Fragment

Monitoring zgodny z RODO. Praktyczny poradnik z wzorami dla sektora publicznego i prywatnego

Michał Kibil

Rozdział II. Monitoring wizyjny miejsca pracy

1. Pod obserwacją

Od ponad 30 lat obserwujemy dynamiczny rozwój monitoringu wizyjnego. Z początku mogły sobie na niego pozwolić tylko obiekty o szczególnym znaczeniu (takie jak obiekty wojskowe czy też elektrownie) – dzisiaj monitoring wizyjny jest stosowany praktycznie wszędzie.

Z biegiem czasu, wraz z rozwojem technologii (wpływającym na miniaturyzację kamer oraz znaczny spadek ich ceny), a także upowszechnieniem idei poszerzonej kontroli (za wyższe dobro przyjmuje się bezpieczeństwo prywatne i publiczne niż prywatność osób nagrywanych), monitoring zaczął wkraczać w praktycznie każdy aspekt naszego życia. Kamery monitorujące ulice stały się nieodłącznym elementem miejskiego krajobrazu. Monitorujemy już nie tylko skwery i ulice, lecz także biura, sklepy, restauracje, a nawet – jak wskazuje Fundacja Panoptykon[1] – toalety publiczne. Prościej jest wskazać pojedyncze przykłady obiektów, które nie są monitorowane, niż wymieniać te, w których kamery są instalowane.

Nowoczesne rozwiązania monitoringu wizyjnego pozwalają precyzyjnie identyfikować osoby pozostające w obiektywie kamery, a jak pokazuje przykład chiński, wykryć także popełniane przez nie wykroczenia lub przestępstwa, a następnie podjąć decyzję o ukaraniu. Przedsiębiorcy coraz częściej rozszerzają funkcjonalności monitoringu wizyjnego o analitykę behawioralną (np. klientów galerii handlowych), wprowadzane są reklamy dostosowujące się do obserwującej je osoby czy też połączenia monitoringu wizyjnego i kamer termowizyjnych rozpoznawające w zakładach pracy osoby chore.

[1] Zob. https://panoptykon.org/files/monitoring-wizyjny-w-zyciu-spolecznym_raport-z-badan.pdf (dostęp: 19.6.2020 r.).

Nie ma dzisiaj żadnych technicznych przeszkód, aby w oparciu o monitoring wizyjny nie rozliczać rzeczywistego czasu pracy pracownika, nie rozpocząć wykrywania zachowań niepożądanych czy też nie wprowadzać systemów kontroli dostępu opartych na naszej biometryce. Wszystko pozostaje w granicach wyobraźni osoby, która chciałaby takie rozwiązania wprowadzać – nie na wszystko przy tym pozwalają przepisy prawa.

2. Od Dzikiego Zachodu do RODO

Stosowanie monitoringu wizyjnego (w uzasadnionych prawnie przypadkach) jest odstępstwem od prawa do ochrony życia prywatnego i do ochrony własnego wizerunku. Akceptujemy go, bo ma nam zapewniać bezpieczeństwo (a przynajmniej w większości przypadków tak jest tłumaczone jego wprowadzenie) lub chronić nasze inne istotne interesy. „Żadne z pozostałych zastosowań nie przemawia do ludzkiej świadomości tak mocno jak konieczność chronienia się przed zachowaniami szkodliwymi i niebezpiecznymi dla zdrowia i życia ludzi”[2].

Jak wskazuje EROD: „Chociaż osoby fizyczne mogą czuć się swobodnie z nadzorem wideo skonfigurowanym na przykład w określonym celu bezpieczeństwa, należy podjąć (muszą istnieć) gwarancje, aby uniknąć niewłaściwego użycia (takiego nagrania) do zupełnie innych i – dla osoby, której dane dotyczą – nieoczekiwanych celów (np. celu marketingowego, monitorowania wydajności pracowników itp.)”[3]. Niezależnie od tego, czy się z tym zgadzamy, czy też nie – w celu wprowadzenia odpowiednich gwarancji bezpieczeństwa, także w obszarze monitoringu, wprowadzono RODO.

Wszystkie poniższe wskazówki co do stosowania monitoringu wizyjnego, oparte zostały na przepisach RODO, przepisach Kodeksu Pracy oraz aktualnych wytycznych UODO, Europejskiej Rady Ochrony Danych, Grupy Roboczej Art. 29 oraz Europejskiego Inspektora Ochrony Danych (EIOD).

3. Wymogi co do stosowania monitoringu wizyjnego w zakładach pracy wprowadzone przez RODO

3.1. Przetwarzanie danych przy wykorzystaniu monitoringu wizyjnego

Zanim rozpoczniemy analizę, jak powinniśmy wdrożyć monitoring w zakładzie pracy, powinniśmy najpierw rozważyć, czy na pewno odnosi się do nas RODO.

---

[2] *J. Skórzyńska-Ślusarek*, Monitoring wizyjny w życiu społecznym. Raport z badań, Fundacja Panoptykon, Warszawa 2013.

[3] Wytyczne EROD Nr 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń video, wersja 2.0. przyjęta 29.1.2020 r.

Co wymaga wyraźnego podkreślenia, **nie każde wykorzystywanie kamer wideo (także w zakładzie pracy) będzie wymagało stosowania przepisów o ochronie danych osobowych**.

Zasadniczo **przepisów RODO nie będziemy stosowali tam, gdzie przy wykorzystaniu kamery danej osoby nie można zidentyfikować, bezpośrednio lub pośrednio**.

Europejska Rada Ochrony Danych w swoich wytycznych wskazuje, że pod RODO nie będzie podlegać m.in.:

1) **użycie atrap kamer** (ich wykorzystanie w żaden sposób nie jest ograniczone przez polskie przepisy),
2) **nagranie z dużej wysokości, jeżeli nie można na nim zidentyfikować żadnej konkretnej osoby**, czy też
3) **używanie kamery wideo wspierającej parkowanie samochodu**, jeżeli nie zbiera ona żadnych informacji (nie nagrywa obrazu jakiejkolwiek osoby fizycznej lub tablicy rejestracyjnej innego samochodu).

W kontekście atrap kamer należy zasygnalizować, że pomimo iż w żaden sposób nie przetwarzamy przy ich pomocy danych osobowych (bo nie jest to fizycznie możliwe), według UODO takie atrapy powinny być zakazane, jako wprowadzające u potencjalnie monitorowanych poczucie ingerencji w sferę prywatności. Stanowisko UODO nie stanowi jednak wiążącego zakazu, a raczej oczekiwanie kierowane do ustawodawcy. Ponieważ – jak zostało to wskazane powyżej – kamery takie nie stanowią elementu monitoringu wizyjnego (bo nie są przetwarzane z ich wykorzystaniem żadne dane osobowe), a ustawodawca nie zabronił nam ich stosować, ciężko uznać ich używanie za niedopuszczalne.

W kontekście wyjątku od zasady w postaci używania kamery wideo wspierającej parkowanie, należy wyraźnie podkreślić, że pomimo pokusy szukania analogii **nie można tego wyjątku rozszerzać na przypadki stosowania monitoringu z udziałem operatora bez opcji nagrywania**. W przeciwieństwie do kamery cofania montowanej w samochodzie, użycie przez pracodawcę monitoringu, który nie utrwala obrazu, jest takim samym przetwarzaniem danych osobowych pracowników, jak zapisywanie tego obrazu na fizycznym dysku.

3.2. Podstawa przetwarzania danych

Jeżeli nasz monitoring spełnia wymogi kwalifikujące go do podlegania pod RODO, pierwszym krokiem, jaki musimy wykonać, jest wybór podstawy przetwarzania danych (podstawy zakładania monitoringu w zakładzie pracy). Według wytycznych EROD, zasadniczo każda podstawa przetwarzania wskazana w art. 6 RODO może uzasadniać stosowanie monitoringu wizyjnego w zakładzie pracy (chociaż ciężko zrozumieć, w jaki sposób stosowanie monitoringu mogłoby być uzasadnione wykonywaniem umowy zawartej między pracodawcą a osobą nagrywaną). Przy powyższym zasadniczo **za najbardziej właściwy uznaje się uzasadniony interes administratora** (art. 6 ust. 1 lit. f RODO), a tam gdzie będziemy mieli do czynienia z przetwarzaniem w interesie publicznym, dodatkową podstawą może być także art. 6 ust. 1 lit. e RODO.

Trzeba jednak **odradzić opieranie monitoringu na zgodzie osób podlegających monitoringowi**. Z ogólnych zasad RODO wynika, że zgoda dla swojej ważności musi być udzielona dobrowolnie, konkretnie, świadomie i jednoznacznie. Stosując monitoring w zakładzie pracy, przeważnie obejmujemy nim większą liczbę osób niż pojedynczy pracownik. Tym samym, bazując na zgodzie, należałoby uzyskać zgodę od każdej osoby monitorowanej i każda ze zgód musiałaby spełniać powyższe warunki. Ponadto trzeba by było udowodnić, że zgody wszystkich osób mieliśmy przed nagraniem, a w przypadku cofnięcia zgody musielibyśmy zaprzestać nagrywania. Można wątpić, czy oparcie monitoringu na uzyskanej zgodzie ma jakikolwiek sens.

Jak wskazuje EROD w swoich wytycznych, w stosunkach pracy, opieranie monitoringu na zgodzie pracownika jest wątpliwe z jeszcze jednego powodu. Mianowicie relacja pracownicza tworzy pewną nierówność, w której pracodawca może wydać pracownikowi wiążące polecenie służbowe, a pracownik obowiązany jest je wykonać. Pracodawca płaci pracownikowi wynagrodzenie za jego pracę. Ostatecznie od pracodawcy zależy, czy pracownik będzie nadal pracownikiem, czy też nie. W tych okolicznościach racjonalne jest wątpienie, czy jakakolwiek zgoda pracownika, udzielana pracodawcy, będzie wyrażana dobrowolnie (co, jak wskazano, jest warunkiem skuteczności takiej zgody).

3.3. Uzasadniony interes

Jeżeli przy wprowadzaniu monitoringu wizyjnego wybraliśmy podstawę uzasadnionego interesu (co – jak zostało wskazane powyżej – jest najlepszym możliwym rozwiązaniem), w pierwszej kolejności jesteśmy zobowiązani przeprowadzić tzw. test równowagi.

Wskazany test polega na:
1) ustaleniu, czy faktycznie istnieją uzasadnione interesy pracodawcy do wprowadzania monitoringu oraz czy interesy te są zgodne z prawem, konkretne i rzeczywiste,
2) zidentyfikowaniu interesów lub podstawowych praw i wolności podmiotu, które mogą być naruszone przez stosowanie przez nas monitoringu,
3) dokonaniu ważenia interesów administratora i osoby, której dane dotyczą – tj. określenie, czyj interes jest ważniejszy,
4) ustaleniu (zgodnie z zasadą minimalizacji), czy przetwarzanie danych osobowych w danych okolicznościach jest konieczne,
5) udokumentowaniu przeprowadzonej analizy i wyniku testu.

3.3.1. Ustalenie istnienia interesu pracodawcy

Gdy ustalamy, czy mamy uzasadniony interes we wprowadzaniu monitoringu, nie mamy do wyboru zbyt wielu opcji, na których monitoring moglibyśmy oprzeć. Zgodnie z przepisami KP mamy tylko kilka przyczyn, ze względu na które możemy stosować monitoring w zakładzie pracy. Są to:
1) zapewnienie przez pracodawcę bezpieczeństwa pracowników,
2) zapewnienie przez pracodawcę ochrony mienia,
3) zapewnienie przez pracodawcę kontroli produkcji,
4) zapewnienie zachowania informacji poufnych.

Jeżeli powód, dla którego chcemy wprowadzić monitoring, mieści się w jednej z powyższych kategorii, a jednocześnie jest zgodny z prawem, konkretny i rzeczywisty, nasz interes w stosowaniu monitoringu jest uzasadniony.

Ponieważ ustawodawca, projektując przepisy KP, najwyraźniej uznał, że pracodawcy, chcąc stosować monitoring, zawsze będą się mieścić w przytaczanych kategoriach powodów, **powyższy katalog jest zamknięty**. Oznacza to, że pracodawca nie może stosować monitoringu wizyjnego m.in. ze względu na swoje inne uzasadnione potrzeby, np.:

1) potrzebę sprawdzania postępów pracownika w pracy,
2) potrzebę weryfikacji, czy pracownicy nie dopuszczają się zachowań niepożądanych w pracy,
3) potrzebę weryfikacji obecności pracownika w pracy.

Przykład

Na gruncie art. 22^2 § 3 KP, nawet jeżeli nagranie z monitoringu mogłoby służyć pomocą w wyjaśnieniu zarzutu mobbingu, pracodawca, stosując monitoring, nie może wykorzystać zapisu wideo do takiego dodatkowego celu.

Niezależnie od tego, że wybrany powód stosowania monitoringu będzie mieścił się w którymś z przedstawionych celów, pracodawca nie będzie zwolniony od badania, czy jego interes w stosowaniu monitoringu jest wystarczająco istotny.

Zarówno UODO, jak i EROD, a także EDPS rekomendują weryfikację, czy potrzeba stosowania monitoringu wynika jedynie z poczucia podmiotu wprowadzającego monitoring wizyjny, czy też jest to zobiektywizowana potrzeba. Z pewnością, jeżeli przed wdrożeniem monitoringu wizyjnego (lub w trakcie jego stosowania) kogokolwiek przyłapano na kradzieży, oszustwie lub wandalizmie, pracodawca nie będzie miał problemu, aby wykazać, że jego interes jest istotny. Co jednak, jeżeli taka sytuacja nigdy nie wystąpiła? Pracodawca, analizując swoje ryzyka, powinien wyraźnie określić, dlaczego w jego przypadku występują wskazane wyżej zagrożenia w wyższym stopniu niż w standardowym zakładzie pracy. Może to wynikać z charakteru pracy pracowników (np. pracy z gotówką lub jej ekwiwalentami, takimi jak kupony rabatowe), położenia zakładu pracy w niebezpiecznej okolicy, potencjalnego dostępu do mienia pracowników przez osoby niepowołane, jak też dostępu do szczególnie poufnych informacji (np. w związku z pracą dla podmiotu notowanego na Giełdzie Papierów Wartościowych).

Ważne

Ponieważ to na pracodawcy spoczywa ciężar wykazania jego uzasadnionego interesu, rekomendowane jest zbieranie dowodów potwierdzających szczególną potrzebę pracodawcy co do stosowania monitoringu wizyjnego w celu realizacji konkretnych interesów.

3.3.2. Ustalenie interesów osób monitorowanych

Kolejnym krokiem jest identyfikacja praw i interesów osób, które mają i mogą być przez nas monitorowane. Najczęściej będziemy konfrontować się z prawem do zachowania przez pracownika prywatności, prawem do ochrony życia prywatnego, czci i dobrego imienia, a także prawem nienaruszalności godności osobistej (które to zagadnienie może

się pojawiać szczególnie w przypadku, gdyby monitoring miał rejestrować pracownika w krępujących go sytuacjach).

Jak wskazuje motyw 47 RODO, gdy rozważamy, jakie prawa i interesy osób monitorowanych moglibyśmy naruszać naszym monitoringiem, powinniśmy także rozważyć, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu.

Przykład

Nie można zakładać, że pracownik powinien spodziewać się, że monitoring będzie stosowany w kuchni, w której przygotowuje sobie posiłek, a potem go spożywa. Jeżeli monitoring miałby być tam wprowadzony, musiałoby to zostać wyraźnie przekazane wszystkim, którzy takim monitoringiem mieliby być objęci, z wyraźnym wykazaniem, dlaczego ich prywatność podczas spożywania posiłków ma być zakłócana poczuciem bycia monitorowanym. Umieszczenie tabliczki informacyjnej nie byłoby wystarczające.

3.3.3. Ważenie interesów administratora i osoby monitorowanej

Gdy już wiemy, jakie mamy potrzeby pod kątem wprowadzania monitoringu oraz jakie są prawa i interesy osób, które będziemy monitorować, musimy ustalić, który z interesów jest ważniejszy – ich czy nasz? Na tak postawione pytanie nie ma jednoznacznej odpowiedzi. Przy podejmowaniu decyzji o stosowaniu monitoringu administrator powinien rozważyć, w jakim stopniu monitorowanie wpływa na interesy, podstawowe prawa i wolności monitorowanych osób oraz czy powoduje to naruszenia lub negatywne konsekwencje w odniesieniu do ich praw. Później można odpowiedzieć sobie na pytanie, co będzie obiektywnie gorsze – naruszenie tego konkretnego interesu osoby monitorowanej, czy narażenie zakładu pracy na określone ryzyko.

Przykład

Sytuacją, w której interes pracodawcy jest generalnie ważniejszy od interesu osoby monitorowanej, będzie stosowanie bieżącego monitoringu w sklepie w galerii handlowej, gdzie ze względu na doświadczenia właściciela dochodziło wcześniej do wielu kradzieży, kamera skupiona jest na produktach, a zarówno pracownicy, jak i klienci sklepu pojawiają się tylko w poszczególnych minutach filmu. Prawne interesy osób uwiecznianych na obrazie z monitoringu są naruszane jedynie w znikomym stopniu, a właściciel sklepu zapewnia konieczną ochronę swojego mienia.

Przykład

Interes pracodawcy będzie mniej istotny od interesu osoby monitorowanej w przypadku umieszczenia kamer monitoringu skierowanych na osobiste szafki lub kontenerki pracowników, bez wcześniejszych incydentów wskazujących na kradzieże przez pracowników jakichkolwiek dóbr. Naturalnie istnieje interes w tym, żeby zapewniać bezpieczeństwo mienia pracodawcy, ale w tym wypadku przeważa prawo pracownika do prywatności zawartości jego osobistej szafki.

Zarówno istnienie uzasadnionego interesu, jak i ustalenie interesów i praw osób monitorowanych, a także kwestia ustalania wagi interesów (w tym konieczności stosowania monitoringu) powinny być poddawane okresowym (np. corocznym) ocenom i rewidowane.

3.3.4. Minimalizacja przetwarzania

Teoretycznie stwierdzając, że interes pracodawcy przeważa nad interesem pracownika, moglibyśmy uznać, że można montować monitoring. Nic bardziej mylnego. Przed rozpoczęciem stosowania monitoringu wizyjnego (a także podczas okresowych kontroli adekwatności stosowanych środków) pracodawca musi rozważyć, czy monitoring wizyjny jest odpowiedni oraz niezbędny do osiągnięcia pożądanego celu. Zgodnie z wytycznymi EROD monitoring wizyjny powinien być stosowany tylko wtedy, kiedy oczekiwanego celu (np. zabezpieczenia mienia) nie można osiągnąć za pomocą innych środków, mniej ingerujących w podstawowe prawa i wolności osoby, której dane dotyczą.

Przykład

Jeżeli monitoring wizyjny miałby być wprowadzany ze względu na ryzyko, że pracownik będzie zgrywał dane na USB, lepszym rozwiązaniem jest zablokowanie portów USB. Jeżeli z kolei monitoring wizyjny miałby być wprowadzony ze względu na ryzyko kradzieży rzeczy z szafek pracowniczych, pracodawca w pierwszej kolejności powinien rozważyć zastosowanie kłódek zabezpieczających dostęp do szafek.

W każdym przypadku decyzja co do stosowanych środków spoczywa na pracodawcy, niemniej jednak monitoring wizyjny, w ujęciu wytycznych wszystkich organów, powinien być stosowany jako ostateczna alternatywa (gdy żaden inny środek nie doprowadzi do celu – np. zabezpieczenia banknotów przed kradzieżą przez pracownika).

Pod kątem minimalizacji przetwarzania pracodawca, wprowadzając monitoring, powinien rozważyć m.in., czy stosowanie monitoringu wizyjnego jest potrzebne przez cały dzień (czy np. można ograniczyć go do godzin nocnych) oraz jaki obszar ma być objęty monitoringiem. Musi być on maksymalnie zawężony (w tym zakresie, w którym przetwarzany jest wizerunek poszczególnych osób), a w miarę możliwości technicznych obszary, które nie powinny być objęte monitoringiem, trzeba wypikselować (alternatywnie zaciemnić).

Pomimo że standardem przy stosowaniu monitoringu jest umożliwienie bieżącego śledzenia obrazu z kamer, wskazany tryb postępowania powinien być stosowany tylko wtedy, gdy istnieje konieczność złapania kogoś „na gorącym uczynku" bądź śledzenie obrazu z kamer może zapobiec powstaniu lub zwiększeniu wymiaru szkody pracodawcy.

3.3.5. Dokumentacja

Ponieważ to na administratorze ciąży obowiązek wykazania, że spełnił wszystkie wymogi RODO, także w przypadku stosowania monitoringu, powinien on udokumentować wszystkie kroki powyżej wskazywanego testu równowagi. Brak podjęcia wskazanego działania może administratora narazić na odpowiedzialność określoną w odrębnych przepisach.

4. Pozostałe wymogi dotyczące stosowania monitoringu

Z pewnością przy stosowaniu monitoringu w zakładzie pracy nie możemy zapomnieć o:
1) odpowiednim poinformowaniu osób monitorowanych o monitoringu,
2) stosowaniu prawidłowych okresów retencji (usuwania danych, których nie powinniśmy dalej przetwarzać), a także
3) zapewnieniu przestrzegania pozostałych praw obserwowanych.

4.1. Obowiązek informacyjny

Zgodnie z wytycznymi EROD[4] w przypadku stosowania monitoringu wizyjnego obowiązek informacyjny powinien zostać spełniony w nieco odmienny sposób od tego, do którego jesteśmy przyzwyczajeni. Zaleca się, aby spełnienie obowiązku zostało rozdzielone na dwie kategorie informacji:
1) **informację graficzną o stosowanym monitoringu**, umieszczoną przed wejściem w strefę objętą monitoringiem, mniej więcej na wysokości oczu osób, do których ta informacja jest kierowana, obejmującą co najmniej:
   a) przyczyny stosowania monitoringu,
   b) oznaczenie administratora,
   c) dane kontaktowe do administratora,
   d) informacje, które mają największy wpływ na osobę monitorowaną, takie jak:
      – czas przetwarzania danych,
      – fakt obsługi monitoringu przez operatora,
      – informację o przekazywaniu danych z monitoringu do podmiotów trzecich (np. firmy ochroniarskiej współpracującej z administratorem),
   e) odesłanie do źródła wszystkich informacji dotyczących przetwarzania danych (zarówno dostępnego *on-line* – np. przez odesłanie z wykorzystaniem kodu QR[5] – jak i w miarę możliwości do informacji, gdzie można pozyskać pełną wersję informacji – w formie papierowej lub pod jakim numerem telefonu);
2) **pełną informację o przetwarzaniu danych osobowych, związaną ze stosowanym monitoringiem**, zgodną z art. 13 i 14 RODO. Co istotne, jeżeli pracownik lub współpracownik otrzymał informację o przetwarzaniu jego danych osobowych, nie trzeba przekazywać mu nowej informacji o monitoringu – **wystarczy zaktualizować poprzednią**.

Ważne

Europejska Rada Ochrony Danych nie wymaga oznaczania graficznie kamery umieszczonej w zakładzie pracy. W ocenie wskazanego organu wystarczające jest umieszczenie oznaczenia przed daną strefą objętą monitoringiem. Ponieważ w zasadniczej części przypadków pracodawca, moni-

[4] Wytyczne EROD Nr 3/2019 w sprawie przetwarzania danych osobowych za pośrednictwem urządzeń video, wersja 2.0. przyjęta 29.1.2020 r.
[5] *Quick Response Code* – alfanumeryczny, dwuwymiarowy, matrycowy, kwadratowy kod graficzny opracowany przez japońskie przedsiębiorstwo Denso-Wave w 1994 r., wykorzystywany powszechnie jako odesłanie do strony internetowej przez jego odczyt z wykorzystaniem aparatu fotograficznego w telefonie komórkowym.

torując poszczególne pomieszczenia, będzie miał różne cele, dla każdej odrębnej strefy powinna być przygotowana odrębna informacja lub tabliczka.

Artykuł 22^2 § 9 KP jako alternatywę dla wprowadzenia graficznej informacji o monitoringu wprowadza ogłoszenia dźwiękowe. Nie przekreślając racjonalności wskazanego rozwiązania, należy wyraźnie podkreślić, że jeżeli pracodawca zdecydowałby się na taką formę przekazywania informacji, powinien się liczyć z koniecznością powtarzania komunikatu przy zatrudnianiu każdego kolejnego pracownika, a tam gdzie monitoring będzie obejmował osoby trzecie, przy wejściu np. każdego nowego klienta do sklepu.

4.2. Okres przetwarzania danych

Przepisy KP są wyjątkowo jednoznaczne w zakresie terminu usunięcia danych pozyskanych z monitoringu wizyjnego. Zgodnie z art. 22^2 KP nagranie powinno być usunięte w ciągu 3 miesięcy od dnia, w którym zostało sporządzone. **Aby wypełnić wymóg co do retencji, rekomendowane jest wprowadzenie funkcji automatycznego kasowania danych po upływie czasu nie dłuższego niż 3 miesiące.**

Wyjątkiem od wskazanego terminu jest sytuacja, w której nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa (czyli raczej nie w postępowaniu wewnętrznym, które co do zasady – poza komisją pojednawczą – nie jest uregulowane przepisami) lub pracodawca dowiedział się, że mogą one stanowić dowód w takim postępowaniu. W tych przypadkach termin usunięcia ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

Pewne wątpliwości co do stosowania tego przepisu mogą się pojawić w przypadku, gdy przed upływem 3 miesięcy żadne postępowanie nie zostanie zainicjowane, ale pracodawca zostanie poinformowany o możliwości zainicjowania tego typu postępowania (np. przez kierowanie do pracodawcy wezwania do zapłaty związanego z wypadkiem przy pracy). W takim przypadku należy przyjąć, że pracodawca będzie legitymowany do zarchiwizowania tej części materiałów wideo (o ile monitorował bezpieczeństwo pracowników, które można rozumieć jako bezpieczeństwo BHP), które mogą stanowić dowód w sprawie (obrazujących zdarzenia, do których pracownik odniósł się w wezwaniu), do upływu terminu przedawnienia roszczeń pracownika. Zarchiwizowany materiał, wraz z kopią zawiadomienia pracownika, dla bezpieczeństwa powinien być pozostawiony w prowadzonej przez pracodawcę dokumentacji dotyczącej przetwarzania danych osobowych.

Co jest istotne, gdy pracodawca przekaże kopię nagrania, np. do postępowania sądowego, przestanie odpowiadać za kwestię retencji danych zgromadzonych przez sąd. Sąd będzie odpowiadać za materiał zgromadzony w aktach sprawy jako odrębny administrator, na podstawie właściwych przepisów określających sposób prowadzenia i archiwizowania akt postępowania.

4.3. Pozostałe prawa obserwowanych

Na ogólnych zasadach, stosowanych także względem monitoringu wizyjnego, osoba, której dane są przetwarzane, jest uprawniona do:

1) wcześniej wspomnianego **prawa do informacji** o istnieniu monitoringu w określonym miejscu, jego zasięgu, celu, nazwie podmiotu odpowiedzialnego za instalację, jego adresie i danych do kontaktu. Jeżeli pracodawca nie zrealizował wcześniej tego obowiązku lub zrealizował go w niepełny sposób, osoba monitorowana może się upomnieć o swoje prawa;
2) **dostępu do nagrań** w uzasadnionych przypadkach oraz tak, aby nie naruszało to interesów osób trzecich, które mogłyby na tym monitoringu się znaleźć. Na potrzeby udostępniania zapisów monitoringu pracodawca powinien wprowadzić odpowiednią procedurę, którą również na potrzeby swojego zakładu pracy może włączyć do zapisów regulaminów pracy (np. w części dotyczącej wyjaśniania incydentów);

Ważne

Udostępniając materiał wideo osobie zainteresowanej, udostępniajmy tylko tę część, która może dotyczyć tej osoby. Pozostałe zapisy nie są do jej wglądu.

3) **prawo żądania usunięcia danych jej dotyczących**, o ile pracodawca nie wykaże, że jego interes w utrzymaniu danego fragmentu zapisu jest istotniejszy – np. ze względu na ujawnione nadużycia;
4) **prawo do anonimizacji wizerunku** na zarejestrowanych obrazach i/lub usunięcia dotyczących jej danych osobowych, o ile pracodawca nie wykaże, że jego interes w utrzymaniu danego fragmentu zapisu jest istotniejszy – np. ze względu na ujawnione nadużycia;
5) **prawo do przetwarzania danych przez ograniczony czas**, jeżeli pracodawca nie stosuje się do zasad retencji określonych powyżej.

5. Monitoring wizyjny a dane biometryczne

Co zostało podkreślone we wcześniejszej części komentarza, dzisiejsza technologia pozwala w pełnym zakresie łączyć monitoring wizyjny z metodami analizy obrazów. W ten sposób możliwe jest rozpoznawanie osób uwiecznionych na materiale wideo, analizowanie zachowań pracowników, weryfikacja, jak pracownik porusza się po terenie zakładu pracy, jaką ma temperaturę ciała, a także wiązanie wskazanych zachowań i motoryki ze zautomatyzowanym podejmowaniem decyzji.

Zgodnie ze stanowiskiem UODO[6] taki system monitoringu będzie w rzeczywistości w każdym przypadku przetwarzał dane biometryczne w rozumieniu art. 9 ust. 1 RODO.

[6] Zob. https://uodo.gov.pl/pl/file/1200 (dostęp: 19.6.2020 r.).

Istnieją podzielone poglądy co do tego, czy w polskich zakładach pracy jest w ogóle możliwe (a jeżeli tak, to w jakim zakresie) stosowanie tego typu systemów monitoringu wizyjnego, w powiązaniu z funkcjami analizy biometrycznej.

Na gruncie samego RODO odmienne stanowisko wyraziła Grupa Robocza Art. 29 w opinii Nr 2/2017 na temat przetwarzania danych w miejscu pracy[7] (gdzie wskazuje, że „takie działania w nieproporcjonalny sposób naruszają prawa i wolności pracowników, dlatego też zasadniczo uznaje się je za bezprawne"), a odmienne EROD w swoich najbardziej aktualnych wytycznych dotyczących monitoringu wizyjnego, gdzie wskazuje, że przetwarzanie danych biometrycznych w ramach stosowanego monitoringu jest na gruncie RODO prawnie możliwe (pod określonymi warunkami). Autor niniejszego rozdziału uważa stanowisko EROD za bardziej prawidłowe (tak długo jak istnieje przesłanka z art. 9 RODO do przetwarzania danych).

Ograniczeniem co do stosowania wskazanych systemów monitoringu wizyjnego, obejmujących analitykę biometryczną, jest brak możliwości powołania się na interes pracodawcy (jako że art. 9 RODO nie przewiduje takiej podstawy), a co do zakresu stosowania monitoringu, przepisy KP, który (abstrahując od tego, że w zapisach dotyczących monitoringu wizyjnego w ogóle nie odnosi się do danych sensytywnych) w ogólnych postanowieniach dotyczących przetwarzania danych osobowych ograniczył możliwość przetwarzania danych biometrycznych tylko do dwóch przypadków:

1) gdy nastąpiło to z inicjatywy pracownika (co jest czymś zdecydowanie szerszym od zgody pracownika),
2) bez wymogu zgody pracownika, gdy jest to niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę lub dostępu do pomieszczeń wymagających szczególnej ochrony.

Patrząc na zbieg przepisów, poza sytuacją, w której pracownicy wyjdą ze wspólną inicjatywą wprowadzenia rozwiązania łączącego funkcje monitoringu wizyjnego oraz biometryki (np. wszyscy zgodnie wyjdą z inicjatywą monitorowania temperatury ciała pracowników w okresie epidemiologicznym), jedynym przypadkiem, w którym wydaje się być dopuszczalne stosowanie tego typu rozwiązań, jest wprowadzanie systemów monitoringu wizyjnego, których celem jest umożliwianie dostępu pracownikom do poszczególnych pomieszczeń zakładu pracy wymagających szczególnej ochrony lub dostępu do szczególnie ważnych informacji. Tak długo, jak istnieje wskazane ograniczenie w KP, pracodawcy mogą się obawiać (pod kątem kontroli UODO) wprowadzania innych rozwiązań (niezależnie od tego, jak wspierałyby ich pracę).

W każdym wypadku tego typu operacje wymagać będą dokonania oceny skutków dla ochrony danych na podstawie art. 35 ust. 3 lit. b RODO obok wymaganej dla systemów monitoringu oceny na podstawie lit. c tego samego przepisu.

Na podstawie oceny skutków należy:

1) dokonać modyfikacji polityk, procedur i procesów dla monitoringu wizyjnego,

[7] Zob. https://uodo.gov.pl/pl/file/18 (dostęp: 19.6.2020 r.).

2) zastosować niezbędne środki bezpieczeństwa dla ochrony danych i dla zminimalizowania zidentyfikowanych ryzyk lub nawet skonsultować się z UODO[8], gdyby ocena potwierdziła, że przetwarzanie spowoduje wysokie ryzyko pomimo zastosowanych środków bezpieczeństwa.

6. Zakaz stosowania ukrytego monitoringu

Zasadniczo, zarówno UODO, jak i EROD oraz EIOD wskazują, że **bezwzględnie niedozwolone jest stosowanie ukrytego monitoringu**.

Przeciw takiemu rozumieniu przepisów wypowiedział się w 2019 r. ETPCz. Jak zostało wskazane w wyroku z 17.10.2019 r. wydanym w sprawie *López Ribalda i inni przeciwko Hiszpanii* (1874/13, Legalis), ETPCz uznał, że stosowanie wobec pracowników ukrytego nadzoru za pomocą kamer wideo może być usprawiedliwione w określonych sytuacjach. Taką sytuacją – zdaniem sądu – jest uzasadnione podejrzenie poważnych uchybień pracowniczych oraz ryzyko dużych strat firmy. Sąd w rozpatrywanej przez siebie sprawie uznał, że w takim przypadku nie mamy do czynienia z naruszaniem prawa do prywatności, na której ochronę powołują się wszystkie wskazane powyżej organy, odmawiając pracodawcom prawa do stosowania ukrytego monitoringu. Sprawa dotyczyła 14 pracowników hiszpańskiego supermarketu, którzy w sposób zorganizowany okradali sklep. Umieszczenie ukrytych kamer pozwoliło ujawnić ich bezprawne działania. Była to więc nietypowa i dosyć skrajna sytuacja.

Czy wskazane orzeczenie daje pracodawcom wolną rękę do stosowania ukrytego monitoringu? W żadnym wypadku nie. Wydaje się ono jednak kluczowe w sytuacji wystąpienia u pracodawcy przypadku analogicznego do tego w hiszpańskim supermarkecie oraz przy poszukiwaniu argumentacji do zważenia interesów pracodawcy (administratora) oraz osób, których dane są przetwarzane, tak aby wskazany monitoring można było wyjątkowo wprowadzić.

Aby uniknąć zarzutu niespełnienia obowiązku informacyjnego, w razie konieczności zastosowania ukrytego monitoringu lepiej traktować go jako monitoring dodatkowy, wobec pełnego, jawnego monitoringu, przy jednoczesnym założeniu, że informacje o wprowadzeniu monitoringu w celu ochrony mienia będą dotyczyły wszystkich kamer – i tych jawnych, i tych raczej niewidocznych.

[8] Na podstawie art. 36 ust. 1 RODO oraz art. 57 ust. 1 OchrDanychU, gdy w wyniku przeprowadzonej oceny skutków dla ochrony danych na liście badanych operacji przetwarzania znajdą się operacje, dla których ryzyko naruszenia praw i wolności oszacowane zostało jako wysokie i gdy administrator danych nie może znaleźć środków wystarczających do zmniejszenia (zminimalizowania) tego ryzyka do dopuszczalnego poziomu (art. 36 RODO), administrator danych może wystąpić do UODO o uprzednie konsultacje. Jak wskazuje UODO (https://uodo.gov.pl/pl/127/216; dostęp: 19.6.2020 r.) uprzednie konsultacje są narzędziem służącym do współpracy pomiędzy organem nadzorczym oraz administratorem, a ich celem jest jak najlepsze zabezpieczenie operacji przetwarzania danych osobowych przez administratora przy współpracy organu nadzorczego.

7. Ograniczenia w stosowaniu monitoringu

Na gruncie KP, poza wcześniej wspominanymi ograniczeniami dotyczącymi monitoringu biometrycznego, przewidziane zostały także ograniczenia dotyczące miejsca umieszczania monitoringu.

Kodeks pracy przewiduje dwa wyłączenia:
1) **bezwzględne** – z którego wynika że bez jakiegokolwiek wyjątku zabronione jest umieszczanie monitoringu w pomieszczeniach udostępnianych zakładowej organizacji związkowej oraz
2) **względne** – zabraniające umieszczania monitoringu wizyjnego w pomieszczeniach sanitarnych, szatniach, stołówkach oraz palarni.

Monitoring w tych miejscach jest możliwy do zastosowania, jeżeli:
1) jest to niezbędne do realizacji celu, dla którego wprowadzany jest monitoring,
2) nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób.

Ważne

Zasadniczo monitoring pomieszczeń sanitarnych wymaga w każdym wypadku uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.

Pomimo wątpliwości, jakie sygnalizuje się w części komentarzy, wskazany zakaz w żadnym zakresie nie jest iluzoryczny. Prawodawca widząc, że mogą wystąpić przypadki, w których ze względu np. na ochronę mienia pracodawcy konieczne jest zastosowanie monitoringu w pomieszczeniach sanitarnych, wprowadził rozwiązania zabezpieczające pracowników przed uznaniową decyzją pracodawcy, a także środki techniczne, które powinny zostać w takim przypadku zastosowane, aby w żaden sposób nie naruszyć godności lub innych dóbr osobistych pracownika (chociażby polegające na nagraniu pracownika, który się przebiera).

8. Stosowanie pozostałych zasad określonych w RODO

Poza szczególnymi zasadami przetwarzania danych osobowych charakterystycznymi dla monitoringu wizyjnego (o których mowa w niniejszym rozdziale), do monitoringu będą znajdowały także zastosowanie pozostałe reguły przetwarzania danych osobowych wynikające z RODO. Tak samo jak w przypadku innych obszarów, w których ochrona danych osobowych ma zastosowanie, powinniśmy wdrożyć każdorazowo rozwiązania techniczne i organizacyjne, które będą proporcjonalne do poziomu ryzyka, a także charakteru praw i wolności osób, których dane będą przetwarzane. Ze względu na pewną wrażliwość danych, które mogą być zarejestrowane na monitoringu, szczególnie istotne wydaje

się stosowanie do wcześniej wspomnianych procedur, ograniczających lub wyłączających dostęp do nagranych treści.

9. Wzór zapisu Regulaminu Pracy odnoszącego się do monitoringu wizyjnego

Przykładowy wzór zapisu Regulaminu Pracy odnoszącego się do monitoringu wizyjnego

§ ...

Monitoring wizyjny

1. W celu zapewnienia bezpieczeństwa pracowników, zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę, kontroli produkcji, a w szczególności w celu zapewnienia skutecznej ochrony mienia Pracodawcy, zgodnie z art. 5, 6 ust. 1 lit. c i f Rozporządzenia Parlamentu Europejskiego i Rady (UE) z 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 (ogólne rozporządzenie o ochronie danych) na terenie całego zakładu pracy (wewnątrz i na zewnątrz budynku), z wyjątkiem pomieszczeń określonych w ust. 2, wprowadza się monitoring wizyjny rejestrujący obraz wideo.

2. Pomieszczenia sanitarne, szatnie, stołówka, palarnia, pomieszczenie udostępnione na działalność związkową oraz inne pomieszczenia, w których, w razie zainstalowania monitoringu, mogłoby dojść do naruszenia prywatności i godności pracowników, są wolne od monitoringu wizyjnego.

3. Wejście do każdego pomieszczenia objętego monitoringiem wizyjnym jest oznaczone odpowiednimi znakami słowno-graficznymi.

4. Dostęp do materiałów pozyskanych z monitoringu, obsługę systemu kamer przemysłowych oraz pieczę nad przechowywaniem i niszczeniem nagrań z kamer przemysłowych sprawują wyznaczone w tym celu i odpowiednio przeszkolone osoby.

5. Materiały pozyskane z monitoringu będą przechowywane przez okres nie dłuższy niż 3 miesiące. Zapisy są niszczone przez nadpisanie zapisanego materiału nowym materiałem.

6. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu lub pracodawca powziął wiadomość, że mogą one stanowić dowód w postępowaniu, termin przechowywania zapisów monitoringu ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

7. Szczegółowe zasady przetwarzania danych osobowych w ramach monitoringu wizyjnego, w tym pełną informację dotyczącą przetwarzania danych z wykorzystaniem monitoringu wizyjnego, określa polityka monitoringu zakładu pracy dostępna w wersji papierowej w biurze HR.

10. Podsumowanie

Jak zostało wskazane na początku rozdziału, przez ostatnie lata przywykliśmy do stosowania monitoringu. Sami powszechnie (oraz coraz chętniej) udostępniamy informacje

o sobie oraz nasz wizerunek (w tym obejmujące nas materiały wideo) w sieci. Naturalnie w takich przypadkach (przeważnie) robimy to świadomie. Sama ta kwestia powinna skłaniać nas do refleksji, że walka z monitoringiem jest jak walka z wiatrakami. Monitoring jest narzędziem m.in. chroniącym interesy pracodawców i taka jest jego główna rola. Tak samo jak powszechnie stosowana kamera samochodowa nie jest on narzędziem mającym wywoływać strach u osób obserwowanych, tylko koniecznym środkiem do walki z nadużyciami.

Pomimo że od strony technicznej nie ma żadnych ograniczeń, aby wdrażać systemy monitoringu łączące jego funkcjonalności ze sztuczną inteligencją (aby zwiększyć jego efektywność w wykrywaniu nadużyć), tak długo, aż ustawodawca nie usunie omawianych w niniejszym rozdziale ograniczeń z treści KP, faktycznie nie będzie możliwe stosowanie tego typu innowacyjnych rozwiązań. Powyższe naturalnie nie dotyczy zakładów pracy, w których pracują wyłącznie osoby zatrudnione na podstawie umów cywilnoprawnych do nich nie będą miały zastosowania rygorystyczne przepisy KP.

Podstawa prawna:

- art. 5, 6 ust. 1, art. 9, 13–14, 35 ust. 3 lit. b, motyw 47 RODO,
- art. 22^2 KP.