Antoni Bojańczyk

Karnoprawne aspekty ochrony prawa pracownika do tajemnicy komunikowania się : (część II)

Palestra 48/3-4(543-544), 76-89

2003

Antoni Bojańczyk

KARNOPRAWNE ASPEKTY OCHRONY PRAWA PRACOWNIKA DO TAJEMNICY KOMUNIKOWANIA SIĘ (Część II)

1. W części I-szej niniejszego opracowania („Palestra", nr 1–2, 2003) został zarysowany abstrakcyjny model prawa do ochrony tajemnicy komunikowania się, ukształtowany w oparciu o gwarancje konstytucyjne. Zaproponowana została również definicja przedmiotu ochrony prawnej Rozdziału XXXIII k.k. Model ten (a także założenie definicyjne) możemy obecnie wykorzystać przy rozważaniach prowadzonych na płaszczyźnie prawnokarnej.

Zakładamy zatem, że istnieją dwa odrębne układy (układ pomiędzy komunikującymi się i układ do którego należą pozostałe podmioty), między którymi nie może być – co do zasady – żadnego przenikania (ingerencji podmiotów z układu zewnętrznego w układ istniejący pomiędzy podmiotami komunikującymi się). Otóż wskazać należy, że taki abstrakcyjny model – oczywiście przy uwzględnieniu specyfiki uregulowania kodeksu karnego – może być również dość przydatny do analizy kwestii odpowiedzialności karnej z art. 267 § 1 k.k. Trzeba uznać, że stosunek komunikowania się pomiędzy dwoma (lub więcej) dowolnymi podmiotami korzysta nie tylko z ochrony konstytucyjnej, lecz także – co ma gwarantować realne przestrzeganie postanowień konstytucyjnych – z ochrony karnoprawnej, określonej szczegółowo w wyżej wymienionym przepisie.

Wraz z przeniesieniem na grunt ustawy karnej model prawa do ochrony komunikowania się (przy zachowaniu jego podstawowego kształtu) powinien zostać uzupełniony o trzy dodatkowe elementy, charakterystyczne już tylko dla karnoprawnej gwarancji tajemnicy komunikowania się.

Po pierwsze (1), odczytanie art. 267 § 1 k.k. upoważnia do stwierdzenia, że podmiot naruszający tajemnicę komunikowania się przez uzyskanie informacji wymienianej (za pomocą różnych środków technicznych[1]) pomiędzy dwoma podmiotami komunikującymi się popełnia występek. Należy przy tym zauważyć, że wystar-

[1] I tak informacja może zostać uzyskana przez otwarcie zamkniętego pisma, podłączenie się do przewodu służącego do przekazywania informacji bądź też przełamanie elektronicznego, magnetycznego lub innego szczególnego zabezpieczenia (art. 267 § 1 k.k.).

czające do przypisania winy za przełamanie tajemnicy komunikowania się jest już samo uzyskanie informacji, nie jest zatem konieczne zapoznanie się z nią – „uzyskać" bowiem to tyle co „osiągnąć, otrzymać, zdobyć"[2], „(...) osiągnąć to co było przedmiotem starań; dostać, pozyskać (...)". Rozwiązanie to jest właściwe, użyte w ustawie znamię czasownikowe „uzyskać" pozwala szczęśliwie na przecięcie u podstaw wszelkich sporów dowodowych związanych z tym, czy sprawca się z uzyskaną informacją zapoznał czy też nie.

W doktrynie przedstawiona została jednak odmienna i – jak się wydaje – nietrafna interpretacja znamienia ustawowego „uzyskiwać", odwołująca się[3] do przedwojennej wykładni S. Glasera i A. Mogilnickiego dokonanej na gruncie art. 253 § 1 k.k. z 1932 r. Autorzy ci uznali, że przez „«uzyskanie» rozumie się zapoznanie się z treścią danej wiadomości"[4]. (Niestety na poparcie tej tezy nie przytaczają żadnych argumentów).

A. Adamski[5] twierdzi, że „aby przypisać sprawcy winę (za przestępstwo z art. 267 § 1 k.k. – *A.B.*) nie wystarczy, tak jak poprzednio (tj. wg k.k. z 1969 r. – *A.B.*), udowodnić mu, że bez zgody osoby uprawnionej otworzył on cudze pismo zamknięte, lecz, że pismo to otworzył i przeczytał". Uznaje, że „naruszenie poufności informacji następuje tu bowiem z chwilą «uzyskania informacji», czyli zapoznania się z jej treścią" (*op. cit.*, s. 46). (Na marginesie trzeba zauważyć, że do takiego wniosku niechybnie prowadzi A. Adamskiego przyjęta wcześniej definicja informacji. W jej świetle po prostu niemożliwe jest, by uzyskanie informacji dokonało się inaczej niż poprzez zapoznanie się z jej treścią). Podobnie B. Kunicka-Michalska, która uznaje wprost, że „pojęcie uzyskania informacji zakłada (...) dojście treści informacji do wiadomości sprawcy. Chodzi bowiem o uzyskanie informacji (czyli jej treści w znaczeniu przyjętym przez autorów), a nie jej nośnika"[6].

---

[2] *Jedenastotomowy Słownik Języka Polskiego PWN* pod red. W. Doroszewskiego, Warszawa 1976, t. IX, T-Wyf., s. 792.

[3] A. Adamski, *Prawo karne komputerowe...*, Warszawa 2000, s. 46; tenże, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle Konwencji Rady Europy.* Toruń 1999 r., s. 22, B. Kunicka-Michalska, *Przestępstwo przeciwko ochronie informacji i wymierzaniu sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz*, Warszawa 2000, s. 492.

[4] S. Glaser i A. Mogilnicki, *Kodeks karny. Komentarz.* Kraków 1934, s. 831.

[5] A. Adamski, *Prawo karne...*, s. 47; tenże, *Przestępczość w cyberprzestrzni...*, s. 22.

[6] *Op. cit.*, s. 492. Wskazać trzeba także na pewną zasadniczą sprzeczność w rozumowaniu B. Kunickiej-Michalskiej. Przyjmuje ona definicję informacji zaproponowaną przez B. Michalskiego, która nie czyni wyraźnego rozróżnienia na informację abstrakcyjną (proces myślowy) i zapisaną na nośniku (a więc szerokie) rozumienie pojęcia, nie ograniczające się do samego tylko procesu myślowego polegającego na odczytaniu z danego zapisu pewnych twierdzeń opisowych lub abstrakcyjnych. Odrzuca – słusznie zresztą – definicję informacji A. Adamskiego uznając (dość enigmatycznie), że „mogłoby (to) uczynić mało zrozumiałymi nasze dalsze rozważania". Twierdzenie to stoi więc w oczywistej sprzeczności z wcześniejszym założeniem terminologicznym autorki. Uzyskanie informacji (rozumianej tak, jak zostało to przedstawione przez B. Kunicką-Michalską) nie jest w żadnym wypadku równoznaczne tylko z zapoznaniem się z treścią informacji.

Wydaje się, że Autorzy ci nadają pojęciu „uzyskiwać" znaczenie nieprawidłowe, sprzeczne z jego znaczeniem z języka potocznego. Nie jest to uzasadnione. Gdyby ustawodawca chciał inaczej zdefiniować znamię przestępstwa z art. 267 § 1 k.k. (np. w kierunku proponowanym przez B. Kunicką-Michalską i A. Adamskiego) to nie użyłby innego zwrotu (np. zapoznaje się, poznaje), wyraźnie wskazującego na intencję jego odmiennej interpretacji. Wyrazowi „uzyskać", w żadnym razie nie można przypisać znaczenia tożsamego z zapoznaniem się z informacją. Można bowiem informację tylko uzyskać w formie zapisu (rozmaitego zresztą rodzaju), lecz nie trzeba się z nią (jej treścią) zapoznać, by wypełnić znamię z art. 267 § 1 k.k. Trafny jest zatem pogląd W. Wróbla[7], który stoi na stanowisku, że „poprzez pojęcie uzyskania należy rozumieć nie tylko wejście we władanie nośnika, na którym zapisano informację (kartki papieru, taśmy magnetofonowej, taśmy filmowej, dyskietki komputerowej), ale także skopiowanie zapisu informacji (poprzez przepisanie, wykonanie kserokopii, lub fotokopii, skopiowanie zapisu na nośniku komputerowym), czy też zapoznanie się z informacją w sposób umożliwiający jej zrozumienie". Pogląd identyczny prezentuje P. Kardas [„Uzyskanie informacji to (...) zdobycie nad nią władztwa przez sprawcę, zdobycie możliwości jej swobodnego wykorzystania, decydowania o jej przeznaczeniu. Może się ono przejawiać objęciem we władanie nośnika, na którym zapisana jest informacja, skopiowaniem zapisu informacji (...)."[8]]. Na marginesie należy wskazać, że ten zasługujący w pełni na aprobatę wniosek P. Kardasa stoi jednak w sprzeczności z wcześniej przyjętymi przez tego Autora założeniami teoretycznymi. Bo jeżeli Autor uznaje, że „informacja" to tylko tyle co r e z u l t a t (podkr. – *A.B.*) procesu interpretacji danych, to powinien chyba konsekwentnie przyjąć, iż „uzyskanie" informacji w rozumieniu art. 267 § 1 k.k. to tylko proces zachodzący w umyśle odbiorcy zapisu informacji, który prowadzi do interpretacji zapisu i jej właściwego odczytania i nie może ono polegać np. na objęciu nośnika, na którym jest zapisana informacja lub skopiowaniu zapisu informacji. Wydaje się więc, że jest to *sui generis* „pułapka" definicyjna.

Art. 267 § 1 k.k. chroni zatem tajemnicę komunikowania się rygorystycznie, zakładając (słusznie zresztą), że już samo dokonanie takich czynności, które doprowadzają sprawcę do wejścia w posiadanie (nawet bez zapoznania się z nimi) informacji wymienianych pomiędzy innymi podmiotami powinno być penalizowane.

---

[7] *Kodeks karny. Część szczególna* (red. A. Zoll), t. II, Kraków 1999 r., s. 1004. Por. również O. Górniok, S. Hoc, St. M. Przyjemski: *Kodeks karny. Komentarz*, t. III, Gdańsk 1999, s. 233–323, teza 4 [„Zachowanie sprawcy określa znamię czasownikowe «uzyskuje». W języku potocznym oznacza ono otrzymywanie czegoś, osiąganie tego, czego się chciało, dostawanie. (...) Podłączanie się do przewodu to działanie, w którego rezultacie sprawca m o ż e (podkr. – *A.B.*) otrzymywać wiadomości dla niego nieprzeznaczone, przysyłane tym przewodem", oraz A. Marek, *Komentarz do kodeksu karnego. Część szczególna*, Warszawa 2000, s. 682].

[8] P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego, Czasopismo prawa karnego i nauk penalnych*. Półrocznik Polskiej Akademii Umiejętności (Rok IV, 2000, z. IV), s. 67.

Nie ma jednak przestępstwa określonego w tym przepisie, jeśli informacja jest uzyskiwana (2) legalnie [czyli na podstawie upoważnienia prawnego (uprawnienia)[9]] lub (3) jest to informacja przeznaczona dla podmiotu uzyskującego informację. Przez informację nieprzeznaczoną dla podmiotu ją uzyskującego, należy rozumieć taką informację, która nie jest do danego podmiotu skierowana (zaadresowana)[10].

Aby zatem stwierdzić byt przestępstwa z art. 267 § 1 k.k. w układzie pracodawca–pracownik niezbędne jest określenie, czy pracodawca uzyskuje informacje przekazywane przez swego pracownika legalnie (a) oraz czy jest to informacja do której – być może – podmiot ten ma uprawnienia faktyczne (b) [czy wiadomość przekazywana przez pracownika jest dla niego p r z e z n a c z o n a (do niego skierowana, jest on adresatem tej wiadomości)].

Ad a. Udzielenie odpowiedzi na pierwsze z postawionych pytań nie nastręcza w zasadzie większych trudności. W ustawodawstwie polskim (*de lege lata*) nie istnieje podstawa prawna, która uprawniałaby pracodawcę do podłączania się do prywatnych rozmów telefonicznych prowadzonych przez pracownika[11]. Takie działanie jest zatem bezprawne w rozumieniu kodeksu karnego.

Ad b. Kwestia druga, tj. sprawa ustalenia, czy pracodawca ma uprawnienie do uzyskiwania rozmów (korespondencji elektronicznej) pracownika jest bardziej złożona. Komunikowanie się dwóch podmiotów podlega (poza przewidzianymi ograniczeniami prawnymi) bezwzględnej ochronie prawnej. Na pierwszy rzut oka wydaje się zatem, że rozmowa telefoniczna (względnie wymiana poczty elektronicznej) pracownika z podmiotem zewnętrznym korzysta z przywileju ochrony tajemnicy komunikowania się – i to nie tylko konstytucyjnego, lecz również karnoprawnego.

Jest to jednak twierdzenie częściowo błędne, ponieważ w istocie rzeczy – jak zobaczymy – nie zawsze mamy tu do czynienia z sytuacją ingerencji podmiotu trzeciego (pracodawcy) w tajemnicę komunikowania się dwóch innych podmiotów. Dla jasności wywodu kwestia ta powinna zostać poddana analizie na dwóch odrębnych płaszczyznach: (1) w odniesieniu do rozmów telefonicznych (listów elektronicznych) służbowych (ściśle związanych z wykonywaną pracą) oraz w odniesieniu do (2) komunikacji prywatnej (niezwiązanej z wykonywaną pracą, odnoszącej się do kręgu życia prywatnego pracownika).

Przed przejściem do rozważań na temat uprawnienia pracodawcy do uzyskiwania treści prywatnych (służbowych) rozmów telefonicznych (korespondencji elektronicznej) niezbędna jest uwaga dotycząca technicznych aspektów działania pracodawcy, tj. metody uzyskiwania informacji wymienianej przez podmioty (z których jednym jest właśnie pracownik). Należy zwrócić uwagę, że nie

[9] Por. A. Marek, *op. cit.* Warszawa 2000, s. 275, tenże, *Prawo karne*, Warszawa 2001, s. 681–682.
[10] Por. O. Górniok, *op. cit.*
[11] Por. A. Adamski, *Przestępczość w cyberprzestrzeni...*, s. 28.

każdy sposób działania pracodawcy, który w ostatecznym rozrachunku prowadzi do uzyskania informacji można zakwalifikować jako odpowiadający znamionom czynu określonego w art. 267 § 1 k.k. Sprawca tego przestępstwa musi działać w następujący sposób: (1) otwierać zamknięte pismo, (2) podłączać się do przewodu służącego do przekazywania informacji lub (3) przełamywać elektroniczne, magnetyczne lub inne szczególne zabezpieczenie informacji. Działanie polegające na podsłuchiwaniu rozmów telefonicznych prowadzonych na liniach zakładu pracy wypełnia znamiona czynu określonego w § 1 art. 267 kodeksu karnego. Nie ulega bowiem wątpliwości, że mamy do czynienia w tym przypadku z podłączeniem się do przewodu służącego do przekazywania informacji (linia telefoniczna). Bez znaczenia jest fakt, że podłączenie do linii odbywa się fizycznie wewnątrz zakładu pracy (zazwyczaj za pomocą specjalnie zaprogramowanej centrali telefonicznej), a nie na zewnątrz (np. podłączenie do kabla telefonicznego w studzience lub na słupie telefonicznym). Uzyskanie (otrzymanie, osiągnięcie) informacji odbywa się przez jej podsłuchiwanie i automatyczne nagrywanie.

Inaczej ma się sprawa z uzyskiwaniem przez pracodawcę e-maili przychodzących i wychodzących ze skrzynki pocztowej prowadzonej przez pracodawcę na jego własnym serwerze dla pracowników. Art. 267 § 1 k.k. określa przestępstwo *hackingu*[12], czyli nieuprawnionego włamywania się do systemu komputerowego, by uzyskać informacje zastrzeżone[13]. Sprawcą takiego czynu jest *hacker*. Czy można uznać, że pracodawca jest *hackerem*?

Ze względu na strukturę systemu (to podlegający pracodawcy administrator systemu informatycznego zakłada i prowadzi konta pocztowe dla pracowników, wydaje hasła dostępu do skrzynek pocztowych itd.) do uzyskania tych informacji (listów elektronicznych) nie jest konieczne ani przełamanie zabezpieczeń elektronicznych, ani też żadnych innych szczególnych zabezpieczeń. Zasoby poczty elektronicznej znajdujące się w poszczególnych skrzynkach są bezpośrednio dostępne dla pracodawcy[14]. W tej sytuacji nie można mówić o bycie przestępstwa z art. 267 § 1 k.k.[15].

---

[12] *(To) hack:* < 3. use a computer to gain unauthorized access to data> (wykorzystywać komputer w celu uzyskania danych bez należytego uprawnienia), *The Concise Oxford Dictionary*, Tenth Ed. Oxford University Press. Oksford 1999, s. 638.

[13] Na temat *hackingu* w polskim kodeksie karnym por. b. ciekawe i obszerne uwagi A. Adamskiego, *Prawo karne...*, s. 45–55.

[14] Na marginesie tych rozważań zauważyć należy, że firmy coraz częściej zaopatrują się w tzw. programy cenzurujące (!). Pozwalają one na wyławianie spośród przesyłanej korespondencji listów, w których pada określony wyraz lub zbiór wyrazów (np. nazwa firmy lub jej kontrahentów). Ułatwia to kontrolę korespondencji pracowników, nie ma w związku z tym konieczności zatrudniania całego sztabu ludzi, którzy zajmowaliby się wyłącznie lekturą setek maili przychodzących i wychodzących z firmy. Załatwia to za nich automat. Listy takie podlegają „zatrzymaniu" przez administratora systemu i analizie.

[15] Por. W. Wróbel, *op. cit.*, teza 7 do art. 267 § 1 k.k.; O. Górniok, *op. cit.*, s. 323.

Wyjątek stanowi sytuacja, gdy znajdujące się w skrzynce pocztowej e-maile (oraz załączniki do nich) są zaszyfrowane z użyciem programu typu *encryption* (programu szyfrującego). Nie jest to istotne, kto dany list zaszyfrował (pracownik-nadawca czy też nadawca zewnętrzny). List taki, ze względu na to, że nie jest możliwe jego odczytanie bez programu rozszyfrowującego, klucza albo hasła rozszyfrowującego nie jest dostępny dla pracodawcy w sposób identyczny jak „zwykła", niekodowana poczta elektroniczna przesyłana z i do jego serwera. Dlatego też jego odczytanie wiąże się z przełamaniem innego szczególnego zabezpieczenia (w postaci programu szyfrującego, klucza, kodu itp.) i tu niewątpliwie dochodzi do zaistnienia jednego ze znamion przestępstwa określonego w art. 267 § 1 k.k.

Na marginesie warto wspomnieć o charakterystycznym aspekcie uzyskania przez pracodawcę informacji zaszyfrowanych. Intencją ustawodawcy było – jak się wydaje – dokonanie rozróżnienia na informację w znaczeniu ścisłym (jej definicja została przedstawiona w cz. I niniejszego opracowania) oraz na informację, która przez zastosowane przez nadawcę specjalne zabezpieczenia (elektroniczne, magnetyczne lub inne – art. 267 § 1 k.k. *in fine*) nie może być odczytana przez każdą osobę. Nie jest zatem dostępna za pomocą „zwykłych" systemów odczytu – np. języka, którego znaczenia (przypisane do danych form lub zwrotów) nie są utajnione, są ogólnodostępne. Przykład: jeśli sprawca nagrywa rozmowę prowadzoną w języku suahili (język z rodziny bantu używany w krajach Afryki Wschodniej) to tym samym uzyskuje informację, która – choć zapisana w egzotycznym np. dla przeciętnego Europejczyka języku – może być odczytana za pomocą ogólnodostępnego słownika suahili. Inaczej ma się sytuacja, jeśli pracodawca uzyskuje informację specjalnie zaszyfrowaną (zakodowaną). Może ona zostać odczytana tylko za pomocą szyfru/klucza których jest – z samej swej natury[16] – tajny i niedostępny dla osób niepowołanych. W ten sposób mają one zamknięty dostęp do danej informacji. Dopóki zatem sprawcy nie uda się przetworzyć szyfru/kodu (przez przełamanie szyfru, który jest innym specjalnym zabezpieczeniem w rozumieniu art. 267 § 1 k.k.) i zapisać tak uzyskanej „czystej" (odszyfrowanej, zdekodowanej) informacji na nośniku w formie zapisu językowego bądź się z nią zapoznać, dopóty nie można przypisać mu sprawstwa przestępstwa z art. 267 § 1 k.k. Oznacza to zatem, że uzyskanie zaszyfrowanych wiadomości przez pracodawcę przez ich zapis na nośniku informacji w postaci zaszyfrowanej za przestępstwo z wyżej wymienionego przepisu uznane być nie może.

Godzi się także przytoczyć zaprezentowany przez A. Adamskiego pogląd, zgodnie z którym przechwytywanie informacji (korespondencji elektronicznej)

[16] Szyfr to «rodzaj kodu, zapis tekstu za pomocą systemu umownych znaków w celu zatajenia tekstu przed osobami niepowołanymi» (w:) *Mały słownik języka polskiego* pod red. E. Sobol, Warszawa 1999, s. 917.

za pomocą komputera wyposażonego w odpowiedni program wypełnia dyspozycję z art. 267 § 2 k.k.[17]. Odmiennie wypowiada się W. Wróbel, który twierdzi, że komputer na którym zainstalowano oprogramowanie umożliwiające uzyskiwanie zakodowanych informacji przesyłanych w sieci komputerowej lub sporządzanie dodatkowej kopii bez wiedzy osoby uprawnionej nie jest urządzeniem specjalnym w rozumieniu art. 267 § 2 k.k.[18]. Nawet jeśli uznać zasadność tezy A. Adamskiego, że komputer wyposażony w specjalne oprogramowanie do uzyskiwania informacji posiada cechy urządzenia wymienionego w art. 267 § 2 k.k. *in fine*, to wątpliwym jest fakt, czy serwer pracodawcy jest specjalnym urządzeniem podobnym do urządzenia podsłuchowego lub wizualnego. Wydaje się, że art. 267 § 2 k.k. zakłada posługiwanie się urządzeniami, których podstawową cechą jest taka konstrukcja, która umożliwia uzyskiwanie informacji z pozycji zewnętrznej wobec układu, w którym informacje są przekazywane. Słusznie chyba zauważa W. Wróbel, że „urządzenie specjalne" o którym mowa w powyższym przepisie to tylko urządzenie w sposób specjalny przystosowane do uzyskiwania informacji zabezpieczonych przed dostępem osób postronnych, nie mają zaś takiego charakteru służące do uzyskiwania informacji urządzenia powszechnie dostępne. W tym sensie serwer pracodawcy, na którym poczta jest dostępna bez konieczności instalacji szczególnych urządzeń nie może być narzędziem przestępstwa z art. 267 § 2 k.k. Na serwerze dostępna jest cała zawartość skrzynki pocztowej pracownika – nie ma więc konieczności stosowania jakichś specjalnych urządzeń pozwalających pracodawcy te informacje uzyskać.

Reasumując: z zakresu dalszych rozważań na temat uprawnień pracodawcy do uzyskiwania informacji wymienianych przez jego pracownika z innymi podmiotami należy wyłączyć działania polegające na uzyskiwaniu niezakodowanych (nieszyfrowanych) listów elektronicznych obsługiwanych z serwera pracodawcy z art. 267 § 1 k.k. Można zatem mówić wyłącznie o ewentualnej odpowiedzialności karnej pracodawcy za uzyskiwanie informacji przez dekodowanie lub rozszyfrowywanie odpowiednio zabezpieczonych listów elektronicznych (przełamywanie innego szczególnego zabezpieczenia). Dalsze rozważania (jeśli chodzi o uzyskiwanie przez pracodawcę poczty elektronicznej własnych pracowników) odnoszą się więc tylko do działań polegających na przełamywaniu szczególnych zabezpieczeń informacji przekazywanej w formie e-maili lub załączników do nich. Paradoksalnie zatem sama natura systemu skrzynek poczty elektronicznej prowadzonej dla pracowników przez pracodawcę sprawia, że znajdująca się w nich niekodowana poczta nie korzysta z ochrony karnoprawnej. Próbę oceny tej swoistej luki karnoprawnej przedstawiam poniżej.

[17] *Op. cit.*, s. 59 i n. Autor przytacza przykłady metod przechwytywania informacji.
[18] W. Wróbel, *op. cit.*, s. 1010.

Ad 1) Komunikacja służbowa pracownika. O ile nie ulega wątpliwości, że brak jest podstawy prawnej (brak uprawnienia w rozumieniu art. 267 § 1 k.k.[19]) do uzyskiwania przez pracodawcę informacji w drodze podłączenia do przewodu telefonicznego czy elektronicznej skrzynki pocztowej pracownika, o tyle można zasadnie twierdzić, że informacje wymieniane za pomocą tych środków komunikacji z podmiotami trzecimi nawiązującymi kontakt z pracodawcą za pośrednictwem pracownika i uzyskiwane w drodze podsłuchu i nagrywania są jednak p r z e z n a c z o n e dla pracodawcy.

Jeśli bowiem we wzorcowym (*sit venia verbo*) przypadku przestępstwa z art. 267 § 1 k.k. mamy do czynienia z sytuacją, w której stosunek pomiędzy dwoma komunikującymi się podmiotami, korzystający z konstytucyjnej oraz karnoprawnej ochrony tajemnicy komunikowania się, poddany zostaje bezprawnej i karalnej ingerencji zewnętrznej, to w wypadku, gdy podsłuchiwany przez pracodawcę jest jego własny pracownik, trudno mówić o takiej wzorcowej konfiguracji faktycznej prawnej.

Należy bowiem uznać, że pracownik prowadząc komunikację (rozmowy telefoniczne, wymianę e-maili) *stricte* służbową, w gruncie rzeczy reprezentuje pracodawcę, działając tylko w jego imieniu. Sytuacja ingerowania w tajemnicę komunikowania się jest zatem tylko p o z o r n a , gdyż w rzeczywistości w wyżej opisanej konfiguracji prawnej i faktycznej pracownik i pracodawca stanowią po prostu jeden podmiot. Nie może więc być mowy o ingerencji w prawo do tajemnicy komunikowania się, gdy „ingerującym" jest właśnie jeden z podmiotów tworzących układ objęty ochroną.

W rozmowach telefonicznych (korespondencji elektronicznej) z klientami firmy pracownik porusza tematy dotyczące spraw należących do zakresu jego obowiązków służbowych. Są to zatem – w szerokim tego słowa rozumieniu – sprawy (tematy, zagadnienia) pozostające w wyłącznej gestii pracodawcy. Pracodawca ma prawo wiedzieć jak przebiegają i czego dotyczą rozmowy służbowe pracownika. Odnoszą się one bezpośrednio do sfery interesów pracodawcy i są prowadzone w jego imieniu. Mamy tu więc do czynienia z sytuacją, gdzie określona informacja (treść komunikacji pomiędzy pracownikiem a podmiotem zewnętrznym w stosunku do niego) – jak słusznie zauważa W. Wróbel[20] – ma kilku dysponentów. Ustalenie prawa danego podmiotu do dysponowania wymaga posłużenia się różnymi kryteriami. W. Wróbel wymienia m.in. własność przedmiotu będącego nośnikiem informacji,

[19] W art. 267 § 1 k.k. wymieniono dwa dodatkowe kryteria, które musi spełnić sprawca, by zakwalifikować jego czyn jako przestępstwo z tego przepisu: informacja musi być uzyskiwana bez uprawnienia oraz nie może być dla niego przeznaczona. Art. 267 § 2 mówi tylko o uzyskiwaniu informacji bez uprawnienia, nie ma zatem znaczenia przy bycie przestępstwa fakt, czy uzyskiwana informacja była dla uzyskującego przeznaczona czy nie. Odmiennie, i chyba niezasadnie, A. Adamski, *Prawo karne*..., s. 63.

[20] W. Wróbel, *op. cit.*, s. 969.

treść informacji, fakt jej sporządzenia przez określoną osobę[21]. W interesującym nas przypadku łączna analiza choćby dwóch z powyższych kryteriów oceny (służbowa treść informacji, fakt jej sporządzenia/przekazania przez pracownika w ramach obowiązków służbowych) upoważnia do twierdzenia, że jednym z dysponentów informacji przekazywanej przez pracownika podczas rozmowy służbowej jest pracodawca.

Wydaje się zatem, że treść tych rozmów stanowi w rozumieniu art. 267 § 1 k.k. informację, która jest przeznaczona dla pracodawcy. Pracownik jest bowiem tylko *porteparole* pracodawcy i w żadnym razie nie można zasadnie twierdzić, że treść rozmowy służbowej należy do sfery prywatnej pracownika. Podobnie nie można tu mówić o tajemnicy komunikowania się. Owszem, komunikowanie się pracownika z interesantem lub klientem jest objęte tajemnicą komunikowania się i osoby trzecie nie mogą w nią w żaden sposób ingerować. Taką osobą trzecią nie jest jednak pracodawca, gdyż to w gruncie rzeczy on jest jednym z dwóch komunikujących się podmiotów (z tą tylko różnicą, że w jego imieniu występuje pracownik). Co więcej, jest on (pracodawca) nie tylko adresatem wymienianej informacji (informacja jest dla niego przeznaczona), ale także – jako podmiot reprezentowany tylko przez pracownika – tej informacji nadawcą. Zatem zarówno informacja „przychodząca" do pracodawcy (za pośrednictwem pracownika), jak i informacja „wychodząca" od pracodawcy (też za pośrednictwem pracodawcy) jest dla niego przeznaczona.

Zjawisko to można jeszcze lepiej pokazać na przykładzie rozmowy służbowej prowadzonej przez dwóch pracowników tej samej firmy. Jest oczywiste, że informacje, które pracownicy ci sobie wzajemnie przekazują pozostają wyłącznie w sferze spraw pracodawcy i poza sferą prywatności pracownika (życia prywatnego pracownika). Jeśli zatem chodzi o rozmowy służbowe pracowników, to w relacji pracodawca/pracownik/rozmówca pracownika nie występują ani żadne ograniczenia płynące z konstytucyjnego prawa do ochrony prywatności, ani z prawa do tajemnicy komunikowania się. Pracownik nie jest bowiem (w tym układzie) podmiotem odrębnym od pracodawcy, który (pracodawca) jest władny zapoznać się z treścią przeznaczonej dla niego komunikacji (informacji).

Nie można zatem w przypadku podsłuchiwania i nagrywania przez pracodawcę rozmów służbowych (uzyskiwania elektronicznej korespondencji służbowej) mówić o popełnieniu przestępstwa przeciwko ochronie informacji z art. 267 § 1 kodeksu karnego.

Ad 2) Komunikacja prywatna pracownika. Rozmowy prywatne prowadzone są przez każdego prawie pracownika, który ma dostęp do aparatu telefonicznego w pracy (służbowej elektronicznej skrzynki pocztowej). Z pewnością nie jest do uzasadnione. Mimo tego, że rozmowy odbywają się na szkodę finansową pracodawcy, który płaci za czas rozmowy i za czas nieprzepracowany przez pracownika, nie ma

[21] *Ibidem*.

to żadnego wpływu na wyłączenie odpowiedzialności karnej sprawcy. Poza sporem jest wszakże to, że prywatna rozmowa pracownika to przekaz informacji, które z samej swej istoty nie są przeznaczone dla podmiotu, który je uzyskuje (pracodawca). Należy podkreślić, że przez podłączenie się do linii telefonicznej i nagrywanie rozmowy pracodawca narusza dwie odrębne sfery prywatności – swego pracownika i jego rozmówcy (rozmówców), który (którzy) oczywiście w takim samym stopniu jak pracownik nie zdaje (zdają) sobie sprawy z naruszenia przez inny podmiot tajemnicy komunikowania się. Pokrzywdzonych jest więc w tej sytuacji dwóch (ingerencja w odrębny układ komunikacji pomiędzy dwoma pracownikami). Mamy zatem bez wątpienia do czynienia z przestępstwem z art. 267 § 1 k.k. ściganym na wniosek osoby pokrzywdzonej i naruszeniem konstytucyjnego prawa do prywatności i tajemnicy komunikowania się.

Inaczej ma się sprawa z uzyskiwaniem nieszyfrowanej korespondencji elektronicznej pracownika wychodzącej i przychodzącej na jego konto służbowe. Jak już wcześniej wskazano, uzyskiwanie przez pracodawcę treści korespondencji elektronicznej nie odpowiada jednemu ze znamion przestępstwa określonego w art. 267 § 1 k.k. (pracodawca nie przełamuje szczególnych zabezpieczeń chroniących dostęp do informacji). Wynika z tego, że – w odróżnieniu od uzyskiwania rozmów telefonicznych przez pracodawcę – uzyskiwanie niezaszyfrowanych e-maili nie może być penalizowane, niezależnie od tego czy są to maile służbowe czy prywatne[22].

Żadnych zmian w tym zakresie nie wprowadza projekt nowelizacji kodeksu karnego (wersja z grudnia 2001), który przewiduje uzupełnienie art. 267 § 1 k.k. o jeszcze jedno znamię czasownikowe (obok „przełamywania" uzyskiwanie informacji może się odbywać także w drodze „omijania" zabezpieczeń chroniących informację).

Prywatna korespondencja elektroniczna prowadzona ze służbowej skrzynki pocztowej nie podlega zatem praktycznie żadnej ochronie karnoprawnej, choć bez wątpienia korzysta z ochrony konstytucyjnej. Rozwiązanie to należy ocenić krytycznie – pracownik nie dysponuje bowiem stosownym narzędziem karnoprawnym pozwalającym na ochronę naruszonego dobra prawnego. Wydaje się jednak, że niemożliwe jest zaproponowanie – *de lege ferenda* – takiego brzmienia art. 267 § 1 k.k. aby był chroniony w jednakowym stopniu interes pracodawcy (którego nie można zmusić do wyłączenia spod swej kontroli prowadzonych i finansowanych przez siebie służbowych skrzynek pocztowych na należącym do niego serwerze[23]) oraz prawo do ochrony tajemnicy komunikowania się pracownika. Rozwiązania

[22] Nie dotyczy to jednak – jak zostało zauważone – e-maili zaszyfrowanych lub zakodowanych przez nadawców. Jeśli jednak pracodawca przełamuje szyfr albo kod chroniący e-mail służbowy (problem jednak w tym, jak to określić), to nie popełnia przestępstwa z art. 267 § 1 k.k., bo – i tu mają pełne zastosowanie rozważania z punktu Ad 1) – informacja ta jest dla niego p r z e z n a c z o n a .

[23] Co *de facto* równałoby się z koniecznością opracowania nowych systemów informatycznych całkowicie blokujących administratorom dostęp do „własnych" adresów pocztowych.

takiego szukać należy nie na płaszczyźnie prawa karnego, lecz raczej poprzez właściwe informowanie pracowników o warunkach i zasadach korzystania ze służbowych skrzynek pocztowych[24]. Pracodawca może i powinien określić, że skrzynki te służą tylko (jak sama nazwa wskazuje) do korespondencji służbowej, która może być przez pracodawcę przeglądana w dowolnym momencie i uprawienie to obejmuje także pocztę prywatną. Jej prowadzenie przez pracownika odbywałoby się z pełną świadomością, że może być i będzie ona poddawana kontroli przez pracodawcę. Dodać trzeba, że informowany o tym, że służbowy adres elektroniczny nie korzysta z ochrony prawa do prywatności i że wiadomości przesyłane do skrzynki są dostępne także dla pracodawcy powinien być również podmiot, który chce skierować e-mail na taki adres. [*Notabene* taka właśnie jest praktyka w coraz większej ilości dużych firm. Oto przykład typowego *disclaimer'a* (zrzeczenia się, zrezygnowania) zamieszczanego we wszystkich listach nadawanych przez pracowników angielskiego BBC: *This e-mail (and any attachments) is confidential and may contain personal views which are not the views of the BBC unless specifically stated. If you have received it in error, please delete it form your system, do not use, copy or disclose the information in any way not act in reliance on it and notify the sender immediately.* ***Please note that the BBC monitors e-mail sent or received. Further communication will signify your consent to this.*** (podkr. – AB)] Tylko takie rozwiązanie pozwoliłoby – mimo luki w gwarancyjnych normach karnych – na uwzględnienie interesów pracodawcy z jednoczesnym pełnym poszanowaniem konstytucyjnego prawa do ochrony tajemnicy komunikowania się.

2. Poza (przedstawioną powyżej) warstwą teoretyczną dotyczącą odpowiedzialności karnej za naruszenie prawa pracownika do ochrony tajemnicy komunikowania się niemniej istotna jest – jak się wydaje – praktyczna możliwość ścigania przestępstwa z art. 267 § 1 k.k. popełnionego przez pracodawcę na szkodę pracownika.

Wymieńmy tu dwa aspekty, które w praktyce mogą spowodować znaczne trudności w aktywacji i prowadzeniu postępowania karnego.

Pierwszy z tych czynników może doprowadzić do zamknięcia drogi karnoprawnej u jej zarania. Jak wiadomo, przestępstwo z art. 267 § 1 k.k. jest przestępstwem publicznoskargowym, ale uruchomienie ścigania następuje na wniosek (przestępstwo wnioskowe). Jak podaje L. Gardocki[25], dwie są przyczyny zakwalifikowania danego przestępstwa do grupy przestępstw wnioskowych. Jedną z nich – jak właśnie przy występku z art. 267 § 1 k.k. – jest uznanie przez ustawodawcę motywacji pokrzywdzonego, który ze względu na rozmiary szkody lub jej wyrównanie przez

[24] B. Fischer, *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*, Kraków 2000, s. 193 proponuje, by kontrola korespondencji na poziomie firmy była regulowana na mocy umowy pomiędzy pracownikiem a pracodawcą.

[25] L. Gardocki, *Prawo karne*, Wyd. 7, Warszawa 2001, s. 59.

sprawcę uznaje, że nie opłaca mu się żądać wszczęcia postępowania karnego i być następnie zmuszonym do występowania w roli świadka podczas procesu. Dlatego też, uznając stosunkowo niewielką wagę czynu, ustawodawca przyznaje swobodę samemu pokrzywdzonemu w wyborze: wszcząć postępowanie karne czy też nie. Rozwiązanie to – w kontekście omawianego tu przestępstwa – nie jest zbyt fortunne. Trudno bowiem wyobrazić sobie by pracownik po wykryciu, że pracodawca podsłuchiwał jego rozmowy telefoniczne wykazywał nadmierną chęć do występowania na drogę procesu karnego. Procesu ze wszystkimi jego niezbędnymi (a niekorzystnymi dla pracownika) atrybutami: polaryzacją interesów oskarżenia i strony biernej, koniecznością zeznawania przez świadka-pracownika na niekorzyść firmy, jawnością postępowania, rozgłosem medialnym mogącym towarzyszyć ciekawej dla mediów sprawie itp. Z pewnością wszystkie te okoliczności nie będą żadną zachętą dla kogokolwiek stojącego przed trudnym wyborem złożenia wniosku o ściganie. A co dopiero dla pracownika, który dla pociągnięcia pracodawcy do odpowiedzialności karnej za działanie na jego szkodę na szali sprawiedliwości złożyć musi swe zatrudnienie i rozpocząć trudną batalię prawną – i to jeszcze o niepewnym wyniku. Do tych okoliczności należy dodać jeszcze jedną. Uruchomienie postępowania publicznoskargowego na wniosek będzie prawdopodobnie postrzegane przez otoczenie pracownika (niewnikające zapewne w niuanse karnistyczne) jako „rzucenie rękawicy pracodawcy", „wypowiedzenie wojny" itp. Z pewnością nie ułatwi to pokrzywdzonemu decyzji.

Jeśli doszłoby mimo wszystko to wszczęcia postępowania karnego, to od razu pojawia się cały zespół problemów *sensu stricto* dowodowych, które w istocie mogą doprowadzić do trwałego paraliżu raz wszczętego postępowania. Wymieńmy tylko pierwsze z brzegu.

Jak udowodnić, że pracodawca rzeczywiście podsłuchiwał? Jak dowieść, że uzyskiwał (poza rozmowami służbowymi, do których ma pełne prawo), także rozmowy prywatne? Jak dotrzeć do właściwych osobowych źródeł dowodowych, zważywszy, że w zasadzie wszyscy świadkowie oskarżenia będą pracownikami tej samej firmy i ich chęć do zeznawania na niekorzyść pracodawcy z pewnością nie będzie zbyt wielka? Jak rozbić zintegrowaną grupę, którą stanowią osoby zatrudnione u tego samego pracodawcy?

Tych kilka uwag skłania do daleko posuniętej powściągliwości jeśli idzie o praktyczną użyteczność art. 267 § 1 k.k. jako instrumentu chroniącego prawo pracownika do ochrony tajemnicy komunikowania się. Węzeł problemów (obawa przed złożeniem wniosku o ściganie, kwestie dowodowe), który powstaje wówczas, gdy przestępstwo z art. 267 § 1 k.k. dokonywane jest w układzie pracodawca-pracownik może w praktyce okazać się zbyt trudny do rozsupłania.

3. Ochrona prawa do komunikacji w rozumieniu szerokim (informacja o fakcie porozumiewania się). Odrębną kwestią (niemniej wszakże interesującą), którą wypada wreszcie poruszyć w niniejszym opracowaniu (z konieczności jednak skrótowo tylko) jest problem zapoznawania się przez pracodawcę z wykazami pozwa-

lającymi na ustalenie, z jakimi podmiotami komunikował się pracownik. Wymaga ona osobnych rozważań, prowadzonych w oderwaniu od uwag dotyczących komunikowania się w znaczeniu ścisłym (uzyskiwania informacji wymienianej pomiędzy podmiotami prowadzącymi komunikację). Taką metodę analizy wymusza przedstawiona na wstępie konstrukcja konstytucyjnego prawa do ochrony komunikowania się, a rozważania co do występowania karnej odpowiedzialności za zapoznawanie się z wykazami wypada prowadzić równolegle do analizy konstytucyjnej.

W praktyce problem dotyczy nie tylko tzw. billingów, tzn. wykazów rozmów prowadzonych z danego numeru telefonicznego, ale także rejestrów rozmów przychodzących i wychodzących z firmowych centralek telefonicznych oraz rejestru wiadomości pocztowych wysyłanych ze skrzynki elektronicznej.

De lege lata kwestia jest uregulowana w zasadzie tylko w prawie konstytucyjnym, a za przepisem konstytucyjnym (art. 49) nie poszły odpowiednie przepisy karne. Obecnie więc otrzymywanie przez pracodawcę wykazów komunikacji prowadzonej z zapewnionych przez niego urządzeń (telefony, komputery) nie jest objęte skorelowaną z gwarancją konstytucyjną ochroną karnoprawną. Rozwiązanie takie (jeśli chodzi o regulację karnomaterialną) nie może być ocenione negatywnie. O ile zrozumiała jest bezwzględna ochrona prawa do ochrony tajemnicy komunikowania się pracownika w rozumieniu ścisłym (treść przekazywanej informacji), o tyle objęcie penalizacją naruszania prawa do ochrony tajemnicy komunikowania się w znaczeniu szerokim (fakt porozumiewania się dwóch podmiotów) w układzie, gdy pracownik korzysta z urządzeń należących do pracodawcy i przez niego utrzymywanych byłoby tożsame z – absurdalnym wprost – pozbawieniem pracodawcy możliwości kontroli zasadności i celowości ponoszonych przez niego wydatków oraz kontroli wykorzystywania urządzeń przez pracownika.

Wydaje się, że właściwe jest (w układzie pracodawca-pracownik) pozostawienie poza obszarem regulacji karnoprawnej prawa do ochrony tajemnicy komunikowania się w znaczeniu szerokim (fakt prowadzenia komunikacji z innym podmiotem). Przemawia za tym następujący argument. Jak już wyżej wspomniano, dobru prawnemu w postaci informacji można przypisać określonego dysponenta. Dysponentem informacji w postaci billingu (rejestru rozmów/wysłanych e-maili), jeśli wziąć pod uwagę jej treść (wykaz dokonanych za pomocą urządzenia należącego do pracodawcy połączeń) jest właśnie pracodawca. Co więcej, w przypadku billingu to ustawa określa prawo abonenta-pracodawcy (w przypadkach przewidzianych ustawą lub umową o świadczenie usług telekomunikacyjnych) do otrzymania od operatora szczegółowego wykazu usług telekomunikacyjnych (art. 36 ust. 1 Ustawy z 21 lipca 2001 r. – Prawo telekomunikacyjne, Dz.U. Nr 73 z 2000 r., poz. 852). I to on – a nie pracownik – ma prawo do dysponowania wykazem połączeń. Dlatego też – *de lege ferenda* – dostęp do tego rodzaju informacji nie tylko nie powinien, ale nie może być penalizowany.

4. Teoretyczne wyodrębnienie dwóch płaszczyzn analizy prawnokarnej (uzyskiwanie informacji z rozmów służbowych pracowników oraz z rozmów prywatnych)

nie zamyka zagadnienia. Problem „hurtowego" podsłuchiwania i nagrywania oraz kontroli korespondencji elektronicznej przez pracodawców pozostaje nierozwiązany. Z jednej strony pracodawcy we własnym interesie starają się kontrolować kontakty firmy z podmiotami zewnętrznymi. Z drugiej strony łamią konstytucyjne prawo do prywatności, naruszają tajemnicę komunikowania się oraz popełniają przestępstwo. Jeśli więc uznamy, że pracodawca ma interes w kontrolowaniu rozmów służbowych swych pracowników, to należałoby wprowadzić ustawową podstawę do takich czynności, najlepiej w Kodeksie pracy[26]. Wydaje się, że niezbędne byłoby obwarowanie takiej możliwości koniecznością uprzedzenia pracowników o podsłuchiwaniu (nagrywaniu) rozmów służbowych i zakazie prowadzenia telefonicznych rozmów prywatnych. Konieczne byłoby także zadbanie o interes osób prowadzących rozmowy z pracownikami. Także one powinny być lojalnie uprzedzane o rejestrowaniu rozmowy. Trzeba więc szukać rozwiązań prawnych gwarantujących pracownikom i ich rozmówcom prawdziwą tajemnicę komunikowania się, a pracodawcy – właściwą kontrolę nad działaniami pracowników.

Sprostowanie

W pierwszej części artykułu Antoniego Bojańczyka pt. „Karnoprawne aspekty ochrony prawa pracownika do tajemnicy komunikowania się" opublikowango w numerze 1–2/2003 „Palestry" z winy korekty zostały pominięte przypisy. Tekst z przypisami jest opublikowany na stronach internetowych: www.adwokatura.org.pl.

[26] Por. A. Adamski, *Przestępczość w cyberprzestrzeni*..., s. 28.