ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3066
PRZEGLĄD PRAWA I ADMINISTRACJI LXXVIII
WROCŁAW 2008

SYLWIA JAROSZ-ŻUKOWSKA
Uniwersytet Wrocławski

KONSTYTUCYJNOPRAWNE ASPEKTY OCHRONY TAJEMNICY KOMUNIKOWANIA SIĘ W INTERNECIE

1. KONSTYTUCYJNE I PRAWNOMIĘDZYNARODOWE PODSTAWY OCHRONY TAJEMNICY KOMUNIKOWANIA SIĘ

Tajemnica korespondencji jest jedną z klasycznych, tradycyjnych wolności jednostki i od dawna gwarantowana jest konstytucyjnie. Podstawę konstytucyjnej ochrony tajemnicy korespondencji stanowi przepis art. 49 Konstytucji RP, statuujący wolność i ochronę tajemnicy komunikowania się oraz dopuszczający ich ograniczenie jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

Zaznaczyć trzeba jednak, że omawiana tutaj tajemnica komunikowania się pozostaje w bliskim związku z innymi konstytucyjnymi prawami i wolnościami. Przede wszystkim wymienić należy prawo do prywatności z art. 47 konstytucji, gdyż – jak się wydaje – tajemnica komunikowania się jest jednym z jego przejawów. Oddzielne uregulowanie tej wolności w art. 49 konstytucji tłumaczyć należy wolą dodatkowego podkreślenia jej znaczenia i tradycyjnego charakteru[1].

Wiele wspólnego ma także wolność komunikowania się z wyrażoną w art. 54 wolnością wyrażania poglądów, z tym że od tej ostatniej różni się „[…] okolicznością zwracania się z najrozmaitszymi treściami, dotyczącymi tak spraw prywatnych, jak i publicznych, do konkretnie (indywidualnie) określonych osób, z intencjonalnie zawartym tu stanowiskiem nieudostępniania tych treści osobom postronnym. Natomiast »wolność słowa« […] polega na adresowaniu swego stanowiska do nieokreślonych indywidualnie osób (»wszystkich«)”[2].

Jak wskazuje się w literaturze, aby zastosować w konkretnym przypadku ochronę, przewidzianą w art. 49 ustawy zasadniczej „występować musi fakt

[1] M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, Wrocław 2002, s. 41.

[2] P. Sarnecki, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. III, Rozdział II „Wolności, prawa i obowiązki człowieka i obywatela”. Uwagi do art. 49, red. L. Garlicki, Warszawa 2003, s. 2.

porozumiewania się za pomocą pewnego środka przekazu, a nie bezpośrednio, w drodze osobistej rozmowy, przy fizycznej obecności uczestników w jednym miejscu”[3]. Zauważyć trzeba jednak, że przepis ten posługuje się dwoma pojęciami, tj. „wolności komunikowania się” oraz „tajemnicy komunikowania się”. Jakkolwiek obie te sfery funkcjonowania jednostki pozostają ze sobą w ścisłym związku, to czym innym jest wolność komunikacji, a czym innym jej tajemnica. Odrębność tę ilustruje zwłaszcza ochrona przed podsłuchem (także komputerowym), w którego przypadku nie chodzi o uniemożliwienie komunikowania się osób między sobą, ale wręcz przeciwnie o to, by jak największa liczba rozmów została podsłuchana. Idzie w tym przypadku zatem nie tyle o ograniczenie wolności komunikowania się osób, ale o przejęcie informacji przekazywanych w poufny sposób[4].

Tajemnica komunikowania się jest niewątpliwie kontynuacją, wyrażonej w poprzednich polskich konstytucjach, klasycznej tajemnicy korespondencji, którą w obowiązującej konstytucji zastąpiono innym określeniem z uwagi na jednoznaczne kojarzenie się określenia „korespondencja” jedynie z pisemnymi formami przekazu[5].

Konstytucja, używając szerszego aniżeli „tajemnica korespondencji” pojęcia „tajemnica komunikowania się”, w bardziej nowoczesny sposób chroni tę wolność jednostki, mając na względzie fakt, że współcześnie „korespondencja” przybiera nie tylko postać pisemną (listu), lecz także formę elektroniczną – telefon, telefaks, teleks, e-mail. „Konstytucja zakazuje komukolwiek zapoznawania się z treścią wiadomości bez względu na to, jaką formę one przyjmują (słowo, obraz, dźwięk itp.) przekazywanych pomiędzy podmiotami prawa za pośrednictwem wszelkiego typu mediów, jeśli wiadomości te przeznaczone są wyłącznie do adresata wskazanego przez nadawcę”[6].

Pojęciem tajemnicy korespondencji, a nie komunikacji, posługują się natomiast akty prawa międzynarodowego. Przepis art. 17 MPPOiP stanowi bowiem, iż „nikt nie może być narażony na samowolę lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego część i dobre imię”. Natomiast art. 8 EKPC stanowi, że „każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji” (ust. 1). Na podstawie zarówno jednego, jak i drugiego aktu rozwinęło się jednak bogate w tym zakresie orzecznictwo, które pojęcie korespondencji rozumie możliwie szeroko.

---

[3] P. Sarnecki, *op. cit.*, s. 1.

[4] Tak słusznie, I. Dobosz, *Przesłanki cywilnoprawnej ochrony przed podsłuchem*, ZNUJ, z. 58/1992, s. 89.

[5] P. Sarnecki, *op. cit.*, s. 2.

[6] P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Warszawa 2000, s. 67–68.

Komitet Praw Człowieka dostrzega, obok najbardziej klasycznych zagrożeń tajemnicy korespondencji, także zagrożenia poufności komunikowania się realizowanego za pomocą urządzeń telekomunikacyjnych, zwłaszcza polegające na naruszaniu poufności kontaktów różnorodnymi środkami technicznymi, np. urządzeniami podsłuchowymi. Zdaniem Komitetu waga tych niebezpieczeństw wymaga wprowadzenia ustawowego zakazu „inwigilacji czy to elektronicznej lub innej, podsłuchu telefonicznego, telegraficznego, jak i rejestrowania i nagrywania treści komunikowanych w innej formie”[7].

Także zdaniem ETPC pojęcie „korespondencja” w rozumieniu Konwencji należy rozumieć szeroko jako „komunikowanie się – w różnych formach – w celu nawiązania kontaktów z innymi osobami”[8]. Zauważyć przy tym trzeba, że zarówno w Pakcie, jak i Europejskiej Konwencji dobro osobiste człowieka, jakim jest korespondencja, występuje obok trzech innych pojęć: życia prywatnego, rodzinnego, mieszkania. Terminy te różnią się od siebie, ale też w dużej części pokrywają się. Wszystkie bowiem wiążą się bezpośrednio z ochroną życia prywatnego. Z tego względu dopuszczalność nadzoru telekomunikacyjnego podpada zarówno pod zakres ochrony życia prywatnego, mieszkania, jak i – omawianej tutaj – korespondencji[9].

Zatem zarówno konstytucja, jak i akty prawa międzynarodowego wyszły naprzeciw współczesnym potrzebom ochrony informacji, przyjmując, że określenie „komunikować się” obejmuje, oprócz tradycyjnych, wszelkie rozwinięte media porozumiewania się ludzi między sobą. Przepis art. 49 ustawy zasadniczej daje zatem wyraźną podstawę, by w odniesieniu do informacji przekazywanych za pomocą Internetu używać szerszego pojęcia „tajemnicy komunikacji”. Określenie to wydaje się w tym przypadku bardziej precyzyjne, jakkolwiek odnotować należy fakt powszechnego posługiwania się także pojęciem „korespondencja elektroniczna”. W tym wypadku odpowiednikiem tradycyjnego listu jest e-mail. Używanie obu tych terminów wydaje się uzasadnione, choćby ze względu na dużą zbieżność ochrony tajemnicy korespondencji i komunikacji, a zwłaszcza jej *ratio legis*. Zanim bowiem nastała era komputerów, prawna ochrona informacji dotyczyła głównie tajemnicy korespondencji oraz innych tajemnic (zawodowej, państwowej i służbowej). Z chwilą powstania systemów informatycznych powstała konieczność ochrony prawnej przetwarzanej w tych systemach informacji. Jej bezpieczeństwo określane jest w doktrynie przy użyciu trzech podstawowych kryteriów: dostępności, integralności i poufności. Ta ostatnia definiowana jest jako „wyłącz-

[7] J. Braciak, *Prawo do prywatności*, [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, pod red. B. Banaszaka, A. Preisnera, Warszawa 2002, s. 300–301. Por. też J. Braciak, *Prawo do prywatności*, Warszawa 2004, s. 82–89.

[8] Decyzja X. i Y. v. Belgia z 13.05.1982 r. za: M.A. Nowicki, *Europejski Trybunał Praw Człowieka*, *Orzecznictwo*, t. 2: *Prawo do życia i inne prawa*, Zakamycze 2002, s. 603.

[9] J. Braciak, *op. cit.*, s. 306.

ny dostęp osób uprawnionych do określonych informacji i ochrona danych przed ich odczytaniem lub kopiowaniem przez osoby do tego nieupoważnione”[10].

Najbardziej popularnym sposobem komunikacji elektronicznej jest poczta elektroniczna e-mail. Stanowi ona prywatny środek przekazywania informacji między określonymi osobami, do której dostęp zabezpieczony jest hasłem, a każde konto e-mail ma określonego właściciela indywidualnego lub instytucjonalnego[11]. Podobnie jak w przypadku korespondencji pisemnej, osobom komunikującym się w ten sposób towarzyszy wola nieudostępniania treści przekazu osobom postronnym.

Innym rodzajem komunikowania się w Internecie jest uczestnictwo w grupach lub listach dyskusyjnych, a więc przesyłanie informacji między pojedynczą osobą a grupą adresatów. Z tego względu ten rodzaj komunikacji definiuje się jako „jeden do wielu”. Grupy dyskusyjne są miejscem publicznego wyrażania poglądów przez e-mail, dostępnych dla odbiorców na serwerach grup dyskusyjnych. Z tego względu do korespondencji e-mailowej kierowanej do grup dyskusyjnych należy odnosić przede wszystkim art. 54 konstytucji, gwarantujący wolność wypowiedzi i wyrażania poglądów. Korespondencja ta objęta jest jednak także ochroną art. 49 ustawy zasadniczej. Idzie tu zwłaszcza o ochronę przed jej przechwytywaniem, zmienianiem treści czy anulowaniem.

Ochrona tajemnicy komunikowania się, odnoszona zarówno do korespondencji pisemnej, jak i elektronicznej, związana ściśle z poufnością określonego przekazu między określonymi osobami zakłada:

– po pierwsze, zakaz zmuszania adresatów do ujawniania treści otrzymywanych przekazów;

– po drugie, zakaz podejmowania prób zdobycia informacji o tych treściach bez zgody adresata; dotyczy on wszystkich podmiotów, także organów władzy publicznej;

– po trzecie, ochronę samego faktu, że jest się w ogóle adresatem określonych przekazów[12].

Zatem „tajemnica komunikacji” polegać będzie na „ukryciu treści komunikatu (informacji, wypowiedzi, zwierzeń, wrażeń, uczuć itp.) przed innymi osobami niebędącymi wybranym przez autora komunikatu adresatem (innymi adresatami)”[13]. Nie chodzi przy tym o tajemnicę zawartą w treści komunikatu, ale o stosunek osób komunikujących się do tej treści. Daje to podstawę do wyróżnienia komunikacji interpersonalnej poufnej oraz dostępnej dla innych osób. Co istotne, o poufności decyduje wola komunikujących się osób, z tym że jej wyrażenie jest łatwiejsze w przypadku korespondencji pisemnej (list) aniżeli elektronicz-

[10] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 40–41.

[11] M. Matuzik, *Netykiety. Regulacje etyczne i prawne przepływu informacji w Internecie*, Zeszyty Prasoznawcze 1, 2/2000, a także http//matysoss.w..interia.pl/ArtZP.htm.

[12] P. Sarnecki, *op. cit.*, s. 3.

[13] I. Dobosz, *op. cit.*, s. 91.

nej[14]. Jednak właśnie ze względu na owe trudności w stworzeniu warunków zapewniających poufność, ochrona tajemnicy komunikacji (zwłaszcza w Internecie) jest tym bardziej potrzebna.

Zauważyć też trzeba, że naruszenie tajemnicy komunikacji oznaczać będzie każdą ingerencję osoby trzeciej, nie tylko w treść komunikatu, ale także polegającą na zmianie jego treści lub zniszczeniu. Naruszenie tajemnicy komunikacji należy rozumieć bowiem szeroko, a jej ochronę powinno się odnosić nie tylko do poufności określonego przekazu, ale także jego integralności (ochrony korespondencji jako takiej)[15]. Podkreślić trzeba jednak, że do naruszenia tajemnicy korespondencji może dojść jedynie w ramach komunikacji indywidualnej.

Tajemnica korespondencji wymieniona została także *expressis verbis* w art. 23 k.c. wśród innych dóbr osobistych, takich jak zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, nietykalność mieszkania, twórczość naukowa, artystyczna, wydawnicza i racjonalizatorska. Wymienione jedynie przykładowo dobra osobiste, a wśród nich tajemnica korespondencji podlegają ochronie kodeksu cywilnego, niezależnie od ochrony przewidzianej w innych przepisach prawa (prawa autorskiego lub karnego). W przeciwieństwie do ustawy zasadniczej kodeks cywilny posługuje się pojęciem „tajemnica korespondencji", a nie „tajemnica komunikowania się". Powstaje zatem pytanie, jak należy rozumieć pojęcie korespondencji użyte w art. 23 k.c. Wskazać można dwa sposoby rozwiązania tej wątpliwości. Według pierwszego, pojęcie to należy rozumieć najszerzej, obejmując nim wszelkie sposoby komunikacji, tj. od tradycyjnych (pismo, telefon, telegraf), po komunikację elektroniczną czy audiowizualną[16]. Taka interpretacja pojęcia „korespondencja" użytego w art. 23 k.c. pozwala na objęcie tym terminem nieznanych wcześniej form komunikowania się. Drugie rozwiązanie zakłada natomiast konieczność elastycznej interpretacji art. 23 k.c., pozwalającej na wyprowadzenie z tego przepisu nowego, pozakodeksowego dobra osobistego, a więc „tajemnicy komunikacji". Konieczność takiego zabiegu interpretacyjnego uzasadnia się w literaturze faktem, iż „dobrem chronionym, o którym mowa w art. 23 k.c., jest tajemnica dotycząca obu tych form porozumiewania się interpersonalnego, tj. „korespondencji" i „komunikacji", jednakże samo użyte w tym artykule określenie „tajemnica korespondencji" oznacza tylko jedną z tych form, a mianowicie tę, która posługuje się nośnikiem fizycznym (listem)"[17].

Wydaje się, że fakt pojawienia się nowych środków rejestrowania wypowiedzi nie wymaga bezwzględnie wyodrębniania kolejnego dobra osobistego, niewymienionego w art. 23 k.c. w postaci wolności i tajemnicy komunikowania się. Wystarczy bowiem szersze rozumienie dobra tam zamieszczonego, a więc tajemnicy

[14] *Ibidem*, s. 91.

[15] Wyrazem tego jest przewidziana w art. 268 § 1 k.k. karalność naruszenia integralności komputerowego zapisu informacji.

[16] P. Bogdalski, *Cywilnoprawne aspekty ochrony informacji*, PUG, z. 7–8, 1996, s. 2.

[17] I. Dobosz, *op. cit.*, s. 91.

korespondencji, chociaż nie budzi wątpliwości, że w odniesieniu do informacji przepływających w sieci pojęcie tajemnicy komunikacji jest bardziej precyzyjne.

Zagadnienie stosowania wskazanych wyżej norm konstytucyjnych i prawnomiędzynarodowych, zapewniających wolność i ochronę tajemnicy komunikowania się pojawia się z całą ostrością przy posługiwaniu się sieciami informatycznymi. W tym kontekście powstaje podstawowe pytanie, a mianowicie czy ochroną, o której mowa w art. 49 ustawy zasadniczej, objęte są wszelkie treści przekazywane w Internecie? Idzie tu zwłaszcza o konieczność pogodzenia konstytucyjnej ochrony tajemnicy komunikowania się z – niebudzącą wątpliwości – potrzebą kontrolowania przez państwo informacji znajdujących w sieciach, zwłaszcza ze względu na ochronę bezpieczeństwa państwa i porządku publicznego[18].

Zasadniczy problem sprowadza się zatem do tego, jak zminimalizować niebezpieczeństwo, jakie niesie ze sobą korzystanie z Internetu, polegające na możliwości ujawnienia poufnych danych, które znajdują się w sieciach, ich fałszowania czy zmieniania przekazywanych danych, przy jednoczesnej ochronie interesu publicznego, związanego zwłaszcza z koniecznością zwalczania przestępstw.

Kwestia ta wymaga także rozsądnego pogodzenia ochrony słusznych interesów użytkowników Internetu w zachowaniu poufności przekazywanych danych, realizowanej poprzez kodowanie komunikatów zamieszczanych w sieci z koniecznością monitorowania treści szczególnie niebezpiecznych. Dotyczy to zwłaszcza rozpowszechniania pornografii, prowadzenia agitacji, np. przez organizacje terrorystyczne czy inne skrajne ugrupowania, a więc, najogólniej rzecz ujmując, wykorzystywania Internetu do prowadzenia działalności przestępczej.

Problemem pojawiającym się w praktyce, który dyskutowany jest szeroko także w innych krajach, jest kwestia skutecznego zabezpieczenia ochrony tajemnicy korespondencji pracowników przesyłanej pocztą elektroniczną.

Na te dylematy zwraca uwagę także Rekomendacja RE 3/97, wskazując, iż należy umożliwić zainteresowanym zachowanie anonimowości, m.in. przy przesyłaniu e-maili. W dokumencie tym stwierdzono też, że pozostawienie jednostce decyzji w sprawie zachowania anonimowości ma zasadnicze znaczenie dla zabezpieczenia jej prywatności oraz swobodnego wyrażania opinii w systemie on-line. Z tego względu „restrykcje prawne dotyczące anonimowości lub technicznych środków w tym zakresie powinny mieć charakter proporcjonalny oraz być ograniczone do zakresu pozwalającego respektować interesy powszechnie chronione w społeczeństwie demokratycznym”[19].

Problematyce ochrony prywatności w Internecie poświęcona została także Rekomendacja RE 5/99. Ostrzega ona użytkowników Internetu, że nie jest to miejsce bezpieczne, a każda czynność wykonana w Internecie pozostawia ślady. Istniejące zabezpieczenia nigdy nie są dostateczne i jedynym wyjściem byłoby stworzenie

[18] J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 19.

[19] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Zakamycze 2002, s. 227–228.

przez państwa-strony RE kodeksu etyki odwołującego się do podstawowych zasad i norm współżycia społecznego[20].

Formułowanie zasad sieciowego savoir-vivre'u, swoistych kodeksów etyki zawodowej czy środowiskowej jest konieczne choćby ze względu na to, że reguły obowiązujące w globalnej sieci nie zostały w Polsce jak dotąd spisane w jednym akcie i są przedmiotem regulacji prawa konstytucyjnego, cywilnego, karnego, pracy oraz autorskiego. Regulacje dotyczące wyłącznie funkcjonowania Internetu tworzone są także przez firmy w formie regulaminów zakładania i korzystania z kont e-mailowych. Zasady sieciowej etykiety (tzw. netykieta) odnaleźć można także w internetowych portalach oraz innych stronach WWW, poświęconych problematyce Internetu. Netykieta jest zbiorem niepisanych zasad postępowania w sieci, odnoszących się głównie do poczty elektronicznej oraz grup dyskusyjnych, a rzadziej także do kanałów IRC[21].

Zasady netykiety formułują pod adresem użytkowników poczty elektronicznej ważne, z punktu widzenia zachowania poufności przekazywanych informacji (tajemnicy komunikacji) zalecenia i ostrzeżenia. Zalecają one m.in.: dokładne przemyślenie treści listu, którego po wysłaniu nie można już cofnąć, ostrożność w odpowiadaniu na listy pochodzące z grup dyskusyjnych (odpowiedź może dotrzeć do wszystkich osób, do których dotarł list, na który odpowiadamy, a nie tylko do jego nadawcy), cytowanie tylko tych fragmentów listu, do którego odnosi się odpowiedź, sprawdzanie codziennie poczty, zakładanie, że poczta może być przejęta przez innych[22].

Netykieta nie zastąpi jednak prawnych regulacji dotyczących przepływu informacji w Internecie, dzisiaj rozrzuconych w aktach należących do różnych gałęzi prawa. Postuluje się także, wzorem innych państw (np. Stanów Zjednoczonych), uchwalenie odrębnej ustawy o poszanowaniu korespondencji elektronicznej, zwłaszcza w stosunkach pracodawca – pracownik.

2. PODMIOT PRAWA DO TAJEMNICY KOMUNIKOWANIA SIĘ W ŚWIETLE ART. 49 KONSTYTUCJI RP

Podmiotem prawa do tajemnicy komunikowania się, o którym mowa w art. 49 Konstytucji jest „każdy", a więc zarówno osoby fizyczne, jak i osoby prawne prawa prywatnego. Zakaz naruszania tajemnicy komunikowania się skierowany jest zatem do wszystkich podmiotów prawa. Obowiązek zachowania poufności spoczywa także na adresatach korespondencji, wówczas gdyby ujawnienie treści

[20] Por. także Rekomendację 4/95 dotyczącą ochrony danych osobowych w telekomunikacji ze szczególnym uwzględnieniem usług telefonicznych.

[21] IRC – Internet Relay Chat, M. Matuzik, *Netykiety*...

[22] J. Zieliński, *Etykieta sieciowa*, Wiadomości Internetowe, 1997, http//www.winter.pl/netykieta.html.

przekazu stanowiło naruszenie sytuacji prawnej nadawców, zwłaszcza ich prawa do prywatności[23]. Potwierdza to także wyrok Sądu Apelacyjnego z 7.11.1995 r.[24], w świetle którego „rodzaj przesyłki, jej treść oraz konsekwencje poznania treści przez osoby trzecie" powinny skłaniać nadawcę do takiego zabezpieczenia jej treści, aby zapoznanie się z nią nie było dla osób trzecich łatwe. Nie ma przy tym znaczenia, czy ktoś faktycznie zapoznał się z treścią przesyłki, czy też nie, a także, czy pismo zawierało wiadomości o charakterze tajemnicy[25]. Odnosi się to także do wysyłającego e-mail w takich warunkach, że bez większych trudności można zapoznać się z jego treścią. W tej sytuacji adresat przesyłki, zawierającej informacje o charakterze osobistym, swoje roszczenia o naprawienie szkody może kierować zasadniczo wobec jej nadawcy, a nie osoby trzeciej, która zapoznała się z jej treścią. Zatem ujawnienie korespondencji, np. e-maila, będzie stanowiło naruszenie tego dobra osobistego, jeżeli jego treść będzie dotyczyła szczegółów życia intymnego, na upublicznienie których adresat nie wyraził zgody[26], jak też gdy zostaną naruszone prawa autorskie nadawcy korespondencji[27].

2.1. TAJEMNICA KORESPONDENCJI ELEKTRONICZNEJ PRACOWNIKA

W kontekście ustalenia zakresu podmiotowego przepisu art. 49 ustawy zasadniczej na osobną uwagę zasługuje ważne zagadnienie uprawnienia pracodawców do monitorowania korzystania przez pracowników z Internetu. Dotyczy to zwłaszcza kwestii ochrony korespondencji elektronicznej pracownika w stosunkach z pracodawcą. Powstaje pytanie, czy pracownik korzystający z przydzielonego mu do wykonywania obowiązków służbowych komputera może odmówić pracodawcy wglądu do zgromadzonej w nim korespondencji. Czy zasada przyjęta w kodeksie pracy, zgodnie z którą pracownik ma obowiązek rozliczenia się ze wszystkich składników powierzonego mienia, odnosi się także do korespondencji, np. handlowej, prowadzonej za pomocą Internetu?

Odpowiedź na powyższe pytania zależy – jak się wydaje – od charakteru prowadzonej przez pracownika korespondencji, a mianowicie od tego, czy jest to ko-

[23] P. Sarnecki, *op. cit.*, s. 3.

[24] Por. J. Panowicz-Lipska, *Glosa do wyroku Sądu Apelacyjnego w Łodzi*, I ACR 529/95, OSP 1996, z. 7–8, poz. 143, s. 373. Por. też E. Woch, *Sfera życia prywatnego i jej ochrona przez naruszeniami w Cyberprzestrzeni*, [w:] *Internet 2000. Prawo – ekonomia – kultura*, R. Skubisz (red.), Lublin 2000, s. 78.

[25] J. Panowicz-Lipska, *Glosa do wyroku Sądu…*, s. 373.

[26] E. Woch, *Sfera życia prywatnego…*, s. 78–79.

[27] Por. ustawę o prawie autorskim i prawach pokrewnych z 4.02.1994 r. (Dz.U. z 2000 r., Nr 80, poz. 904 – t.j.) regulującą także zasady ochrony adresata korespondencji. Jeżeli adresat nie wyraził innej woli, korespondencję można udostępnić swobodnie dopiero po 20 latach po jego śmierci. Wcześniejsze opublikowanie wymaga zezwolenia jego współmałżonka, a w jego braku kolejno dzieci, rodziców lub rodzeństwa (art. 82).

respondencja służbowa czy prywatna. W tym zakresie pomocne mogłoby się okazać sięgnięcie do orzecznictwa organów międzynarodowych oraz ustawodawstw innych państw, dotyczących ochrony tajemnicy korespondencji elektronicznej.

Jako przykład wskazać można amerykańską ustawę z 1986 r. o poszanowaniu prywatności korespondencji elektronicznej (*Electronic Communications Privacy Act*), na podstawie której pracodawcy nie mogą kontrolować korespondencji e-mailowej pracowników przekazywanej w systemie ogólnodostępnym bez ich wyraźnej zgody złożonej na piśmie. Samo ostrzeżenie o ewentualności kontroli korespondencji nie może być równoznaczne z uzyskaniem zgody na taką kontrolę. Natomiast – co istotne – e-mail przesyłany wyłącznie w wewnętrznej sieci firmy nie jest objęty wspomnianą ustawą[28].

Z kolei w orzecznictwie niemieckim – jak wskazują J. Barta, R. Markiewicz – dominuje pogląd, że nie można domniemywać zgody pracownika, któremu powierzono miejsce do pracy z dostępem do telefonu i Internetu, na sprawdzanie go w zakresie korzystania z tych urządzeń[29]. Stosownie do tego w Niemczech specjalna grupa robocza do spraw mediów sformułowała szczegółowe wytyczne dotyczące prywatności korzystania z Internetu przez pracowników[30]. Co istotne, odrębnie potraktowała tę kwestię w odniesieniu do służbowej oraz prywatnej korespondencji elektronicznej pracownika, jakkolwiek w obu przypadkach punktem wyjścia było przyjęcie założenia, iż korzystanie z Internetu w miejscu pracy nie może prowadzić do całkowitej kontroli ze strony pracodawcy nad zatrudnionymi osobami.

Jeżeli chodzi o korzystanie z poczty elektronicznej w celach służbowych, omawiane wytyczne przyjmują, iż: 1. Pracodawca ma prawo do hasłowego sprawdzania czy surfowanie lub wysyłanie korespondencji przez pracownika ma naturę służbową. Jednak automatyczna, pełna kontrola przez pracodawcę byłaby już potraktowana jako poważne wkroczenie w sferę praw osobistych zatrudnionego i jest dozwolona tylko w wyjątkowych wypadkach; 2. Szczególnym kategoriom pracowników (np. psychologom, lekarzom, pedagogom itd.), którzy przy swoich czynnościach zawodowych stykają się z osobistymi tajemnicami i którzy znajdują się w specjalnym stosunku zaufania ze swoim partnerem komunikacyjnym muszą być zapewnione środki, które wykluczą możliwość zapoznania się z treścią korespondencji przez osoby nieupoważnione; 3. Z wychodzącymi i przychodzącymi pismami służbowymi w postaci poczty elektronicznej, pracodawca ma prawo za-

[28] Zob. MAN *Poczta elektroniczna i prywatność korespondencji*, „Rzeczpospolita" z 13–14.07.1996 r.

[29] J. Barta, R. Markiewicz, *Internet*..., s. 246.

[30] Grupa robocza utworzona została w ramach 63. Konferencji przedstawicieli szczebla federalnego oraz lokalnego właściwych do spraw ochrony danych osobowych, poświęconej wymaganiom dotyczącym ochrony danych osobowych osób zatrudnionych i ich partnerów komunikacyjnych, która odbyła się w dniach 7–8.03.2002 r.; zob. J. Kurek, *Prywatność korzystania z Internetu pracowników w Niemczech*, www.vagla.pl/publikacje.htm.

poznawać się w takim zakresie, jak z pisemną korespondencją służbową. Może on zarządzić na przykład, aby każde wychodzące lub przychodzące pismo zostało mu podane do wiadomości. Ponadto, ze względów bezpieczeństwa, mogą być przechwycone fragmenty poczty lub załączniki.

Inne zasady przyjęto natomiast w odniesieniu do poczty elektronicznej prowadzonej na użytek prywatny. Po pierwsze, pracodawca nie jest zobowiązany do zapewnienia osobom zatrudnionym możliwości korzystania z Internetu i poczty elektronicznej dla celów prywatnych. Jeżeli jednak wyrazi taką zgodę, wówczas elektroniczna korespondencja podlega ochronie, a co za tym idzie kontrola treści wiadomości jest co do zasady niedopuszczalna. Z tego względu na przykład prywatna korespondencja mylnie zaadresowana jako służbowa powinna być niezwłocznie przekazana do wyłącznej wiadomości adresata. Pracodawca może jednak uzależnić swoją zgodę na korzystanie z poczty elektronicznej dla celów prywatnych od dochowania przez osoby zatrudnione odpowiednich reguł i zasad postępowania, a zwłaszcza poddania się określonemu rodzajowi kontroli. Dotyczy to zwłaszcza względów bezpieczeństwa i pewności danych, ze względu na które prywatne listy elektroniczne mogą zostać przechwycone przez pracodawcę. Taki sposób postępowania powinien być jednak wcześniej podany do wiadomości pracowników[31].

Co ważne, wytyczne wymagają, by te same warunki korzystania z Internetu zapewnione były przy korzystaniu z Intranetu (wewnętrznej sieci firmy). Zauważyć także należy, że w Niemczech postuluje się uchwalenie obszernej regulacji ustawowej dotyczącej właśnie ochrony danych osobowych pracownika w związku z coraz większymi możliwościami korzystania w miejscu pracy z technik informacyjnych i komunikacyjnych.

Takich regulacji brakuje niewątpliwie także w Polsce, niemniej jednak wzorem rozwiązań przyjmowanych w innych krajach oraz w orzecznictwie odrębnie należy odnieść się do korespondencji służbowej i prywatnej pracownika.

Gdy idzie o tę pierwszą pracodawca ma prawo w każdej chwili wglądu do jej treści, a z chwilą ustania stosunku pracy pracownik ma obowiązek zwrócić wszystkie pozostawione do jego dyspozycji narzędzia pracy, w tym komputer, oraz pozostawić w stanie nienaruszonym nośniki, na których dokumentował swoją pracę[32]. Zatem, jeżeli pracownik prowadzi korespondencję służbową, wysyłając i otrzymując listy elektroniczne, występując przy tym w imieniu pracodawcy nie może powoływać się na ochronę tajemnicy korespondencji, zarówno na gruncie konstytucji, prawa cywilnego, jak i prawa karnego[33]. Nie oznacza to jednak,

[31] *Ibidem*.

[32] W. Orżewski, *E-mail – tajemnica korespondencji*, Portal WYDAWCA – Rynek wydawniczy/prawo, s. 2–3.

[33] Zresztą – jak się słusznie wskazuje w literaturze – „sama natura systemu skrzynek poczty elektronicznej prowadzonej dla pracowników przez pracodawcę sprawia, że znajdująca się w nich niekodowana poczta nie korzysta z ochrony prawnokarnej". W przypadku bowiem e-maili przy-

że kontrola tego rodzaju korespondencji przez pracodawcę nie jest w żaden sposób limitowana. Trzeba bowiem odróżnić inwigilację pracownika, przed którą chroni art. 11[1] k.p. (pracodawca jest obowiązany szanować godność i inne dobra osobiste zatrudnionego) oraz dopuszczalną formę kontroli efektywności wykorzystywania czasu pracy oraz ochrony uzasadnionych interesów pracodawcy (np. tajemnicy handlowej)[34]. Kwestią dyskusyjną jest natomiast, czy pracodawca ma obowiązek uprzedzić pracownika o możliwości i formach tego typu kontroli[35]. Wydaje się, że przestrzeganie w tym przypadku zasady transparentności pozwoliłoby unikać konfliktów pomiędzy pracodawcami i pracownikami oraz stosowania środków nadmiernie ingerujących w sferę prywatności pracowników[36].

Podkreślić trzeba jednak, że prawa pracodawcy do kontroli służbowej korespondencji elektronicznej pracownika (choć poddanej pewnym ograniczeniom, o czym dalej) nie można odnosić do podsłuchiwania jego rozmów telefonicznych. W tym duchu wypowiedział się także ETPC, który w orzeczeniu Halford przeciwko Wlk. Brytanii[37] stwierdził, że podsłuchiwanie rozmów telefonicznych prowadzonych w miejscu pracy może stanowić ingerencję w prawo do ochrony życia prywatnego i korespondencji. Zdaniem Trybunału ingerencja, by była legalna, musi spełniać kryterium zgodności z ustawą, zainteresowanemu zaś powinny przysługiwać środki odwoławcze. W analizowanej przez ETPC sprawie warunek zgodności z ustawą nie został spełniony, ponieważ ustawodawstwo brytyjskie normowało jedynie stosowanie podsłuchu w publicznych sieciach telekomunikacyjnych, podczas gdy w tej konkretnej sprawie podsłuchiwano rozmowy pracownika prowadzone z telefonu włączonego do wewnętrznej sieci telekomunikacyjnej pracodawcy. W tej konkretnej sprawie Trybunał musiał odpowiedzieć na pytanie, czy granice ochrony życia prywatnego i tajemnicy korespondencji są inne w przypadku podsłuchu rozmów telefonicznych prowadzonych z telefonu domowego, a inne w przypadku rozmów prowadzonych z telefonu biurowego. Trybunał udzielił na to pytanie odpowiedzi przeczącej, stwierdzając, że rozmowy

---

chodzących i wychodzących ze skrzynki pocztowej prowadzonej na serwerze pracodawcy dla jego pracowników nie jest konieczne przełamywanie żadnych zabezpieczeń elektronicznych, magnetycznych lub innych szczególnych zabezpieczeń, o których mowa w art. 267 § 1 k.k. Oznacza to, że zasoby poczty elektronicznej znajdujące się w takich skrzynkach są bezpośrednio dostępne dla pracodawcy, w związku z czym trudno w tej sytuacji mówić o przestępstwie z art. 267 k.k., A. Bydło, *Czy pracownik korzysta z tajemnicy korespondencji*, www.Infor.pl, artykuł opublikowany w Serwisie Prawno-Pracowniczym 18/2004.

[34] H. Kwiatkowska, *Służbowe skrzynki e-mailowe to własność pracodawcy*, „Rzeczpospolita" z dnia 7.01.2008 r.

[35] Takie stanowisko w tej kwestii zajął m.in. Rzecznik Praw Obywatelskich J. Kochanowski, którego zdaniem z przepisów kodeksu pracy nie można wyprowadzić tak daleko idącego uprawnienia pracodawców w postaci kontroli służbowej korespondencji pracownika i udostępniania jej do wglądu innym pracownikom. W jego opinii celowe jest zatem – wobec braku wyraźnej regulacji kodeksu pracy w tym zakresie – informowanie pracownika o zamiarze takiej kontroli.

[36] Inaczej np. H. Kwiatkowska, *Służbowe skrzynki e-mailowe...*

[37] Orzeczenie z 25.06.1997 r. za: A. Adamski, *op. cit.*, s. 63.

telefoniczne z miejsca pracy, podobnie jak z domu, mogą być objęte pojęciem „życie prywatne" i „korespondencji" z art. 8 Konwencji[38].

Podsłuchiwanie rozmów telefonicznych przez pracodawcę niewątpliwie odpowiada sytuacji przewidzianej w art. 267 § 2 k.k. W przypadku natomiast monitorowania korespondencji elektronicznej pracownika (służbowej i prywatnej) można mieć wątpliwości co do zasadności odnoszenia do tej sytuacji art. 267 k.k. Wyjątkiem od tej zasady jest sytuacja, w której wiadomości znajdujące się w skrzynce pocztowej prowadzonej na serwerze pracodawcy zostały zaszyfrowane za pomocą programu szyfrującego[39]. Bardziej kategoryczny pogląd – choć dyskusyjny – wyraził natomiast A. Adamski, że brakuje u nas podstaw prawnych do stosowania przez pracodawców kontroli rozmów telefonicznych i innych telekomunikacyjnych przekazów informacji własnych pracowników w miejscu pracy. Jego zdaniem, w świetle standardów międzynarodowych oraz art. 49 Konstytucji RP „prawo do inwigilowania obywateli przy pomocą środków technicznych przysługuje wyłącznie władzy publicznej i może być realizowane tylko przez jej właściwie umocowanych i działających zgodnie z prawem funkcjonariuszy"[40]. Pogląd taki autor ten, zdaje się odnosić zarówno do korespondencji służbowej, jak i prywatnej, co nie wydaje się uzasadnione.

W tym kontekście powstaje zatem pytanie, czy dostępność służbowych skrzynek poczty elektronicznej dla pracodawcy powoduje, że z przywileju ochrony tajemnicy komunikowania się nie korzysta także korespondencja prywatna pracownika. Niewątpliwie zacząć trzeba od tego, że w zakresie stosunku pracy nie powinno być w ogóle mowy o korespondencji prywatnej[41]. Jeżeli jednak jest już ona prowadzona, to powstaje pytanie, czy racjonalne byłoby domniemanie jej prywatności?

Wydaje się, że zbyt daleko idący jest pogląd, że pracownik korzystający dla celów prywatnych ze służbowego sprzętu musi liczyć się z tym, że treść jego

[38] Por. szerzej M.A. Nowicki, *Podsłuch uwarunkowany*, „Rzeczpospolita" z 27.08.1997 r.

[39] A. Bydło, *op. cit.*, s. 2. Por. też A. Bajończyk, *Karnoprawne aspekty ochrony prawa pracownika do tajemnicy komunikowania* się, Palestra nr 1–2, 2003, a także I. Politowska, M. Szmit, *Bezprawie w sieci, czyli o prawnych aspektach bezpieczeństwa informacji przechowywanych i przesyłanych w systemach i sieciach informatycznych*, www.boston-review, nr 2/2007.

[40] Zdaniem tego autora każda inna osoba, która w celu uzyskania nieprzeznaczonej dla niej informacji działa w sposób określony w przepisie art. 267 § 2 (podsłuch komputerowy), narusza dyspozycję tego przepisu. Dotyczy to w równym stopniu zarówno pracownika agencji ochroniarskiej, zakładającego na zlecenie podsłuch w cudzym lokalu, hakera uprawiającego szpiegostwo komputerowe za pomocą sieci komputerowych, jak i pracodawcy monitorującego rozmowy telefoniczne lub pocztę elektroniczną swoich pracowników; A. Adamski, *op. cit.*, s. 63.

[41] Biorąc pod uwagę okoliczności konkretnego przypadku, możliwe jest nawet uznanie, że nagminne korzystanie ze skrzynki służbowej do celów prywatnych, zwłaszcza jeśli zbiega się z innymi uchybieniami pracownika, stanowi ciężkie naruszenie podstawowych obowiązków pracowników w myśl art. 52 § 1 pkt 1 k.p.; A. Malinowski, *Obowiązki pracodawcy w związku z wykorzystywaniem komputera. Czy pracodawca może sprawdzać zawartość poczty elektronicznej*, GP nr 178/2007 z dnia 13.09.2007 r.

korespondencji odczytana zostanie przez pracodawcę, chociażby w procesie selekcji korespondencji służbowej pracownika[42]. W sytuacji gdy pracodawca wyraził zgodę na korzystanie przez pracownika ze służbowej skrzynki pocztowej do celów prywatnych, nie może – co do zasady – zapoznawać się z treścią przesyłanej za jej pośrednictwem korespondencji elektronicznej. Zakres prywatnego korzystania z takich skrzynek, jego warunki, a także zakres kontroli i konsekwencje związane z niedochowaniem tych warunków powinny zostać pracownikowi wyraźnie zakomunikowane. Ewentualne sprawdzanie przez administratora sieci prywatnej poczty elektronicznej pracownika pod kątem potencjalnych wirusów, co wiąże się z zapoznaniem się z treścią korespondencji, powinno być dozwolone za zgodą konkretnego pracownika[43]. Na takim stanowisku stanął także Europejski Trybunał Praw Człowieka w wyroku z 3.04.2007 r. w sprawie Copland v. the United Kingom (no 62617/00), w którym uznał, że brak powiadomienia pracownika o monitorowaniu rozmów telefonicznych lub korespondencji elektronicznej (a także przeglądania stron internetowych) można rozpatrywać z punktu widzenia naruszenia prawa do prywatności (art. 8 Konwencji).

W myśl art. 8 ust. 2 EKPC ingerencja władzy publicznej w sferę poszanowania życia prywatnego, w tym korespondencji, jest niedopuszczalna z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym państwie prawnym. W rozważanej sprawie Trybunał nie przesądził o tym, czy monitorowanie korespondencji pracowników jest „konieczne w demokratycznym państwie prawnym". Skoncentrował się na podstawie prawnej tego rodzaju działań, stwierdzając, że w momencie ingerencji nie obowiązywało w Wlk. Brytanii prawo, które pozwalałoby na monitorowanie pracowników (w tym ich korespondencji elektronicznej), a więc nie było to działanie w granicach przewidzianych przez ustawę[44], o czym mowa w art. 8 ust. 2 Konwencji.

W przywołanym wyroku Trybunał w sposób niebudzący wątpliwości wypowiedział się jedynie w kwestii konieczności istnienia podstawy ustawowej dla kontroli korespondencji elektronicznej pracownika. Zatem – jak się wydaje – samej kontroli nie wykluczył, potwierdzając że „pracodawca ma prawo do sporadycznych kontroli korespondencji pracowników"[45], z czego należy wnosić, że niedopuszczalne jest długotrwałe (nagminne) monitorowanie pracownika. Wy-

[42] W. Orżewski, *op. cit.*, s. 3.

[43] Pracodawca nie ma jednak obowiązku informowania pracownika o dokonywaniu automatycznej kontroli korespondencji e-mailowej za pomocą programu komputerowego. W tym przypadku nie dochodzi bowiem do ustalenia treści e-maila, ale jego stanu technicznego, por. M. Chakowski, *Pracodawca może monitorować korespondencję elektroniczną swoich pracowników*, GP nr 250, 27.12.2007 r., www.gazetaprawna.pl.

[44] Zasady monitorowania pracowników przyjęte zostały w Wlk. Brytanii w 2000 r. w ustawie *The Regulation of Investigatory Powers Act* (RIPA), a więc już po fakcie monitorowania pracownika opisanym przez Lynette Copland w sprawie rozważanej przez ETPC.

[45] D. Dörre Nowak, *Pracodawcy wolno kontrolować korespondencję pracowników*, „Rzeczpospolita" z dnia 7–9.04.2007 r.

pada jednak żałować, że nie sformułował żadnych wytycznych pod adresem ustawodawcy co do przesłanek i zakresu monitoringu w miejscu pracy. Nie ułatwia to tym samym rozwiązywania polskich problemów z tym związanych, zwłaszcza wobec braku regulacji ustawowej tej kwestii, o którą zabiega także Rzecznik Praw Obywatelskich. Wymogi, jakie muszą spełnić pracodawcy przy monitorowaniu pracowników, formułuje natomiast projekt dyrektywy UE dotyczącej omawianej tutaj problematyki. Do nich zalicza się: zgodność działań pracodawców z prawem (zakaz stosowania form monitoringu sprzecznych z prawem), usprawiedliwiony cel (zwłaszcza ochrona systemu informatycznego i danych przed wirusami, bezpieczeństwo pracowników, ochrona tajemnicy handlowej), proporcjonalność zastosowanych środków (zakaz nadmiernej ingerencji w życie pracowników), transparentność monitoringu (informacja o formie kontroli i zakresie dopuszczalnego korzystania z poczty służbowej dla celów prywatnych), spełnienie wymagań określonych w przepisach o ochronie danych osobowych[46]. Jest to zatem katalog przesłanek zbliżony do tych, o których stanowi art. 31 ust. 3 Konstytucji RP.

3. PRZYKŁADOWE NARUSZENIA TAJEMNICY KOMUNIKOWANIA SIĘ W INTERNECIE

W przypadku dobra osobistego, jakim jest tajemnica komunikacji, charakterystyczne jest nie tylko nowe jej pojmowanie, a więc odejście od tradycyjnego jej rozumienia jako korespondencji pisemnej, ale także pojawienie się nowych form naruszeń tego dobra, które ma już przecież ugruntowaną pozycję w doktrynie i orzecznictwie. Do naruszeń tajemnicy komunikacji w Internecie skłania przede wszystkim łatwość tego rodzaju działań, a także dużej mierze bezkarność sprawców tych naruszeń[47]. Jak słusznie podkreśla się w literaturze, korespondencja elektroniczna często traktowana jest jako powszechnie dostępna, chociaż ma ona przecież zarówno swojego konkretnego nadawcę, jak i konkretnego adresata[48]. Bez wątpienia także przy okazji komunikacji elektronicznej przedmiotem wymagającym ochrony jest szczególna więź między nadawcą komunikatu a jego odbiorcą z uwagi na poufny charakter korespondencji[49]. Z tego względu o naruszeniu tajemnicy komunikacji można mówić już wówczas, gdy tylko jedna osoba poza adresatem komunikatu pozna jego treść.

Niektóre z form naruszeń tajemnicy korespondencji elektronicznej nie różnią się praktycznie od podobnych działań, które występują poza Internetem i doty-

[46] G. Orłowski, *Strasburski wyrok, polskie problemy*, por więcej http://prawo.vagla.pl.

[47] P. Waglowski, *Naruszenie dóbr osobistych w Internecie i ich cywilnoprawna ochrona na podstawie przepisów k.c.*, Warszawa 1999, s. 30–31, http://www.vagla.pl.

[48] W. Orżewski, *E-mail – tajemnica korespondencji*, PORTAL WYDAWCA – rynek wydawniczy/prawo.

[49] P. Bogdalski, *op. cit.*, s. 2.

czą tradycyjnej korespondencji. Jako przykład można podać rozesłanie korespondencji elektronicznej danej osoby, które może spowodować naruszenie jej dobra osobistego w postaci nazwiska, pseudonimu lub twórczości naukowej bądź artystycznej tej osoby[50].

Przykładem naruszania wolności i tajemnicy komunikowania się, do którego dochodzić może w Internecie jest tzw. *fake mail* (fałszywy list), za pomocą którego można wprowadzić w błąd odbiorcę listu co do tożsamości nadawcy. Za pomocą takiego fałszywego listu podszywający się może naruszyć zarówno dobra osobiste innych osób (cześć, dobre imię), jak i osoby, pod którą się podszył. Co istotne *fake mail* może także spowodować naruszenie tajemnicy komunikacji, w sytuacji gdy fałszywy nadawca skłania adresata do przesłania odpowiedzi na kontrolowany przez siebie adres. W wyniku takiej wymiany e-maili osoba podszywająca się może wejść w posiadanie korespondencji do niej niekierowanej. W wyniku *fake maila* może dojść także do zablokowania konta e-mailowego danej osoby. Przyczyną tego może być np. fałszywe zapisanie „ofiary" na listy dyskusyjne, które nie wymagają potwierdzenia uczestnictwa lub wysłanie do grupy dyskusyjnej fałszywego listu z bardzo atrakcyjną propozycją (np. sprzedaży jakiegoś towaru po bardzo niskiej cenie)[51].

Formą naruszenia wolności komunikowania się jest także tzw. spaming. Konstytucja w art. 49 używa bowiem formuły „wolność komunikowania się", a nie „wolność komunikowania", a co za tym idzie obejmuje niewątpliwie także „wolność od otrzymywania (określonego rodzaju) przesłań"[52]. W skrajnych przypadkach spaming może doprowadzić do zapełnienia skrzynki pocztowej niechcianą korespondencją, co powoduje w konsekwencji niemożność przyjmowania jakiejkolwiek innej poczty elektronicznej, a nawet zalogowania się na konto e-mailowe. W takich przypadkach zdarza się, że administratorzy sieci automatycznie kasują niechcianą korespondencję pochodzącą z podejrzanego źródła bez względu na jej zawartość. W tym przypadku mamy jednak do czynienia z sytuacją, w której w obronie przed spamem dochodzi do naruszenia wolności i tajemnicy komunikowania się w wyniku kasowania (anulowania) korespondencji skierowanej do danej osoby[53].

Kolejnym przykładem ataków internetowych na dobro osobiste, jakim jest wolność i tajemnica komunikowania się, jest tzw. *sniffing*, polegający na instalowaniu specjalnego oprogramowania służącego do przechwytywania haseł, treści listów

[50] P. Waglowski, *Naruszenie dóbr*..., s. 50.

[51] P. Waglowski, *Internet i Netykieta a dobra osobiste człowieka*, 2004, http//www.vagla.pl. Artykuł opublikowany także [w:] *Internet – fenomen społeczeństwa informacyjnego*, Częstochowa 2000.

[52] P. Sarnecki, *op. cit.*, s. 3.

[53] Konkretny przypadek tego rodzaju działań opisuje P. Waglowski, *Naruszenie dóbr*..., s. 50–51.

lub innych informacji i przesyłaniu ich do systemu włamywacza[54]. W literaturze spotkać można pogląd, że już samo przygotowanie urządzeń podsłuchowych stanowi zagrożenie dobra osobistego, jakim jest tajemnica komunikacji[55]. Niektóre z przedstawionych wyżej działań wyczerpują znamiona czynów karalnych, przewidzianych w rozdziale XXXIII kodeksu karnego „Przestępstwa przeciwko informacji". Ich analiza wykracza jednak poza ramy niniejszego opracowania.

4. OGRANICZENIA TAJEMNICY KOMUNIKOWANIA SIĘ

W myśl przepisu art. 49 zd. 2 konstytucji wolność i tajemnica komunikowania się, przysługująca każdej jednostce, może być ograniczona jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Ponadto, podobnie jak w przypadku wszystkich innych praw i wolności, konieczne jest spełnienie przesłanek z art. 31 ust. 3 ustawy zasadniczej oraz art. 8 ust. 2 EKPC.

Niewątpliwie wprowadzanie ograniczeń tajemnicy komunikowania się uzasadnione jest potrzebą walki z przestępczością oraz koniecznością zapewnienia bezpieczeństwa państwu i jego obywatelom. W dobie rewolucji informacyjnej i szerokiego wykorzystywania technik komputerowych przez zorganizowane grupy przestępcze konieczne jest zapewnienie organom wymiaru sprawiedliwości dostępu do systemów komputerowych w celu zabezpieczania dla celów dowodowych informacji przechowywanych w tych systemach, ich przeszukiwania, elektronicznej obserwacji, a przede wszystkim stosowania tzw. podsłuchu komputerowego.

Zasadne wydaje się w tym miejscu nawiązanie do orzecznictwa ETPC, gdzie sformułowano wiele warunków, których spełnienie pozwala na uznanie tajnej kontroli korespondencji czy podsłuchu, w tym komputerowego, za legalne. W sprawie Klass i inni v. Niemcy Trybunał zaaprobował regulacje ustawowe legalizujące kontrolę korespondencji, pod warunkiem że dokonuje się jej wyjątkowo i są podstawy, by uznać, że jest ona konieczna w demokratycznym społeczeństwie w interesie bezpieczeństwa państwa lub dla ochrony porządku i zapobiegania przestępstwom. Trybunał wymaga także istnienia odpowiednich i skutecznych gwarancji przeciwko ewentualnym nadużyciom. Do minimalnych gwarancji, chroniących przed nadużyciami w związku ze zastosowaniem tzw. podsłuchu sądowego zaliczył: zdefiniowanie kategorii osób, wobec których można stosować podsłuch na podstawie nakazu sędziego, rodzaj przestępstw, w związku z którymi można go wydać, maksymalna długość okresu stosowania, procedura przygotowania raportów o treści zarejestrowanych rozmów, określenie okoliczności, w których zapisy muszą być zniszczone i inne (sprawy Kruslin i Huvig v. Fran-

[54] P. Waglowski, *Internet i Netykieta*..., oraz tenże, *Naruszenie dóbr*..., s. 55–56.
[55] I. Dobosz, *Przesłanki cywilnoprawnej*..., s. 95.

cja)[56]. Jakkolwiek wymienione gwarancje dotyczyły stosowania podsłuchu telefonicznego, to można je odnieść także do dopuszczalności stosowania podsłuchu komputerowego.

W tym miejscu można zadać pytanie, jak mają się wskazane wyżej zasady do praktyki działania służb ochrony państwa. Jak daleko sięga inwigilacja internautów przez te służby? Czy nie dochodzi do konfliktu pomiędzy uprawnieniami tych organów a przysługującym każdemu prawem do prywatności? Aktywność organów państwa w zakresie monitorowania informacji znajdujących się w sieci zwiększyła się zwłaszcza po ataku terrorystycznym na World Trade Center. Największe kontrowersje budzi posługiwanie się przez FBI specjalnym systemem „Carnivore", którego zadaniem jest elektroniczny monitoring przepływających przez sieć danych, między innymi kontrolowanie wysyłanych e-maili[57]. Starszym tego typu systemem jest „Echelon", projekt o szerszym zakresie, gdyż oprócz USA zaangażowane są w niego także Wielka Brytania, Australia i Nowa Zelandia.

W praktyce, prowadzony za pomocą takich systemów globalny podsłuch może godzić zarówno w prywatność indywidualnych użytkowników sieci, jak i interesy przedsiębiorców (zwłaszcza europejskich), którzy – jak się podejrzewa – wskutek elektronicznego podsłuchu tracą ogromne dochody na rzecz konkurencji z USA. Zarzuty tego rodzaju pod adresem Stanów Zjednoczonych i Wielkiej Brytanii są wyjaśniane przez Komisję Europejską UE[58].

Także w Polsce zaobserwować można zwiększoną aktywność organów ochrony państwa w kierunku inwigilowania sieci. W ustawodawstwie istnieje zresztą wiele wyjątków od sformułowanego w art. 267 § 2 k.k. zakazu inwigilacji. Możliwość posługiwania się podsłuchem komputerowym w postępowaniu karnym przewiduje przede wszystkim art. 237 w związku z art. 241 k.p.k.[59] Biorąc jednak pod uwagę ochronę tajemnicy komunikowania się i ochronę przed ingerencją w sferę życia osobistego jednostki, ograniczono dopuszczalność stosowania podsłuchu tylko do wyliczonych enumeratywnie, najpoważniejszych przestępstw[60]. Niezależnie od podsłuchu procesowego prawo karne dopuszcza także tzw. podsłuch operacyjny[61]. Szczegółowe kwestie dotyczące zasad prze-

[56] M.A. Nowicki, *Europejski Trybunał*..., s. 603–604.

[57] 18.09.2001 r. Senat USA pozwolił FBI na oficjalne stosowanie kontrowersyjnego systemu, por. szerzej P. Kępiński, *Internetowa prywatność a uprawnienia organów państwa*, www.vagla.pl./publikacje.htm.

[58] *Ibidem*.

[59] Ustawa z 6.06.1997 r. kodeks postępowania karnego (Dz.U. nr 89, poz. 555).

[60] Szerzej na ten temat K. Dudka, *Podsłuch komputerowy w polskim procesie karnym – wybrane zagadnienia praktyczne*, PriP nr 1, 1999, s. 69 i n.

[61] Podstawę prawną jego prowadzenia stanowią: art. 19 ustawy o Policji z 6.04.1990 r. (Dz.U. z 2007 r., Nr 43, poz. 277 – t.j.), art. 36 ustawy o kontroli skarbowej z 28.09.1991 r. (Dz.U. z 2004 r., nr 8, poz. 65 – t.j.), art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu z 24.05.2002 r. (Dz.U. z 2002 r., Nr 74, poz. 676 ze zm.) oraz art. 17 ust. 5 ustawy o Centralnym Biurze Antykorupcyjnym z 9.06.2006 r. (Dz.U z 2006 r., Nr 104, poz. 708).

prowadzania czynności operacyjnych związanych z podsłuchem regulują stosowne rozporządzenia[62].

Sposobem na utrudnienie pracy elektronicznym „szpiegom" jest kodowanie informacji przesyłanych drogą elektroniczną. Jednym z bardziej kontrowersyjnych zagadnień ściśle związanych z ograniczeniami wolności i tajemnicy komunikowania się jest jednak pytanie o to, czy posiadacz komputera może być zmuszony do ujawnienia zakodowanych danych. Problem ten wiąże się z dopuszczalnością stosowania metod kryptograficznych, a więc przekształcania komunikatów powszechnie zrozumiałych w komunikaty szyfrowe (kodowane) czytelne tylko dla odbiorcy posiadającego odpowiedni klucz deszyfrujący. W literaturze wskazuje się, że jest to jeden z bardziej spornych problemów związanych z posługiwaniem się sieciami komputerowymi, a zwłaszcza Internetem[63]. Uzasadnieniem dla stosowania kryptografii w sieciach komputerowych jest dążenie do zapewnienia prawa do prywatności oraz prawa do tajemnicy korespondencji w zakresie posługiwania się pocztą elektroniczną. Idzie tu m.in. o zabezpieczenie przed praktykami polegającymi na przechwytywaniu wiadomości przepływających przez Internet, zmienianiu jej treści i przekazywania dalej do adresata bądź na anulowaniu korespondencji kierowanej do grup dyskusyjnych. O usuwanie korespondencji kierowanej do grup dyskusyjnych krytykujących scjentologów oskarżano członków Kościoła scjentologicznego[64].

Gdy idzie o dopuszczalność stosowania metod kryptograficznych, spotkać można skrajne poglądy, które z jednej strony domagają się wolności kodowania w Internecie, z drugiej zaś w ogóle sprzeciwiają się swobodnemu „podsłuchiwaniu" korespondencji elektronicznej. Przeważają jednak bardziej umiarkowane poglądy, wedle których stosowanie kryptografii powinno być dozwolone, ale nie w pełni i w określonych przypadkach. Stanowisko takie uzasadnione jest obawami, że kodowanie może ułatwiać prowadzenie w sieci działalności przestępczej, np. działalności terrorystycznej, prowadzenia nielegalnych transakcji finansowych, rozpowszechniania pornografii. Jak się wskazuje w literaturze „ograniczenia w zakresie kodowania dyktowane są walką z organizacjami i gru-

[62] Kontrowersje budziło rozporządzenie Ministra Infrastruktury z 24.01.2003 r., wydane na podstawie art. 40 ust. 3 ustawy Prawo Telekomunikacyjne, w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Rozporządzenie wywołało obawę niekontrolowanego podsłuchu internetowych przekazów informacji, a także wątpliwości co do konstytucyjności obciążania dostawców usług internetowych obowiązkiem wprowadzania na własny koszt systemu pozwalającego na kontrolę przekazów informacji**,** por. P. Waglowski, *Podsumowanie wydarzeń związanych z Internetem obserwowanych przez pryzmat prawa*, http//www.vagla.pl. W obecnym stanie prawnym kwestie te reguluje Rozporządzenie Ministra Transportu z 30.04.2007 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego (Dz.U. Nr 90, poz. 603).

[63] J. Barta, R. Markiewicz, *Internet a*..., s. 21, oraz tychże *Ochrona danych*..., s. 228 i n.

[64] J. Barta, R. Markiewicz, *Internet a*..., s. 21.

pami przestępczymi, które w przeciwnym razie mogłyby uzyskać efektywną, wolną od podsłuchu i nie poddającą się kontroli ze strony państwa, międzynarodową sieć porozumiewania się"[65].

[65] *Ibidem*, s. 24. W Niemczech zarówno prawicowi, jak i lewicowi ekstremiści jako jedni z pierwszych zaczęli używać poczty elektronicznej, aby usprawnić komunikację. Organizacje prawicowe założyły 10 mailboksów („Thule-Network"), w których rozpowszechniali materiały propagandowe, por. M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, www.vagla.pl/publikacje.htm.