Sebastian Ożóg

Monitoring pracownika w sieci komputerowej

Polski Rocznik Praw Człowieka i Prawa Humanitarnego 2, 159-170

2011

Polski Rocznik Praw Człowieka i Prawa Humanitarnego 2
UWM w Olsztynie 2011 ISSN 2082-1786

Sebastian Ożóg
Uniwersytet Wamińsko-Mazurski w Olsztynie, Katedra Praw Człowieka i Prawa Europejskiego

Monitoring pracownika w sieci komputerowej

Słowa kluczowe: prawa człowieka, prawa pracownicze, prawo do prywatności, monitoring pracownika, ochrona danych osobowych.

Nowoczesne technologie zmieniają nasz świat – to prawda, o której w dobie społeczeństwa informacyjnego nikogo nie trzeba przekonywać. Dostęp do informacji za pośrednictwem podłączonych do Internetu urządzeń (nie tylko komputerów, ale także telefonów komórkowych czy nawet telewizorów) ma charakter powszechny. W czerwcu 2009 r. współczynnik penetracji Internetu dla polskich gospodarstw domowych wyniósł 36,7% dla sieci stacjonarnych i 13,3% dla sieci mobilnych.[1] Korzyści płynące z bezpośredniego dostępu do informacji doceniają także pracodawcy, coraz powszechniej tworzący firmowe sieci komputerowe, zapewniające stały dostęp do Internetu wszystkim komputerom danego przedsiębiorstwa. Bezpośredni dostęp do zasobów informacyjnych Internetu oraz tzw. telefonii internetowej (telefonii IP) przynosi pracodawcom szereg ułatwień i oszczędności, a w przypadku niektórych stanowisk pracowniczych umożliwia wręcz ich funkcjonowanie poza zakładem pracy.

Oczywiście nowoczesną technologię, neutralną samą w sobie, można wykorzystać na różne sposoby, nie wszystkie pożądane przez pracodawcę. Narastającym wśród pracowników, negatywnym zjawiskiem jest tzw. *cyberslacking*, czyli wykorzystywanie Internetu w pracy do celów prywatnych. Według badania przeprowadzonego przez firmę Gemius w listopadzie 2007 r. w Polsce do *cyberslackingu* przyznawało się 93% osób mających dostęp do Internetu w pracy, przy czym aż 74% badanych nie widziało w takim zachowaniu niczego nagannego.[2] Za pośrednictwem firmowej sieci komputerowej

[1] Raport Urzędu Komunikacji Elektronicznej „Technologie dostępu do sieci Internet w Polsce" z grudnia 2009 r. dostępny pod adresem: <http://www.uke.gov.pl/uke/redir.jsp?place=galleryStats&id=24117>, dostęp: 30 października 2010 r.

[2] R. Grabarek, *Cyberslacking, czyli pracownik się obija*, Gazeta.pl: Technologie. Artykuł dostępny pod adresem: <http://technologie.gazeta.pl/technologie/1,81028,7571064,Cyberslacking__czyli_pracownik_sie_obija.html>, dostęp: 30 października 2010 r.

pracownicy najczęściej sprawdzają prywatną pocztę elektroniczną i przeglądają strony www, około 1/3 badanych używa także w pracy komunikatorów internetowych i dokonuje zakupów przez Internet.[3] Przeprowadzone przez firmę E-marketing badania „Internet w pracy" wskazują, że jedna trzecia pracowników spędza na swobodnym przeglądaniu Internetu godzinę dziennie, a 7 % pracowników spędza tak ponad trzy godziny.[4]

Oprócz „nieszkodliwego" przeglądania stron www, pracownicy potrafią także pobierać i rozpowszechniać za pośrednictwem sieci p2p (*peer-to-peer*) nielegalne oprogramowanie, nielicencjonowane kopie utworów audiowizualnych czy pornografię dziecięcą. Internet bywa także wykorzystywany do działalności wprost szkodliwej dla pracodawcy poprzez udostępnianie konkurencji plików komputerowych, stanowiących tajemnicę przedsiębiorstwa pracodawcy, a nawet instalowanie oprogramowania, umożliwiającego dostęp z zewnątrz do komputerów przedsiębiorstwa (tzw. *backdoor*). Poza tym, nawet bez złej woli ze strony pracownika, Internet przeglądany bez zachowania środków ostrożności łatwo może stać się źródłem infekcji szkodliwym oprogramowaniem (tzw. trojanami, robakami i wirusami komputerowymi), za pomocą którego można wykorzystać sieć pracodawcy do bezprawnego pozyskiwania jego danych, wysyłania innym odbiorcom niechcianej korespondencji elektronicznej (tzw. *spamu*) lub przeprowadzania ataków na inne systemy komputerowe.

W odpowiedzi na takie postępowanie, w celu zabezpieczenia sieci wewnętrznej, pracodawcy wdrażają różnorodne systemy monitorowania firmowych zasobów komputerowych. Nadzorowane urządzenia stanowią ostatecznie mienie pracodawcy, a czas spędzany przez pracowników w firmie jest przez niego opłacany. Zrozumiałe jest więc oczekiwanie pracodawcy, by udostępnione przezeń dla świadczenia pracy środki nie były wykorzystywane w innych celach.

Naprzeciw takiemu zapotrzebowaniu pracodawców wychodzą producenci oprogramowania, tworzący aplikacje umożliwiające śledzenie instalowanych i uruchamianych przez pracownika programów, analizowanie treści komunikatów wprowadzanych z jego klawiatury, monitorowanie poczty internetowej (zarówno jej treści, jak i adresów, pod które jest wysyłana) oraz adresów otwieranych stron internetowych. Programy te umożliwiają śledzenie właściwie każdego działania podjętego z użyciem komputera, umożliwiając ich rejestrację i późniejsze odtworzenie. Niektórzy producenci takiego oprogramowania uprzedzają również, że skorzystanie z wybranych opcji bez powiadamiania pracownika może być nielegalne i powodować pociągnięcie pracodawcy do odpowiedzialności z tytułu naruszenia dóbr osobistych pracownika.[5]

---

[3] Ibidem.

[4] J. Kaniewski, *Monitoring pracowników*, „Serwis Prawno-Pracowniczy" 51/2008 z 16 grudnia 2008 r., s. 9.

[5] Internetowe witryny programów komputerowych tego rodzaju, które zawierają noty prawne, wskazujące na konieczność informowania pracownika o stosowaniu monitoringu, to np.: <http://statlook.pl> czy <http://www.okoszefa.pl>, dostęp: 30 października 2010 r.

Komputer pracodawcy wraz z zainstalowanym na nim oprogramowaniem należy traktować jako udostępnione pracownikowi narzędzie pracy. Pracodawca ma więc prawo oczekiwać, że narzędzie to będzie wykorzystywane zgodnie z treścią wiążącej strony umowy o pracę, ma on także prawo sprawdzać, czy jest tak w rzeczywistości. Każdy pracodawca powinien zatem móc kontrolować, nie przekraczając wyznaczonych prawem granic, przebieg i jakość świadczonej pracy oraz jej efekty, a także monitorować sposób wykonywania pracy przez pracowników i ich wydajność. W przypadku pracy przy stanowisku, mającym dostęp do sieci Internet, pracodawca, stosownie do treści art. 120 kodeksu pracy (k.p.),[6] może ponadto ponosić odpowiedzialność za działania pracowników względem osób trzecich, co tym bardziej uzasadnia wprowadzenie jakiejś formy nadzoru.[7]

Polskie prawo w zasadzie jednak nie reguluje kwestii monitoringu pracowników – próżno szukać dotyczących tej kwestii przepisów w obowiązującym kodeksie pracy. Szczątkową regulację w tym zakresie odnajdziemy w załączniku do rozporządzenia w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe.[8] W punkcie 10 lit. e) tego załącznika zakazano „dokonywania jakościowej i ilościowej kontroli pracy pracownika" bez jego wiedzy. Regulacja ta wskazuje więc, że pracownik powinien być o monitorowaniu swojej pracy na komputerze poinformowany. Nie rozstrzyga jednak szeregu kwestii szczegółowych dotyczących form monitoringu, ich zakresu oraz rodzaju danych podlegających kontroli.[9]

W tej sytuacji należy dokonać swoistej rekonstrukcji substancji prawnie chronionej na gruncie innych przepisów. W szczególności należy wziąć pod uwagę regulację konstytucyjną, zobowiązania prawno-międzynarodowe, a także wybrane przepisy kodeksu pracy, kodeksu cywilnego (k.c.)[10] i innych ustaw, które, w zależności od zaistniałego stanu faktycznego, mogą czasami znaleźć zastosowanie. Ostateczny zakres możliwości monitorowania pracownika jest wypadkową dwóch przeciwstawnych interesów prawnych – z jednej strony prawa pracodawcy do nadzorowania i organizacji procesu pracy, zaś z drugiej prawa pracownika do ochrony jego prywatności.

Jeśli chodzi o podstawowe obowiązki pracownika to – zgodnie z art. 100 § 1 k.p. – jest on obowiązany wykonywać swoją pracę sumiennie i starannie

---

[6] Ustawa Kodeks pracy z dnia 26 czerwca 1974 r. (Dz.U. z 1974 r. nr 24, poz. 141 z późn. zm.).

[7] G. Orłowski, *Pracownik monitorowany*, „Personel i Zarządzanie" 12/2004, s. 30.

[8] Załącznik „Minimalne wymagania bezpieczeństwa i higieny pracy oraz ergonomii, jakie powinny spełniać stanowiska pracy wyposażone w monitory ekranowe" do rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. (Dz.U. Z 1998 r. nr 148, poz. 973).

[9] Z uwagi na istotność omawianej kwestii *de lege ferenda* należy postulować, by została ona uregulowana w sposób bardziej zupełny, w akcie rangi ustawowej. Przepisy wskazywane w dalszej części artykułu mają charakter ogólny, a konieczność ich powoływania powodowana jest właśnie brakiem bardziej szczegółowej regulacji w tej dziedzinie.

[10] Ustawa Kodeks cywilny z dnia 23 kwietnia 1964 r. (Dz.U. z 1964 r., nr 16, poz. 93 z późn. zm.).

oraz stosować się do dotyczących pracy poleceń przełożonych. W szczególności pracownik powinien przestrzegać ustalonego czasu pracy (art. 100 § 2 pkt 1 k.p.), regulaminu i porządku pracy (art. 100 § 2 pkt 2 k.p.), a także dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę (art. 100 § 2 pkt 4 k.p.). Nie ulega wątpliwości, że korzystanie z Internetu w pracy w celach prywatnych, ponad ustaloną przez pracodawcę normę, można traktować zarówno jako naruszenie ustalonego czasu pracy, jak i jej porządku. Pracownik jest też zobowiązany chronić mienie pracodawcy w postaci udostępnionego mu komputera i nie narażać go np. na ryzyko infekcji szkodliwym oprogramowaniem, pochodzącym z przeglądanych stron internetowych. Oprogramowanie takie może następnie umożliwić dokonywanie nadużyć i przestępstw z komputerów pracowniczych, a także skopiowanie z nich danych o charakterze poufnym.

Przy stosunkowo niskiej świadomości osób korzystających z Internetu co do zagrożeń z tym związanych, naturalną reakcją pracodawców jest w tej sytuacji instalowanie aplikacji chroniących ich sieć komputerową przed szkodliwym oprogramowaniem, a także przed niepożądanymi zachowaniami pracowników. Programy takie zabezpieczają system komputerowy na różnych poziomach dostępu, często także monitorując aktywność pracowników w celu określenia wydajności ich pracy i wychwycenie działań niepożądanych z punktu widzenia pracodawcy. Takie działania pracodawca powinien jednak rozpocząć od wyraźnego ukształtowania polityki dostępu do Internetu w miejscu pracy i określenia, czy i na jakich zasadach dopuszcza, bądź zakazuje korzystania z Internetu w celach nie związanych z wykonywaną pracą. Bez wprowadzenia wyraźnego ograniczenia w tym zakresie w regulacjach zakładowych nie można domniemywać istnienia całkowitego zakazu korzystania z Internetu w celach prywatnych w miejscu pracy (poza przypadkami gdy bezsprzecznie wpływałoby to na wydajność pracownika).

W literaturze zaleca się udostępnianie pracownikom możliwości przeglądania Internetu czy sprawdzania prywatnej poczty elektronicznej.[11] W tym celu proponuje się pracodawcom np. tworzenie dwóch kont pracownika – prywatnego i służbowego.[12] Podczas gdy pierwsze byłoby monitorowane zasadniczo tylko co do czasu korzystania z niego (a więc jego wpływu na wydajność pracownika), drugie podlegałoby szerszemu nadzorowi (także co do jakości i efektów świadczonej pracy). W ten sposób cele pracodawcy, takie jak utrzymanie wydajności pracy i nadzór nad jej wykonywaniem, byłyby nadal realizowane, a ryzyko naruszenia prywatności pracownika zostałoby

[11] A. Lach, *Monitorowanie pracownika w miejscu pracy*, „Monitor Prawa Pracy" 10/2004, Legalis.

[12] Article 29 Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace*, przyjęty 29 maja 2002 r. (5401/01/EN/Final WP 55), dostępny w Internecie pod adresem: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf>, dostęp: 30 października 2010 r.

zminimalizowane. Oczywiście pracodawca w ramach regulacji zakładowej może tę kwestię ukształtować inaczej i wyraźnie zabronić wykorzystywania komputerów pracowniczych do celów prywatnych.

Niezależnie od przyjętej polityki pracodawcy w tej kwestii, dopiero przy jasnym sprecyzowaniu zasad korzystania z Internetu może on formułować wyraźne oczekiwania w tym względzie wobec pracowników i – w przypadku ich nierespektowania – stosować odpowiedzialność dyscyplinarną. W takiej sytuacji, w celach dowodowych, konieczne może się okazać wprowadzenie programowego monitoringu, umożliwiającego śledzenie i rejestrowanie aktywności pracownika w sieci pracodawcy. Trzeba jednak zaznaczyć, że taki komputerowy nadzór nie może naruszać granic obowiązującego prawa, w szczególności nie może naruszać prawa do prywatności pracowników.

Zgodnie z art. 11^1 k.p. pracodawca jest obowiązany szanować godność i inne dobra osobiste pracownika. Jest to jeden z podstawowych obowiązków pracodawcy – jego naruszenie może skutkować możliwością rozwiązania przez pracownika umowy o pracę bez wypowiedzenia i domagania się wypłaty odszkodowania (art. 55 § 1^1 k.p.). Poza godnością dobra osobiste pracownika nie zostały w art. 11^1 k.p. szczegółowo określone, co powoduje konieczność wykazania ich istnienia na gruncie konkretnych stanów faktycznych, będących przedmiotem postępowania sądowego. Ponadto, w związku z treścią art. 300 k.p., do spraw pracowniczych należy stosować odpowiednio art. 23 k.c., na podstawie którego chronione są wszelkie dobra osobiste człowieka. Co prawda w przepisie tym nie wskazano wprost godności czy prywatności, jako wartości chronionych (choć wskazano np. tajemnicę korespondencji), to jednak, z uwagi na przykładowy („w szczególności") charakter wyliczenia, dyspozycja tego przepisu obejmuje wszelkie możliwe do zrekonstruowania dobra osobiste. Potwierdzeniem tego jest orzecznictwo Sądu Najwyższego, które niejednokrotnie wyprowadzało wartości chronione z dóbr takich, jak prywatność czy godność jednostki.[13] W jednym z takich wyroków[14] podkreślono, że każdy pracodawca powinien traktować swych pracowników z szacunkiem i liczyć się z ich poczuciem własnej godności i wartości osobistej, w związku z czym nie może on bezpodstawnie negatywnie odnosić się do pracownika i wyrażać się o nim w sposób poniżający wśród innych pracowników. Nie narusza natomiast godności osobistej pracownika krytyczna ocena wykonanych przez niego zadań, nawet niesłuszna, jeżeli nie powoduje ona krzywdzącej pracownika dyskwalifikacji zawodowej i nie zawiera sformułowań zbędnych, wykraczających poza potrzebę.[15]

---

[13] Tak np. w wyroku Sądu Najwyższego z 28 kwietnia 2004 r. (sygn. akt III CK 442/02), wskazującym, że może stanowić naruszenie prywatności przetwarzanie określonych danych osobowych, czy w wyroku SN z dnia 21 marca 2007 r. (sygn. akt I CSK 292/06), rekonstruującym m.in. pojęcie godności osobistej jako wewnętrznego przekonania człowieka o swoim moralnym i etycznym nieposzlakowaniu oraz czci, jako wyrazu pozytywnego ustosunkowania się innych ludzi do wartości osobistej i społecznej określonej jednostki.

[14] Wyrok Sądu Najwyższego z 3 marca 1975 r. (sygn. akt I PR 16/75).

[15] Wyrok Sądu Najwyższego z 6 grudnia 1973 r. (sygn. akt I PR 493/73).

W przypadku naruszenia dóbr chronionych treścią art. 23 k.c. przez pracodawcę, odpowiedniemu zastosowaniu podlega także art. 24 k.c., na podstawie którego każda osoba, której dobro osobiste zostało zagrożone, może żądać zaniechania takiego działania i dopełnienia wszelkich czynności niezbędnych do usunięcia skutków takiego naruszenia. Niezależnie od tych roszczeń można także żądać odpowiedniego zadośćuczynienia pieniężnego za doznaną krzywdę na podstawie art. 448 k.c. Sąd Najwyższy uznał jednak, że w przypadku rozwiązania (także wadliwego) stosunku pracy przez pracodawcę stosowanie przepisów prawa cywilnego o ochronie dóbr osobistych możliwe jest tylko wtedy, gdy w związku z tym rozwiązaniem pracodawca naruszy dobro osobiste pracownika poza zakresem stosunku pracy, podejmując działania nie mieszczące się w ukształtowanej przez ustawodawcę formie i treści czynności prawnej rozwiązującej stosunek pracy.[16]

Prawo do ochrony życia prywatnego (prywatności) każdej osoby w naszym kraju wynika wprost z art. 47 polskiej Konstytucji.[17] Doniosłość tego prawa uwidacznia m.in. okoliczność, że prawo to jest, stosownie do treści art. 233 ust. 1 Konstytucji, nienaruszalne nawet w ustawach ograniczających inne prawa, wydawanych w stanie wojennym i wyjątkowym. Dodatkowo, zgodnie z art. 49 Konstytucji, w Polsce „zapewnia się wolność i ochronę tajemnicy komunikowania się", a „ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie". Nie ulega wątpliwości, że powyższa regulacja dotyczy także monitorowania komputerów i ich komunikacji z Internetem. Niemal każda forma monitorowania pracownika stanowi ingerencję w jego życie prywatne,[18] jednak nie każda pociąga za sobą naruszenie tajemnicy komunikowania się. Nadzorowanie komputera może więc czasami powodować „jedynie" ingerencję w prywatność (np. poprzez monitorowanie adresów przeglądanych stron internetowych czy nazw uruchamianych na komputerze aplikacji), a czasami także naruszenie tajemnicy komunikowania się (tak będzie np. przy monitoringu treści poczty elektronicznej, komunikatorów internetowych czy telefonii IP). Z tego powodu pracodawca powinien różnicować zasady swojego postępowania i zakres ich uzgodnienia z pracownikiem w zależności od rodzaju „komputerowej" aktywności pracownika, podlegającej nadzorowi oraz formy samego nadzoru. W żadnej jednak sytuacji monitorowanie pracownika nie powinno być dopuszczalne, jeżeli nie został on o tym wcześniej poinformowany. Dodatkowo, ponieważ ograniczenie wolności komunikowania się, zgodnie z art. 49 Konstytucji, może nastąpić wyłącznie w drodze ustawy, a kwestia monitoringu pracowników nie

[16] Wyrok SN z 16 listopada 2000 r. (sygn. akt I PKN 537/00).

[17] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. nr 78, poz. 483 z późn. zm.).

[18] Nie będzie jednak ingerencją monitorowanie w ramach oznaczonej aplikacji, np. czynności projektanta w programie komputerowym, pod warunkiem nadzorowania wyłącznie tego programu. Większość istniejących na rynku programów do nadzoru pracowników nie posiada jednak takiej funkcjonalności i monitoruje wszystkie aktywne w danym systemie aplikacje.

została dotychczas w ten sposób uregulowana, dyskusyjne jest, czy kontrola pracownika naruszająca jego tajemnicę komunikowania się, w ogóle jest dopuszczalna.[19] O istotności tego ograniczenia świadczy chociażby krąg podmiotów, które mogą, w drodze ustawowo wprowadzonego wyjątku, dokonać ingerencji w wolność komunikowania się – są to służby takie jak np. kontrola skarbowa, Policja, czy Agencja Bezpieczeństwa Wewnętrznego.[20] W ramach czynności operacyjnych mogą one stosować m.in. podsłuch, jednak co do zasady wyłącznie za zgodą sądu.[21] Istotne jest też, że informacje pozyskiwane w ten sposób przez uprawnione służby powinny być trudne bądź niemożliwe do uzyskania za pomocą innych, mniej ingerujących w prywatność, środków.

Tymczasem monitorujący komunikację pracownika pracodawca działa obecnie bez wyraźnych podstaw prawnych, a co ważniejsze bez jakiejkolwiek kontroli proporcjonalności podjętych przez niego środków i ich zasadności w konkretnej sytuacji. Nie ulega wątpliwości, że samo uprawnienie pracodawcy do „organizowania pracy w sposób zapewniający pełne wykorzystanie czasu pracy" jest zbyt ogólną podstawą do wprowadzenia środków tak głęboko ingerujących w prywatność pracowników.[22] Nieistnienie regulacji w tym zakresie jest niewątpliwie luką prawa pracy, przy czym trudne do zaakceptowania jest tłumaczenie Ministerstwa Pracy i Polityki Społecznej, jakoby „szybki i ciągły rozwój technologii informatycznych, telekomunikacyjnych oraz przekazu elektronicznego sprawiał, że nie jest możliwe uregulowanie w przepisach prawa pracy wszystkich aspektów tej sprawy".[23] Z uwagi na wymagania konstytucyjne i prawnomiędzynarodowe, regulacja w tym zakresie jest niezbędna. Obecnie pracodawca stosujący monitoring może, w zależności

---

[19] Chyba że pracodawca wyraźnie zakazał oznaczonych form komunikacji o charakterze prywatnym w czasie pracy lub przekazywana informacja miałaby charakter prawnie chronionej (np. na podstawie ustawy o ochronie informacji niejawnych (Dz.U. z 2005 r. nr 196, poz. 1631 z późn. zm.). Wymagania konstytucyjne są w tym zakresie zbieżne z wymaganiami, powoływanych w dalszej części artykułu, umów międzynarodowych, które zakładają konieczność ustawowej regulacji każdej formy ingerencji w korzystanie z praw człowieka.

[20] Por. art. 237 Kodeksu postępowania karnego (Dz.U. z 1997 r. nr 89, poz. 555 z późn. zm.), art. 19 ustawy o Policji (Dz.U. z 2007 r. nr 43, poz. 277 z późn. zm.) czy art. 36c ustawy o kontroli skarbowej (Dz.U. z 2004 r. nr 8, poz. 65 z późn. zm.).

[21] W przypadkach niecierpiących zwłoki możliwe jest, co prawda, podjęcie doraźnej kontroli operacyjnej, powinna być ona jednak następnie zatwierdzona przez sąd w terminie 5 dni. W razie nieudzielenia przez sąd zgody organ zarządzający musi wstrzymać kontrolę operacyjną oraz dokonać protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania.

[22] Stanowisko Rzecznika Praw Obywatelskich powoływane w artykule *RPO: pracodawcy nie mogą kontrolować maili pracowników*, <http://wiadomosci.gazeta.pl/Wiadomosci/1,80708,4801398.html>, dostęp: 30 października 2010 r.

[23] Odpowiedź podsekretarza stanu w Ministerstwie Pracy i Polityki Społecznej – z upoważnienia ministra – na interpelację nr 12970 z dnia 27 listopada 2009 r. w sprawie zasad montowania monitoringu w zakładach pracy, dostępna na stronie Biura Prasowego Kancelarii Sejmu: <http://orka2.sejm.gov.pl/IZ6.nsf/main/0F5E9040>, dostęp: 30 października 2010 r.

od sytuacji, ryzykować naruszenie dóbr osobistych pracownika, a nawet zakwalifikowanie swoich działań jako przestępstwa nielegalnego podsłuchu z art. 267 kodeksu karnego.[24]

Nasuwa się pytanie, czy – wobec braku upoważnienia ustawowego do ingerencji w tajemnicę komunikacji – w ogóle dopuszczalny jest monitoring pracownika w tym zakresie. Należałoby tu rozważyć możliwość monitoringu wprowadzanego za zgodą pracowników. Dysponowanie zgodą osoby uprawnionej z tytułu ochrony dóbr osobistych zasadniczo wyłącza bezprawność ingerencji. Zgoda pracownika na „podsłuchiwanie" jego komunikacji niewątpliwie może powodować brak naruszenia. Takie rozwiązanie budzi jednak pewne wątpliwości z uwagi na przewagę pracodawcy nad pracownikiem i możliwość wpływania tego pierwszego na swobodę udzielenia zgody przez pracownika. Dyskusyjne jest, czy pracownik postawiony przed wyborem, czy pracować w warunkach monitorowania, czy też nie pracować u danego pracodawcy w ogóle, ma pełną swobodę w podjęciu decyzji. Z drugiej strony takie właśnie może być oczekiwanie pracodawcy – by pracowały u niego osoby mające już na etapie rozpoczynania zatrudnienia świadomość monitoringu i wyrażające na to zgodę, tak by pracodawca miał pełną kontrolę nad przebiegiem i jakością świadczonej pracy oraz jej efektami. W tym przypadku pracownik rozpoczynający zatrudnienie formalnie ma swobodę co do wyrażenia zgody na monitorowanie swoich działań (co jednak nie zawsze będzie oznaczać pełną swobodę w znaczeniu materialnym).[25] Przyjmując, że takie działanie w ramach zgody pracownika byłoby dopuszczalne, zgodę tę należałoby uzyskiwać apriorycznie, najlepiej w ramach umowy o pracę, razem z innymi warunkami zatrudnienia, ewentualnie w osobnym oświadczeniu, złożonym w tej sprawie. Nie ulega wątpliwości, że zarówno informacja, jak i ewentualna zgoda na wprowadzenie monitoringu powinny mieć charakter wyprzedzający w stosunku do jego uruchomienia. Ponadto pracownik powinien znać zasady takiego nadzoru, tak by nie miał wątpliwości, w jakich sytuacjach i w jakim zakresie mu podlega.

Regulacja ochrony prywatności w polskiej Konstytucji jest zasadniczo tożsama co do zakresu wartości chronionych[26] z art. 8 Europejskiej Konwencji Praw Człowieka,[27] który w § 1 stanowi, że „każdy ma prawo do własnego

[24] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001, s. 28.

[25] Swoboda decyzji pracownika w takiej sytuacji jest zawsze dyskusyjna i powinna być oceniania indywidualnie, w zależności od zaistniałych okoliczności. Tak np. za naruszenie praw pracownika i swobody wyrażenia przez niego woli uznał Naczelny Sąd Administracyjny sytuację, w której pracownik, na prośbę pracodawcy, wyraził zgodę na pobranie od siebie odcisków linii papilarnych w celu umożliwienia monitorowania czasu pracy za pomocą czytników tych linii zainstalowanych przy wejściach do budynku pracodawcy (wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009 r., sygn. akt I OSK 249/09).

[26] T. Liszcz, *Ochrona prywatności pracownika w relacjach z pracodawcą*, „Monitor Prawa Pracy" 1/2007, Legalis.

[27] Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4 listopada 1950 r., ratyfikowana przez Polskę 19 stycznia 1993 r. (Dz.U. z 1993 r. Nr 61, poz. 284 z późn. zm.).

życia prywatnego i rodzinnego oraz do tajemnicy korespondencji i do nietykalności mieszkania". Orzekający na podstawie Konwencji Europejski Trybunał Praw Człowieka szczegółowo wypowiedział się co do zasad monitorowania pracownika na tle cytowanego przepisu w sprawie *Copland przeciw Wielkiej Brytanii*.[28] W czasie gdy doszło do wydarzeń stanowiących podstawę skargi, w Wielkiej Brytanii, podobnie jak aktualnie w Polsce, nie obowiązywały jeszcze przepisy dostatecznie regulujące monitorowanie pracowników.[29] W orzeczeniu tym Trybunał jednoznacznie potwierdził, że zarówno wysyłana z pracy poczta elektroniczna (e-mail), jak i monitorowanie przeglądania Internetu są objęte ochroną w ramach art. 8 § 1 Konwencji,[30] a brak informacji ze strony pracodawcy o stosowaniu monitoringu uzasadnia oczekiwanie pracownika, że jego komunikacja będzie miała charakter prywatny.[31] Bez znaczenia pozostaje fakt, czy gromadzone dane zostaną następnie w jakikolwiek sposób ujawnione, czy wykorzystane przeciw pracownikowi – naruszeniem prywatności jest bowiem już sam fakt ich gromadzenia.[32]

Ponadto Trybunał stwierdził, że nie może stanowić podstawy takiej ingerencji prawo nie spełniające wymagań co do jego jakości, w szczególności regulujące przedmiotową kwestię w sposób ogólnikowy i nieprzewidywalny. Przepisy muszą w jasny sposób określać okoliczności, w których jednostka powinna liczyć się z możliwością naruszenia jej prywatności, a także, jakie środki i na jakich zasadach mogą być w takiej sytuacji zastosowane.[33] Wprowadzenie odpowiednich przepisów to oczywiście obowiązek państwa, trzeba jednak zauważyć, że brak regulacji w tej dziedzinie nie może stanowić podstawy dla przedsięwzięcia przez pracodawcę środków, które wyraźnie przepisami prawa nie zostały przewidziane. Jeśli bowiem prawo nie reguluje danej kwestii dostatecznie, to na gruncie art. 8 § 2 Konwencji należy przyjąć, że „ingerencja taka nie jest zgodna z prawem".[34] W przedmiotowej sprawie, z uwagi na brak podstaw prawnych do wprowadzenia monitoringu przez pracodawcę, Trybunał uznał, że doszło do naruszenia art. 8 Konwencji.[35] Z uwagi na podobieństwo aktualnego stanu polskiej regulacji prawnej (czy raczej jej braku) do sytuacji prawnej zaistniałej w sprawie *Copland*, należy przyjąć, że *de lege lata* wprowadzenie przez polskiego pracodawcę monitoringu Internetu bez wiedzy pracownika także będzie skutkowało naruszeniem art. 8 Konwencji.

---

[28] *Copland przeciw Wielkiej Brytanii* – wyrok ETPC z 3 kwietnia 2007 r. (skarga nr 62617/00), HUDOC.

[29] Kwestia ta została w Wielkiej Brytanii uregulowana w roku 2000 w ramach *The Regulation of Investigatory Powers Act 2000 ("the 2000 Act")* oraz *The Telecommunications (Lawful Business Practice) Regulations 2000*.

[30] *Copland...*, ust. 41.

[31] Ibidem, ust. 42.

[32] Ibidem, ust. 43–44.

[33] Ibidem, ust. 46–47.

[34] Ibidem, ust. 48.

[35] Ibidem, ust. 49.

Prawo do prywatności podlega także ochronie na podstawie art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych.[36] System kontrolny Paktu (w przypadku ratyfikacji Protokołu Fakultatywnego,[37] obejmujący także prawo do skargi indywidualnej), nie jest systemem *stricte* sądowym – decyzje Komitetu Praw Człowieka nie wiążą wprost organów państw-stron. Nie zmienia to jednak faktu, że jako ratyfikowana umowa międzynarodowa jest on w Polsce źródłem prawa i można się na niego powoływać, w szczególności gdy przepisy krajowe nie regulują wyczerpująco przedmiotowej kwestii. Swoistej (niewiążącej) wykładni traktatu w zakresie rozumienia poszczególnych praw dokonuje Komitet Praw Człowieka w drodze tzw. Uwag Ogólnych do Paktu – w przypadku art. 17 Paktu są to Uwagi Ogólne nr 16.[38]

Pomimo iż podstawową funkcją Paktu jest ochrona przed naruszeniami ze strony państwa, to w przypadku prawa do prywatności Komitet w swych uwagach wskazuje, że „prawo to powinno być chronione przed wszelkimi ingerencjami i zamachami, niezależnie od tego czy dokonywałoby ich państwo, czy też osoby fizyczne lub prawne".[39] Obowiązkiem państwa jest zaś „zapewnić środki prawne i pozaprawne gwarantujące powstrzymanie takich ingerencji i zamachów, na równi z ochroną samego prawa".[40] W świetle cytowanych uwag Komitetu, biorąc pod uwagę zasadniczy brak krajowej regulacji dotyczącej monitorowania pracowników, można mieć wątpliwości, czy Polska prawidłowo wypełnia swoje zobowiązania traktatowe w tym zakresie. Ponadto Komitet podkreśla, że choć ochrona prywatności nie ma charakteru bezwzględnego, to jednak wszelka ingerencja powinna być dokonywana wyłącznie wtedy, gdy jest niezbędna z punktu widzenia społeczeństwa, w ramach obowiązującego prawa i przez uprawnione do tego organy.[41] Niedopuszczalna jest ingerencja, która nie została wyraźnie przewidziana przez prawo danego państwa,[42] co – w przypadku braków polskiej regulacji – stawia pod znakiem zapytania legalność jakichkolwiek form monitoringu pracowników. Dodatkowo Komitet wskazuje, że przepisy regulujące ingerencję powinny być maksymalnie szczegółowe, aby wyeliminować arbitralność decyzji osób jej dokonujących. W przypadku korespondencji (także elektronicznej) Komitet oczekuje od państw zagwarantowania jej poufności i inte-

[36] Międzynarodowy Pakt Praw Obywatelskich i Politycznych, uchwalony 19 grudnia 1966 r., wszedł w życie 23 marca 1976 r., przez Polskę ratyfikowany 3 marca 1977 r., wszedł w życie wobec Polski 18 czerwca 1977 r. (Dz.U. z 1977 r. Nr 38, poz. 167).

[37] Protokół Fakultatywny, przewidujący prawo do skargi indywidualnej do Komitetu Praw Człowieka, ratyfikowany przez Polskę 14 października 1991 r., wszedł w życie wobec Polski 7 lutego 1992 r. (Dz.U. z 1994 r. Nr 23, poz. 80).

[38] *General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17)* z 8 kwietnia 1988 r. (tłum. wł.), dostępne w Internecie pod adresem: <http://www2.ohchr.org/english/bodies/hrc/comments.htm>, dostęp: 30 października 2010 r.

[39] Ibidem, ust. 1.

[40] Ibidem.

[41] Ibidem, ust. 8.

[42] Ibidem, ust. 3.

gralności – powinna ona być dostarczona do adresata „bez jej otwierania czy odczytywania w inny sposób", zaś „wszelkie elektroniczne i inne środki inwigilacji, przechwytywanie telefonicznych, telegraficznych i innych form komunikacji, podsłuchy oraz nagrywanie rozmów powinny być zabronione".[43] Nie wyklucza to możliwości dokonania ingerencji w tak zakreśloną tajemnicę komunikacji, jednak mogą to uczynić wyłącznie ustawowo upoważnione podmioty, w zakresie przez prawo przewidzianym, w celach zgodnych z założeniami, celami i postanowieniami Paktu.[44]

W świetle przedstawionych powyżej uwag uregulowanie monitoringu korzystania z Internetu przez pracowników nie jest proste. W szczególności, nie można apriorycznie zanegować lub potwierdzić prawa pracodawcy do stosowania takiego środka kontroli. Podstawowe znaczenie ma bowiem zakres takiego monitoringu i zasady jego zastosowania. To na ich podstawie można stwierdzić, czy i w jakich sytuacjach taka ingerencja będzie uznana za dopuszczalną.

Aby pracodawca mógł posłużyć się monitoringiem Internetu, konieczne jest przede wszystkim poinformowanie o tym pracownika. Warto zadbać o pisemne potwierdzenie świadomości pracowników w tym względzie, poprzez wprowadzenie stosownego zapisu w umowie o pracę lub osobne oświadczenie o zapoznaniu się z regulaminem pracy w tym zakresie. Zasady działania takiego systemu nadzorowania pracowników muszą być ponadto szczegółowo określone, tak by nie było wątpliwości, kiedy i w jakim zakresie działania pracowników zostaną utrwalone. Nie można też zapominać o tym, że wprowadzane środki muszą być proporcjonalne do zagrożeń, co powinno przekładać się na zróżnicowanie zakresu monitoringu w zależności od rodzaju stanowiska pracy i zakresu obowiązków danego pracownika. Celem uniknięcia wątpliwości, czy w ramach nadzorowania pracownika pracodawca nie przekroczył granic prywatności, być może warto zastosować się do wspominanej wcześniej sugestii Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych i wprowadzić system odrębnych kont prywatnych i pracowniczych. Tylko te drugie powinny być monitorowane szczegółowo, np. co do treści transmitowanych za pośrednictwem sieci komunikatów. Użytkowanie konta prywatnego powinno być monitorowane tylko co do czasu, przez który się z niego korzysta. W ten sposób minimalizuje się ryzyko przypadkowego naruszenia prywatności. Pracownik jest w tej sytuacji należycie chroniony, a w przypadku utrwalenia komunikacji o charakterze prywatnym, wychodzącej z konta służbowego, niejako sam się na naruszenie naraża, działa bowiem w pełnej świadomości archiwizowania swoich poczynań. Nie sposób oczywiście przewidzieć wszelkich możliwych do zaistnienia sytuacji, ale przygotowanie właściwej polityki monitorowania Internetu w miejscu pracy powinno ograniczyć sytuacje wątpliwe do minimum. Ponadto należy oczekiwać, że w najbliższej przyszłości polski ustawodawca

[43] Ibidem, ust. 8.
[44] Ibidem, ust. 3.

ureguluje tę kwestię bardziej szczegółowo – w sposób umożliwiający określenie, w jakich sytuacjach i w jakim zakresie ingerencja w prywatność pracownika będzie dopuszczalna.

EMPLOYEE MONITORING IN COMPUTER NETWORK

Key words: human rights, workers rights, right to privacy, employee monitoring, personal data protection.

Summary

Article is about increasing employers' need for the measures of monitoring of the employee's access to the computer network. The main purpose of this paper is to point out lacks of Polish legal regulation in the matter and attempt to find legal basis in this situation.

In the introductory part of the article author presents some basic statistical data about behaviours of the employees working in corporation computer networks having access to the Internet, especially so called *cyberslacking*. Author considers briefly most common negative consequences of such behaviour and their potential implications. Then the article touches upon the software measures preventing such actions and possible abuses of the workers' right to privacy and freedom of communication.

In the following part the article presents rudimentary Polish regulation contained in the regulation of the Ministry of Labour and Social Policy about work safety and industrial hygiene, Polish labour code and civil code. Author also touches upon the propositions on the separation of the worker's private and professional computer accounts given by the Article 29 Data Protection Working Party in the W*orking document on the surveillance of electronic communications in the workplace.*

Then the article concentrates on the possibilities and limits of employee's monitoring and their consequences in the scope of Polish Constitution (art. 47 and also specifically art. 49). Author considers possible interim measures for the employers and presents some postulates as for the future legislation. As a main point of consideration author takes the art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, taking into account the *Copland vs United Kingdom* case, in which the European Court for Human Rights in detail considered situation of the employee monitoring via the electronic and software measures when lacking country's legal regulation.

Next, the article considers Polish obligations in the scope of the art. 17 of the Covenant on the Civil and Political Rights, mostly taking into account the *General Comment No. 16 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)*, in which the Human Rights Committee presents it's reasoning and interpretation of the subject.

In conclusion the author suggests how the Polish employer should proceed and how should he regulate monitoring of the access to the Internet of his employees to minimize the threat of potential workers' privacy intrusion.