Kontrola pracownika w zakresie powierzonego mu przez pracodawcę sprzętu służbowego

Anna Pułka

radca prawny, doktorantka Wydziału Prawa,
Administracji i Ekonomii Uniwersytetu Wrocławskiego

Wyposażenie pracownika w określone narzędzia pracy ma na celu optymalną organizację procesu pracy. Narzędzia te powinny być używane przez pracownika do realizacji powierzonych mu przez pracodawcę zadań służbowych, a to, czy faktycznie tak jest, może być kontrolowane przez pracodawcę. Zarówno dopuszczalność, jak i granice poszczególnych kompetencji kontrolnych pracodawcy nie zostały uregulowane wprost w żadnym akcie prawnym. Analogicznie wygląda kwestia ochrony prawa pracowników poddawanych różnym formom kontroli. Jednocześnie rozwój techniki i brak adekwatnych regulacji prawnych wyznaczających ramy dopuszczalnej kontroli pracowników przez pracodawców stwarza i będzie nadal powodował spory nie tylko natury teoretycznej, ale i praktycznej. Autorka podejmuje próbę wskazania ram prawnych kontroli pracowników, odwołując się do orzecznictwa i poglądów doktryny, dochodząc do wniosku, że podstawowymi warunkami dopuszczalnej kontroli pracowników są: proporcjonalność podjętych przez pracodawcę środków do osiągnięcia wyznaczonych celów oraz jasne, przejrzyste reguły kontroli podane do wiadomości pracowników, a w niektórych przypadkach stosowane pod warunkiem uzyskania na nie zgody każdego z pracowników objętych monitoringiem.

Uwagi wprowadzające

Pracownik, który otrzymał od pracodawcy sprzęt na podstawie powierzenia z obowiązkiem wyliczenia się albo zwrotu, będzie ponosił odpowiedzialność za powierzone mu mienie na zasadach określonych w przepisach kodeksu pracy (art. 124–127). Nie jest to jednak jedyny obowiązek nałożony na pracownika, któremu pracodawca powierzył sprzęt służbowy.

Zatrudniający, dostarczając narzędzie pracy, np. komputer, telefon itp., ma prawo kontrolować, w jaki sposób podwładny korzysta z powierzonego mu sprzętu, jednak musi to czynić zachowując pewne zasady i nie przekraczając określonych granic. Jest to tym trudniejsze, że w Polsce, podobnie zresztą jak w innych krajach członkowskich Unii Europejskiej, nie ma kompleksowych regulacji prawnych dotyczących monitoringu w miejscu pracy.

Wyjątkiem w prawie polskim jest regulacja dotycząca dopuszczalności monitoringu aktywności pracowników w systemie informatycznym pracodawcy, zawarta w załączniku do rozporządzenia Ministra Pracy i Polityki Socjalnej z 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe[1]. Przy projektowaniu, doborze i modernizacji oprogramowania, a także przy planowaniu wykonywania zadań z użyciem ekranu monitora pracodawca powinien uwzględniać fakt, że bez wiedzy pracownika nie można dokonywać kontroli jakościowej i ilościowej jego pracy.

Jednocześnie problematyka kontrolowania pracownika w miejscu pracy, wobec rozwoju nowoczesnych technologii przetwarzania informacji, nie może być niedostrzegana przez pracodawców. Jest bowiem ważnym składnikiem zarządzania firmą, a wszelkie nieprawidłowości mogą narażać firmę na różnego rodzaju ryzyko i związane z nim negatywne konsekwencje prawne i finansowe, począwszy od okazania słabości w zarządzaniu firmą przez jej władze poprzez uzyskanie przez osoby nieuprawnione dostępu do informacji będących tajemnicą przedsiębiorstwa[2], a skończywszy na odpowiedzialności cywilnej[3] czy nawet quasi-karnej pracodawcy[4], np. w przypadku używania przez pracownika nielegalnego oprogramowania.

Posiłkowo, jak przyjmuje się w doktrynie i orzecznictwie, można wyinterpretować pewne ogólne zasady dotyczące kontroli nad działaniami pracownika z przepi-

sów następujących aktów prawnych: Konstytucji RP, kodeksu cywilnego, ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, kodeksu karnego[5].

Poniższe rozważania odnoszą się do sytuacji, gdy sprzęt komputerowy oraz inny sprzęt umożliwiający gromadzenie, ściąganie oraz przetwarzanie danych i informacji, z którego korzystają pracownicy, jest własnością pracodawcy i został przekazany pracownikom w celu świadczenia pracy.

Kontrola pracownika w prawie pracy

Sprzęt i oprogramowanie powierzone pracownikowi

Podstawowymi obowiązkami pracownika są: pozostawanie w czasie pracy w dyspozycji pracodawcy, wykonywanie pracy określonego rodzaju na rzecz pracodawcy, pod jego kierownictwem oraz w miejscu i czasie wyznaczonym przez pracodawcę (wynika to zwłaszcza z art. 22 § 1 k.p. oraz art. 128 k.p.), a także dbałość o dobro zakładu pracy (art. 100 § 2 pkt 4 k.p.). Pracodawca powinien natomiast organizować pracę zatrudnionych przez siebie pracowników w sposób zapewniający pełne wykorzystanie przez nich czasu pracy oraz uzyskiwanie wysokiej wydajności i należytej jakości pracy (art. 94 pkt 2 k.p.). Obowiązkiem pracodawcy jest zapewnienie pracownikowi stanowiska pracy, które będzie umożliwiało prawidłowe wykonywanie powierzonych mu obowiązków. Jednym z elementów takiego stanowiska pracy może być (jeżeli wynika to z zakresu obowiązków pracownika na danym stanowisku) sprzęt komputerowy wraz z oprogramowaniem oraz telefon służbowy, które pracownik otrzymuje w momencie rozpoczęcia pracy i które niejednokrotnie służą mu jako podstawowe narzędzia pracy.

Powierzenie pracownikowi ww. sprzętu nie pozbawia pracodawcy prawa własności, prawa do kontrolowania prawidłowości korzystania z niego przez każdego z pracowników, którym sprzęt ten został oddany do dyspozycji w celu wykonywania obowiązków pracowniczych. Przy czym należy opowiedzieć się za poglądem, iż: „interpretacja art. 100 § 2 pkt 4 k.p. nie może prowadzić do kreowania swoistego pracowniczego wszechobowiązku poddawania się kontroli w każdym przypadku i dowolnym zakresie, na polecenie pracodawcy. Obowiązek dbałości o dobro zakładu pracy może być dla potrzeb kontrolnych uściślany do węższego pracowniczego obowiązku poddania się kontroli tylko w razie istnienia wyraźnie uzasadnionych potrzeb, związanych z ochroną zakładu pracy i w razie niekolidującym z innymi odnośnymi regulacjami prawnymi i dobrami objętymi prawną ochroną"[6]. Granic tej kontroli należy upatrywać w art. 31 ust. 3 Konstytucji RP, który przewiduje, iż: „ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw".

Zakaz używania sprzętu do celów prywatnych

Pracodawca, chcąc w sposób legalny egzekwować od pracowników obowiązek wykorzystywania powierzonego im sprzętu wyłącznie do celów służbowych, musi wprowadzić jasne i jednoznaczne zasady dotyczące sposobu wykorzystywania tego sprzętu, w szczególności może zakazać wykorzystywania go do celów prywatnych. Tego rodzaju zakaz może być wprowadzony:

- ogólnie wobec wszystkich pracowników:
  - w układzie zbiorowym pracy lub w regulaminie pracy albo specjalnie w tym celu stworzonym regulaminie korzystania ze sprzętu służbowego; w myśl art. 104 § 2 k.p. obowiązek wprowadzenia regulaminu pracy ciąży na pracodawcy, który zatrudnia więcej niż 20 osób, a układy zbiorowe są dobrowolne; oznacza to, że u niektórych pracodawców może nie funkcjonować ani regulamin pracy, ani układ zbiorowy pracy;
  - w drodze zarządzenia pracodawcy, które zostanie podane do wiadomości pracowników w sposób zwyczajowo przyjęty w danym zakładzie pracy;
- indywidualnie poprzez:
  - wprowadzenie stosownych postanowień do umów o pracę: w przypadku gdy u pracodawcy nie ma ani regulaminu pracy, ani układu zbiorowego pracy lub też ww. dokumenty są, ale nie zawierają stosownych zapisów;
  - przyjęcie od pracownika w momencie powierzania mu sprzętu służbowego oświadczenia, iż będzie go używał wyłącznie w celach służbowych.

Niezależnie jednak od formy wprowadzenia ww. zakazu należy pamiętać, iż dla celów dowodowych zalecane jest, aby pracownik wyraził na piśmie zgodę na objęcie go postanowieniami dotyczącymi tego zakazu. Jeśli więc zakaz nie jest ujęty w indywidualnych postanowieniach umowy o pracę lub w protokole przekazania sprzętu (potwierdzonym podpisem przez pracownika), sugeruje się, aby od każdego pracownika odbierać pisemne oświadczenie o zaznajomieniu się z wewnętrznymi regulacjami obowiązującymi w zakładzie pracy dotyczącymi tej kwestii (np. z regulaminem pracy, zarządzeniem pracodawcy). Oświadczenie takie powinno być załączone do akt osobowych pracownika.

W trakcie obowiązywania zakazu pracownik, chcąc używać powierzonego mu sprzętu do celów prywatnych, powinien uzyskać na to zgodę pracodawcy.

Należy podkreślić, iż oprócz bezwzględnego zakazu wykorzystywania sprzętu służbowego do celów prywatnych pracodawca może zdecydować się na wprowadzenie jedynie pewnych ograniczeń w tym zakresie. Przy czym także i w tym przypadku o zakresie tych ograniczeń pracodawca powinien informować wszystkich pracowników, których ma dotyczyć to ograniczenie.

Ponadto należy pamiętać, że jeśli pracodawca nie wprowadzi wyraźnego zakazu korzystania z komunikatorów internetowych czy portali społecznościowych przy użyciu powierzonego sprzętu komputerowego itp.,

nie może później wyciągać negatywnych konsekwencji wobec pracowników, którzy z nich korzystają (chyba że pracownik zainstaluje sobie w tym celu na sprzęcie służbowym nielegalne oprogramowanie).

Zakaz używania komputera służbowego do celów prywatnych może dotyczyć również zakazu przechowywania na nim prywatnych dokumentów pracownika. Wówczas, jeśli pracownik chce zapisywać prywatne pliki na komputerze służbowym, musi uzyskać na to uprzednio zgodę pracodawcy. Niemniej jednak, złamanie tego zakazu przez pracownika nie oznacza, że pracodawca może swobodnie przeglądać czy usuwać prywatne dokumenty pracownika zapisane na służbowym sprzęcie. W takiej bowiem sytuacji pracodawca może jedynie wyciągnąć wobec pracownika konsekwencje służbowe, o których będzie mowa niżej.

Ochrona godności i innych dóbr osobistych pracownika a uprawnienie pracodawcy do kontrolowania pracownika

Zgodnie z art. 47 Konstytucji RP: „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Powyższą regulację konkretyzuje art. 51 dotyczący prawa jednostki do ochrony danych osobowych oraz art. 49 dotyczący ochrony komunikowania się. Art. 233 Konstytucji gwarantuje natomiast, iż godność człowieka nie może być ograniczona nawet w czasie stanu wojennego i wyjątkowego. Wszystkie te zasady konstytucyjne mają ponadgałęziowe znaczenie, a zatem są istotne również w zakresie prawa pracy[7].

Zgodnie z art. 111 k.p. pracodawca jest obowiązany szanować godność i inne dobra osobiste pracownika. Zarówno ten przepis, jak i ogólne przepisy prawa cywilnego dotyczące ochrony dóbr osobistych (w szczególności art. 23 i 24 k.c.), za podlegające wspomnianej ochronie uważają prawo do prywatności pracownika, w tym tajemnicę korespondencji.

Prywatność, mimo że jest wartością powszechnie chronioną, nie podlega jednocześnie ochronie absolutnej[8].

Przenosząc powyższe rozważania na analizowane w niniejszym artykule zagadnienia, należy się zastanowić nad kwalifikacją skutków używania przez pracownika do celów prywatnych, mimo obowiązującego go zakazu wprowadzonego przepisami wewnątrzzakładowymi, sprzętu powierzonego mu przez pracodawcę, a w szczególności gdy posługuje się w tych celach służbową skrzynką e-mailową czy też telefonem komórkowym.

Należy uznać, iż w takiej sytuacji mamy do czynienia ze zbiegiem dwóch wartości podlegających ochronie prawnej: z jednej strony mamy bowiem dobra osobiste pracownika, a z drugiej — zasadę właściwego użytkowania mienia powierzonego przez pracodawcę i stanowiącego własność pracodawcy.

Ogólne przepisy prawa pracy (np. art. 22 § 1 k.p. stanowiący, iż przez nawiązanie stosunku pracy pracownik zobowiązuje się do wykonywania pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem) dają pracodawcy prawo kontrolowania czasu pracy pracownika poprzez badanie wykonywania przez niego obowiązków pracowniczych. Zgodnie zaś z art. 94 pkt 2 k.p. do obowiązków pracodawcy należy, między innymi, organizowanie pracy w sposób zapewniający pełne wykorzystanie czasu pracy, jak również osiąganie przez pracowników, przy wykorzystaniu ich uzdolnień i kwalifikacji, wysokiej wydajności i należytej jakości pracy — również więc i z tego przepisu można wywieść prawo pracodawcy do kontroli pracy pracownika. O ile brakuje szczegółowych przepisów w tym zakresie, o tyle praktyka i orzecznictwo wypracowały pewne zasady, które odnoszą się do sposobów przeprowadzania monitoringu pracy. Uznaje się, iż do skorzystania przez pracodawcę ze środków kontroli może dojść, w zasadzie, w trzech sytuacjach, uzasadnionych jego interesem:

- ❒ w celu oceny wydajności i efektywności pracy pracownika — w ramach działań prewencyjnych;
- ❒ w razie nieobecności pracownika w miejscu pracy, gdy zachodzi konieczność uzyskania istotnych danych znajdujących się w komputerze służbowym pracownika;
- ❒ w razie uzyskania przez pracodawcę informacji, że może dochodzić do naruszeń obowiązków pracowniczych określonych w art. 100 § 1 pkt 4 k.p. (prowadzenia przez pracownika działalności sprzecznej z interesem pracodawcy, a nawet działalności nielegalnej lub przestępczej) — pracodawca ponosi bowiem odpowiedzialność za działania i zaniechania pracowników wobec osób trzecich.

Niezależnie od powyższego pracodawca musi mieć na uwadze zasadę proporcjonalności i każdorazowo stosować takie formy kontroli, które są adekwatne do zaistniałej sytuacji i proporcjonalne do celu, jaki pracodawca chce osiągnąć, możliwie w najmniejszym stopniu ingerując w życie pracowników. Konieczne jest zatem, aby działania pracodawcy były podejmowane w usprawiedliwionym celu, a wszelkie stosowane przez niego środki były transparentne, tj. pracownicy powinni wiedzieć, jakiej formie kontroli są lub mogą być poddawani oraz czy, a jeżeli tak, to w jakim zakresie, mogą wykorzystywać powierzone im urządzenia do celów prywatnych. Jest to najważniejszy z obowiązków pracodawcy, którego spełnienie przesądza o legalności wszelkiego rodzaju kontroli przeprowadzanej wobec pracownika. Pośrednio wynika on z przepisów regulujących kwestie bezpieczeństwa i higieny pracy, zgodnie z którymi, przykładowo, pracodawca, który zamierza powierzyć pracownikowi do wykonywania zadania, przy których pracownik będzie korzystał z ekranu monitora komputerowego, powinien uwzględnić fakt, iż bez wiedzy pracownika nie można dokonywać kontroli jakościowej i ilościowej jego pracy. Jeśli więc pracownik został poinformowany o obowiązującym u pracodawcy zakazie używania sprzętu komputerowego do celów prywatnych, jakościowa i ilościowa kontrola ze strony pracodawcy wykonywanej przez danego pracownika pracy jest prawnie dopuszczalna pod warunkiem posiadania przez pracownika wiedzy na temat tej kontroli[9]. Czyli, jak się wydaje, zarówno zakres, jak i zasady przeprowadzania tej kontroli muszą być znane pracownikowi, a on sam powinien mieć zagwarantowane przez pracodawcę

prawo do uczestniczenia w czynnościach kontrolnych. Wykładnia celowościowa pkt. 10 lit. e powołanego wyżej załącznika do rozporządzenia Ministra Pracy i Polityki Socjalnej z 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe przemawia za tezą o dopuszczalności przeprowadzania kontroli w z góry ustalonych okresach, jeśli zostały one przewidziane w regulacjach wewnątrzzakładowych wprowadzających zakaz używania sprzętu do celów prywatnych.

Z uwagi na to, że nie ma przepisów, które przewidywałyby formę poinformowania pracownika o zamiarze przeprowadzenia kontroli, należy uznać, iż informacja taka może zostać przekazana w dowolny sposób. Niemniej jednak, mając na względzie ewentualne roszczenia pracownika w przypadku braku takiej informacji, rekomenduje się, aby dla celów dowodowych była ona każdorazowo przekazywana pracownikowi w formie pisemnej.

W przypadku pracowników, którzy w sposób ciągły pracują przy komputerach i korzystają ze służbowej skrzynki e-mailowej, tego rodzaju informacja może być przekazana drogą e-mailową[10]. Również Europejski Trybunał Praw Człowieka uznał za niedozwolone sprawdzanie poczty elektronicznej bez powiadomienia o tym pracownika i bez określenia zasad takiego monitoringu, stanowiąc, iż: „zbieranie i przechowywanie informacji osobistych związanych z korzystaniem przez skarżącą z telefonu, a także z poczty elektronicznej oraz Internetu, bez jej wiedzy, sprowadzało się do ingerencji w jej prawa do poszanowania życia prywatnego i korespondencji w rozumieniu art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności"[11]. W obliczu niezwykle skromnego orzecznictwa krajowego[12] w tej materii oraz braku stosownych regulacji w prawie krajowym, powyższy wyrok Trybunału, odnosząc się do obowiązujących również w Polsce postanowień Konwencji o ochronie praw człowieka i podstawowych wolności, ma niezmiernie istotne znaczenie dla praktyki.

Przy czym, jak wskazał Minister Pracy i Polityki Społecznej[13], kontrolowanie przez pracodawcę pracowników nie wymaga uzyskania od nich zgody na określony rodzaj kontroli wykonywania pracy. W konsekwencji jedynym warunkiem, który zdaniem Ministra Pracy i Polityki Społecznej musi być spełniony w tym przypadku, jest świadomość i wiedza pracownika o potencjalnej możliwości stosowania przez pracodawcę w zakładzie pracy różnych form monitoringu, nie zaś wyraźna zgoda pracownika na kontrolę świadczenia przez niego pracy.

Powyższe stanowisko Ministra Pracy i Polityki Społecznej w przedmiocie ewentualnej zgody pracownika na stosowanie przez pracodawcę określonego rodzaju kontroli wykonywania pracy nie jest jednomyślnie aprobowane w doktrynie. Część autorów[14], powołując się na przepisy ustawy o ochronie danych osobowych, kreuje wręcz obowiązek uzyskania przez pracodawcę w określonych sytuacjach indywidualnej zgody pracownika na monitoring w miejscu pracy. Stosowanie takich środków kontroli prowadzi zawsze, czy to pośrednio czy bezpośrednio, do pozyskiwania i gromadzenia informacji o pracownikach, uzasadniając niejako stosowanie w tych sytuacjach przepisów ustawy o ochronie danych osobowych. Na szczególną uwagę w tym zakresie zasługuje art. 23 ustawy zawierający zamknięty katalog rozłącznych przesłanek dopuszczalności przetwarzania danych osobowych. Oznacza to, że aby wykorzystywanie danych można było uznać za działanie legalne, wystarczające jest spełnienie jednej z nich, a nie wszystkich łącznie. Tytułem przykładu, można wyróżnić następujące przesłanki:

- wyrażenie zgody na przetwarzanie danych przez osobę, której dane dotyczą;
- jeżeli przetwarzanie danych jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych lub osób trzecich, którym dane te są przekazywane, a ich przetwarzanie nie narusza praw i wolności osób, których dane dotyczą.

W świetle powyższego należy przyjąć, iż zasadą jest uzyskiwanie zgody przez pracodawcę na przetwarzanie danych osobowych pracownika poprzez monitorowanie wykonywania obowiązków służbowych, jeżeli za zastosowaniem danego środka kontroli nie stoi prawnie usprawiedliwiony cel pracodawcy. Z kolei indywidualna zgoda pracownika na objęcie go monitoringiem nie będzie wymagana, jeżeli pracodawca jest w stanie wykazać, że uzyskiwanie i gromadzenie określonych informacji dotyczących pracowników w drodze monitoringu jest niezbędne do wypełniania prawnie usprawiedliwionych celów (np. zwiększenia wydajności pracy przez ograniczenie przeglądania przez pracowników w czasie pracy stron internetowych bądź zminimalizowania kosztów rozmów telefonicznych przez wyeliminowanie lub ograniczenie rozmów prywatnych) oraz jeżeli zastosowane metody kontroli są adekwatne do wspomnianych wyżej celów pracodawcy.

Co więcej, zgoda pracownika na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda powinna być bowiem wyrażona w oddzielnym oświadczeniu w sposób wyraźny, świadomy i jednoznaczny oraz wyróżniać się spośród innych pochodzących od danego pracownika informacji i oświadczeń. Jak wynika z orzecznictwa, czynności takiej nie konwaliduje ani późniejsze poinformowanie pracownika o treści aktów wewnątrzzakładowych, w których zostały uregulowane kwestie przetwarzania danych osobowych, ani umożliwienie pracownikowi zgłoszenia zastrzeżeń co do pewnych form przetwarzania danych osobowych[15].

Na marginesie należy dodać, iż pracodawca jest obowiązany zapewnić, przy zastosowaniu odpowiednich środków technicznych i organizacyjnych, by uzyskiwane za pomocą monitoringu informacje o pracownikach były zabezpieczone przed udostępnianiem osobom nieupoważnionym. Ustawa o ochronie danych osobowych przewiduje w tym zakresie szereg wymogów, które pracodawca, organizując monitoring, powinien spełnić zarówno w zakresie personalnym oraz technicznym, jak i organizacyjnym (art. 36–39 ustawy o ochronie danych osobowych).

Niezależnie od przedstawionych stanowisk w przedmiocie uzyskania zgody pracownika na kontrolę świadczenia pracy, należy podkreślić, iż niewyrażenie przez pracownika zgody na kontrolę może być przyczyną uzasadniającą wypowiedzenie przez pracodawcę umowy o pracę, jeżeli pracodawca udowodni, że dana forma kontroli była niezbędna dla właściwego funkcjonowania zakładu pracy.

Reasumując, dla zapewnienia legalności kontroli konieczne jest wprowadzenie nie tylko przejrzystych reguł korzystania przez pracowników ze sprzętu służbowego[16], ale również poinformowanie pracownika o zamiarze jej przeprowadzenia przez pracodawcę (najlepiej na piśmie), natomiast obowiązek uzyskania zgody pracownika na objęcie go kontrolą będzie zależał od okoliczności danego przypadku, w tym w szczególności od istnienia prawnie usprawiedliwionych celów pracodawcy. Zarówno zakaz bądź ograniczenie korzystania przez pracowników ze sprzętu służbowego do celów prywatnych, jak i możliwość przeprowadzania okresowych kontroli wykonywania tego zakazu/ograniczenia mogą zostać wprowadzone przez pracodawcę w trakcie trwania stosunku pracy. W takim przypadku, zwłaszcza w sytuacji gdy pracownik miał nieograniczoną możliwość korzystania z powierzonego mu sprzętu do celów prywatnych, powyższe zmiany powinny być wprowadzane przez pracodawcę z zastosowaniem odpowiednich okresów przejściowych, dających pracownikowi możliwość dostosowania się do nowych zasad. W zależności od sposobu wprowadzenia tego rodzaju zmian — wobec każdego pracownika, którego te zmiany dotyczą, pracodawca powinien, w przypadku gdy zmianie ulega umowa o pracę, postąpić zgodnie z dyspozycją art. 29 § 4 k.p. i aneksować umowę o pracę, a w pozostałych przypadkach, dla celów dowodowych, odebrać od pracownika oświadczenie o zaznajomieniu się przez tego pracownika z nowymi zasadami.

Tajemnica korespondencji a poczta elektroniczna

Tajemnica korespondencji, stanowiąca dobro osobiste pracownika podlegające ochronie, dotyczy tylko i wyłącznie korespondencji prywatnej pracownika, natomiast poczta służbowa może być w sposób dowolny (oczywiście po uprzednim poinformowaniu pracownika o kontroli) monitorowana przez pracodawcę. Należy bowiem uznać, że pracownik prowadzi korespondencję e-mailową w imieniu pracodawcy, a skrzynka e-mailowa jest swoistym narzędziem jego pracy, powierzonym mu przez pracodawcę. Zatem pracodawca ma prawo wglądu do służbowej skrzynki pocztowej i nie stanowi to naruszenia dóbr osobistych pracownika. Należy jednak pamiętać, że jeśli pracodawca zezwoli pracownikowi na wykorzystywanie skrzynki pocztowej w celach prywatnych, wówczas w ramach kontroli nie może on przeglądać wiadomości zawierających treści prywatne, a tylko te mające charakter służbowy.

Pracodawca ma również, jak wskazano wyżej, prawo wprowadzić całkowity zakaz wykorzystywania służbowej skrzynki e-mailowej do celów prywatnych.

Należy podkreślić, iż uwagi odnośnie do monitorowania przez pracodawcę korespondencji e-mailowej pracowników zachowują aktualność w odniesieniu do rozmów telefonicznych. W konsekwencji pracodawca nie ma prawa podsłuchiwać prywatnych rozmów telefonicznych prowadzonych przez pracownika, natomiast w odniesieniu do rozmów służbowych, jako rozmów związanych z działalnością pracodawcy i prowadzonych w jego imieniu, decydują okoliczności konkretnego przypadku. Co do zasady pracodawca jest uprawniony do kontroli wykorzystania telefonów służbowych do celów związanych ze świadczeniem pracy, jednak powinien uprzedzić pracownika o możliwości przeprowadzenia takiej kontroli oraz poinformować go, iż nie powinien korzystać z telefonu służbowego do celów prywatnych[17].

Tajemnica przedsiębiorstwa pracodawcy

W praktyce kontrola skrzynek e-mailowych pracowników może stwarzać najwięcej problemów ze względu na możliwość naruszenia przez pracodawcę dóbr osobistych pracownika. Jednak w sytuacji, gdy mamy do czynienia z pracownikiem dopuszczonym przez pracodawcę do informacji stanowiących tajemnicę przedsiębiorstwa czy też do innego rodzaju poufnych, ważnych i wrażliwych danych — można w sposób indywidualny uregulować kwestie kontroli skrzynki pocztowej takiego pracownika i poinformować go, że kontrolą będą objęte także wiadomości mające charakter prywatny.

Zgodnie ze stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych, w sytuacji kiedy pracodawcy wprowadzą precyzyjne przepisy wewnątrzzakładowe dotyczące korzystania z poczty e-mailowej i w sposób właściwy przedstawią je pracownikom, nie muszą się obawiać zarzutów o naruszenie tajemnicy korespondencji pracowników. Należy jednak pamiętać, iż tego rodzaju działanie pracodawcy musi być uzasadnione jego ważnym interesem, zaś aby zabezpieczyć się przed ewentualnymi zarzutami ze strony pracownika, sugeruje się uzyskanie pisemnej zgody pracownika na przeglądanie przez pracodawcę wszystkich wiadomości w skrzynce pocztowej, w tym także tych mających charakter prywatny. Niezależnie jednak od zgody pracownika, należy mieć na uwadze, iż każdy przypadek powinien być analizowany indywidualnie, a ponieważ dobra osobiste pracownika są wartością chronioną, pracodawca musi być bardzo ostrożny w kontroli korespondencji prywatnej. Taka kontrola musi być każdorazowo uzasadniona ważnym interesem pracodawcy oraz okolicznościami danej sprawy (np. dostępem pracownika do informacji poufnych i niebezpieczeństwem ich wykorzystywania do celów prywatnych).

Środki kontroli przysługujące pracodawcy

W celu przeprowadzenia zgodnej z prawem kontroli, tj. po spełnieniu jej wymogów, o których była mowa wyżej (a w szczególności po uprzednim poinformowaniu pracowników o zamiarze przeprowadzenia kontroli sprzętu służbowego), pracodawca może zastosować, między innymi, następujące środki:

❒ tzw. oprogramowanie szpiegujące[18] — pracodawca ma techniczne możliwości zainstalowania na powierzonym pracownikowi sprzęcie, nie tylko komputerowym, ale również w telefonie komórkowym, iPadzie lub innym tego typu urządzeniu, oprogramowania, które umożliwia monitorowanie tego, co użytkownik danego sprzętu z nim robi; nie oznacza to, że prawnie są to metody w pełni dozwolone; przykładowo środkiem, który jest technicznie możliwy do zastosowania, ale który jest kwestionowany w doktrynie jako zbyt daleko ingerujący w prawa pracownika i naruszający jego prawo do prywatności oraz stanowiący przejaw kontroli totalnej, jest robienie przez pracodawcę tzw. zrzutów ekranowych co kilka/kilkanaście sekund, rejestrujących każdy ruch pracownika w komputerze; tego rodzaju działanie może być także potraktowane jako nieuprawnione rejestrowanie i gromadzenie danych osobowych pracownika;

❒ blokada stron internetowych — ma to znaczenie w sytuacji, gdy pracownicy mają nieograniczony dostęp do Internetu i korzystają z różnego rodzaju portali społecznościowych, komunikatorów internetowych i innych stron internetowych do celów prywatnych; w takiej jednak sytuacji całkowita blokada powinna być uzasadniona ważnym interesem pracodawcy, a jej zastosowanie nie powinno wpływać na możliwość prawidłowego wykonywania obowiązków pracowniczych;

❒ przeglądanie poczty elektronicznej — jak już szczegółowo opisano wyżej, pracodawca ma, co do zasady, prawo wglądu do poczty służbowej; wiadomości prywatne są poza zasięgiem pracodawcy i z wyjątkiem opisanych wcześniej przypadków pracodawca nie ma prawa ich przeglądać;

❒ podsłuch — w wyjątkowych sytuacjach podsłuch jest dopuszczalny, gdy oznacza on nagrywanie i odsłuchiwanie rozmów telefonicznych pracowników, których praca polega na odbywaniu rozmów z klientami, kontrahentami itp.; w takim przypadku działanie pracodawcy może być uzasadnione koniecznością kontroli jakości świadczenia pracy i zapewnienia prawidłowego sposobu jej wykonywania; zasadą jest jednak, że pracodawca nie ma możliwości zainstalowania w miejscu pracy podsłuchu i niepoinformowania o tym pracowników; takie działanie byłoby sprzeczne z prawem i naruszałoby dobra osobiste pracowników;

❒ wgląd do dokumentów służbowych — wszelkie dokumenty sporządzone przez pracownika stanowią własność pracodawcy; pracodawca ma prawo przeglądania tych dokumentów niezależnie od tego, czy znajdują się one w komputerze pracownika, czy na serwerze firmy; w przypadku, gdy pracownik zabezpieczy dokumenty hasłem, pracodawca ma prawo żądać, aby pracownik mu to hasło ujawnił; niemniej należy jednak pamiętać, że ww. uprawnienie pracodawcy nie rozciąga się na dokumenty prywatne przechowywane przez pracownika w komputerze służbowym (niezależnie od tego, czy przechowywanie takich dokumentów w komputerze służbowym jest w ogóle dopuszczalne, czy też nie);

❒ zakaz posiadania nośników danych — w celu ochrony danych pracodawcy zgromadzonych w komputerze służbowym bądź na serwerze firmowym, do którego pracownik ma dostęp, pracodawca może wprowadzić zakaz wnoszenia i używania w pracy wszelkiego rodzaju nośników danych — płyt CD, DVD, pamięci USB itp.;

❒ dostęp do danych bilingowych — pracodawca, jako podmiot opłacający rachunki za telefony służbowe, ma prawo do uzyskania wykazu połączeń jako abonent usług telekomunikacyjnych; nie jest on jednak uprawniony do przetwarzania danych dotyczących numerów wybieranych przez konkretnego pracownika, gdyż takie działanie godziłoby w przepisy ustawy o ochronie danych osobowych;

❒ stosowanie kamer — zastosowanie przez pracodawcę tego środka kontroli należy uznać za dopuszczalne, jeżeli ma on na celu zabezpieczenie pracodawcy przed rzeczywistymi bądź potencjalnymi działaniami pracowników, które wyrządzają lub mogą wyrządzić pracodawcy szkodę, jak również — co budzi największe kontrowersje — jeżeli celem pracodawcy jest zmotywowanie pracowników do wydajniejszej pracy i działanie to zastępuje inne formy działań mających na celu zwiększenie wydajności i efektywności pracy; możliwe zatem jest zastosowanie przez pracodawcę omawianej metody przy łącznym spełnieniu następujących warunków[19]:

— nie jest dopuszczalne instalowanie kamer w miejscach, gdzie pracownik bądź też inna osoba (np. klient) może zasadnie oczekiwać zachowania swojej prywatności,

— o monitoringu należy uprzedzić osoby, które mogą znaleźć się w jego zasięgu — pracownik powinien mieć świadomość, jakie miejsca są monitorowane,

— zapisy obrazu powinny być przechowywane jedynie przez czas niezbędny dla celów monitorowania i w warunkach zabezpieczających je przed dostępem osób niepowołanych — niezachowanie wymogów bezpieczeństwa i ochrony danych może narazić pracodawcę na odpowiedzialność karną przewidzianą przepisami ustawy o ochronie danych osobowych.

Powyższe wyliczenie ma charakter jedynie przykładowy. W praktyce działy IT przedsiębiorców z reguły dostosowują sposoby i formy przeprowadzania kontroli i monitoringu sprzętu komputerowego pracowników do potrzeb danego pracodawcy. Należy jednak pamiętać, że każde z rozwiązań zaproponowanych przez dział IT powinno być wdrażane przy zastosowaniu zasad, o których była mowa wyżej (w szczególności zasady uprzedniego poinformowania pracowników o kontroli).

Jednocześnie należy wskazać, iż kwestia tego, kto osobiście będzie przeprowadzał kontrolę pracownika (czy będzie to np. menedżer, kierownik działu czy informatyk) również nie jest uregulowana prawnie. W sytuacji, gdy zgodnie z założeniami polityki firmowej zakłada się, iż kontrole tego rodzaju mają być wykonywane

przez dwie osoby, sugeruje się, aby w momencie informowania pracownika o kontroli wskazać również nazwiska osób, które tę kontrolę przeprowadzą, lub też kwestia ta może być uregulowana ogólnie w przepisach wewnątrzzakładowych. Niemniej jednak, nawet w przypadku, gdy tego rodzaju wskazania nazwisk nie będzie, a zostaną spełnione inne warunki kontroli, należy uznać, iż będzie ona przeprowadzona legalnie. Jak się wydaje, jedną z osób przeprowadzających kontrolę powinna być osoba upoważniona przez pracodawcę (czyli przez zarząd) do wykonywania w jego imieniu czynności z zakresu prawa pracy.

Konsekwencje złamania zakazów przez pracownika

Kary porządkowe

W przypadku złamania przez pracownika zakazów/ograniczeń ustalonych przez pracodawcę, a dotyczących powierzonego mu sprzętu komputerowego, pracodawca może wyciągnąć wobec pracownika odpowiednie konsekwencje służbowe. Przy czym w każdej sytuacji, gdy pracodawca sięga po kary porządkowe, musi je stosować uwzględniając okoliczności faktyczne danej sprawy, jak też treść przepisów wewnątrzzakładowych obowiązujących u pracodawcy lub treść oświadczeń złożonych przez pracownika dotyczących powierzonego mu sprzętu.

W sytuacji, gdy zakaz używania sprzętu komputerowego do celów prywatnych został w sposób jasny pracownikowi zakomunikowany, a po przeprowadzeniu kontroli okaże się, iż pracownik zakaz ten złamał, pracodawcy przysługuje możliwość nałożenia na pracownika kary porządkowej. Zgodnie z art. 108 § 1 k.p. karami tymi są nagana i upomnienie. Należy jednak pamiętać, że kara nie może być zastosowana po upływie 2 tygodni od powzięcia przez pracodawcę wiadomości o naruszeniu obowiązku pracowniczego i po upływie 3 miesięcy od dopuszczenia się tego naruszenia. Przed wymierzeniem kary pracownikowi należy go wysłuchać, a informacja o nałożonej karze powinna być włączona do akt osobowych danego pracownika.

Rozwiązanie umowy o pracę

W szczególnych sytuacjach, gdy używanie sprzętu komputerowego do celów prywatnych wpływa na jakość czy ilość pracy, pracodawca może rozwiązać z pracownikiem umowę o pracę za wypowiedzeniem (art. 32 k.p.), a w wyjątkowych przypadkach bez wypowiedzenia (art. 52 § 1 k.p.).

Pracodawca może rozważać rozwiązanie umowy z pracownikiem (w zależności od konkretnego przypadku za wypowiedzeniem lub bez wypowiedzenia) w następujących, przykładowo wskazanych, sytuacjach:

- gdy pracownik naruszył obowiązki pracownicze, np. mimo zakazu używania sprzętu do celów prywatnych złamał blokady stron internetowych i używał komputera do wykonywania zadań niezleconych przez pracodawcę, a w szczególności korzystania z portali społecznościowych lub świadczenia innej pracy za pomocą Internetu, przez co w sposób znaczący i długotrwały spadała jego wydajność;
- gdy w czasie trwania umowy o pracę doszło do popełnienia przez pracownika przestępstwa, które uniemożliwia dalsze zatrudnianie go na zajmowanym stanowisku, jeżeli przestępstwo to jest oczywiste lub zostało stwierdzone prawomocnym wyrokiem.

W jednym z wyroków Sąd Najwyższy uznał, że: „korzystanie przez pracownika z telefonu służbowego w celu udziału w grach towarzyskich, narażające pracodawcę na znaczną szkodę, może być zakwalifikowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych (art. 52 § 1 pkt 1 k.p.)”[20]. W kolejnym wyroku Sąd Najwyższy stwierdził, że korzystanie przez pracownika, zwłaszcza na kierowniczym stanowisku, z firmowego komputera i oprogramowania w celu osiągnięcia korzyści w ramach własnej działalności gospodarczej, jest ciężkim naruszeniem podstawowych obowiązków pracowników[21].

Warto podkreślić, że aby można było uznać, iż zachowanie pracownika polegające na używaniu służbowego sprzętu do celów prywatnych stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych, powinno ono występować przez dłuższy okres i mieć charakter ciągły, a co za tym idzie: „jednorazowe skorzystanie przez pracownika z laptopa pracodawcy na potrzeby osobiste nie uzasadnia zwolnienia w trybie dyscyplinarnym”[22].

Wskazuje się także, iż notoryczne przeglądanie stron internetowych w godzinach pracy w celach prywatnych może w pewnych sytuacjach stanowić uzasadnioną przyczynę wypowiedzenia pracownikowi umowy o pracę, zaś jako przykład podaje się sytuację, gdy pracownik przez okres dwóch tygodni zajmuje się w godzinach pracy przeglądaniem stron internetowych w celach prywatnych i w tym czasie, w opinii pracodawcy i w oparciu o posiadane przez pracodawcę dowody, pracuje nieefektywnie. Jednak każdorazowo należy uwzględnić okoliczności wpływające na ten stan faktyczny, może się bowiem okazać, że niewykonywanie pracy w ww. okresie nie było zawinione przez pracownika, a leżało po stronie pracodawcy.

Źródło informacji o przyczynie wypowiedzenia umowy o pracę

Problematyczna pozostaje kwestia, czy pracodawca wypowiadając pracownikowi umowę o pracę (czy też rozwiązując stosunek pracy bez wypowiedzenia) ma prawo uczynić to z przyczyny, o której dowiedział się w nieuprawniony sposób (np. poprzez naruszenie tajemnicy korespondencji). Wydaje się, iż takie postępowanie pracodawcy nie powinno mieć miejsca, aczkolwiek praktyka przedstawia się zgoła odmiennie. W takiej sytuacji pracownik ma jednak prawo złożyć odwołanie do sądu pracy. W toku ewentualnego postępowania sądowego po stronie pracodawcy leży obowiązek wykazania, iż przyczyna rozwiązania stosunku pracy podana pracownikowi faktycznie zaistniała.

Powstaje pytanie, czy pracodawca może udowodnić fakt wystąpienia ww. przyczyny poprzez odwołanie się do bezprawnie nagranych rozmów pracowników czy uzyskanych dokumentów. Żaden przepis procedury cywilnej nie reguluje wprost problemu dopuszczalności takich dowodów. Z art. 227 k.p.c. wynika, iż przedmiotem dowodu mogą być wszelkie fakty mające dla rozstrzygnięcia sprawy istotne znaczenie. Ponadto, zgodnie z art. 309 k.p.c., można posługiwać się wszelkimi środkami dowodowymi, nawet jeśli nie zostały wprost wymienione w przepisach procedury cywilnej. Formalnie więc przepisy procedury cywilnej dopuszczają powoływanie się przez strony na omawiane dowody. Niemniej jednak trzeba mieć na uwadze, iż niezależnie od zasad omawianej kontroli wkraczanie w sferę prywatności pracownika może być uznane za sprzeczne z zasadami współżycia społecznego, normami etycznymi i dobrymi obyczajami.

W wyroku z 6 lipca 1999 r. Sąd Apelacyjny w Warszawie stwierdził, iż gromadzenie materiału dowodowego w procesie i prezentowanie go przez strony nie powinno odbywać się z naruszeniem zasad współżycia społecznego[23]. Sąd Najwyższy zaś uznał, że nie ma zasadniczych powodów do całkowitej dyskwalifikacji dowodu np. z nagrań rozmów telefonicznych, nawet gdy nagrań tych dokonywano bez wiedzy drugiej strony[24]. Jako wiodący należy uznać pogląd, zgodnie z którym co do zasady dowody z podsłuchów, zapisów rozmów telefonicznych, monitoringu czy cudzej korespondencji, jeśli zostały uzyskane bez zgody zainteresowanego, nie powinny być dopuszczone w postępowaniu cywilnym. Działanie podjęte w celu ich uzyskania narusza dobra osobiste: tajemnicę korespondencji i prawo do prywatności. Sąd jednak może dopuścić takie dowody, jeśli uzyskujący je działał w obronie usprawiedliwionego interesu prywatnego, a interes ten przedstawia wartość znacznie wyższą niż ochrona prywatności i tajemnicy komunikowania się osoby, której dobra zostały naruszone.

Środki obrony prawnej posiadane przez pracownika

W przypadku naruszenia dóbr osobistych pracownika

Zgodnie z art. 111 k.p. pracodawca jest zobowiązany szanować godność i inne dobra osobiste pracownika. Należy bowiem pamiętać, iż monitoring pracownika może być niejednokrotnie uznany za ingerencję pracodawcy w sferę praw osobistych pracownika (w szczególności naruszenie jego prawa do prywatności czy tajemnicy korespondencji), co może pociągnąć za sobą negatywne konsekwencje dla pracodawcy. W szczególności, w przypadku bezprawnego przeglądania przez pracodawcę prywatnych wiadomości pracownika (mimo iż znajdują się one w służbowej skrzynce e-mailowej), pracownikowi przysługuje prawo do złożenia skargi do Generalnego Inspektora Ochrony Danych Osobowych, w trybie przewidzianym w ustawie o ochronie danych osobowych, lub wytoczenia powództwa cywilnego o ochronę dóbr osobistych.

W myśl art. 24 k.c. w ramach postępowania cywilnego pracownik może się domagać:

- w razie zagrożenia dobra osobistego działaniem pracodawcy — zaniechania bezprawnego działania pracodawcy;
- w razie dokonanego już naruszenia:
  - — dopełnienia czynności potrzebnych do usunięcia jego skutków (w szczególności, aby osoba, która dopuściła się naruszenia, złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie),
  - — zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny,
  - — naprawienia szkody przez pracodawcę na zasadach ogólnych (jeżeli wskutek naruszenia dobra osobistego pracownikowi została wyrządzona szkoda majątkowa).

Odpowiedzialność karna pracodawcy

Dodatkowo, na marginesie, należy wskazać, że zgodnie z art. 267 § 1 k.k.: „kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". W świetle poglądów doktryny nie stanowi przestępstwa z art. 267 zapoznanie się z pocztą mailową gromadzoną na serwerze, chyba że następuje to poprzez przełamanie kodu szyfrującego treść poczty[25]. Tak więc w przepisie tym chodzi wyłącznie o takie otwarcie zamkniętego pisma, które wymaga usunięcia zabezpieczeń. Przeglądanie korespondencji zamieszczonej w pamięci komputera, o ile nie jest zabezpieczona hasłem, nie stanowi przestępstwa z art. 267 § 1 k.k.

Niemniej jednak należy mieć na uwadze, iż każdy przypadek musi być analizowany indywidualnie i w zależności od sposobu działania pracodawcy, od systemu zabezpieczeń sprzętu służbowego czy też od charakteru informacji gromadzonych przez pracownika, może zależeć wypełnienie znamion czynu zabronionego.

Ponadto należy podkreślić, iż na mocy art. 218 k.k. karze podlega pracodawca, który złośliwie lub uporczywie narusza prawa pracownika wynikające ze stosunku pracy.

Podsumowanie

Zarówno dopuszczalność, jak i granice poszczególnych kompetencji kontrolnych pracodawcy nie zostały uregulowane wprost w żadnym akcie prawnym. Analogicznie wygląda kwestia ochrony prawa pracowników poddawanych różnym formom kontroli. Jednocześnie rozwój techniki i brak adekwatnych regulacji prawnych wyznaczających ramy dopuszczalnej kontroli pracowników przez pracodawców stwarza i będzie nadal powodował

spory nie tylko natury teoretycznej, ale i praktycznej. To, czy ramy prawne tej kontroli powinny wynikać z przepisów rangi ustawowej, czy powinny być raczej stanowione przez autonomiczne prawo pracy, a w szczególności regulaminy pracy czy też układy zbiorowe, jest kwestią drugorzędną.

Podstawowymi warunkami dopuszczalnej kontroli pracowników jest proporcjonalność podjętych przez pracodawcę środków do osiągnięcia wyznaczonych celów oraz jasne, przejrzyste reguły kontroli podane do wiadomości pracowników, a w niektórych przypadkach stosowane pod warunkiem uzyskania na nie zgody każdego z pracowników, objętego monitoringiem.

Pracodawca może wprowadzić zakaz lub ograniczenie dotyczące używania przez pracowników powierzonego im sprzętu do celów prywatnych. O tego rodzaju zakazie/ograniczeniu pracownik musi zostać poinformowany przez pracodawcę bądź to w formie wprowadzenia odpowiednich przepisów wewnątrzzakładowych, bądź też indywidualnie, poprzez wprowadzenie stosownych zapisów do umów o pracę lub zebranie oświadczeń od pracowników o przyjęciu ww. zakazu do wiadomości.

Tajemnica korespondencji, stanowiąca dobro osobiste pracownika podlegające ochronie, dotyczy tylko i wyłącznie korespondencji prywatnej pracownika, natomiast poczta służbowa może być w sposób dowolny przez pracodawcę monitorowana.

W sytuacji, gdy zakaz używania sprzętu do celów prywatnych został w sposób jasny pracownikowi zakomunikowany, a po przeprowadzeniu kontroli okaże się, iż pracownik zakaz ten złamał, pracodawca ma możliwość nałożenia na pracownika kary porządkowej w postaci nagany lub upomnienia. W uzasadnionych interesem pracodawcy okolicznościach pracodawca może również rozwiązać z pracownikiem umowę o pracę.

W przypadku przeprowadzenia przez pracodawcę bezprawnej kontroli pracownika, w tym jego prywatnych wiadomości e-mailowych (mimo iż znajdują się w służbowej skrzynce e-mailowej), pracownikowi przysługuje możliwość złożenia skargi do Generalnego Inspektora Ochrony Danych Osobowych, w trybie przewidzianym w ustawie o ochronie danych osobowych, lub wytoczenia powództwa cywilnego o ochronę dóbr osobistych.

Przypisy

[1] DzU z 1998 r. nr 148, poz. 973. Zgodnie z pkt. 10 lit. e załącznika określającego minimalne wymagania bezpieczeństwa i higieny pracy oraz ergonomii, jakie powinny spełniać stanowiska pracy wyposażone w monitory ekranowe.

[2] W myśl art. 11 ust. 4 ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (DzU z 2003 r. nr 153, poz. 1503 z późn. zm.) przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

[3] Podstawą dochodzenia roszczeń cywilnych od spółki może być, między innymi, art. 79 ustawy z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, DzU z 2006 r, nr 90, poz. 631 z późn. zm.

[4] Ustawa z 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (DzU z 2012 r. nr 769) w art. 16 ust. 1 pkt 11 przewiduje odpowiedzialność podmiotu zbiorowego za czyny przeciwko własności intelektualnej zabronione pod groźbą kary, określone w art. 115–118[1] prawa autorskiego. Karą przewidzianą dla podmiotu zbiorowego za przestępstwo osoby fizycznej jest nałożenie kary pieniężnej w wysokości do 5% przychodu określonego w trybie przepisów o podatku dochodowym od osób prawnych, osiągniętego w roku podatkowym poprzedzającym wydanie orzeczenia lub wydatków poniesionych w roku poprzedzającym wydanie orzeczenia, jeśli przychód jest niższy niż 1 mln zł.

[5] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (DzU nr 78, poz. 483 z późn. zm.), ustawa z 23 kwietnia 1964 r. Kodeks cywilny (DzU nr 16, poz. 93 z późn. zm.), ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (DzU z 2002 r. nr 101, poz. 926 z późn. zm.), ustawa z 6 czerwca 1997 r. Kodeks karny (DzU nr 88, poz. 553 z późn. zm.).

[6] M. Skąpski, *Wpływ pracowniczego obowiązku dbałości o dobro zakładu pracy na zakres kompetencji pracodawcy do kontrolowania pracownika* (w:) *Kontrola pracownika. Możliwości techniczne i dylematy prawne*, red. Z. Góral, Warszawa 2010, s. 75.

[7] H. Szewczyk, *Ochrona dóbr osobistych w zatrudnieniu*, Warszawa 2007, s. 122 i n.

[8] Pogląd wyrażony w: M. Safjan, *Prawo do ochrony życia prywatnego* (w:) *Szkoła Praw Człowieka*, Helsińska Fundacja Praw Człowieka, Warszawa 2006, s. 214.

[9] Zgodnie z pkt. 10 lit. e załącznika do rozporządzenia Ministra Pracy i Polityki Socjalnej z 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe.

[10] Za istnieniem obowiązku uprzedniego poinformowania pracowników o kontroli opowiedział się Sąd Najwyższy w wyroku z 13 kwietnia 1972 r. (sygn. akt I PR 153/72, OSNC 1972/10/184), który, co prawda, zapadł pod rządami starego kodeksu pracy i na tle innego stanu faktycznego, ale potwierdza, że przeszukiwanie członków załogi w celu zapobieżenia wynoszeniu mienia zakładu pracy jest zgodne z prawem i nie narusza dóbr osobistych pracowników, o ile pracownicy zostali uprzednio poinformowani o możliwości stosowania tego rodzaju kontroli.

[11] Wyrok Europejskiego Trybunału Praw Człowieka z 3 kwietnia 2007 r., sprawa Copland przeciwkoko Wielkiej Brytanii, nr 62617/00.

[12] O problematyce stosowania przez pracodawcę nowoczesnych technologii nadzoru nad zatrudnionymi dyskutowano w dniu 17 lutego 2011 r. Organizatorami spotkania byli Kolegium Prawa ALK, Generalny Inspektor Ochrony Danych Osobowych oraz Prawnicze Koło Naukowe Summa Sapientia. Tematy wystąpień i wypowiedzi dotyczyły między innymi problematyki wykorzystywania przez pracodawców no-

woczesnych technologii nadzoru nad pracownikami, takich jak: monitoring audiowizualny, GPS, podsłuchiwanie i nagrywanie rozmów telefonicznych oraz wykorzystywanie danych biometrycznych pracownika (m.in. linii papilarnych). W czasie spotkania zastanawiano się również nad propozycją prawnego uregulowania kwestii będących przedmiotem dyskusji. Za rozsądny uznano postulat przeprowadzenia wnikliwych badań, debaty naukowej i konsultacji społecznych przed wprowadzeniem zmian w prawie pracy dotyczących obszaru danych osobowych. Informacja dostępna na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych: http://www.giodo.gov.pl/1520101/-id_art/3950/j/pl/

[13] Zgodnie z odpowiedzią Ministra Pracy i Polityki Społecznej z 21 grudnia 2009 r. na interpelację poselską nr 12970 w sprawie zasad montowania monitoringu w zakładach pracy.

[14] Por. D. Döre-Nowak, *Monitoring w miejscu pracy a prawo do prywatności*, „Praca i Zabezpieczenie Społeczne" 2004, nr 9; M. Szczepanek, *Prawo pracownika do prywatności a monitoring w miejscu pracy* (dostęp: 1.03. 2013). Dostępny w Internecie: http://www.e-ochronadanych.pl/a, 306, prawo-pracownika-do-prywatnosci-a-monitoring-w-miejscu-pracy.html

[15] Wyrok Naczelnego Sądu Administracyjnego z 4 kwietnia 2003 r., II SA 2135/02, „Wokanda" 2004/6/30.

[16] H. Szewczyk, *Ochrona dobór osobistych a podstawowe formy kontroli pracowników* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2011, z. 3.

[17] M. Szczepanek, jw.

[18] Programy szpiegujące (ang. *spyware*) to programy komputerowe, których celem jest obserwacja działań użytkownika. Rodzajem takiego oprogramowania jest *Mobile Software Spy*, które w niezauważalny sposób monitoruje całą aktywność posiadacza telefonu komórkowego lub iPada. Pozwala, w zależności od opcji, na, między innymi, rejestrowanie rozmów i dźwięków w jego otoczeniu, podsłuch w czasie rzeczywistym, przesyłanie kopii wiadomości.

[19] A. Lach, *Monitorowanie pracownika w miejscu pracy*, „Monitor Prawa Pracy" 2004, nr 10.

[20] Wyrok Sądu Najwyższego z 15 maja 1997 r., I PKN 93/97, OSNP 1998/7/208.

[21] Wyrok Sądu Najwyższego z 6 lipca 2011 r., II PK 13/11, „Monitor Prawa Pracy" 2011/10/539–541.

[22] Wyrok Sądu Najwyższego z 4 listopada 2010 r., II PK 110/10, LEX nr 678013.

[23] Wyrok Sądu Apelacyjnego w Warszawie z 6 lipca 1999 r., I ACa 380/99, OSA 2001/4/21.

[24] Wyrok Sądu Najwyższego z 25 kwietnia 2003 r., IV CKN 94/01, LEX nr 80244.

[25] W. Wróbel, *Komentarz do art. 267 Kodeksu karnego*, stan prawny: 2006.03.2001, LEX.

Summary

Equipping an employee with specific working tools aims at the providing an optimal organisation of the working process. Such tools should be used by the employee to carry out his/her professional duties entrusted by the employer and the fact whether this is indeed the case may be controlled by the employer. Both the admissibility and the boundaries of individual powers of control of the employer have not been governed directly in any legislation. The same applies to the protection of employee rights subjected to various forms of control. At the same time, the development of technology and the lack of adequate regulations, setting out a framework for acceptable employee controls by employers, creates and will continue to create disputes not only theoretical in nature, but also practical. The author attempts to specify and point the legal framework of controlling employees, referring to the judicial practice and the legal doctrine, concluding that the prerequisites for acceptable employee control are: the proportionality of measures taken by the employer to achieve its objectives and clear, transparent rules for control communicated to the employees and, in some cases, obtaining a consent of each employee covered by surveillance.