowanej) czyjeś nazwisko, pseudonim czy zdjęcie (a więc wizerunek) konkretnej osoby – naruszane są te dobra osobiste. Innym przykładem naruszenia dobra osobistego może być podszywanie się pod kogoś na forum. W takiej sytuacji również dochodzi do naruszenia dobra osobistego w postaci nazwiska czy pseudonimu. Zatem nietrudno jest doszukać się naruszenia dóbr osobistych podczas „rozmów" prowadzonych na forum.

Traffic data i retencja danych

Dane dotyczące ruchu, określane jako *traffic data*, to dane przetwarzane w celu przekazania komunikatu w sieciach komunikacji elektronicznej lub naliczania opłat. Dane dotyczące ruchu zamiennie nazywane są również danymi eksploatacyjnymi lub transmisyjnymi i zawierają mnóstwo danych dotyczących np. położenia terminala użytkownika czy informacji o sieci[38]. Zatem użytkownik sieci podczas korzystania z Internetu pozostawia pewną ilość elektronicznych „śladów", które są nośnikami informacji o jego życiu prywatnym. Dane dotyczące ruchu naruszają prywatność użytkowników, bowiem owe „elektroniczne ślady" przetwarzane są bez jego wiedzy[39]. Administrator zbiera, raportuje oraz archiwizuje informacje na temat danych o ruchu użytkowników sieci w usłudze internetowej. Zabieg ten nazywany jest retencją danych. Z uwagi na fakt, iż dostęp osób trzecich do danych w Internecie pozwala na ustalenie wielu istotnych z punktu widzenia interesu publicznego okoliczności (np. ułatwiających walkę z przestępczością), co równocześnie oznacza inwigilację życia prywatnego użytkowników Internetu, ustawodawca dąży do wypracowania kompromisu między tymi dwiema kwestiami, wyrazem czego jest szereg przepisów prawnych konstytuujących zakazy przetwarzania danych osobowych usługobiorcy w określonym czasie, o czym będzie mowa w dalszej części niniejszego artykułu.

Zestawienia i anonimizacja danych (profile osobowościowe)

Wykorzystywanie oprogramowania, które pozwala na zatrzymywanie przez usługodawców danych na temat konkretnego użytkownika, jak również dokonywanie przez nich zestawienia tych danych, stanowią zagrożenie i naruszenie dobra osobistego osoby fizycznej w postaci jej prywatności. Zbiór danych dotyczących danego użytkownika pozwala na stworzenie tzw. profilu osobowościowego, który stanowi źródło zagrożenia anonimowości[40].

Phishing

Spotykany w Internecie na szeroką skalę *phishing* oznacza łamanie zabezpieczeń (*cracking*), w celu pozyskania osobistych, poufnych informacji, a także prywatnych danych za pomocą sfałszowanych stron internetowych, wiadomości e-mail, które do złudzenia przypominają oryginał. Phishingiem nazywamy próby wyłudzenia danych (np. adresu e-mail), „łowienia" haseł dostępu. Użytkownik Internetu nie jest świadomy, że dane przez niego

[38] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 268.
[39] J. Barta, R. Markiewicz, *Handel elektroniczny. Prawne problemy*, Kraków 2005, s. 534.
[40] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, s. 231 i nast.

uzupełniane nie trafią do odpowiedniej instytucji, a do podmiotu nieuprawnionego. W praktyce tworzone są strony internetowe, które w bierny sposób osaczają klienta, oferując mu na sprzedaż rozmaite towary. W chwili finalizowania przez użytkownika transakcji, wszystkie poufne dane wystarczające do wykorzystania cudzej karty kredytowej są przechwytywane przez podmiot nieuprawniony[41]. Phishing stanowiący kradzież tożsamości jest zjawiskiem bardzo niebezpiecznym, narażającym użytkowników Internetu na straty materialne, różne trudności i przykrości, ale także na oskarżenie o przestępstwo, którego się nie popełniło. Ponadto na płaszczyźnie dóbr osobistych zjawisko phishingu wymierzone jest przede wszystkim w wolność i prawo do prywatności użytkownika, jak również w jego wizerunek poprzez podszywanie się za niego.

World Wide Web

Termin *World Wide Web* pochodzi z języka angielskiego i oznacza „ogólnoświatową sieć". Nazwa hosta dla serwera Web oznaczana jest jako WWW. Większość adresów internetowych zaczyna się właśnie od przedrostka „WWW" z uwagi na powszechne nazywanie hostów internetowych (serwerów) zgodnie z usługami, które oferowały. Przeglądanie stron internetowych WWW rozpoczyna się bądź od wpisania adresu strony w przeglądarce internetowej, bądź przez podanie linku do strony. World Wide Web jest usługą internetową, która mylnie utożsamiana jest z całym Internetem. Pojęcia World Wide Web i Internet są często stosowane zamiennie w życiu codziennym. Jednakże ich zakres jest zupełnie inny. Internet to globalny system połączonych ze sobą sieci komputerowych, natomiast sieć Web jest aplikacją działającą w Internecie.

Nazwiska i pseudonimy osób fizycznych, jak również nazwy osób prawnych, określające ich tożsamość, bardzo często zostają naruszane w związku z używaniem adresów stron WWW. Nie każda ingerencja w chronioną sferę identyfikacji zarówno osoby fizycznej, jak również osoby prawnej prowadzi do naruszenia tych dóbr, a jedynie taka, która zagraża lub narusza sferę identyfikacji osoby fizycznej bądź prawnej i jest bezprawna. Chodzi tutaj o sytuację, gdy za pośrednictwem strony WWW są emitowane informacje niezgodne z prawdą czy negatywne, krytyczne oceny mogące narazić na utratę np. zaufania przez osobę fizyczną[42]. World Wide Web stanowi równocześnie prostą drogę dla przestępców rozprzestrzeniających „złośliwe" oprogramowanie. Przestępczość prowadzona w Internecie polega na kradzieży i bezprawnym wykorzystaniu cudzej tożsamości (w tym nazwiska, pseudonimu), gromadzeniu poufnych informacji czy oszustwach. Większość przestępstw związanych jest z manipulacją internetową, oznaczającą modyfikowanie cudzych stron WWW[43]. Do naruszenia dóbr osobistych bardzo często dochodzi na tzw. „Antystronach", które są tworzone przez „przeciwników" osób, które udostępniają stronę WWW w sieci Internet. Na „Antystronach" umieszczane są sformułowania obraźliwe, zmyślone, częstokroć wulgarne, godzące w cześć osoby fizycznej bądź prawnej.

[41] P. Waglowski, *Prawo w sieci...*, s. 353.
[42] J. Ożegalska-Trybalska, *Adresy internetowe: Zagadnienia cywilnoprawne*, „Prace Instytutu Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego" 2003, zeszyt 84, s. 237 i nast.
[43] R. Skubisz, *Internet – problemy prawne*. Materiały z konferencji zorganizowanej 2 grudnia 1998 r. w Lublinie, Lublin 1999, s. 183.

Sniffing

Sniffing (termin pochodzący z języka angielskiego oznaczający „węszenie") to zagrożenie polegające na przechwytywaniu i analizowaniu danych przepływających w sieci przy wykorzystaniu specjalnego programu komputerowego, jakim jest sniffer. Cechą analizatora jest przełączenie karty sieciowej w tryb mieszany, w którym urządzenie odbiera wszystkie ramki z sieci, również te nieadresowane bezpośrednio do niego; mogą one być uruchamiane także na routerze lub na komputerze będącym jedną ze stron komunikacji sieciowej. W zakresie sniffingu, określanym również jako niedozwolony podsłuch, mieści się monitorowanie, słuchanie zawartości transmisji danych komputerowych, obserwowanie, bądź przechwytywanie informacji, które nie są transmitowane jako publicznie dostępne. Poprzez wchodzenie w posiadanie danych konkretnego użytkownika w jakikolwiek wskazany powyżej sposób dochodzi do naruszenia dóbr osobistych związanych z tajemnicą komunikacji oraz prawem do prywatności.

Poczta elektroniczna (e-mail)

Sposobem do prowadzenia szybkiej i taniej korespondencji za pomocą Internetu jest korzystanie z poczty elektronicznej. Termin „poczta elektroniczna" pochodzi od angielskiego słowa *electronic mail*. W potocznym nazewnictwie używany jest skrót *e-mail*. Poczta elektroniczna służy do przesyłania wiadomości tekstowych. W literaturze definiowana jest jako system ogólnoświatowej komunikacji elektronicznej, w ramach której komputer może być używany do tworzenia wiadomości w jednym terminalu, która to wiadomość zostanie wyświetlona na terminalu odbiorcy po zalogowaniu się przez niego do systemu[44]. Do obsługi poczty elektronicznej służy specjalne oprogramowanie, takie jak programy: Sendmail, Exim czy Qmail. Aktualnie dostawcy usług internetowych oferują dostęp do poczty elektronicznej poprzez przeglądarkę internetową WWW (Webmail).

Poczta elektroniczna niesie ze sobą problemy związane z naruszeniem dóbr osobistych. Rozsyłanie do osób trzecich zdjęć przerobionych za pomocą fotomontażu, które przedstawiają osobę z niekorzystnym świetle, stanowi naruszenie jej wizerunku. W sytuacji gdy adres sugeruje błędnie związek danej osoby z dysponentem adresu, powoduje to narażenie użytkownika na utratę czci lub dobrego imienia[45]. Przesyłanie za pomocą poczty e-mail informacji nieprawdziwych może naruszyć dobro osobiste osoby fizycznej w postaci nazwiska lub pseudonimu, twórczości artystycznej czy naukowej, w zależności od treści wysłanej informacji. Z pojęciem poczty elektronicznej nierozerwalnie łączy się konieczność określenia granic prywatności w Internecie.

IV. OCHRONA DÓBR OSOBISTYCH NA PODSTAWIE USTAWY O ŚWIADCZENIU USŁUG DROGĄ ELEKTRONICZNĄ

Artykuł 23 k.c. odnoszący się do ochrony dóbr osobistych człowieka, ma szczególny charakter. Przewiduje, iż dobra osobiste pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach prawnych. W praktyce oznacza to, że ochrona nie ogranicza się tylko do przepisów kodeksu cywilnego. Szereg innych regulacji poza cywilnoprawnymi rangi ustawowej również przewiduje uzyskanie ochrony dóbr oso-

[44] J. Kulesza, *Międzynarodowe prawo...*, s. 114.
[45] J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 275.

bistych (np. w prawie karnym czy administracyjnym). Ustawodawca w artykule 23 k.c. nie wskazuje środków ochrony. Te wyszczególnia, i to w sposób niewyczerpujący, w artykule 24 k.c. Dobra osobiste chronione są wyłącznie przed ich bezprawnym zagrożeniem lub naruszeniem. Naruszenie to nie musi być zawinione[46]. Z powyższego należy wywnioskować, iż nie każde zagrożenie lub naruszenie dobra osobistego uzasadnia jego ochronę. Ochrona dobra osobistego nie przysługuje wówczas, gdy zaistnieją okoliczności wyłączające bezprawność. W tym miejscu należy tylko ograniczyć się do zasygnalizowania (z uwagi na fakt, iż to zagadnienie nie stanowi przedmiotu zainteresowania niniejszego artykułu), że okolicznościami wyłączającymi bezprawność jest zgoda uprawnionego, działanie na podstawie przepisu oraz działanie w obronie interesu publicznego[47].

Przedmiotem rozważań niniejszego rozdziału będzie ochrona wybranych dóbr osobistych przewidziana w akcie prawnym rangi ustawy, jakim jest Ustawa o świadczeniu usług drogą elektroniczną. Przedmiotowa ustawa stanowi implementację części postanowień[48] dyrektywy 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[49], jak również dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej[50].

Ustawa obejmuje swoim zakresem trzy grupy zagadnień. Reguluje obowiązki usługodawców świadczących usługi drogą elektroniczną, zasady wyłączenia odpowiedzialności usługodawcy z tytułu świadczenia tych usług, jak również zasady ochrony danych osobowych osób fizycznych korzystających z takich usług. Na potrzeby niniejszej publikacji wskazane zostaną wybrane regulacje Ustawy o świadczeniu usług drogą elektroniczną, wyselekcjonowane z punktu widzenia ochrony dóbr osobistych, jak również, w dalszej części publikacji, przedstawione zostaną regulacje dotyczące odpowiedzialności za naruszenie dóbr osobistych w Internecie przez treści w nim publikowane.

Spamming, poczta elektroniczna (e-mail)

Intensywnie rozwijający się obrót elektroniczny uwidocznił mankamenty komunikacji za pośrednictwem Internetu. Okazało się, że opracowane zasady netykiety nie stanowią skutecznej ochrony przed niechcianą korespondencją[51]. W polskim ustawodawstwie spamming to „przesyłanie niezamówionej informacji handlowej"[52]. Artykuł 10 u.ś.u.d.e., ma fundamentalne znaczenie dla kwestii niezamawianej korespondencji za pomocą poczty

[46] M. Pazdan [w:] *Kodeks cywilny*..., s. 154 i nast.
[47] A. Cisek, *Dobra osobiste i ich niemajątkowa ochrona w kodeksie cywilnym*, Wrocław 1989, s. 71 i nast.
[48] Chodzi o postanowienia dotyczące m.in. obowiązków informacyjnych usługodawcy, zasad posługiwania się informacją handlową oraz zasad odpowiedzialności pośredników w dostarczaniu informacji.
[49] 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 Dz. Urz. WE L 178/1 z dnia 17.07.2000 r. Dyrektywa określana również dyrektywą o handlu elektronicznym.
[50] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej Dz. Urz. WE L 201/37 z dnia 31.07.2002. Dyrektywa określana również dyrektywą o prywatności i łączności elektronicznej.
[51] G. Rączka, *Ochrona usługobiorcy usług elektronicznych*, Toruń 2007, s. 99 i nast.
[52] J. Kulesza, *Ius internet* ..., s. 44.

e-mail[53]. Konstytuuje on zakaz przesyłania niezamawianych informacji handlowych skierowanych do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, zwłaszcza poczty elektronicznej. W praktyce przyjmuje się, że art. 10 u.ś.u.d.e. wprowadza zakaz wysyłania tzw. spamu, jednakże z jedną uwagą. W praktyce pod pojęciem „spam", rozumie się niechcianą korespondencję zarówno o charakterze handlowym, jak również niehandlowym. Natomiast 10 u.ś.u.d.e. dotyczy tylko i wyłącznie spamu o charakterze informacji handlowej. Ponadto należy podkreślić, iż zakaz wysyłania spamu obejmuje wykorzystanie wszystkich możliwych środków komunikacji elektronicznej, jakie zostały określone w art. 2 pkt 5 u.ś.u.d.e. Artykuł 10 ust. 1 u.ś.u.d.e. zakazuje przesyłania „niezamawianych" informacji handlowych. W konsekwencji oznacza to, że dla wysłania informacji handlowej wymagane jest uzyskanie ze strony odbiorcy wcześniejszej zgody, która może być wyrażona w postaci udostępnienia przez odbiorcę identyfikującego go adresu elektronicznego (art. 10 ust. 2 u.ś.u.d.e.)[54]. Ponadto zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści i może być odwołana w każdym czasie (art. 4 ust. 1 u.ś.u.d.e.). Tym samym w prawie polskim przyjęto system *opt-in*, który uzależnia rozsyłanie korespondencji od uzyskania uprzedniej zgody usługobiorcy[55]. W świetle powyższych uwag należy podkreślić, że na gruncie Ustawy o świadczeniu usług drogą elektroniczną przesyłanie informacji handlowej bez zgody usługobiorcy jest zakazane. Zgodnie z regulacją zawartą w art. 24 u.ś.u.d.e. czyn taki nosi znamiona wykroczenia, ściganego na wniosek pokrzywdzonego i zagrożone jest karą grzywny. Ponadto sankcja za naruszenie zasady przesyłania informacji handlowej bez zgody usługobiorcy przewidziana jest także w art. 10 ust. 3 u.ś.u.d.e., bowiem przepis ten przewiduje, iż działanie takie stanowi czyn nieuczciwej konkurencji (tj. działanie sprzeczne z prawem lub dobrymi obyczajami, zagrażające lub naruszające interes innego przedsiębiorcy lub klienta) w rozumieniu Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[56]. Na zwrócenie uwagi zasługuje również art. 11 u.ś.u.d.e., dzięki któremu zawarte w nim odesłanie umożliwia rozszerzenie zakresu ewentualnych skutków poprzez stosowanie, w sprawach nieuregulowanych tą ustawą, przepisów kodeksu cywilnego, jak również innych ustaw[57].

Cookies, sniffing, phishing

Problematykę naruszeń dóbr osobistych poprzez krótkie pliki tekstowe, zawierające informacje zapisywane w systemie informatycznym, stosowane w celu identyfikacji użytkowników sieci, czyli *cookies*, reguluje art. 6 u.ś.u.d.e. Usługodawca jest zobowiązany zapewnić usługobiorcy dostęp do aktualnej informacji. Zakres przedmiotowy informacji obejmuje dwie kwestie. Po pierwsze, mają to być informacje na temat szczególnych zagrożeń związanych z korzystaniem z usługi świadczonej drogą elektroniczną. Po drugie, winny być to informacje o funkcji i celu oprogramowania lub danych niebędących składnikiem

[53] D. Kasprzycki, *Spam* ..., s. 152.
[54] J. Gołaczyński, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009, s. 111 i nast.
[55] Przeciwieństwem systemu *opt-in* jest system *opt-out*, który pozwala usługodawcom na przesyłanie usługobiorcom komercyjnych wiadomości, jeżeli tylko oni nie sprzeciwili się temu.
[56] Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 1993 r., nr 47, poz. 211 z późn. zm.
[57] G. Rączka, *Ochrona usługobiorcy...*, s. 133.

treści usługi, wprowadzanych przez usługodawcę do systemu teleinformatycznego, którym posługuje się usługobiorca. Dostęp do informacji nie jest dostępem bezpośrednim. Konsekwencją powyższego jest możliwość doręczenia przez usługodawcę informacji w każdy dowolny sposób, w formie elektronicznej, ale i każdej innej, ogólnodostępnej. Ponadto ustawodawca wskazuje, iż ma on zapewnić dostęp do informacji cechującej się aktualnością[58].

Jeśli chodzi o *cookies*, ze szczególną uwagą należy przyjrzeć się regulacji pkt 2 art. 6 u.ś.u.d.e. Ustawodawca przewiduje w nim materię realizacji obowiązku informacyjnego w zakresie aktualizacji wskazanych przez usługodawcę informacji dotyczących oprogramowania lub danych niebędących składnikiem treści usługi co do jego funkcji i celu. Odnosi się to do oprogramowania, które ma na celu stworzenie właściwych zabezpieczeń, jak również oprogramowania o rodzaju reklamowym lub statystycznym wkraczającego w sferę prywatności usługobiorcy.

Artykuł 6 pkt 1 u.ś.u.d.e. ma na celu zapewnienie bezpieczeństwa korzystania z usług świadczonych drogą elektroniczną, w szczególności uchronienie przed zagrożeniami takimi jak spam, sniffing, oprogramowanie typu spyware (oprogramowanie szpiegujące), phishing czy piractwo. Z uwagi na fakt, iż w art. 6 ust. 1 u.ś.u.d.e. zrezygnowano z próby wskazania zagrożeń, na które ustawodawca ma zwrócić uwagę, należy odnieść się do dokumentów unijnych[59] pomocnych w zdefiniowaniu owych zagrożeń. Odnośnie do phishingu należy jeszcze przywołać jeden artykuł Ustawy o świadczeniu usług drogą elektroniczną. Odpowiedzialność z tytułu naruszenia dóbr osobistych przez podmiot nieuprawniony poprzez kradzież tożsamości jest jedną z odpowiedzialności, o których mowa w art. 14 u.ś.u.d.e. Właściciel np. portalu społecznościowego nie będzie ponosił odpowiedzialności, jeśli po uzyskaniu urzędowego zawiadomienia albo po uzyskaniu wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych. W sytuacji braku reakcji może dochodzić do samodzielnej odpowiedzialności podmiotu, który świadczy usługi.

Traffic data

Zgodnie z wcześniejszymi uwagami nazwa *traffic data* oznacza dane eksploatacyjne, transmisyjne. W Ustawie o świadczeniu usług drogą elektroniczną przyjęto środki prawne, które przewidują możliwość przechowywania takich danych w wyznaczonych ramach czasowych. W artykule 19 ust. 1 u.ś.u.d.e. ustawodawca wprowadził zakaz przetwarzania danych usługobiorcy po zakończeniu korzystania z usługi świadczonej drogą elektroniczną. Od tego zakazu ustawa przewiduje pewne wyjątki, wskazując tylko kilka grup danych, wymienionych

[58] D. Lubasz [w:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, red. D. Lubasz, M. Namysłowska, Warszawa 2011, s. 127 i nast.

[59] Dokumenty takie jak Dyrektywa 98/84/WE Parlamentu Europejskiego i Rady z dnia 20 listopada 1998 r. w sprawie prawnej ochrony usług opartych lub polegających na warunkowym dostępie (Dz. Urz. UE L 320 z 28.11.1998 r.); opinia Europejskiego Komitetu Ekonomiczno-Społecznego dotyczącego komunikatu Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie „Bezpieczeństwo sieci i bezpieczeństwo informacji: propozycja strategicznego podejścia europejskiego" (Dz. Urz. UE C 48 z 21.02.2002 r.); komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – Dialog, partnerstwo i przejmowanie inicjatywy" (SEC(2006) 656 z dnia 31.05.2006, COM(2006) 251 wersja ostateczna).

w ust. 2 art. 19 u.ś.u.d.e. Pierwsza grupa dotyczy danych niezbędnych do rozliczenia usługi lub dochodzenia roszczeń z tytułu braku opłaty za usługę. Rozliczenie usługi świadczonej drogą elektroniczną nie może ujawniać rodzaju, czasu trwania, częstotliwości i innych parametrów technicznych poszczególnych usług, z których skorzystał usługobiorca, chyba że zażądał on szczegółowych informacji w tym zakresie. Kolejna grupa danych to dane niezbędne do celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, za zgodą usługobiorcy. Możliwość przetwarzania danych osobowych dotyczy również tzw. niedozwolonego korzystania z usługi w sytuacjach wskazanych w art. 21 ust. 1 u.ś.u.d.e. Przedmiotowy artykuł reguluje sytuację, w której usługodawca uzyskał informację o korzystaniu przez usługobiorcę z usługi świadczonej drogą elektroniczną niezgodnie z regulaminem lub z obowiązującymi przepisami. Wówczas usługodawca może przetwarzać dane osobowe usługobiorcy w zakresie niezbędnym do ustalenia odpowiedzialności usługobiorcy, pod warunkiem że pomoże w utrwaleniu dla celów dowodowych fakt uzyskania oraz treść tych wiadomości. Wreszcie ostatnią grupę danych możliwych do przetwarzania stanowią dane dopuszczone do przetwarzania na podstawie odrębnych ustaw lub umowy.

Zestawienia i anonimizacja danych (profile osobowościowe)

Niebagatelnym problemem są działania dotyczące zestawiania danych i tworzenia profilów osobowościowych użytkowników sieci Internet, które stanowią poważne zagrożenie dla prywatności użytkowników.

Do problemu zestawienia danych Ustawa o świadczeniu usług drogą elektroniczną odnosi się w art. 19 ust. 4, który zawiera ograniczenie zestawienia informacji o aktywności osób fizycznych w Internecie[60]. Ustawa dopuszcza dokonywanie zestawienia danych dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę (art. 19 ust. 2 pkt 2 u.ś.u.d.e.). Jednakże zestawienia danych dla ww. celów można dokonać wyłącznie odnośnie do danych wymienionych w art. 18 ust. 4 oraz ust. 5 u.ś.u.d.e. Ponadto konieczne jest, aby osoba, której dane dotyczą, wyraziła wcześniej zgodę na ich przetwarzanie. Natomiast bez uprzedniej zgody osoby, której dane dotyczą, można zestawić tylko dane wymienione w art. 18 ust. 4 i ust. 5 u.ś.u.d.e., jednakże muszą zostać usunięte jakiekolwiek oznaczenia identyfikujące usługobiorcę lub zakończenie sieci telekomunikacyjnej albo system teleinformatyczny, z którego korzystał (anonimizacja danych), chyba że usługobiorca wyraził uprzednio zgodę na nieusuwanie tych oznaczeń.

Poufność komunikacji

Obowiązkiem, jaki polski ustawodawca nakłada na usługodawców, jest wymóg zapewnienia bezpieczeństwa poufności przekazywanych w sieci wiadomości. Wolą ustawodawcy było zagwarantowanie prywatności i poufności przy korzystaniu przez usługobiorców z usług świadczonych drogą elektroniczną, jak również bezpieczeństwa ich świadczenia[61].

[60] J. Gołaczyński, *Ustawa o świadczeniu usług...*, s. 152.
[61] D. Lubasz [w:] *Świadczenie usług...*, s. 133.

Przepis art. 7 nakazuje usługodawcy umożliwienie usługobiorcy nieodpłatne skorzystanie z usługi w taki sposób, aby do treści przekazu, który jest przedmiotem usługi, nie miały dostępu osoby nieuprawnione (art. 7 pkt. 1 lit. a u.ś.u.d.e.), jak również zapewnienia jednoznacznej identyfikacji stron oraz potwierdzenia faktu złożenia oświadczeń woli i ich treści (art. 7 pkt 1 lit. b u.ś.u.d.e.). Omawiana regulacja nie wymienia katalogu zabezpieczanych usług, jak również technik zabezpieczeń. Ustawodawca uznał, iż procedury stosowane na rynku wypracują wskazania w tym zakresie[62]. W zakresie realizacji obowiązku z art. 7 pkt 1 lit. b u.ś.u.d.e. ustawodawca odsyła w szczególności do bezpiecznego podpisu elektronicznego w rozumieniu Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym[63]. Weryfikacja podpisu elektronicznego chroni przekaz przed ingerencją i zniekształceniem, jak również pozwala na identyfikację osoby, która go składa[64].

V. ODPOWIEDZIALNOŚĆ ZA NARUSZENIE DÓBR OSOBISTYCH W INTERNECIE PRZEZ TREŚCI W NIM PUBLIKOWANE

Z odpowiedzialnością za naruszenie dóbr osobistych w Internecie wiąże się występowanie kilku podmiotów.

W pierwszej kolejności są to podmioty, które umieszczają i dostarczają materiały własnego autorstwa w Internecie (z ang. *content providers*). Internet stanowi swoistą furtkę dla anonimowych autorów wyrażających, w dość swobodny sposób, różnego rodzaju niewłaściwe wypowiedzi. Częstokroć wypowiedzi te cechuje niezgodność ich treści z prawdą, wulgarność, przez co obrażają inne osoby. Poprzez używanie i stosowanie takich wypowiedzi w sieci dochodzi do bezprawnego wykorzystywania nazwiska osoby fizycznej (bądź firmy osoby prawnej), zniesławienia i zniewagi[65] innej osoby, naruszenia jej czci lub wizerunku, co w konsekwencji prowadzi do naruszenia dóbr osobistych. Możliwości form naruszenia dóbr osobistych jest wiele. Służyć temu celowi mogą chociażby strony www, „chat" bądź inne fora dyskusyjne, jak również poczta e-mail. W literaturze[66] podkreśla się, że zawarcie treści szkalującej w przesyłce e-mailowej skierowanej do danej osoby jest o wiele bardziej obciążone aniżeli tradycyjna korespondencja, bowiem jej autorowi może zostać postawiony zarzut naruszenia nie tylko tajemnicy korespondencji, ale też prywatności lub czci. Autor naruszający dobra osobiste w Internecie ponosi również odpowiedzialność w ramach tzw. linkingu[67] i framingu[68]. Mimo trwających w literaturze analiz tej problematyki można przyjąć[69], iż osoba, która publikuje na zwykłej stronie nie może kontrolować zasięgu publikacji. Jednakże musi przyjąć ryzyko, że taki materiał może dotrzeć do bardzo szerokiej publiczności i w związku z powyższym autor tekstu naruszającego dobra osobiste

[62] Ibidem, s. 134.
[63] Ustawa z dnia 18 września 2001r. o podpisie elektronicznym, Dz.U. z 2001, nr 130, poz. 1450 z późn. zm.
[64] J. Gołaczyński, *Ustawa o świadczeniu usług* ..., s. 91.
[65] Zniesławienie i zniewaga podlega sankcjom przewidzianym w Ustawie z dnia 06 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r., nr 88, poz. 553 z późn. zm.).
[66] A. Wojciechowska [w:] J. Barta, R. Markiewicz, *Media a dobra osobiste*..., s. 388.
[67] Przy linkingu strona internetowa wprawdzie nie zawiera wypowiedzi, które godziłyby w dobra osobiste, jednakże odsyła za pomocą hiperlinku do innej strony, która już takie wypowiedzi zawiera.
[68] Istota framingu, jako odmiany linkingu, polega na włączeniu na stronę www hiperlinku, którego użycie przez użytkownika Internetu sprawia, że inna strona www zostanie wyświetlona w „ramkach" pierwotnej strony www.
[69] A. Wojciechowska [w:] J. Barta, R. Markiewicz, *Media a dobra osobiste* ..., s. 389 i nast.

innej osoby ponosi odpowiedzialność cywilną. Na początku aktualnych rozważań nie bez powodu użyto sformułowania „anonimowi autorzy" zniesławiających wypowiedzi. Niestety, w większości przypadków ustalenie osoby autora owych treści jest trudne, wręcz niemożliwe. Wówczas odpowiedzialność zostaje niejako przeniesiona z niezidentyfikowanego, anonimowego autora na podmiot odsyłający ze swojej strony www do strony, która zawiera wypowiedź stanowiącą naruszenie dobra osobistego. Tym oto stwierdzeniem należy przejść do omówienia drugiej grupy podmiotów odpowiedzialnych za naruszenie dóbr osobistych w Internecie poprzez publikowane w nim treści.

W drugiej kolejności należy zatem wymienić podmioty, które świadczą usługi przechowywania bądź przekazywania informacji w Internecie (dostawcy pośredniczący w dostępie do treści). W tej grupie podmiotów wyróżnia się trzy kategorie. Dwie pierwsze stanowią kolejno podmioty zarządzające siecią (*network providers*), jak również podmioty zapewniające wyłącznie dostęp do Internetu (*access providers).* Obie kategorie podmiotów nie ponoszą odpowiedzialności za naruszenia dóbr osobistych przez treści udostępniane w Internecie, w przeciwieństwie do trzeciej kategorii dostawców pośredniczących w dostępie do treści, jaką tworzą dostawcy usług internetowych (*service providers*)[70].

Ze szczególną uwagą należy przyjrzeć się problematyce odpowiedzialności dostawców usług (*service providers*). W tym celu konieczne jest odniesienie się do regulacji u.ś.u.d.e, a zwłaszcza do regulacji art. 12–15. U.ś.u.d.e. nie zawiera regulacji dotyczącej odpowiedzialności dostawców usług internetowych, a jedynie reguluje odpowiedzialność od strony negatywnej, wskazując sytuacje, w których dostawcy usług są od niej wyłączeni. Wyłączenie dotyczy odpowiedzialności o charakterze cywilnym, karnym, jak również administracyjnym[71].

Według art. 12 u.ś.u.d.e. nie ponosi odpowiedzialności za treść przekazywanych danych ten, kto spełni trzy warunki w nim przewidziane. Mianowicie nie ponosi odpowiedzialności ten, kto nie jest inicjatorem transmisji, zatem nie podejmuje on decyzji o jej rozpoczęciu, nie wybiera odbiorcy danych, jak również nie wybiera i nie modyfikuje informacji będących przedmiotem transmisji. Przedstawiony przepis dotyczy wyłączenia odpowiedzialności z tytułu świadczenia usług *mere conduit.* Usługi te polegają na umożliwieniu zwykłego przesyłu informacji. Wyłączenie odpowiedzialności obejmuje podmiot, który przesyła na wskazane adresy pocztę elektroniczną o wskazanej treści, bez ingerencji w nią, jak również sytuację krótkotrwałego przechowywania danych (tzw. pakietowej transmisji danych w sieciach komputerowych)[72].

Drugą sytuację, w której dostawca usług internetowych nie ponosi odpowiedzialności, określa art. 13 u.ś.u.d.e. dotyczący usług *cachingu.* Usługa ta polega na automatycznym i krótkotrwałym pośrednim przechowywaniu danych celem przyśpieszenia ponownego dostępu do nich[73]. Przesłanką wyłączenia odpowiedzialności podmiotu świadczącego usługi *cachingu* jest po pierwsze to, aby dostawca nie usuwał ani nie modyfikował danych, po drugie posługiwał się uznanymi i stosowanymi zwykle w tego rodzaju działalności technikami informatycznymi określającymi parametry techniczne dostępu do danych i ich aktualizowania. Trzecią przesłanką wymienioną w art. 13 ust. 1 pkt 3 u.ś.u.d.e. jest oko-

[70] A. Wojciechowska [w:] J. Barta, R. Markiewicz, *Media a dobra osobiste*..., s. 390.
[71] J. Gołaczyński, *Ustawa o świadczeniu usług*..., s. 127.
[72] Ibidem, s. 130.
[73] P. Podrecki, *Podział i rodzaje umów w Internecie*, [w:] *Prawo Internetu*, red. P. Podrecki, Warszawa 2007, s. 52.

liczność, że dostawca nie zakłóca posługiwania się technikami informatycznymi uznanymi i stosowanymi zwykle w tego rodzaju działalności w zakresie zbierania informacji o korzystaniu ze zgromadzonych danych. Jeśli usługodawca uzyska wiadomość, że dane zostały usunięte z początkowego źródła transmisji lub dostęp do nich został uniemożliwiony, albo gdy takie działanie nakaże sąd lub inny właściwy organ do zwolnienia z odpowiedzialności podmiotu, który stosuje *caching*, konieczne jest bezzwłoczne usunięcie danych lub zablokowanie do nich dostępu[74].

Trzecią sytuacją, wskazaną w art. 14 u.ś.u.d.e., w której ustawodawca wyłączył odpowiedzialność dostawcy usług, jest tzw. *hosting*, polegający na udostępnianiu przez niego zasobów pamięci serwerowni celem gromadzenia różnych danych. Dane nie pochodzą od podmiotu, który świadczy usługi hostingu, ale od trzeciego podmiotu, jakim jest usługobiorca. W świetle art. 14 u.ś.u.d.e. nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez trzeci podmiot, czyli usługobiorcę, nie wie o bezprawnym charakterze danych bądź związanej z nimi działalności. Po uzyskaniu urzędowego zawiadomienia bądź wiarygodnej wiadomości o bezprawnym charakterze danych, usługodawca musi uniemożliwić dostęp do tych danych. Ponadto usługodawca nie ponosi odpowiedzialności wobec usługobiorcy za szkodę, która powstała wskutek uniemożliwienia dostępu do przechowywanych danych[75]. W instytucji wyłączenia odpowiedzialności nie mieści się sytuacja, gdy usługodawca posiada wobec usługobiorcy zamieszczającego bezprawne informacje uprawnienia kontrolne[76].

Wymienieni powyżej dostawcy usług internetowych, świadczący usługi *mere conduit*, *cachingu*, jak również *hostingu* w celu wyłączenia odpowiedzialności, nie są zobowiązani do kontrolowania przekazywanych, przechowywanych bądź udostępnianych przez nich danych[77]. Z art. 15 u.ś.u.d.e. ściśle związany jest omówiony powyżej art. 14 ust. 1, mający na celu wyłączenie odpowiedzialności cywilnej i karnej dostawcy, wówczas gdy dostawca nieświadomie udostępnia treści o charakterze bezprawnym, w szczególności dane naruszające dobra osobiste osób trzecich[78].

Reasumując, należy zaakcentować, iż w sytuacji braku zasadności stosowania wyłączeń ujętych w art. 12–14 u.ś.u.d.e. odpowiedzialność dostawcy powinna być oceniana według zasad ogólnych przyporządkowanych konkretnym dziedzinom prawa[79].

PODSUMOWANIE

Biorąc pod uwagę powyższe rozważania, należy dojść do wniosku, iż wraz z rozwojem Internetu, który jako specyficzny środek przekazu informacji wykorzystuje różnorodne systemy techniczne, ustawodawca musi stwarzać skuteczne zabezpieczenia prawne, chroniące przed zagrożeniami skierowanymi do użytkowników sieci. Zarówno nauka, jak również orzecznictwo dostarczają nowe postacie dóbr osobistych, a technika coraz to nowe ich zagrożenia. To powoduje, iż występuje ciągła potrzeba dostosowywania regulacji prawnych do zmieniającej się „rzeczywistości internetowej". Internet niejako wymyka się spod

[74] J. Gołaczyński, *Ustawa o świadczeniu usług...*, s. 132.
[75] A. Wojciechowska [w:] J. Barta, R. Markiewicz, *Media a dobra osobiste...*, s. 391.
[76] Zob. art. 14 ust. 4 u.ś.u.d.e.
[77] Zob. art. 15 u.ś.u.d.e.
[78] A. Kuczerawy, *Odpowiedzialność dostawcy usług internetowych*, „Monitor Prawniczy" 2004, nr 4, dodatek, s. 13.
[79] A. Wojciechowska [w:] J. Barta, R. Markiewicz, *Media a dobra osobiste...*, s. 392.

kontroli poszczególnych systemów prawnych i wymaga ciągłej koordynacji[80]. Zawsze konsekwencją postępu w dziedzinie informatyki jest postawienie społeczeństwa przez nowymi problemami na coraz to nowych płaszczyznach związanych z siecią. Podmioty korzystające z sieci stanowią społeczeństwo, które tak jak każde inne potrzebuje norm prawnych, aby czuć się bezpiecznie. Pozostawienie Internetu bez nadzoru i kontroli byłoby możliwe tylko wtedy, gdyby każdy uczestnik obrotu elektronicznego był uczciwy i rzetelny[81].

Konkludując, należy stwierdzić, iż problematyka ochrony dóbr osobistych jest ciągle aktualna i szeroko dyskutowana ze względu na dynamiczny rozwój oraz specyfikę Internetu. Dostosowanie prawa do potrzeb kształtującego się społeczeństwa, którego dobra osobiste są zagrożone i naruszane, należy do najważniejszych problemów, przed jakimi staje współczesne prawo[82]. Oceniając istniejącą sytuację i biorąc pod uwagę intensywny rozwój sieci Internet, z jej korzyściami, ale i wadami, należy spodziewać się, iż ciągle występować będzie potrzeba nowych regulacji prawnych bądź dostosowywania istniejących regulacji prawnych do panującej rzeczywistości.

Bibliografia

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Kraków 2007.
Barta J., Markiewicz R., *Handel elektroniczny. Prawne problemy*, Kraków 2005.
Barta J., Markiewicz R., *Internet a prawo*, Kraków 1998.
Biernatowski P., *Błąd jako wada oświadczenia woli w obrocie elektronicznym*, Warszawa 2011.
Cisek A., *Dobra osobiste i ich niemajątkowa ochrona w kodeksie cywilnym*, Wrocław 1989.
Dmowski S., Rudnicki S., *Komentarz do Kodeksu cywilnego. Księga pierwsza. Część ogólna*, Warszawa 2011.
Gołaczyński J., *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009.
Grzybczyk K., *Naruszenie dobra osobistego w reklamie*, „Rejent" 1999, nr 9.
Grzybowski S., *Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego*, Warszawa 1957.
Grzybowski S. [w:] *System Prawa Cywilnego. Część ogólna*, [w:] *System Prawa Cywilnego*, t. I, red. naczelny W. Czachórski, Wrocław – Warszawa – Kraków – Gdańsk – Łódź 1985.
Janowski J., *Elektroniczny obrót prawny*, Warszawa 2008.
Janowski J., *Informatyka prawa. Zadania i znaczenie w związku z kształtowaniem się elektronicznego obrotu prawnego*, Lublin 2011.
Kasprzycki D., *Spam, czyli niezamawiana komercyjna poczta elektroniczna: zagadnienia cywilnoprawne*, Kraków 2005.
Kawałko A., Witczak H., *Prawo cywilne. Zarys prawa*, Warszawa 2008.
Kremis J. [w:] *Podstawy prawa cywilnego*, red. E. Gniewek, Warszawa 2011.
A. Kuczerawy, *Odpowiedzialność dostawcy usług internetowych*, „Monitor Prawniczy" 2004, nr 4, dodatek, s. 13.
Kulesza J., *Ius internet. Między prawem a etyką*, Warszawa 2010.
Kulesza J., *Międzynarodowe prawo internetu*, Poznań 2010.
Lubasz D. [w:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, red. D. Lubasz, M. Namysłowska, Warszawa 2011.
Matlak A., *Cywilnoprawna ochrona wizerunku*, „Kwartalnik Prawa Prywatnego" 2004, z. 2.
Ożegalska-Trybalska J., *Adresy internetowe: Zagadnienia cywilnoprawne*, „Prace Instytutu Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego" 2003, zeszyt 84.
Pazdan M. [w:] *Kodeks cywilny. Komentarz do artykułów 1-449[1o]*, t. I, red. K. Pietrzykowski, Warszawa 2011.

[80] J. Janowski, *Elektroniczny obrót...*, s. 27.
[81] P. Biernatowski, *Błąd jako wada oświadczenia woli w obrocie elektronicznym*, Warszawa, 2011, s. 10.
[82] A. Stasio, *Umowy zawierane przez Internet*, Warszawa 2002, s. 30.

Pazdan M. [w:] *Prawo cywilne – część ogólna*, t. I, red. M. Safjan [w:] *System Prawa Prywatnego. Prawo cywilne – część ogólna*, t. I, red. naczelny Z. Radwański, Warszawa 2007.
Podrecki P., *Podział i rodzaje umów w Internecie*, [w:] *Prawo Internetu*, red. P. Podrecki, Warszawa 2007.
Radwański Z., *Prawo cywilne – część ogólna*, Warszawa 1997.
Radwański Z., *Prawo cywilne – część ogólna*, Warszawa 2009.
Rączka G., *Ochrona usługobiorcy usług elektronicznych*, Toruń 2007.
Skubisz R., *Internet – problemy prawne*, Materiały z konferencji zorganizowanej 2 grudnia 1998 r. w Lublinie, Lublin 1999.
Sołtysiński S., *Charakter prawny wynalazcy*, Poznań 1967.
Stasio A., *Umowy zawierane przez Internet*, Warszawa 2002.
Waglowski P., *Prawo w sieci. Zarys regulacji internetu*, Gliwice 2005.
Waglowski P., *Spam a prawo. Próba wskazania kierunków badawczych*, „Prawo i Ekonomia w Telekomunikacji" 2003, nr 4.
Wojciechowska A. [w:] J. Barta, R. Markiewicz (red.), *Media a dobra osobiste*, Warszawa 2009.
Wyrzykowski M., *Ochrona danych osobowych*, Warszawa 1999.

Wykaz aktów prawnych

Ustawy

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r., nr 78 poz. 483 z późn. zm.
Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, Dz.U. z 1964, nr 16, poz. 93 z późn. zm.
Ustawa z dnia 06 czerwca 1997 r. – Kodeks karny, Dz.U. z 1997 r., nr 88, poz. 553 z późn. zm.
Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, Dz.U. z 2001 r., nr 130, poz. 1450 z późn. zm.
Ustawa o z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2011 r., nr 134, poz. 779.
Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 1993 r., nr 47, poz. 211 z późn. zm.

Dyrektywy

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz. Urz. WE L 201/37 z dnia 31.07.2002.
Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego, Dz. Urz. WE L 178/1 z dnia 17.07.2000.
Dyrektywa 98/84/WE Parlamentu Europejskiego i Rady z dnia 20 listopada 1998 r. w sprawie prawnej ochrony usług opartych lub polegających na warunkowym dostępie, Dz. Urz. UE L 320 z 28.11.1998 r.

Komunikaty

Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – Dialog, partnerstwo i przejmowanie inicjatywy", SEC(2006) 656 z dnia 31.05.2006, COM(2006) 251 wersja ostateczna.

Opinie

Opinia Europejskiego Komitetu Ekonomiczno-Społecznego dotyczącego komunikatu Komisji do

Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie „Bezpieczeństwo sieci i bezpieczeństwo informacji: propozycja strategicznego podejścia europejskiego" Dz. Urz. UE C 48 z 21.02.2002 r.

Wyroki
Wyrok Sądu Najwyższego z dnia 19 września 1968 r., II CR 291/68.

Streszczenie: Niniejsza publikacja poświęcona została zagadnieniom naruszenia dóbr osobistych w Internecie, jak również ich ochronie na podstawie wybranej polskiej regulacji prawnej. Problematyce naruszenia dóbr osobistych w sieci Internet poświęcono w polskiej literaturze prawniczej niejedną publikację. Jednakże nie może to prowadzić do stwierdzenia, iż nie występuje potrzeba dalszej, szczegółowej analizy tej materii, tym bardziej że rozwój technologii elektronicznej, związanej w szczególności z wykorzystaniem Internetu, dostarcza coraz to nowych form naruszających dobra osobiste w cyberprzestrzeni. Celem niniejszej publikacji, po wprowadzeniu w problematykę dóbr osobistych, jest wskazanie zjawisk występujących w Internecie stanowiących zagrożenie dóbr osobistych i przyczyniających się do ich naruszenia. W prawie polskim nie ma aktu prawnego, który całościowo regulowałby ochronę dóbr osobistych. Poza regulacją polskiego kodeksu cywilnego zadaniu temu usiłuje sprostać szereg aktów prawnych, z których na uwagę zasługuje Ustawa o świadczeniu usług drogą elektroniczną. Przedmiotem zainteresowania publikacji stały się wybrane regulacje Ustawy, wyselekcjonowane z punktu widzenia ochrony dóbr osobistych, które ulegają naruszeniu w Internecie.

Słowa kluczowe: dobra osobiste, Internet, netykieta, spamming, cookies, Usenet, traffic data, retencja danych, phishing, sniffing, poczta elektroniczna, ochrona, usługodawca

INFRINGING OF THE PERSONAL GOODS ON THE INTERNET AND THEIR PROTECTION ON THE BASIS OF THE BILL CONCERNING PROVIDING SERVICES BY THE ELECTRONIC WAY

Abstract: This publication is devoted to the issues of personal goods infringing on the Internet as well as their protection on the basis of the specific Polish law regulation. There are a lot of law pieces of work concerning infringing of the personal goods on the Internet. However, one cannot state that there is no further need to analyze this area in a more detailed way as the development of the electronic technology, especially connected with the usage of the Internet, provides more and more new forms of infringement in the cyberspace. The aim of this work, after introducing the problem of personal goods, is to point the phenomena existing on the Internet that are the threat to the personal goods and cause of the infringement. There is no legislative regulation in the Polish law that would regulate personal goods protection in the holistic way. Apart from the Polish Civil Code there are a lot of deeds that try to succeed in dealing with this matter. There is one deed that deserves special attention namely the Bill concerning providing the services by the electronic way. The subject of this publication is the number of the selected bill regulations, chosen due to the issue of personal goods protection violated on the Internet.

Key words: personal goods, Internet, netiquette, spamming, cookies, Usenet, traffic data, data retention, phishing, sniffing, electronic mail, protection, provider