Przegląd Prawniczy Uniwersytetu Warszawskiego
ISSN 1644-0242
Rok XVII, nr 1/2018
DOI 10.26330/ppuw.2018.01.08

*Dominika Kuźnicka**

Monitorowanie pracownika w miejscu pracy a ochrona prywatności

Monitorowanie pracowników w miejscu ich pracy[1] to zjawisko powszechne i wydaje się, że społecznie akceptowalne. Pracodawcy często wprowadzają narzędzie zwiększonej kontroli z prostych i zrozumiałych przyczyn: chcą zwiększyć efektywność pracowników, sprawdzić, czy pracownicy w godzinach pracy wykonują zlecone im zadania lub by przeciwdziałać kradzieżom i agresywnym zachowaniom. Pomimo, że monitoring wykonywany na zlecenie pracodawcy często ma uzasadnione podstawy, pojawia się obawa, że w dobie nowoczesnych technologii, narzędzia do tego wykorzystywane mogą ograniczać prywatność pracowników. Jeszcze kilka czy kilkanaście lat temu kontrola pracowników sprowadzała się jedynie do sprawdzenia, czy pracownik nie przebywa zbyt długo na przerwie śniadaniowej, a w najgorszym przypadku dotyczyła sprawdzenia stanu trzeźwości w miejscu pracy. Obecnie w większości zakładów pracy duża część czynności wykonywanych przez pracowników związana jest z użyciem Internetu. W związku z tym zmienił się nie tylko zakres kontroli, ale również możliwości techniczne pracodawcy, które mogą być wykorzystane w celu sprawdzenia efektywności czy uczciwości pracowników. Monitorowanie poczty prywatnej i służbowej pracowników, instalowanie kamer w miejscu pracy, wykorzystywanie narzędzi geolokalizacyjnych w pojazdach służbowych czy prześwietlanie historii internetowej przeglądarki, mogą naruszyć prawo do prywatności pracowników.

W związku z powyższym pojawiają się pytania, jaki jest zakres dozwolonego monitoringu dokonywanego przez pracodawcę oraz jakie warunki powinien on spełnić, aby ograniczyć możliwość naruszenia

* Uniwersytet Wrocławski, Wydział Prawa i Administracji, ul. Uniwersytecka 22/26, 50-145 Wrocław, e-mail: dominika.kuznicka@uwr.edu.pl.

[1] Za miejsce pracy w niniejszym opracowaniu uznaje się miejsce świadczenia pracy (zarówno jako stały punkt w znaczeniu geograficznym bądź pewien oznaczony obszar) obustronnie uzgodniony, objęty ogólnym zakazem jednostronnej zmiany przez którąkolwiek ze stron [za:] W. Muszalski, *Komentarz do art. 29 Kodeksu pracy* [w:] *Kodeks pracy: komentarz*, red. W. Muszalski, Warszawa 2011, s. 59.

prawa pracownika do prywatności. Obowiązujące przepisy prawne nie zawierają konkretnych norm prawnych, które w sposób całościowy regulowałyby tę tematykę. Ogólne założenia znajdują się w Kodeksie pracy[2] i ustawie o ochronie danych osobowych[3] , jednocześnie duże znaczenie ma praktyka orzecznicza nie tylko sądów krajowych, ale przede wszystkim Europejskiego Trybunału Praw Człowieka (dalej: ETPC), który wielokrotnie pochylał się nad zagadnieniem zakresu dozwolonego monitoringu w miejscu pracy.

1. Monitoring pracowników – definicja i rodzaje

Za monitorowanie pracowników uważa się takie czynności, które zostały przedsięwzięte w celu zgromadzenia informacji o zatrudnionych pracownikach poprzez poddawanie ich w sposób jawny lub ukryty obserwacji, czy to w sposób bezpośredni czy poprzez wykorzystanie urządzeń elektronicznych[4]. Spośród najbardziej popularnych czynności kontrolnych należy wymienić: kontrolę za pomocą kamer umieszonych na terenie zakładu pracy, kontrolę poczty elektronicznej (prywatnej oraz służbowej), kontrolę odwiedzanych stron www, kontrolę przemieszczania się pracowników przy użyciu urządzeń GPS, kontrolę połączeń telefonicznych. Praktycy wyróżniają następujące rodzaje monitoringu pracowników: monitoring proaktywny, który nastawiony jest na działania prewencyjne, mający na celu ocenę wydajności pracownika oraz monitoring reaktywny, podejmowany dopiero po uzyskaniu informacji o zachowaniu niezgodnym z prawem[5]. Z uwagi na czas, w jakim prowadzony jest monitoring można wyróżnić monitoring ciągły i okresowy, a biorąc pod uwagę fakt poinformowania pracownika o stosowanych narzędziach kontroli – monitoring jawny i ukryty. W doktrynie coraz częściej postuluje się, aby terminu „monitoring" używać jedynie do kontroli wykonywanej przy

---

[2] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2018 r. poz. 108).

[3] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) – dalej: Ustawa o ochronie danych osobowych.

[4] Zob. A. Lach, *Monitorowanie pracownika w miejscu pracy,* MoPr 2004, Nr 10, s. 264 [za:] UK Information Commissioner, *The Employment Practices Data Protection Code*, cz. 3, *Monitoring at Work*.

[5] Tamże.

wykorzystaniu urządzeń elektronicznych, stąd też za monitoring uważa się kontrolowanie poczty e-mail, a tradycyjnej korespondencji – nie[6].

Jednocześnie należy wskazać, że pracodawcy stosują narzędzia monitoringu w celach m.in.:

1) wykrywania i zapobiegania przestępstwom, w tym nadzoru nad mieniem pracodawcy i jednoczesną prewencję w zakresie czynności zabronionych, które mogłyby być podejmowane przez pracowników w odniesieniu do tego mienia;
2) podjęcia działań, które mają na celu ochronę tajemnicy przedsiębiorstwa; zapewnienia odpowiedniej jakości i efektywności wykonywanej pracy;
3) zabezpieczenia pobierania z Internetu treści niedozwolonych bądź takich, których przeniknięcie do systemu komputerowego pracodawcy mogą skutkować jego zainfekowaniem przez wirusy bądź inne programy szpiegowskie;
4) uniknięcia naruszenia dobrego imienia pracodawcy.

W doktrynie podnosi się, że czynności kontrolne powinny być pozbawione cech zamierzonej indywidualnej dolegliwości i zmierzać wyłącznie do skutecznej ochrony mienia pracodawcy, które może być narażone na uszczerbek[7]. Monitorowanie musi mieć swoje uzasadnienie (odpowiednik zasady konieczności)[8]. Pracodawcy mogą również skorzystać z dostępnych w zakładzie urządzeń elektronicznych, używanych przez pracownika w przypadku, nawet usprawiedliwionej, nieobecności w pracy. Uzyskane przez pracodawcę w ten sposób informację mogą wykazać, że pracownik prowadził działalność niezgodną z interesem pracodawcy lub z prawem, a w konsekwencji doprowadzić do zastosowania względem pracownika środków odpowiedzialności karnej, cywilnej czy pracowniczej[9].

W doktrynie wciąż przeważa pogląd wyrażający konieczność poinformowania pracownika o wykorzystywaniu narzędzi monitoringu w miejscu

---

[6] Zob. M. Wujczyk, *Prawo pracownika do ochrony prywatności*, Warszawa 2012.

[7] Por. P. Wąż, *Kontrola osobista pracownika*, Atest 2008, Nr 1, s. 4.

[8] Zob. A. Lach, *Glosa do orzeczenia ETPC w sprawie Copland przeciwko Zjednoczonemu Królestwu*, MoPr 2007, Nr 7, s. 17.

[9] A. Lach, *Monitorowanie…*, s. 265.

pracy osobiście bądź przez wprowadzenie odpowiednich postanowień w regulacjach wewnątrzzakładowych[10]. Jednocześnie Europejski Trybunał Praw Człowieka w swoim orzecznictwie wskazuje również na sytuacje, kiedy poinformowanie pracownika nie jest warunkiem koniecznym. Taki wyrok zapadł w 2010 r. w sprawie *Kopke v. Niemcy*[11]. Trybunał orzekł, że pracodawca jest zwolniony z obowiązku poinformowania pracownika o stosowaniu monitoringu w sytuacji, gdy ma on uzasadnione podejrzenie, że działalność pracownika jest wymierzona w dobro zakładu pracy, a zastosowane środki monitoringu mają na celu wykrycie czynu zabronionego lub zapobieżenie jego skutkom, a cel ten nie może być osiągnięty przy użyciu innych, mniej inwazyjnych metod. Co do zasady jednak, źródeł zasad przeprowadzania kontroli należy poszukiwać w prawie pracownika do poszanowania jego godności i prywatności[12].

O konieczności nie tylko poinformowania pracownika o stosowanych narzędziach monitoringu, ale wręcz o obowiązku uzyskania oświadczenia pracowników o akceptacji prowadzonych przez pracodawcę działań wypowiadał się Naczelny Sąd Administracyjny[13]. Wskazywał on, że wymogiem ważności prowadzonej kontroli przy wykorzystaniu środków elektronicznych, jest przede wszystkim zgodność tych działań z prawem, usprawiedliwiony cel, proporcjonalność, transparentność oraz uwzględnienie przepisów o ochronie danych osobowych. Szczególnie istotną rolę odgrywa świadomość pracowników, że są poddawani monitoringowi, a pracodawca powinien szczegółowo określić zasady prowadzonej kontroli i zapoznać z nimi personel, a następnie uzyskać od każdej osoby potwierdzenie w postaci złożonego na piśmie oświadczenia o ich akceptacji.

Wśród sposobów używanych przez pracodawców w celu kontroli działalności pracownika można wymienić m.in. kontrolę rozmów

---

[10] Zob. P. Litwiński, *Prywatność w miejscu pracy. Refleksje z perspektywy 25 lat* [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość,* red. A. Mednis, Warszawa 2016, s. 49.

[11] Orzeczenie ETPC z 5 października 2010 r., Nr 420/07, *Kopke v. Niemcy* [za:] D. Głowacka, *Prywatność w miejscu pracy w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka* [w:] *Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych. Stan obecny i perspektywy zmiany*, red. T. Wyka, A. Nerka, Warszawa 2012, s. 50.

[12] Por. M. Wujczyk, *Prawo pracownika do ochrony prywatności*, Warszawa 2012, s. 255.

[13] Zob. Wyrok NSA z dnia 13 lutego 2015 r., I OSK 2436/12.

telefonicznych, odwiedzanych stron internetowych, stały monitoring ekranu komputera pracownika, kontrolę poczty e-mail oraz używanie narzędzi pozwalających określić aktualną lokalizację pracownika.

2. Ochrona prywatności i monitoring pracowników w miejscu pracy

Dotychczas jednym z podstawowych przepisów w zakresie ochrony prywatności pracownika, po które chętnie sięgały organy polskie i europejskie był art. 8 Europejskiej Konwencji Praw Człowieka[14]. Zgodnie z jego brzmieniem, każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez prawo i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

Co do zasady, prawo określone w art. 8 EKPC nie jest bezwzględnie chronione i nie można z niego korzystać w każdych okolicznościach. Ma ono przede wszystkim chronić jednostkę przed działaniem organów państwowych, ale również tworzy zobowiązanie pozytywne zapewnienia skutecznego poszanowania życia prywatnego i rodzinnego (domu i korespondencji). W orzecznictwie ETPC podkreśla się, że gwarancje zawarte w omawianym artykule mają na celu umożliwienie rozwoju (bez ingerencji z zewnątrz) osobowości jednostki w jej stosunkach z innymi istotami ludzkimi. Analiza orzecznictwa związanego z ochroną prywatności pracowników w miejscu pracy zostanie przedstawiona w dalszej części niniejszego opracowania.

25 maja 2018 r. weszło w życie Rozporządzenie 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

[14] Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami Nr 3, 5 i 8 oraz uzupełnionej Protokołem Nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284).

95/46 WE[15]. Zakres zmian nim wprowadzonych wymagał również nowelizacji krajowej ustawy o ochronie danych osobowych, która została uchwalona 10 maja 2018 r.

Na gruncie RODO, przetwarzanie danych osobowych pracownika (a nie ma wątpliwości, że monitoring pracowników jest przetwarzaniem danych)[16] możliwe jest wtedy, gdy zostaną spełnione przesłanki wskazane w art. 5 i 6. Przetwarzanie danych może odbywać się jedynie zgodnie z prawem, rzetelnie i przejrzyście, musi być ograniczone do określonego celu, a zakres danych powinien być zminimalizowany tylko do danych niezbędnych dla danego celu, zbierane dane powinny być prawidłowe i aktualne, a zakres ich przechowywania ograniczony. Dane powinny być ponadto przechowywane w sposób zapewniający ich integralność i poufność. Dane mogą być przetwarzane tylko i wyłącznie jeśli zostanie spełniona jedna z przesłane zawartych w art. 6 RODO. W zakresie niniejszego opracowania najważniejsze wydają się być zgoda osoby, której dane dotyczą i niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem[17].

---

[15] Rozporządzenie 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – dalej: RODO (Dz.Urz. L 119 z 4 maja 2016).

[16] W myśl RODO „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, za utrwalanie, zgodnie z definicją „utrwalać" znaczy „rejestrować dźwięki, obrazu na taśmach, płytach w pamięci komputera czy zapisanie tekstu w celu ich późniejszego odtworzenia" (Zob. *Mały Słownik Języka Polskiego* PWN, Warszawa 2000 r., s. 1098), zatem bez wątpienia czynności wchodzące w skład omawianego monitoringu, można uznać za przetwarzanie danych osobowych.

[17] Pozostałe warunki wskazane w art. 6 RODO to: przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy, przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby,

Korzystanie przez administratora danych (pracodawcę) z przesłanki zgody, nie zwalnia go z obowiązku przestrzegania zasad dotyczących przetwarzania danych osobowych, wskazanych w art. 5 ust 1 RODO, w tym w szczególności dotyczących rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych czy ich prawidłowości. Zgoda podmiotu nie może stanowić przesłanki legitymizującej nadmierne, nieadekwatne przetwarzania w stosunku do celu, którego ta zgoda dotyczy[18]. W RODO wykluczono możliwość udzielenia zgody na przetwarzanie danych osobowych poprzez akceptację regulaminu usługi[19]. Wydaje się zatem, że *per analogiam*, taka zgoda nie może zostać wyrażona poprzez akceptację regulaminu pracy bądź innych wewnątrzzakładowych form regulacji.

Jednocześnie, biorąc pod uwagę motyw 155. preambuły RODO, należy uznać zgodę pracowników za podstawową przesłankę umożliwiającą przetwarzanie danych pracowników w tym ich monitoring. Zgodnie z nim w prawie państwa członkowskiego lub w porozumieniach zbiorowych, w tym zakładowych porozumieniach z przedstawicielami pracowników, mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w związku z zatrudnieniem, w szczególności warunki, na których dane osobowe w związku z zatrudnieniem można przetwarzać za zgodą pracownika do celów procedury rekrutacyjnej, wykonywania umowy o pracę, w tym wykonywania obowiązków określonych w przepisach lub w porozumieniach zbiorowych, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy. Również przebieg prac nad RODO wskazuje, że zgoda pracownika powinna być podstawową przesłanką przetwarzania danych

której dane dotyczą, lub innej osoby fizycznej, przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

[18] Zob. D. Lubasz, *Komentarz do art. 6 ust. 1 lit. a* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, stan prawny na dzień 1 października 2017 r., Warszawa 2018, s. 352.

[19] Tamże, s. 353.

osobowych[20]. W pierwotnej wersji projektu RODO, przedstawionej przez Komisję Europejską, w motywie 34. preambuły wskazywano, że „zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w sytuacji wyraźnego braku równowagi między podmiotem danych a administratorem. Dotyczy to w szczególności przypadku, gdy między podmiotem danych a administratorem istnieje stosunek zależności, między innymi wtedy, gdy dane osobowe pracowników są przetwarzane przez pracodawcę w kontekście zatrudnienia (…)". Usunięcie tego fragmentu preambuły z jednoczesnym dodaniem motywu 155. świadczy niewątpliwie o tym, że wolą prawodawcy wspólnotowego było dopuszczenie przetwarzania danych osobowych pracowników (kandydatów do pracy) przez pracodawcę na podstawie zgody[21].

Wydaje się jednak, że przetwarzania danych osobowych pracowników można dokonywać również na podstawie innych przepisów RODO. Odrębną przesłanką stanowiącą uzasadnienie dla monitorowania pracowników i przetwarzania ich danych osobowych przez pracodawcę jest art. 6 ust. 1 lit. f RODO. Wskazana przesłanka umożliwia przetwarzanie danych w sytuacji, gdy jest ono niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Przepis ten znajdował swój odpowiednik w uprzednio obowiązującej ustawie o ochronie danych osobowych[22] (art. 23 ust 1). Przesłanka zawarta w komentowanym artykule ma zwiększyć elastyczność katalogu zawartego w art. 6 ust 1 RODO oraz umożliwić dopuszczenie przetwarzania danych osobowych w przypadkach, które pojawią się dopiero w przyszłości[23].

---

[20] Zob. P. Barta, P. Litwiński, M. Kawecki, R*ozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2017.

[21] Tamże.

[22] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922).

[23] W. Chomiczewski, *Komentarz do art. 6 ust 1 lit. f* [w:] *RODO*…, s. 389.

Przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. f RODO wymaga jednoczesnego spełnienia trzech przesłanek: musi wystąpić prawnie uzasadniony interes, przetwarzanie danych musi być niezbędne dla realizacji celu wynikającego z powyższego interesu, a ponadto interes ten musi mieć charakter nadrzędny dla interesów lub praw i wolności podmiotu danych. Zgodnie z motywem 48. Rozporządzenia, za prawnie uzasadniony interes uznano przetwarzanie danych osobowych w ramach grupy przedsiębiorstw o charakterze administracyjnym i odniesiono to również do przetwarzania danych osobowych pracowników. Z kolei w motywie 49. za przykład prawnie uzasadnione interesu uznano bezpieczeństwo sieci i informacji a także wyjaśniono, że może to obejmować np. zapobieganie nieuprawnionemu dostępowi do sieci, rozprowadzania złośliwych kodów czy przeciwdziałanie uszkodzeniu systemów komputerowych. Wydaje się, że np. odpowiednio zastosowany monitoring poczty elektronicznej pracowników czy kontrola odwiedzanych przez nich witryn internetowych, może stanowić realizację ochrony tego interesu prawnego pracodawcy. Jednocześnie należy podkreślić, że przetwarzanie danych w oparciu o ten przepis może być przeprowadzane wyłącznie, kiedy interes ma charakter rzeczywisty, a przetwarzanie nie ogranicza interesów, praw i wolności pracowników, które mają charakter nadrzędny wobec interesu pracodawcy. Podkreśla się, że w interpretacji art. 6 ust 1 lit. f RODO ogromne znaczenie będą miały rozstrzygnięcia organów nadzorczych, które w sposób kazuistyczny będą mogły wskazywać na zasadność przetwarzania danych w określonych przypadkach. Wydaje się, że umieszczenie monitoringu w celu przeciwdziałaniu kradzieżom i niszczeniu mienia w zakładzie pracy będzie jednak interesem nadrzędny wobec prawa pracownika do zachowania prywatności, o ile monitoring ten nie będzie obejmował miejsc, w których nadzór nie jest konieczny dla realizacji założonego celu np. w toaletach czy przebieralniach[24].

Z możliwości zawartej w art. 6 ust 1 lit. f nie mogą skorzystać organy publiczne w ramach realizacji swoich zadań. Wydaje się zatem, że możliwość monitorowania pracowników na podstawie art. 6 ust. 1 lit f. jest wyłączona w stosunku do pracowników organów administracji publicznej i organów władzy publicznej. Jeżeli uznać, że organy publiczne wykonują

[24] Tamże, s. 400.

swoje zadania bezpośrednio przez zatrudnionych w nich pracowników, należy stwierdzić, że możliwość ich monitorowania na podstawie omawianego artykułu jest wyłączona, bowiem organy te w tym zakresie realizują swoje zadania.

Obowiązująca ustawa o ochronie danych osobowych, w zakresie zmian w Kodeksie pracy, założyła w szczególności dostosowanie brzmienia obowiązujących przepisów prawa pracy do wymogu zawartego w art. 6 ust. 1 lit. c. RODO, który wprowadza przesłankę istnienia obowiązku prawnego, jako podstawy pobierania danych osobowych. W konsekwencji przepisy, które dotychczas zawierały jedynie możliwość żądania określonych danych osobowych w stosunkach pracy, zostały zmienione na obowiązek pobierania tych danych. W ustawie o ochronie danych osobowych zawarto również negatywny katalog danych, których pozyskiwanie przez pracodawcę nie może nastąpić nawet od osoby, która ubiega się o zatrudnienie lub pracownika. Po raz pierwszy w polskim systemie prawnym, uregulowano instytucję monitoringu jako szczególną formę przetwarzania danych osobowych pracowników.

W myśli nowej ustawy, pracodawca może wprowadzić szczególne formy kontroli nad miejscem pracy lub terenem zakładu pracy w postaci monitoringu wizyjnego, jeżeli uzna to za konieczne w celu zapewnienia bezpieczeństwa pracownikom, ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Monitoring wizyjny nie może jednak mieć na celu kontroli pracy wykonywanej przez pracownika oraz nie powinien obejmować pomieszczeń, które nie są bezpośrednio przeznaczone do wykonywania pracy, takich jak pomieszczenia sanitarne, szatnie, stołówki czy palarnie.

Zebrane w ten sposób dane osobowe, pracodawca może przetwarzać tylko dla celów, dla których zostały zebrane oraz przechowywać tylko przez okres niezbędny dla ich realizacji. Pracodawca ma obowiązek poinformowania pracowników o wprowadzonych środkach kontroli nie później niż czternaście dni przed uruchomieniem monitoringu. Nowo zatrudniony pracownik powinien być poinformowany o stosowanym monitoringu przed dopuszczeniem go do pracy. Rozwiązania zaproponowane przez prawodawcę nie realizują postanowień wskazanych w art. 6

ust. 1 lit. a RODO, dotyczących zgody podmiotu, którego dane dotyczą na przetwarzania danych. Wydaje się zatem, że celem ustawodawcy było stworzenie możliwości przetwarzania danych przez pracodawcę w oparciu o art. 6 ust. 1 lit. f.

Jednocześnie takie uregulowanie możliwości przetwarzania danych przez pracodawcę danych pracowników jest dozwolone na gruncie art. 88 RODO. Na jego podstawie państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem. W szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy. Przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.

Odrębnego omówienia wymaga możliwość przetwarzania danych przez osoby fizyczne, które zatrudniają pracowników. Przy zachowaniu pozostałych przesłanek, mogą one przetwarzać dane osobowe swoich pracowników w oparciu o art. 6 ust 1 lit. d RODO, kiedy takie przetwarzanie jest niezbędne dla ochrony żywotnych interesów podmiotu danych lub innej osoby fizycznej. W motywie 46. RODO, znalazły się przykłady żywotnych interesów osoby fizycznej, do której zaliczono m.in. cele humanitarne, monitorowanie epidemii i ich rozprzestrzeniania się, nadzwyczajne sytuacje humanitarne, ale w doktrynie podkreśla się, że do żywotnych interesów można zaliczyć również konieczność

ratowania życia i zdrowia a także ochronę majątku[25]. Wydaje się zatem, że pracodawca, będący osobą fizyczną, może stosować narzędzia monitoringu wobec swoich pracowników bez obowiązku pozyskania ich zgody, w przypadku, gdy ma uzasadnione obawy co do ich uczciwości, a jego działanie ma na celu ochronę jego majątku, a między monitorowaniem pracowników a ochroną zachodzi bezpośredni związek. Jednocześnie ta przesłanka nie może uzasadniać stosowania narzędzi monitoringu przez pracodawców będących osobami prawnymi czy jednostkami organizacyjnymi niebędącymi osobami prawnymi[26]. Na gruncie projektowanej ustawy, polski prawodawca nie dopuścił możliwości skorzystania z tej przesłanki w zakresie monitorowania pracowników, co może stanowić pewną próbę ograniczenia stosowania RODO w tym zakresie.

3. Monitoring wizyjny w miejscu pracy

Przed wejście w życie nowej ustawy o ochronie danych osobowych, kwestia monitorowania pracowników w miejscu pracy nie była przedmiotem regulacji prawnych. Zastosowanie znajdowały przepisy ówcześnie obowiązującej ustawy o ochronie danych osobowych oraz Kodeksu pracy. Jednocześnie, rozbudowane orzecznictwo zarówno sądów krajowych jak i Europejskiego Trybunały Praw Człowieka oraz praktyka organów Unii Europejskiej, a także poglądy doktryny pozostają aktualne również pod rządami RODO i nowej ustawy o ochronie danych osobowych. W doktrynie podkreślano, że podstaw zastosowania monitoringu wizyjnego należy doszukiwać się w ogólnych obowiązkach pracowników jak np. obowiązku dbałości o dobro zakładu pracy, pod warunkiem, że konieczność przeprowadzenia kontroli jest związana z przesłankami takiego pracowniczego obowiązku[27]. Monitoring pracownika w miejscu pracy ma wielorakie skutki: kontrola niepożądanej działalności pracownika

[25] W. Chomiczewski, *Komentarz do art. 6 ust. 1 lit. d* [w:] *RODO…*, s. 378.

[26] Tamże, s. 379.

[27] Zob. 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. 71−72.

w miejscu pracy może przynieść wymierne korzyści finansowe dla pracodawcy, zapobiegać kradzieżom czy agresywnym zachowaniom pracowników[28]. Oprócz negatywnych skutków w zakresie ewentualnego naruszenia godności i prywatności pracownika, można również wskazać na obniżenie motywacji do pracy, poprzez poczucie utraty zaufania ze strony pracownika oraz naturalną potrzebę buntu przeciwko nadmiernym działaniom kontrolnym.

Za A. Lachem można wskazać kilka reguł, które pracodawca powinien wziąć pod uwagę przy instalowaniu monitoringu wizyjnego:

1) nie można instalować kamer w miejscach, gdzie pracownik czy inna osoba może zasadnie oczekiwać zachowania swojej prywatności, np. w przebieralniach, toaletach, prywatnych gabinetach;
2) o monitorowaniu należy uprzedzić osoby, które mogą znaleźć się w jego zasięgu, a w szczególności pracownik powinien wiedzieć, jakie miejsca są monitorowane (na gruncie RODO w określonych, omówionych wyżej przypadkach wymagana jest zgoda pracownika);
3) dokonane zapisy powinny być przechowywane jedynie przez czas niezbędny do monitorowania (np. stwierdzenie kradzieży) i w warunkach zabezpieczających je przed dostępem osób niepowołanych[29].

Przy analizowaniu możliwości zastosowania monitoringu wizyjnego w miejscu pracy, można powołać się na orzeczenie ETPC w sprawie *Peck v. Zjednoczone Królestwo*[30]. Na zasadzie analogii można uznać, że dozwolone jest instalowanie telewizji przemysłowej, jednak monitorowani pracownicy muszą wiedzieć, kto odpowiada za nagrany materiał i kto ma do niego dostęp oraz powinni móc zweryfikować sposób jego przechowywania[31]. Jednocześnie monitoring może być przeprowadzany wyłącznie,

---

[28] Zob. K. Ziółkowska, *Dopuszczalność kontroli osobistej pracownika a obowiązek dbałości o dobro zakładu pracy*, SP 2013, Nr 20, s. 138.

[29] A. Lach, *Monitorowanie*…, s. 207.

[30] Zob. wyrok ETPC z dnia 28 stycznia 2003 r., 44647/98, *Peck v. Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej*.

[31] Zob. D. Głowacka, *Prywatność w miejscu pracy w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka* [w:] *Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych. Stan obecny i perspektywy zmian*, red. A. Nerka, T. Wyka, Warszawa 2012, s. 49.

kiedy wynika z konkretnej potrzeby i jest uzasadniony szczególnymi okolicznościami[32].

W wyroku *Lopez Ribalda i inni v. Hiszpania*[33] ETPC wskazał, że monitorowanie pracowników bez ich wiedzy stanowi naruszenie ich prawa do prywatności. Skargi do Trybunały wnieśli byli pracownicy supermarketu, którego właściciele monitorowali ich stanowiska pracy przy pomocy kamer. Pracodawca zdecydował się na wprowadzenie takiego rozwiązania, po tym jak odkrył znaczne braki magazynowe i zaczął podejrzewać zatrudnionych u niego pracowników o kradzież. Pracodawca zainstalował w zakładzie pracy zarówno kamery widoczne jak i ukryte, o których pracownicy nie wiedzieli. Jednocześnie kamery zarejestrowały jak skarżący kradną towar ze sklepowych spółek, w związku z czym zostali dyscyplinarnie zwolnieni. W swoich skargach zarzucili, że niejawny monitoring ich zachowań w miejscu pracy stanowił naruszenie ich prawa do prywatności i naruszał art. 8 EKPC.

Rząd Hiszpański wskazywał, że monitoring był przeprowadzany przez prywatną firmę, za której działalność państwo nie może ponosić odpowiedzialności. Jednak również w tej sprawie Trybunał odrzucił te argumenty i podkreślił, że na gruncie art. 8 Konwencji każde państwo -strona Konwencji ma pozytywny obowiązek przeciwdziałać zachowaniom prywatnych przedsiębiorców, które mogłyby naruszać prawo jednostki do prywatności. Zgodnie z hiszpańskim prawem, osoby monitorowane muszą być poinformowane o tym, że ktoś gromadzi dane zawierające ich wizerunek, a w omawianej sprawie, taka wiadomość nie została skarżącym przekazana a ich miejsca pracy były pod obserwacją ukrytej kamery. Jednocześnie sądy krajowe uznały taki działanie za uzasadnione biorąc pod uwagę podejrzenie popełnienia przestępstwa kradzieży przez pracowników oraz wskazywały, że nie było innego sposobu na ochronę mienia prawodawcy przed szkodliwym działaniem pracowników, a ingerencja w ich prawa była adekwatna.

Trybunał nie podzielił stanowiska sądów krajowych i uznał zastosowanie niejawnego monitoringu za sprzeczne z EKPC i nieproporcjonalne.

---

[32] Tamże.

[33] Wyrok ETPC z dnia 9 stycznia 2017 r., Nr 1874/13 i 8567/13, *Lopez Ribalda i inni v. Hiszpania.*

Trybunał podkreślił, że prawom pracowniczym należało zapewnić jakąkolwiek ochronę w tym zakresie poprzez chociażby wcześniejsze powiadomienie pracowników o zastosowanym monitoringu. Pracodawca mógł na przykład, udzielić pracownikom ogólnych informacji na temat zasad stosowania monitoringu w sklepie (bez wskazywania konkretnej lokalizacji ukrytej kamery), zgodnie z wymogami krajowej ustawy o ochronie danych osobowych. Tak się jednak nie stało, wobec czego Trybunał stwierdził naruszenie art. 8 Konwencji poprzez naruszenie prawa pracowników do prywatności.

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych (obecnie Prezesa Urzędu Ochrony Danych Osobowych), pracodawca ma prawo do stosowania monitoringu wizyjnego w celu kontroli przebiegu i czasu pracy, o ile istnieje podstawa prawna do takiego działania[34]. Pracodawcy wolno również prowadzić wideo nadzór w celu zapewnienia bezpieczeństwa pracy swoich pracowników lub ochrony życia i zdrowia osób, na przykład w przypadku zdalnego nadzoru pacjentów w salach reanimacyjnych. Jednocześnie, prowadzenie takiego nadzoru nie jest dozwolone w miejscach, w których toczy się życie towarzyskie pracowników takie jak przebieralnie czy toalety. GIODO zauważył również, że niektóre rodzaje działalności w obszarze publicznym wręcz wymagają takiej formy nadzoru, a zaliczyć do nich można między innymi banki, komendy policji, pomieszczenia wykorzystywane przez straż graniczną i im podobne.

Zgodnie ze stanowiskiem GIODO, możliwość wykorzystania monitoringu wizyjnego w miejscu pracy jest uzależniona od poinformowania pracownika o jego prowadzeniu poprzez np. zamieszczenie tabliczki z rysunkiem kamery. Tablice powinny zawierać również informację na temat tego, kto jest administratorem zebranych danych. Jeśli pracownik sprzeciwi się takiej formie nadzoru, pracodawca co do zasady jest zobowiązany do wskazania podstawy prawnej, która zobowiązuje go do jego prowadzenia. Pracodawca ma obowiązek zapewnienia pracownikowi możliwości wglądu w jego dane osobowe, w tym również zapisy z kamer. W przypadkach, gdy w ramach realizacji prawa dostępu pracownicy mogą otrzymać dane

[34] *Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników,* http://www.giodo.gov.pl/pl/1520056/7930, 7.02.2018.

osobowe osoby trzeciej, administrator zobowiązany jest do zapewnienia, że udostępnione zostaną tylko dane dotyczące określonego pracownika np. poprzez podjęcie odpowiednich środków technicznych mających na celu zaciemnienie twarzy innych osób, obecnych na taśmach monitoringu. W przypadku braku takiej możliwości technicznej dostęp do nagrań wideo może być zapewniony tylko za zgodą wszystkich osób, których dane osobowe można znaleźć na nagraniach z wideo nadzoru.

Warto również zwrócić uwagę na stanowisko Ministra Rodziny, Pracy i Polityki Społecznej w odpowiedzi na interpelacje w sprawie ukrytych kamer w miejscu pracy. Zdaniem organu „korzystanie przez pracodawcę z monitoringu za pomocą kamer w celu kontrolowania wykonywania pracy przez pracowników, chronienia pracodawcy przed zagrożeniami zewnętrznymi, np. kradzieżami czy wejściem na teren zakładu pracy osób nieuprawnionych, a także zabezpieczenia się przed ewentualnymi działaniami pracowników, które mogą wyrządzić szkodę pracodawcy lub osobom trzecim, wydaje się dopuszczalne, jednak pod warunkiem, że pracodawca zadba, aby dobra osobiste pracowników nie zostały naruszone oraz aby w jak najmniejszym stopniu ingerować w prywatność pracowników, a także pod warunkiem, że środki stosowane przez pracodawcę będą adekwatne do celów, którym mają służyć. Monitorowanie przez pracodawcę miejsca pracy za pomocą kamer nie wymaga uzyskania od pracowników zgody na takie sprawowanie kontroli wykonywania pracy czy też bezpieczeństwa zakładu pracy lub pracownika w miejscu pracy. Jednakże pracodawca, będąc zobligowany przepisami Kodeksu pracy do szanowania godności oraz dóbr osobistych pracowników, powinien ich poinformować, że miejsca pracy mogą być monitorowane. Zasady stosowanego w zakładzie pracy monitoringu za pomocą kamer mogą wynikać np. z regulaminu pracy lub wewnętrznego zarządzenia pracodawcy i powinny być udostępnione do wiadomości wszystkim pracownikom w zwyczajowo przyjęty sposób, np. poprzez zamieszczenie stosownej informacji na tablicy ogłoszeń”[35]. Jednocześnie Minister, podobnie jak

[35] Odpowiedź podsekretarza stanu w Ministerstwie Pracy i Polityki Społecznej – z upoważnienia Ministra – na interpelacje Nr 21614 w sprawie ukrytych kamer w miejscu pracy, http://www.sejm.gov.pl/Sejm7.nsf/InterpelacjaTresc.xsp?key=0761FE4E, 9.02.2018.

GIODO, wskazuje, że nieuzasadnione jest instalowanie kamer służących do monitoringu wizyjnego w miejscach, w których pracownicy nie wykonują obowiązków służbowych, takich jak toalety, przebieralnie, palarnie czy stołówka.

Chociaż wydawać by się mogło, że monitoring wizyjny jest formą kontroli, która budzi największe kontrowersje, w ostatnich latach dużo większe zainteresowanie wzbudza monitoring poczty e-mail pracowników. Na tym tle pojawia się coraz więcej orzeczeń zarówno sądów krajowych jak i ETPC.

4. Prawo do prywatności w miejscu pracy a poczta e-mail

Monitorowanie przez pracodawcę poczty elektronicznej pracownika prowadzi do skrzyżowania się prawa pracownika do zachowania tajemnicy korespondencji oraz prawa pracodawcy do kontrolowania wykonywanej przez pracownika pracy[36]. Tajemnica korespondencji podlega ochronie zarówno w formie tradycyjnej (np. poczta) jak również nowoczesnej (poczta e-mail), obejmuje swoim zakresem nie tylko treść komunikatu, ale również okoliczności komunikacji z osobami trzecimi tj. dane dotyczące połączeń[37].

W przypadku korzystania w zakładzie pracy przez pracownika zarówno ze skrzynki służbowej jak i prywatnej (np. podczas przerw) należy uznać, że monitoring drugiej z wymienionych co do zasady będzie traktowany jako naruszenie prywatności pracownika[38]. O ile bowiem, na skrzynce służbowej pracownika z założenia powinny znajdować się informacje związane wyłącznie z wykonywanymi przez niego obowiązkami, to skrzynka osobista z założenia zawierać będzie wiadomości dotyczące życia prywatnego pracownika. Jednocześnie wydaje się być społeczne akceptowalne korzystanie przez pracowników z prywatnej poczty elektronicznej w miejscu pracy, kiedy nie koliduje to z wykonywaniem służbowych obowiązków.

---

[36] M. Wujczyk, *Prawo*…

[37] Zob. M.T. Tinnefeld, *Jak Internet zmienia prawne ramy prywatności* [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpot, W. Wiewiórski, Warszawa 2012, s. 8.

[38] M. Wujczyk, *Prawo*…

Inaczej wygląda sytuacja w przypadku służbowej poczty elektronicznej. Przyjmując, że jest ona własnością pracodawcy i powinna służyć jedynie wykonywaniu obowiązków pracowniczych, podkreśla się, że pracodawca ma prawo monitorować działania podejmowane z jej użyciem[39]. Zdaniem Ministra Pracy i Polityki Społecznej pracodawca ma obowiązek uprzedniego powiadomienia pracownika o monitorowaniu jego poczty elektronicznej, jedynie w przypadku, gdy wcześniej zezwolił na wykorzystywanie jej również w celach prywatnych[40]. Jeśli na monitorowaną służbową skrzynkę e-mailową pracownika trafiają również prywatne wiadomości pracodawca, co do zasady nie powinien zapoznawać się z ich treścią[41]. Mogą się jednak zdarzyć takie sytuacje, kiedy pracodawca ma uzasadnione podejrzenia, że treść tych wiadomość może wskazywać na popełnienie przez pracownika czynu zabronionego lub skierowanego przeciwko interesom zakładu pracy, wtedy takie działanie należy uznać za dozwolone. Dobrym przykładem w tym zakresie są uregulowania jakie zostały wprowadzone w Danii, wyróżnia się tam bowiem monitoring ogólny i szczególny. Monitoring ogólny nie ma na celu pozyskanie treści wiadomości elektronicznych, a jedynie zabezpieczenie płynności i bezpieczeństwa pracy, skanowanie systemów ma na celu poszukiwanie niebezpiecznych wirusów lub też sprawdzania wywiązywania się z zasad bezpiecznego korzystania z oprogramowania dostarczonego przez pracodawcę[42]. Za kontrolę szczególną uważa się poznanie zawartości konkretnej wiadomości elektronicznej, która następuje w szczególnych przypadkach np. podejrzenia popełnienia przestępstwa. Jednocześnie,

---

[39] Zob. Odpowiedź Ministra Pracy i Polityki Społecznej na wystąpienie Rzecznika Praw Obywatelskich z dnia 20 grudnia 2007 r., http://www.rpo.gov.pl/pliki/1201784465.pdf, 30.07.2015.

[40] Tamże.

[41] Zob. P. Kral, *Prywatna korespondencja podwładnego poza kontrolą szefa,* http://archiwum.rp.pl/artykul/735641.html, 29.07.2015.

[42] Zob. M. Wujczyk, *Obowiązek poszanowania prywatności pracownika jako warunek legalności monitoringu stosowanego przez pracodawcę* [w:] *Aktualne zagadnienia prawa pracy i polityki socjalnej (zbiór studiów)*, B.M. Ćwiertniak, t. II, Sosnowiec 2013, s. 130.

w Danii zabronione jest kontrolowanie wiadomości opatrzonych klauzulą „prywatne" bez względu na okoliczności, które uzasadniają potrzebę monitoringu[43].

Jednocześnie, trzeba wskazać, że niezależnie od stanowiska Ministra, faktem jest, że raz wysłany email z sieci pracodawcy, na zawsze pozostaje w tej sieci, niezależnie od kroków podjętych przez pracownika w celu jego usunięcia. Wystarczającym jest zatem stwierdzenie, że ktokolwiek ma dostęp do sieci pracodawcy ma faktyczny dostęp do poczty email pracowników, do niego jednak należy decyzja, czy z tego dostępu skorzysta[44].

Jednym z najnowszych orzeczeń w tym zakresie jest wyrok ETPC w sprawie *Bărbulescu v. Rumunii*[45]. W przedmiotowej sprawie Bogdan Mihai Bărbulescu był zatrudniony w firmie prywatnej jako inżynier odpowiedzialny za sprzedaż. Na żądanie pracodawcy utworzył w Internecie konto Yahoo Messenger, aby za jego pośrednictwem odpowiadać na pytania i prośby klientów. W lipcu 2007 roku, pracodawca poinformował Bărbulescu, że jego korespondencja była monitorowana i okazało się, że korzystał on z poczty do celów osobistych, co stanowiło naruszenie regulacji zakładowych i stanowiło podstawę zwolnienia Bărbulescu. Po tym jak dwukrotnie sądy rumuńskie orzekły na korzyść pracodawcy, Bărbulescu rozpoczął postępowanie przed Europejskim Trybunałem Praw Człowieka. W skardze do Trybunału, z powołaniem się na art. 8 Europejskiej Konwencji Praw Człowieka, skarżący zarzucił, że podstawą decyzji pracodawcy o zwolnieniu go z pracy było naruszenie jego prywatności, ponadto uważał, że postępowanie sądowe w jego sprawie nie było rzetelne (art. 6 ust.1 Konwencji). Trybunał stwierdził, że pojęcie „życie prywatne" może obejmować również działalność zawodową i odbywającą się w kontekście publicznym. Ograniczenia dotyczące życia zawodowego jednostki mogą być objęte art. 8 Konwencji o ile wpływają na sposób budowy przez nią swojej tożsamości społecznej przez rozwijanie relacji z innymi. W związku z tym ETPC uznał za warte odnotowania, że właśnie w latach swojej aktywności zawodowej większość ludzi posiada

---

[43] Tamże, s. 131.

[44] Zob. J. Tealby, *E-mail and privacy at work*, JLIS 1999, 10/2, s. 209.

[45] Wyrok ETPC z dnia 5 września 2017 r., *Bărbulescu v. Rumunia*, Nr 61496/0.

znaczne, jeśli nie największe, możliwości rozwijania związków ze światem zewnętrznym.

Z dotychczasowego orzecznictwa ETPC wyraźnie wynika, że komunikowanie się z pomieszczeń biznesowych podobnie, jak z domu, może być objęte pojęciami „życie prywatne" i „korespondencja" w rozumieniu art. 8 Konwencji. Trybunał wielokrotnie badał, czy osoby mogły rozsądnie oczekiwać, że ich prywatność w miejscu pracy będzie szanowana i chroniona. W omawianym kontekście stwierdził, że rozsądne oczekiwanie prywatności jest czynnikiem znaczącym, ale nie musi być decydujące. Przy stosowaniu wymienionych zasad w tej sprawie Trybunał zauważył, że rodzaj usługi komunikatora internetowego jest jedną z form komunikowania się umożliwiającą jednostkom prowadzenie osobistego życia społecznego i podlega regulacjom art. 8 EKPC. Równocześnie, wysyłanie i otrzymywanie informacji są objęte pojęciem „korespondencja", nawet jeśli zostały wysłane z komputera pozostającego w mieniu pracodawcy. Trybunał zauważył jednak, że w przedmiotowej sprawie, pracodawca zabronił pracownikom prowadzić w miejscu pracy jakiejkolwiek działalności o charakterze osobistym i wykorzystywania w tym celu sprzętu pozostającego w zakładzie pracy.

Zakaz wprowadzony przez prawodawcę nie może całkowicie pozbawić pracowników życia prywatnego w miejscu pracy. Poszanowanie życia prywatnego i prywatności korespondencji wymagane jest niezależnie od tego, czy można je w granicach konieczności ograniczyć. W świetle szczególnych okoliczności tej sprawy Trybunał uważał, biorąc pod uwagę wniosek dotyczący stosowania art. 8 oraz fakt, że możliwość korzystania przez skarżącego z prawa do poszanowania życia prywatnego i korespondencji została osłabiona w rezultacie działań prywatnego pracodawcy, że jego zarzut należało zbadać z punktu widzenia obowiązków pozytywnych państwa.

W orzecznictwie ETPC wielokrotnie podkreślano, że wybór środków mających na celu zabezpieczenie uprawnień wynikających z art. 8 k.p.c. pozostaje w granicach swobody państwa, a natura obowiązku zależy od zakresu prywatności, której sprawa dotyczy. Niezależnie od tego, w pewnych okolicznościach można uznać, że państwo nie wypełnia

odpowiednio swoich obowiązków pozytywnych na podstawie art. 8 Konwencji, jeśli nie zapewnia w szczególnym kontekście konkretnego przypadku poszanowania życia prywatnego w relacjach między jednostkami przez stworzenie ram prawnych z uwzględnieniem rozmaitych interesów wymagających ochrony.

Chociaż prawo pracy opiera się na uzgodnionej przez strony umowie, zarówno pracodawca jak i pracownik powinni znać wzajemne prawa i obowiązki i je respektować, z obowiązku pozytywnego państwa wynikającego z art. 8 EKPC rodzi się konieczność nadzorowania, w jaki sposób strony kształtują swoją pozycję w umowach pracy oraz dopilnowania, aby pracodawcy nie nadużywali swojej dominującej pozycji.

Przy wprowadzaniu przez pracodawcę środków monitorowania korespondencji, obowiązkiem władz państwowych jest zapewnienie, aby kontroli towarzyszyły odpowiednie środki zabezpieczające przed nadużyciem. Chociaż Trybunał jest świadomy szybkich zmian w dziedzinie monitoringu elektronicznego, uważa za niezbędne proporcjonalność i gwarancje proceduralne chroniące przed arbitralnością pracodawcy. W tym kontekście władze powinny traktować jako ważne następujące czynniki:

1) sposób powiadomienia pracowników o podjęciu przez pracodawcę monitoringu korespondencji i innych sposobów komunikowania oraz jego implementacji, wskazując, że zgodnie z art. 8 uprzednia notyfikacja powinna jasno wskazywać naturę monitoringu;
2) zakres monitoringu przez pracodawcę i stopień ingerencji w prywatność pracownika, w tym zakresie należy rozróżnić monitorowanie przepływu korespondencji i jej treści, należy również wziąć pod uwagę, czy całość korespondencji albo wyłącznie jej część była monitorowana, jak również, czy monitoring był ograniczony w czasie i jaka liczba osób miała dostęp do jego rezultatów;
3) fakt przedstawienie przez pracodawcę powodów monitoringu komunikowania się i zapoznania się przez pracowników z jego rzeczywistą treścią, która powinna zawierać poważne usprawiedliwienie;

4) ocenę czy cel realizowany przez pracodawcę można było osiągnąć również bez bezpośredniego dostępu do pełnej treści korespondencji pracownika;
5) konsekwencje monitoringu dla pracownika, którego dotyczył oraz sposób użycia przez pracodawcę rezultatów monitoringu, w szczególności, czy służyły osiągnięciu jego deklarowanego celu;
6) korzystanie przez pracodawcę z odpowiednich zabezpieczeń, zwłaszcza w sytuacji, gdy monitoring miał charakter dotkliwy.

Generalny Inspektor Ochrony Danych Osobowych stoi na stanowisku, że monitorowanie służbowej poczty email jest przetwarzaniem danych osobowych w rozumieniu ustawy ochronie danych osobowych. GIODO wskazuje, że pracodawca jest zobowiązany do poinformowania pracowników o możliwości monitorowania służbowej korespondencji email i wykorzystaniu Internetu oraz warunkach pod jakimi pracownicy mogą korzystać z prywatnej poczty przed dopuszczeniem ich do pracy. Pracodawca powinien również poinformować pracowników, czy i pod jakimi warunkami mogą oni korzystać z prywatnej poczty elektronicznej podczas godzin pracy oraz ze służbowej poczty elektronicznej do celów prywatnych oraz jaka jest procedura otwierania służbowej poczty email podczas przedłużającej się nieobecności pracownika oraz jakie są środki techniczne i organizacyjne podjęte przez pracodawcę w celu ochrony danych osobowych.

Wydaje się, że omówione orzeczenie przez najbliższe lata będzie wyznaczało zakres możliwości kontroli pracodawcy. Istotne jest ono również z tego względu, że odwróciło ono dotychczasową linię orzeczniczą, w której opowiadano się za znacznie szerszymi możliwościami kontroli przez pracodawcę służbowej skrzynki e-mailowej pracowników.

5. Dopuszczalność wykorzystywania narzędzi geolokalizacyjnych w nadzorze pracownika

Pracodawcy chętnie korzystają z nowinek technologicznych w celu polepszenia organizacji i usprawniania procesu pracy. Narzędzia takie jak nadajniki lokalizacji GPS pozwalają na sprawne zarządzanie pracownikami wykonującymi swoje obowiązki poza zakładem pracy czy flotą

samochodową. System GPS jest niewątpliwie efektywnym narzędziem kontroli pracowników, jednak podobnie jak monitorowanie poczty e-mail podlega pewnym ograniczeniom. Za najważniejsze z nich należy uznać poinformowanie pracownika o jego stosowaniu oraz wyrażenie przez niego zgody na gromadzenie danych o konkretnym pracowniku, wymaganej przez ustawę o ochronie danych osobowych, jeśli uznać, że dane te dotyczą miejsca pobytu konkretnego pracownika a nie jedynie np. samochodu służbowego[46]. Jednocześnie należy wskazać, że w przypadku, gdy pracownik jest upoważniony do korzystania z samochodu, będącego własnością pracodawcy po godzinach pracy, dane zbierane przez pracodawcę powinny dotyczyć jedynie położenia samochodu, a nie miejsca przebywania samego pracownika[47]. Zdaniem autora opracowania, takie rozwiązanie pomimo pewnej słuszności w jego podstawach jest rozwiązaniem utopijnym. Monitorowanie trasy samochodu jednocześnie wymusza monitorowanie miejsca pobytu jego kierowcy, czyli pracownika.

Pracodawca jako właściciel pojazdu może monitorować, gdzie znajduje się jego samochód, ilość paliwa w baku, czas użytkowania i sposób eksploatacji. Zdaniem GIODO, pracodawca może instalować systemy nadzoru samochodu takie jak GPS bez zgody pracownika wyłącznie wtedy, gdy wymagają tego charakter prowadzonej działalności oraz środki bezpieczeństwa. Jednocześnie, informacja o montowaniu urządzeń GPS powinna znaleźć się w regulaminie pracy, a pracownicy powinni być o tej formie kontroli poinformowani, niezależnie od tego, jakie przesłanki stały za jej wprowadzeniem. Wydaje się, że jeśli pracodawca pozostawia samochód do dyspozycji pracownika, również poza godzinami pracy i nie wprowadził zakazu korzystania z pojazdu do celów osobistych, kontrola powinna odbywać się wyłącznie w godzinach pracy. Jednocześnie, wydaje się być zasadne z punktu widzenia pracodawcy, aby użycie służbowych pojazdów było poddane kontroli również w czasie wolnym pracowników, jeżeli pracodawca nie zezwala na korzystanie z nich w celach

[46] Zob. D. Rowińska, *Kontrola pracowników za pomocą systemu GPS,* http://www.chwp.pl/publikacje/nasze-publikacje/kontrola-pracownikow-za-pomoca-systemu-gps/, 30.07.2015.

[47] Zob. M. Berlak, *Monitorowanie auta powierzonego pracownikowi w oparciu o system GPS*, http://www.wglex.pl/monitorowanie-auta-powierzonego-pracownikowi-w-oparciu-o-system-gps/, 30.07.2015.

prywatnych, a jednocześnie pracownicy nie są zobowiązani do każdorazowego odstawiania ich na teren zakładu pracy. Ani sądy krajowe, ani ETPC nie wypowiedziały się jeszcze w tym zakresie, ale zdaniem autorki niniejszego wywodu, taka kontrola byłaby nieproporcjonalna oraz ingerowała by w prywatność pracowników w sposób niedozwolony przez art. 8 Konwencji.

6. Podsumowanie

Dotychczas obowiązujące przepisy nie zawierały szczególnych regulacji w zakresie dopuszczalności i zakresu monitoringu pracowników w trakcie wykonywania ich obowiązków służbowych. Lukę w tym zakresie uzupełnia działalność ETPC, który w ostatnich latach wypracował stałą linię orzeczniczą. Bez wątpienia należy stwierdzić, że niezależnie od okoliczności, pracodawca jest zobowiązany do poinformowania pracowników o stosowanych narzędziach kontroli i jej zakresie. Stosowane środki kontroli oraz jej natężenie powinny przede wszystkim spełniać wymóg proporcjonalności— pracodawca może wykorzystywać narzędzia monitoringu tylko, kiedy pracownik jest ich świadomy oraz tylko w takim zakresie, jakie są niezbędne do ochrony żywotnych interesów pracodawcy.

Jednocześnie, należy zwrócić uwagę, że odrębne regulacje mogą dotyczyć szczególnych kategorii pracowników, szczególnie tych zatrudnionych w organach administracji publicznej bądź w służbach państwowych. Inny stopień ingerencji w życie prywatne pracownika będzie uzasadnione w przypadku pracowników służb specjalnych bądź tych, którzy w codziennej pracy mają do czynienia z informacjami niejawnymi oznaczonymi klauzulą tajne bądź ściśle tajne. Niemniej, każda taka ingerencja powinna być proporcjonalna oraz odpowiadać prawnie uzasadnionym celom, które pracodawca chce osiągnąć.

Nowa regulacja w zakresie ochrony danych osobowych po raz pierwszy w polskim systemie prawnym reguluje kwestie zastosowania monitoringu w zakładach pracy. Wydaje się jednak, że przedstawiona propozycja jest zbyt szczątkowa i odpowiada na tylko jeden z wielu palących problemów monitoringu pracowniczego. Ograniczenie się prawodawcy jedynie do monitoringu wizyjnego pozostawia wyraźną lukę w zakresie

innych form kontroli, takich jak monitoringu poczty e-mail i komunikatorów internetowych, możliwości przeglądania historii przeglądarki internetowej oraz bieżącego nadzoru nad sposobem wykorzystania przez pracownika oprogramowania służbowych komputerów, czy wykorzystania urządzeń GPS w pojazdach służbowych pracowników. Nie wydaje się być rozsądne uregulowanie tak istotnej kwestii, która ponadto podlega ciągłym zmianom, tylko w tak ograniczonym zakresie. Ustawodawca mógł na tym już etapie nowymi przepisami objąć szerszy zakres zagadnienia monitoringu pracowników.

Kontrowersje budzi nie tylko fakt uregulowania jedynie części sytuacji faktycznych, z którymi spotykają się pracownicy, ale przede wszystkim sposób regulacji monitoringu wizyjnego. Wydaje się, że mógłby on również prowadzić w określonych okoliczności do kontroli efektywności pracowników oraz obejmować szerszy zakres pomieszczeń, aby przy poszanowaniu prywatności pracowników, uwzględnić również słuszny interes pracodawcy. Ograniczenie możliwości stosowania monitoringu wizyjnego jedynie do pomieszczeń, w których wykonywane są obowiązku służbowe, z wyłączeniem np. korytarzy czy stołówek nie zabezpieczy bowiem w sposób wystarczający ani mienia ani dobrego imienia pracodawcy.

Wydaje się również, że szczególnie w zakresie kontroli wykorzystania narzędzi elektronicznych i oprogramowania pracodawcy przez pracowników, ustawodawca powinien umożliwić kierownikom zakładu pracy przeprowadzenie kontroli oraz uwzględnić ich żywotne interesy. W dobie szczególnego zagrożenia cyberprzestępczością, większość zinformatyzowanych zakładów pracy może odnieść większą szkodę przez wprowadzenie przez pracownika złośliwego oprogramowania do systemu pracodawcy, niż przez fakt, że wykradnie on mienie biurowe. Brak regulacji w tym zakresie nie jest korzystny również dla osób zatrudnionych, pozostawia szarą strefę w relacji pracownik–pracodawca i może doprowadzić do naruszenia prawa do prywatności tego pierwszego.

S t r e s z c z e n i e

Monitorowanie pracowników w miejscu ich pracy to zjawisko powszechne i wydaje się, że społecznie akceptowalne. Pracodawcy często wprowadzają narzędzie zwiększonej kontroli z prostych i zrozumiałych przyczyn: chcą zwiększyć efektywność pracowników, sprawdzić, czy pracownicy w godzinach pracy wykonują zlecone im zadania lub by przeciwdziałać kradzieżom i agresywnym zachowaniom. Pomimo, że monitoring wykonywany na zlecenie pracodawcy często ma uzasadnione podstawy, pojawia się obawa, że w dobie nowoczesnych technologii, narzędzia do tego wykorzystywane mogą ograniczać prywatność pracowników. Celem niniejszego artykułu jest zbadanie, kiedy i w jakich warunkach pracodawca może monitorować działalność pracownika oraz jakich narzędzi może w tym celu użyć.

Słowa kluczowe: prywatność, RODO, pracownik, monitoring, ochrona danych

Monitoring the employees at the workplace and protection of his privacy

Summary

Monitoring employees at their workplace is a common phenomenon and seems socially acceptable. Employers often introduce a tool of increased control for simple and understandable reasons: they want to increase the efficiency of employees, check whether employees perform their assigned tasks or counteract theft or aggressive behaviour during working hours. Although the monitoring performed on behalf of the employer often has reasonable grounds, there is a fear that in the era of modern technologies, the tools used for this purpose may limit the privacy of employees. The purpose of this article is to investigate when and under what conditions an employer can monitor the employee's activity and what tools he can use for this purpose.

Keywords: privacy, GDPR, employee, monitoring, data protection

Dominika Kuźnicka,
University of Wrocław, Faculty of Law and Administration,
ul. Uniwersytecka 22/26, 50-145 Wrocław, Poland,
e-mail: dominika.kuznicka@uwr.edu.pl.