# *Przegląd Prawa i Administracji*

Tom CXXXII

Monitoring w zakładzie pracy

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS No 4147

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

# *Przegląd Prawa i Administracji*

## Tom CXXXII

## Monitoring w zakładzie pracy

Pod redakcją
ARTURA TOMANKA

Wydawnictwo Uniwersytetu Wrocławskiego

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

Komitet Redakcyjny
RYSZARD BALICKI, EMILIO CASTORINA (Włochy), JOAN GOUFALEAN (Rumunia), MICHAEL HOLOUBEK (Austria), MARIUSZ JABŁOŃSKI (przewodniczący), ANDREAS JANKO (Niemcy), UWE KIRSCHEL (Niemcy), JAROSŁAW KUNDERA, PIOTR MACHNIKOWSKI, MACIEJ MARSZAŁ, TOMASZ MILEJ (Niemcy), ANDRÉS OLLERO (Hiszpania), MARIAN J. PTAK, DRINOCZI TIMEA (Węgry)

Rada Redakcyjna
JOLANTA BLICHARZ, EMILIO CASTORINA (Włochy), MARIUSZ JABŁOŃSKI, SYLWIA JAROSZ-ŻUKOWSKA, UWE KIRSCHEL (Niemcy), MACIEJ MARSZAŁ, ANDRÉS OLLERO (Hiszpania), KRZYSZTOF WÓJTOWICZ

Redaktor naczelny
MARIUSZ JABŁOŃSKI

Sekretarz Redakcji
SYLWIA JAROSZ-ŻUKOWSKA

Czasopismo jest recenzowane. Lista stałych recenzentów znajduje się na stronie http://wuwr.pl/ppa/reviewers

© Copyright by Wydawnictwo Uniwersytetu Wrocławskiego sp. z o.o., Wrocław 2023

ISSN 0239-6661 (AUWr) ISSN 0137-1134 (PPiA)

Wersją pierwotną czasopisma jest wersja drukowana

Wydawnictwo Uniwersytetu Wrocławskiego sp. z o.o.
50-137 Wrocław, pl. Uniwersytecki 15
tel. 71 3752474, e-mail: sekretariat@wuwr.com.pl


© for this edition by CNS

# SPIS TREŚCI

Słowo wstępne . . . . . 9

## MONITORING ZAKŁADOWY NA TLE KONSTYTUCYJNYM I PRAWNO-PORÓWNAWCZYM

Mariusz Jabłoński, Stosowanie wobec pracowników ukrytego monitoringu wizyjnego — kwestie sporne i niejednoznaczne . . . . . 13
Maciej J. Zieliński, Polski model regulacji monitoringu służbowej poczty elektronicznej na tle porównawczym . . . . . 31

## FORMY MONITORINGU W ZAKŁADZIE PRACY

Tomasz Bakalarz, Monitoring poczty elektronicznej a tajemnica korespondencji pracownika . . . . . 49
Dominika Dörre-Kolasa, Przetwarzanie danych osobowych pracowników w ramach tak zwanych innych form monitoringu . . . . . 63
Tomasz Radziszewski, Wybrane aspekty funkcjonowania monitoringu wizyjnego w świetle regulacji dotyczących szkół i innych placówek oświatowych . . . . . 81
Dariusz Wasiak, Prewencyjny monitoring trzeźwości pracowników. Zarys problematyki . 95
Krzysztof Wygoda, Dopuszczalność przetwarzania danych biometrycznych przez pracodawców — ujęcie modelowe i praktyczne . . . . . 107

## KONTROLA I NADZÓR NAD STOSOWANIEM MONITORINGU

Przemysław Czechowski, Rola inspektora pracy w kontroli i nadzorze stosowania monitoringu przez pracodawcę — wnioski *de lege lata* i *de lege ferenda* . . . . . 119
Janusz Krasoń, Wybrane zagadnienia związane z kontrolą monitoringu wizyjnego w zakładzie pracy prowadzonej przez inspektora pracy w kontekście ochrony danych osobowych . . . . . 139
Łukasz Paroń, Dane z monitoringu jako źródło dowodowe w postępowaniu kontrolnym państwowego inspektora pracy . . . . . 151


© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

# CONTENTS

Foreword . . . . . 9

## WORKPLACE MONITORING AGAINST THE CONSTITITUTIONAL AND COMPARATIVE LEGAL BACKGROUND

Mariusz Jabłoński, The use of hidden video monitoring against employees: Contentious and ambiguous issues . . . . . 13
Maciej J. Zieliński, The Polish regulatory model for the monitoring of business e-mail in a comparative perspective . . . . . 31

## FORMS OF WORKPLACE MONITORING

Tomasz Bakalarz, Monitoring of business e-mail and the confidentiality of employee correspondence . . . . . 49
Dominika Dörre-Kolasa, Processing of employees' personal data in the framework of so-called other forms of monitoring . . . . . 63
Tomasz Radziszewski, Selected aspects of the functioning of video surveillance in light of regulations concerning schools and other educational institutions . . . . . 81
Dariusz Wasiak, Preventive monitoring of employee sobriety: Outline of the issues . . . . 95
Krzysztof Wygoda, Admissibility of biometric data processing by employers: Model and practical approach . . . . . 107

## CONTROL AND OVERSIGHT OVER THE USE OF MONITORING

Przemysław Czechowski, The role of the labour inspector in the control and supervision of the application of monitoring by the employer: *De lege lata* and *de lege ferenda* conclusions . . . . . 119
Janusz Krasoń, Selected issues related to the control of video monitoring in the workplace conducted by a labor inspector in the context of personal data protection . . . . . 139
Łukasz Paroń, Video surveillance as an alternative source of evidence in inspections of state labour inspectors . . . . . 151

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.1

# SŁOWO WSTĘPNE

We współczesnych realiach społeczno-gospodarczych zauważalne są dążenia podmiotów zatrudniających do sięgania po zaawansowane technologie w celu zapewnienia kontroli nad terenem zakładu pracy i różnymi aspektami aktywności pracowników. Dokonujący się niezwykle szybko postęp w dziedzinie informatyki umożliwił przedsiębiorcom i innym organizacjom uzyskiwanie korzyści z nowoczesnych narzędzi oferowanych przez tę dziedzinę wiedzy. Ich popularność jest tym większa, że są stosunkowo mało kosztochłonne i nie stwarzają szczególnych trudności związanych z ich wdrażaniem i eksploatacją. Zarysowana tendencja pozostaje jednak w potencjalnym konflikcie z wartościami wpływającymi na definiowanie praw i wolności osobistych osób fizycznych zatrudnionych w zakładzie pracy: wolnością swobodnego komunikowania się, prawem do prywatności i ochrony danych osobowych. Uzasadniony interes przedsiębiorców i innych organizacji, polegający na wzmocnieniu kontroli nad rożnymi aspektami prowadzenia działalności, grozi zatem potencjalnie naruszeniem sfery autonomii pracobiorcy. Ryzyka związane z tą kolizją rysują się szczególnie ostro w warunkach stosunku pracy. Pracodawca ma bowiem przewagę organizacyjno-prawną nad drugą stroną tego stosunku. Jednocześnie pracownik jest poddany w procesie świadczenia pracy kierownictwu podmiotu zatrudniającego. Niedostatek materialnej równości stron stwarza zagrożenie nadużywania rozwiązań w dziedzinie monitorowania zakładu pracy, korespondencji służbowej pracownika oraz stosowania innych form monitoringu.

W polskim porządku prawnym regulacja monitoringu w zakładzie pracy została w 2018 roku włączona do kodeksu pracy. Rozważania nad monitoringiem nie mogą być jednak sprowadzone do dyskursu prowadzonego w ramach jednej gałęzi prawa, gdyż posiadają one z założenia pierwiastek interdyscyplinarności. Bacznej uwagi wymaga stosunek rozwiązań prawnych do standardów ochrony praw i wolności jednostki ustanowionych w Konstytucji RP i aktach prawa międzynarodowego. Niezbędne jest ustalenie relacji między przepisami o monitoringu i prawem ochrony danych osobowych. Określenie środków prawnych służących jednostce w razie naruszenia jej autonomicznej pozycji wymaga analizy instytucji prawa cywilnego. Niepodważalne znaczenie mają również dociekania prowadzone z punktu widzenia prawa administracyjnego. Kontrola stosowania monitoringu mieści się bowiem w zakresie działania organów nadzoru i kontroli nad warunkami pracy, wśród których należy wymienić przede wszystkim Państwową Inspekcję Pracy.


© for this edition by CNS

Przedstawione wyzwania uzasadniają poświęcenie niniejszego numeru „Przeglądu Prawa i Administracji" zagadnieniom monitoringu w zakładzie pracy. Przekrój zamieszczonych w nim opracowań jest adekwatny do złożoności zarysowanych wyżej kwestii. W wypowiedziach ich autorów widoczne są nawiązania do problematyki ochrony praw podstawowych, ujmowanej z punktu widzenia prawa konstytucyjnego i międzynarodowego publicznego. Modele regulacyjne monitoringu są również rozważane przy odwołaniu się do metody prawno-porównawczej. Treść prezentowanych opracowań odzwierciedla pełne spektrum form stosowania monitoringu zakładowego, odznaczające się rozległością i znacznym stopniem dyferencjacji. Obok monitoringu wizyjnego i korespondencji elektronicznej, omawiana jest tematyka tak zwanych innych form monitoringu przy uwzględnieniu analizy dopuszczalności prewencyjnej kontroli trzeźwości pracowników. Monitoring zakładowy ma również specyfikę zależną od zakresu działania podmiotu uprawnionego do jego stosowania, co wynika z tekstu dotyczącego placówek oświatowych. Osobnym i niezwykle istotnym problemem pozostaje kontrola i nadzór nad stosowaniem monitoringu, przy szczególnym uwzględnieniu środków prawnych będących w dyspozycji inspektora pracy oraz dowodowego znaczenia danych i zapisów uzyskiwanych z monitoringu prowadzonego przez pracodawcę.

Wyrażamy przekonanie, że opracowania zamieszczone w prezentowanym tomie wnoszą istotny wkład do analizy *novum* regulacyjnego, jakim wciąż pozostaje monitoring w zakładzie pracy oraz przyczynią się do odpowiedzi na pytania pojawiające się w dyskusji prowadzonej na ten temat przez przedstawicieli teorii i praktyki prawa.

*Artur Tomanek*


© for this edition by CNS

# MONITORING ZAKŁADOWY NA TLE KONSTYTUCYJNYM I PRAWNO-PORÓWNAWCZYM

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.2

MARIUSZ JABŁOŃSKI
ORCID: 0000-0001-8347-1884
Uniwersytet Wrocławski

# STOSOWANIE WOBEC PRACOWNIKÓW UKRYTEGO MONITORINGU WIZYJNEGO — KWESTIE SPORNE I NIEJEDNOZNACZNE

Abstrakt: W opracowaniu Autor zajmuje się problematyką ochrony autonomii informacyjnej jednostki w kontekście stosowania przez pracodawcę ukrytego monitoringu wizyjnego. Analiza przeprowadzona zostaje z punktu widzenia zgodności przedmiotowej praktyki ze standardami konstytucyjnymi, w tym konstytucyjnym mechanizmem ważenia, a także w korelacji ze stanowiskiem Wielkiej Izby ETPCz wyrażonym w wyroku w sprawie López Ribalda i inni przeciwko Hiszpanii.

Słowa kluczowe: ukryty monitoring wizyjny, ochrona wolności i praw jednostki, ochrona danych osobowych, rozstrzyganie o kolizjach wolności i praw, administrator danych, wyrok ETPCz w sprawie *López Ribalda i inni przeciwko Hiszpanii*

## WPROWADZENIE

Zagadnienie autonomii informacyjnej jednostki jest przedmiotem ożywionego zainteresowania nauki i praktyki stosowania prawa. Nie budzi przy tym wątpliwości, że stały rozwój społeczeństwa informacyjnego, wiążący się ze permanentnym doskonaleniem już istniejących technologii (jak i wdrażaniem zupełnie nowych) służących pozyskiwaniu oraz przekazywaniu danych, musi prowokować do powstawania szeregu wątpliwości lub też sporów dotyczących nie tylko rozumienia szeregu praw i wolności jednostki, ale i sposobu rozstrzygania o kolizjach, do jakich między nimi będzie dochodzić.

Przykładem takiej właśnie spornej kwestii jest problem legalności zastosowania przez pracodawców ukrytego monitoringu wizyjnego. Sytuacja wydawała się w miarę klarowna do czasu wydania przez Wielką Izbę Europejskiego Trybunału Praw Człowieka (dalej: ETPCz) wyroku w sprawie *López Ribalda i inni przeciwko Hiszpanii* (2019), w którym stwierdza się, że tego rodzaju praktyka nie musi być automatycznie identyfikowana z naruszeniem art. 8 Konwencji o Ochronie Praw


© for this edition by CNS

Człowieka i Podstawowych Wolności[1]. Rozstrzygnięcie to sprowokowało dyskusję dotyczącą tego, czy z perspektywy postanowień Konstytucji RP, jak i szeregu innych aktów dotyczących praw pracownika, w tym prywatności, danych osobowych, wolności komunikowania się itp., zastosowanie przez polskiego pracodawcę ukrytego monitoringu byłoby dopuszczalne i tym samym nie prowadziłoby do stwierdzenia przez uprawnione organy (w tym sądy), że stosowanie tego rodzaju technik stanowi oczywisty przykład naruszenia gwarantowanych jednostce (w tym pracownikowi) wolności i praw.

Celem mojego opracowania będzie zaprezentowanie oceny dopuszczalności stosowania przez pracodawcę ukrytego monitoringu wizyjnego z perspektywy poszanowania standardów konstytucyjnych z jednoczesnym wyartykułowaniem pojawiających się wątpliwości i kontrowersji wynikających z konieczności identyfikacji częściowo odmiennych płaszczyzn ochrony w odniesieniu choćby do prawa prywatności i ochrony danych osobowych.

## 1. GWARANCJE AUTONOMII INFORMACYJNEJ JEDNOSTKI W KONSTYTUCJI RP Z 2 KWIETNIA 1997 ROKU

Wolności i prawa osobiste[2] — czyli w praktyce te, które utożsamia się z systemowo wyodrębnioną kategorią uprawnień mających na celu zapewnienie człowiekowi swobodnego rozwoju, wolnego od wszelkich pozaprawnych działań przyjmujących postać zewnętrznej ingerencji — doczekały się w miarę kompleksowego ujęcia (szczególnie w odniesieniu do identyfikacji zakresu gwarancji dotyczących tak zwanej autonomii informacyjnej jednostki) dopiero w treści Konstytucji RP z 2 kwietnia 1997 roku[3]. Nie budzi przy tym wątpliwości, że identyfikacja ta była łatwiejsza po szczegółowym zapoznaniu się polskiego ustrojodawcy z ugruntowanym już rozumieniem pojęcia autonomii osobistej, pojmowanej zarówno jako zasada ogólna prawa (podobnie jak godność i wolność), jak i jako zasada interpretacyjna — definiowanym jako jeden z podstawowych standardów w regionalnym systemie ochrony wolności i praw jednostki Rady Europy, opierającym się na postanowieniach Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności i dodanych do niej Protokołów dodatkowych[4].

---

[1] Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.

[2] Na ten temat zob. L. Wiśniewski, *Wolności i prawa osobiste w Konstytucji RP z 1997 r. i w prawie międzynarodowym*, Poznań 1998.

[3] Konstytucja RP z 2 kwietnia 1997 r., Dz.U. Nr 78, poz. 483 ze zm.; por. np. orzeczenie TK z 24 czerwca 1997 r., K 21/97.

[4] Autonomię osobistą, w tym autonomię informacyjną jednostki utożsamia się z samodzielnym prawem stanowiącym element treści prawa do prywatności oraz pojęciami: „samokreacja" (*self-creation*) lub „samostanowienie" (*self-determination*). Zob. np. wyrok ETPCz z 2 sierpnia 1984 r. w sprawie *Malone przeciwko Wielkiej Brytanii*, skarga nr 8691/79; wyrok ETPCz z 16 grud-


© for this edition by CNS

W wielu opracowaniach dotyczących problematyki autonomii osobistej i informacyjnej[5], autorzy zasadniczo powołują się na wyrok Trybunału Konstytucyjnego z 2002 roku, w którym dokonano identyfikacji tych pojęć (w szczególności drugiego z nich), przyjmując iż jest to prawo podmiotowe „do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, znajdującymi się w posiadaniu innych podmiotów”[6]. Jednocześnie podkreślono w nim fakt korelacji konstytucyjnego prawa do ochrony prywatności (art. 47 Konstytucji RP) z prawem do ochrony danych osobowych (art. 51 Konstytucji RP), stwierdzając, że: „Prawo do ochrony prawnej życia prywatnego zostało zagwarantowane w art. 47 Konstytucji, a niektóre uprawnienia szczegółowe składające się na treść tego prawa — ponadto w innych przepisach konstytucyjnych. Autonomię informacyjną jednostki gwarantuje przede wszystkim art. 51 Konstytucji”[7].

Nie budzi jednocześnie wątpliwości, że owymi „innymi przepisami konstytucyjnymi” są te dotyczące wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji RP)[8], nienaruszalności mieszkania (art. 50), wolności wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji (art. 54 Konstytucji RP), także w wielopłaszczyznowej korelacji z wolnością wyznawania lub

---

nia 1992 r. w sprawie *Niemietz przeciwko Niemcom*, skarga nr 13710/88; wyrok ETPCz z 20 marca 2007 r. w sprawie *Tysiąc przeciwko Polsce*, skarga nr 5410/03, w którym wskazuje się wcześniejsze orzecznictwo Trybunału i Komisji, która przed reformą również podejmowała rozstrzygnięcia. Por. np. wyrok TK z 24 czerwca 1997 r., K 21/96. Na temat orzecznictwa zob. szerzej: M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, Wrocław 2002, s. 41 n.

[5] Por. np. K. Grzybowski, *Autonomia informacyjna jednostki a zgoda na przetwarzanie przez pracodawcę danych osobowych*, „Przegląd Sejmowy” 28, 2020, nr 6 (161), s. 50 n. Zob. też: Wyrok TK z 29 października 2013 r., U 7/12.

[6] Wyrok TK z 19 lutego 2002 r., U 3/01. Por. też: Wyrok TK z 9 lipca 2009 r., SK 48/05; wyrok TK z 26 lutego 2014 r., K 22/10. Szeroko na temat identyfikacji pojęć w orzecznictwie TK z okresu pierwszych lat obowiązywania Konstytucji RP zob. M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, s. 61 n.

[7] Wyrok TK z 19 lutego 2002 r., U 3/01. We wcześniejszym wskazywał zaś: „[...] przepisy konstytucji pozostają w określonej relacji wzajemnej: prawo do prywatności, statuowane w art. 47, zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51. Ten ostatni, rozbudowany przepis, odwołując się aż pięciokrotnie do warunku legalności — *expressis verbis* w ust. 1, 3, 4 i 5 oraz pośrednio przez powołanie się na zasadę demokratycznego państwa prawnego w ust. 2 — stanowi też konkretyzację prawa do prywatności w aspektach proceduralnych”, wyrok TK z 19 maja 1998 r., U 5/97.

[8] Trybunał Konstytucyjny podkreślał, że „Zwrot »komunikować się« oznacza utrzymywanie z kimś kontaktu, porozumiewanie się, a nie jedynie podawanie czegoś do wiadomości, przekazywanie jakiejś informacji czy zawiadamianie o czymś […]. Tak więc wolność komunikowania się ze swej istoty dotyczy swobody porozumiewania się określonych osób i związana jest z poufnością, co tradycyjnie obejmuje się określeniem »tajemnica«” — wyrok TK z 15 lipca 2009 r., K 64/07; wyrok TK z 11 kwietnia 2000 r., K 15/98. Naruszenie zasady tajemnicy korespondencji rozumianej jako możliwość zapoznania się z treścią przesyłki „zawsze należy kwalifikować jako naruszenie przepisów o obowiązku zachowania tajemnicy korespondencji, niezależnie od tego, czy do takiego zapoznania się z treścią przesyłki faktycznie doszło” — wyrok NSA z 28 czerwca 2022 r., II GSK 265/19.


© for this edition by CNS

przyjmowania religii według własnego wyboru oraz jej uzewnętrzniania indywidualnie albo z innymi, publicznie, a także prywatnie (art. 53 ust. 2 Konstytucji RP), jak i z wolnością ogłaszania wyników twórczości artystycznej, badań naukowych (a ponadto również w powiązaniu z wolnością nauczania — art. 73 Konstytucji RP)[9].

Trybunał stwierdził również, że:

> konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji objęte są wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu. Modelowo też w ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się nadto ochrona przed niejawnym monitorowaniem jednostki oraz prowadzonych przez nią rozmów, nawet w miejscach publicznych i ogólnie dostępnych. Nie ma znaczenia, czy wymiana informacji dotyczy życia ściśle prywatnego, czy też prowadzonej działalności zawodowej, w tym działalności gospodarczej. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której konstytucyjna ochrona byłaby wyłączona bądź samoistnie ograniczona. W każdej z tych sfer jednostka ma więc konstytucyjnie gwarantowaną wolność przekazywania i pozyskiwania informacji, w tym udostępniania informacji o sobie samej[10].

Pamiętać również należy, że ochrona życia prywatnego zagwarantowana jest we wszelkich jego aspektach, zarówno bezpośrednio w treści art. 47, jak i co najmniej kilku innych przepisach (art. 39, 41, 45 ust. 2, art. 49, 51, 53, 61 ust. 3; art. 76 Konstytucji RP)[11], a potencjalne naruszenie tej wartości może przybierać różnorakie formy, w tym takie, które nie będą łączyć się bezpośrednio lub nawet pośrednio z przetwarzaniem informacji o zidentyfikowanych osobach fizycznych. Tak kompleksowa ochrona życia prywatnego ma miejsce z uwagi na szerokość tego pojęcia i konieczność uszczegółowienia tych obszarów, które zdaniem prawodawcy zasługują na fundamentalne zabezpieczenie oraz poszanowanie[12].

Celem służącym zagwarantowaniu jednostce autonomii informacyjnej nie jest też wyłącznie sprecyzowanie zasad i mechanizmów jej ochrony przed nieuprawnionym pozyskiwaniem o niej informacji (ograniczenie możliwości przetwarzania informacji przez państwo o określonej osobie prywatnej)[13], które dotyczyć mogą różnych aspektów jego aktywności (w szeroko rozumianym obszarze życia osobistego, rodzinnego, zawodowego), ale w oczywiście szerszej perspektywie prawne zdefiniowanie przesłanek służących legalizacji sfery przetwarzania danych osobo-

[9] Zob. szerzej: M. Sakowska-Baryła, *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022, s. 67–81, 84–101, 109 n.

[10] Wyrok TK z 30 lipca 2014 r., K 23/11.

[11] Zob. szerzej: M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym*, Wrocław 2021, s. 54 n.

[12] Zob. szerzej w szczególności Wyrok TK z 20 marca 2006 r., K 17/05, czy Wyrok TK z 29 października 2013 r., U 7/12.

[13] W odniesieniu do osoby publicznej, a w szczególności do osoby pełniącej funkcje publiczne, ochrona takiej autonomii ma bardziej ograniczony charakter.


© for this edition by CNS

wych oraz prywatności. Ponadto ochrona autonomii ma na celu wyznaczenie granic gwarantowanych formalnie swobód w obszarze pozyskiwania i udostępniania (w tym ekspresji) gromadzonych przez jednostkę informacji (danych, wiedzy itp.). W takim ujęciu chodzi również o skonkretyzowanie płaszczyzn realizacji potwierdzonych konstytucyjnie uprawnień i swobód, które dotyczą tak wertykalnej, jak i horyzontalnej płaszczyzny ich obowiązywania oraz stosowania[14].

Uwzględnienie wertykalnej i horyzontalnej płaszczyzny obowiązywania jest o tyle istotne, że z perspektywy należytej identyfikacji i samej ochrony potwierdzonych jednostce uprawnień (w tym także zapewnionych: wolności od i wolności do) musi ona wiązać się z identyfikacją uprawnionego i zobowiązanego nie tylko w układzie relacji państwo–jednostka, ale i w relacjach między samymi podmiotami prywatnymi. W doktrynie podkreśla się, że pojęcie horyzontalnego działania praw jednostki utożsamiać trzeba ze stosowaniem norm konstytucyjnych jej dotyczących właśnie w stosunkach z zakresu prawa prywatnego, co oczywiste — także w odniesieniu do rozstrzygania sporów cywilnoprawnych i pracowniczych[15].

## 2. USTAWOWE OGRANICZANIE KONSTYTUCYJNYCH WOLNOŚCI I PRAW JEDNOSTKI A KWESTIA PRAKTYCZNEGO ROZSTRZYGANIA O KOLIZJACH DO JAKICH DOCHODZI MIĘDZY NIMI

Dla każdego uprawnionego fundamentalne znaczenie ma to, że ingerencja w sferę gwarantowanych mu konstytucyjnie wolności oraz praw dopuszczalna jest wyłącznie w drodze ustawy (zasada wyłączności ustawy — art. 31 Konstytucji RP)[16], co wiąże się z tym, że wykluczona została możliwość funkcjonowania w systemie prawa jakiejkolwiek regulacji podstawowej nie znajdującej „bezpośredniego oparcia w ustawie i które nie służy jej wykonaniu stosownie do art. 92 Konstytucji”[17].

Regulacja ustawowa musi spełniać wszelkie wymogi konstytucyjne, przede wszystkim musi być rzeczywiście konieczna w demokratycznym państwie pra-

[14] W odniesieniu na przykład do postanowień z zakresu ochrony danych osobowych zob. M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017, s. 32–33, 106–119.

15 Zob. szerzej: M. Safjan, *O różnych metodach oddziaływania horyzontalnego praw podstawowych na prawo prywatne*, „Państwo i Prawo” 2014, nr 2, s. 3 n.; M. Jabłoński, S. Jarosz-Żukowska, *Adresaci konstytucyjnych wolności i praw*, [w:] R. Balicki *et al.*, *Konstytucja i prawo konstytucyjne. Zarys wykładu*, Wrocław 2021, s. 269.

[16] Por. S. Jarosz-Żukowska, *Konstytucyjne przesłanki dopuszczalności ograniczeń prawa własności*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje*, red. L. Garlicki, A. Szmyt, Warszawa 2003, s. 138.

[17] *Ibidem*.


© for this edition by CNS

wa, a z drugiej strony nie może naruszać istoty wolności i praw, czyli *de facto* tych elementów treści uprawnienia (swobody), które mają znaczenie podstawowe (tworzących fundamentalny rdzeń) nie tylko dla identyfikacji sfery chronionej (gwarantowanej), ale i oceny rzeczywistej możliwości skutecznej realizacji przez uprawnionego konkretnego roszczenia z nim związanego. W dotychczasowym orzecznictwie Trybunału Konstytucyjnego ocena z punktu widzenia tej właśnie zasady charakteryzuje się odwołaniem do tak zwanych „względów obiektywnych", identyfikowanych każdorazowo w odniesieniu do oceny charakteru i zakresu ingerencji dokonanej przez prawodawcę. Trybunał zasadniczo formułuje ogólne dyrektywy, jakimi powinien kierować się ustawodawca w celu uniknięcia ewentualnego zarzutu dopuszczenia się naruszenia istoty prawa lub wolności. Generalnie zobowiązany jest on nie tylko powstrzymać się od takiego definiowania norm, które wprowadzałyby faktyczny zakaz korzystania z określonej wolności, ale również od takich, które nadmiernie ograniczałyby daną wolność w oparciu o przesłanki wskazane w treści art. 31 ust. 3 Konstytucji RP, czyli: bezpieczeństwa lub porządku publicznego, ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób[18].

Ustawowa ingerencja nie może przekraczać pewnego stopnia uciążliwości, przyjmując postać nadmiernej ingerencji. W tym zakresie podnosi się, że przedmiotowa ocena wymaga zachowania proporcji między zakresem i charakterem ingerencji (ograniczeń) „a rangą interesu publicznego, który ma w ten sposób podlegać ochronie"[19]. Ten swoisty mechanizm ważenia przysługuje ustawodawcy, a w dalszej kolejności organowi powołanemu do kontroli konstytucyjności prawa, czyli Trybunałowi Konstytucyjnemu. Z dotychczasowej praktyki i ustaleń doktryny wskazać można, że badanie treści ustawy pod kątem ewentualnego stwierdzenia naruszenia zasady proporcjonalności odbywa się w oparciu o trzy kryteria[20]:

— przydatności: ocena dotyczy tego, czy wprowadzana regulacja może w praktyce doprowadzić do osiągnięcia zamierzonego celu;

[18] Obok wymienionych wyżej ustrojodawca posługuje się jeszcze innymi pojęciami, które traktować należy jako wartości uzasadniające ograniczenia konkretnych wolności i praw. Do katalogu tego zaliczyć można między innymi dobro wspólne (art. 1 Konstytucji RP) — w swym orzecznictwie Trybunał Konstytucyjny uznał, że z treści tego przepisu wynika dyrektywa przedłożenia w razie potrzeby dobra ogólnego ponad dobro indywidualne czy partykularny interesu grupowy, co wiąże się z przyjęciem założenia, zgodnie z którym wszyscy obywatele „są w stopniu odpowiednim do swoich możliwości zobowiązani do poświęcenia pewnych interesów własnych dla dobra wspólnego" Zob. szerzej: M. Jabłoński, S. Jarosz-Żukowska, *Prawo konstytucyjne w formie pytań i odpowiedzi*, Wrocław 2003, s. 45–46. Wśród innych wartości warunkowo „nadrzędnych" wobec wolności i praw Konstytucja RP wymienia też ważny interes publiczny (art. 22), ważny interes prywatny (art. 45 ust. 2), dobro publiczne (art. 59 ust. 3 zd. 2), dobro państwa (art. 113) czy ważny interes gospodarczy (art. 61 ust. 3).

[19] L. Garlicki, *Komentarz do art. 31 Konstytucji RP*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 3, red. L. Garlicki, Warszawa 2003, s. 29.

[20] Zob. szerzej: M. Sakowska-Baryła, *Ochrona danych osobowych*…, s. 440 n.


© for this edition by CNS

— konieczności: ocena następuje w oparciu o wykazanie niezbędności ingerencji ustawodawcy w sferę praw i wolności, w szczególności w odniesieniu do dobra, którego ochrona stała się przesłanką jej ochrony;

— proporcjonalności *sensu stricto*: ocena ma na celu stwierdzenie, czy nałożone ograniczenia (stopień i zakres ingerencji) są proporcjonalne do osiągniętych (lub dopiero w przyszłości mających nastąpić) celów oraz korzyści[21].

Jednocześnie, jak wielokrotnie zauważał TK, ograniczenie prawa do prywatności i ochrony danych osobowych poza

> koniecznością wskazania interesu mieszczącego się w katalogu zawartym w art. 31 ust. 3 Konstytucji, przesłanką legalności wkroczenia w zakres autonomii informacyjnej jednostki jest stwierdzenie, że wprowadzona regulacja ustawodawcza jest w stanie doprowadzić do zamierzonych przez nią skutków (zasada przydatności), jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana (zasada konieczności), a jej efekty pozostają w proporcji do ciężarów nakładanych przez nią na obywatela[22].

W konsekwencji:

> Naruszenie prawa konstytucyjnego do ochrony danych osobowych można upatrywać nie tyle więc w samym nałożeniu obowiązku ustawowego […], ale w nałożeniu tego obowiązku w granicach wykraczających poza ramy wyznaczone przez Konstytucję, a więc z pogwałceniem przez ustawodawcę przesłanki „niezbędności w demokratycznym państwie prawnym"[23].

Nie mniej istotne staje się podniesienie, że ogólne powołanie się przez jednostkę na konieczność poszanowania jej prawa prywatności bez choćby uprawdopodobnienia istnienia zagrożeń chronionych dóbr osobistych nie będzie wystarczające do wykazania, iż ochrona taka jest niezbędna[24].

Z innej perspektywy musimy mieć na względzie również to, że w praktyce orzeczniczej definiowanie zakresu i charakteru ochrony prywatności (w szerszym zakresie autonomii informacyjnej) zawsze wiązać się może z koniecznością ważenia dóbr i wartości (w tym konstytucyjnych wolności i praw)[25]. Mechanizm ważenia ma miejsce zawsze wtedy, gdy dochodzi do kolizji konstytucyjnych wol-

[21] W praktyce więc „chodzi o zastosowanie środków niezbędnych w tym sensie, że chronić one będą określone wartości w sposób, bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawa bądź wolności ulegają ograniczeniu" — wyrok TK z 3 października 2000 r., K 33/99.

[22] Por. wyrok TK z 17 czerwca 2008 r., K 8/04 z jednoczesnym odwołaniem się do wyroku TK z 3 października 2000 r., K 33/99.

[23] Por. wyrok TK z dnia 12 listopada 2002 r., SK 40/01.

[24] NSA w wyroku z 30 września 2015 r., I OSK 1853/14 wskazywał: „rozważając możliwość udostępnienia informacji o wynagrodzeniu danej osoby organ powinien każdorazowo analizować, czy jest ona niezbędna z punktu widzenia celów prawa do informacji publicznej, a także czy nie narusza godności i intymności osoby, której taka informacja dotyczy". Zob. też wyrok NSA z 26 maja 2022 r., III OSK 1291/21, czy wyrok SN z 8 listopada 2012 r., I CSK 190/12.

[25] Pewnym standardem, który bierze się pod uwagę jest reguła stosowania prawa w myśl *in dubio pro libertate* oraz *in dubio pro cive* lub *favor debitoris* — zob. wyrok TK z 28 stycznia 2003 r., K 2/02.


© for this edition by CNS

ności oraz praw (na przykład ochrona prywatności a realizacja prawa dostępu do informacji publicznej). Chodzi tu o sytuację, w której „różne jednostki powołują się dla ochrony swoich interesów na różne przysługujące im prawa”[26]. Wtedy też dokonuje się ważenia konstytucyjnie określonych wartości i dóbr (uprawnień i swobód) w kontekście rozstrzygnięcia konkretnych sporów powstałych na tle zindywidualizowanej sytuacji faktycznej i towarzyszących jej przesłanek z wyraźnym uwzględnianiem znaczenia interesu publicznego (jeżeli może być wzięty pod uwagę) jako wartości, która determinuje ostateczne rozstrzygnięcie (tak też na przykład w kontekście art. 45, 47, 51, 54, 61 i innych).

Warto też pamiętać, że pomimo stałej aktywności prawodawcy (zresztą nie tylko krajowego), do kolizji dochodzi w sytuacji braku obowiązywania konkretnej regulacji ustawowej, a także wtedy, gdy ustawodawca posługuje się jedynie ogólnymi (kierunkowymi) dyrektywami i/lub zwrotami niedookreślonymi[27].

Z perspektywy ochrony autonomii informacyjnej jednostki mechanizm ważenia jest stałą praktyką charakteryzującą nie tylko proces udostępniania danych osobowych znajdujących się w dokumentach urzędowych, ale w ogóle danych i informacji dotyczących zidentyfikowanej osoby fizycznej uznawanych za informację publiczną w rozumieniu ustawy o dostępie do informacji publicznej[28], czy choćby w zakresie rozstrzygania o granicach wolności słowa oraz komunikowania się w zderzeniu z koniecznością zapewnienia należytej ochrony prywatności, w tym też czci, dobrego imienia, czy wizerunku[29].

---

[26] B. Banaszak, *Prawa jednostki i systemy ich ochrony*, Wrocław 1995, s. 69.

[27] „W przypadku zaś kolizji samych praw człowieka nie dochodzi do rozstrzygnięcia według schematu »wszystko albo nic«, a rozwiązania na zasadzie schematu »bardziej lub mniej«, co oznacza uwzględnienie obu wolności w większym lub mniejszym stopniu. Nie dochodzi więc do eliminacji, ale do rozwiązania problemu na zasadzie argumentacji prowadzącej do »ważenia zasad«, tj. zadecydowania, że w danym wypadku jedne elementy praw i wolności człowieka winny ustąpić innym, »ważniejszym« w tej konkretnej sytuacji. Mechanizm wyważania skorelowany jest przy tym z zasadą proporcjonalności. Oznacza to, że w sytuacji konfliktu swobód uwzględnia się je obie, ale każdorazowo dokonuje się »ważenia zasad« i stosuje te donioślejsze oraz bardziej adekwatne do danej sytuacji” — A. Kalisz, *Rozwiązywanie kolizji norm i zasad w kontekście praw człowieka*. *Uwagi teoretyczno-prawne*, [w:] *Wolność wypowiedzi* versus *wolność religijna. Studium z zakresu prawa konstytucyjnego, karnego i cywilnego*, red. A. Biłgorajski, Warszawa 2015, s. 17.

[28] Kompleksowo zaprezentowała to M. Sakowska-Baryła, *Ochrona danych osobowych*…, s. 436–489; zob. też: M. Jabłoński, *RODO a dostęp do informacji publicznych. Kwestie dyskusyjne na tle kształtującej się praktyki orzeczniczej sądów administracyjnych*, [w:] *Konstytucjonalizm polski. Refleksje z okazji jubileuszu 70-lecia urodzin i 45-lecia pracy naukowej Profesora Andrzeja Szmyta*, red. A. Gajda *et al.*, Gdańsk 2020, s. 346 n.; M. Jabłoński, K. Wygoda, *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej. Aspekty praktyczne,* Warszawa 2021, s. 151 n. W odniesieniu do tajemnicy przedsiębiorstwa zob. np. wyrok NSA z 8 grudnia 2017 r., I OSK 2799/15.

[29] Zob. np. uchwała Sądu Najwyższego z 18 lutego 2005 r., III CZP 53/04.


© for this edition by CNS

## 3. STOSOWANIE UKRYTEGO NADZORU JAKO INGERENCJA W SFERĘ AUTONOMII INFORMACYJNEJ JEDNOSTKI

Obowiązujące postanowienia konstytucyjne uzupełniane są w Polsce przez różnego rodzaju regulacje ustawowe. W odniesieniu do prawa pracy fundamentalne znaczenie mają te zawarte w treści art. $22^2$–$22^3$ oraz 222 kodeksu pracy[30], nie zapominając również o fundamentalnych gwarancjach powtórzonych w treści innych postanowień tego aktu (art. $11^1$ n.).

Pomijając w tym miejscu ich szerszą analizę, która w literaturze została już przecież odpowiednio zaprezentowana[31], warto jeszcze raz przypomnieć istotę rozstrzygnięcia Wielkiej Izby Europejskiego Trybunału Praw Człowieka w sprawie *López Ribalda i inni przeciwko Hiszpanii*[32]. Stwierdzono w nim, że stosowanie wobec pracowników ukrytego nadzoru za pomocą kamer wideo może być usprawiedliwione w określonych sytuacjach, przede wszystkim wtedy, gdy zachodzi uzasadnione podejrzenie poważnych uchybień pracowniczych oraz ryzyko dużych strat firmy (przedsiębiorcy i zarazem pracodawcy).

Stan faktyczny sprawy jest powszechnie znany i w największym skrócie sprowadza się do wskazania na fakt zainstalowania przez przedsiębiorcę ukrytych kamer (ukryty nadzór wizyjny), które zostały wykorzystane przez personel firmy (ograniczony do minimum krąg uprawnionych) do utrwalenia czynności kradzieży dokonywanych przez pracowników supermarketu (dotyczyło to kilkunastu pracowników, przy czym trzy skarżące były kasjerkami, kolejne dwie sprzedawczyniami „przy ladzie"). Jednocześnie warto dodać, że pracodawca obok kamer ukrytych zainstalował inne (widoczne), oznaczył również strefy podlegające monitorowaniu, nie informując jednak o fakcie „sprzężenia" systemu inwigilacji funkcjonującego w oparciu o urządzenia widoczne oraz ukryte. Z szerszego punktu widzenia ochrony praw pracowniczych istotne jest to, że zwolnieni pracownicy nie mogli zapoznać się z zapisem pochodzącym z ukrytych kamer w trakcie wewnętrznego postępowania zakładowego.

Rozstrzygnięcie Wielkiej Izby Trybunału opierało się na przeprowadzeniu pogłębionego testu w oparciu o kryteria odpowiedniości, konieczności i propor-

[30] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, tekst jedn. Dz.U. z 2022 r. poz. 1510 ze zm.; E. Skunarowska-Drzewiecka, *Komentarz do art. 22² k.p.*, [w:] *Kodeks Pracy. Komentarz*, red. K. Walczak, Warszawa 2020; M. Kuba, *Komentarz do art. 22² k.p.*, [w:] *Kodeks pracy. Komentarz*, t. 1. *Art. 1–93*, red. K.W. Baran, Warszawa 2022, s. 299 n. Na temat interpretacji art. 222 § 6 zob. też: S. Szurgacz, *System kamer to nie tylko kwestia prywatności*, Kancelarie RP, 23.01.2020, https://kancelarierp.pl/system-kamer-to-nie-tylko-kwestia-prywatnosci/ (dostęp: 25.11.2022).

[31] Także w odniesieniu do tożsamości dat nowelizacji przepisów kodeksu pracy i bezpośredniego stosowania postanowień RODO — por. np. O. Dąbrowska, *Kryteria dopuszczalności stosowania monitoringu w miejscu pracy oraz związane z tym obowiązki pracodawcy w świetle reformy ochrony danych osobowych*, „Prawo Mediów Elektronicznych" 2019, nr 1, s. 12 n. oraz cytowana tam literatura.

[32] Wyrok Wielkiej Izby z 17 października 2019 r., skargi nr 1874/13 i 8567/13.


© for this edition by CNS

cjonalności (uzasadnione istnienie podejrzenia niewłaściwego postępowania pracowników, przy jednoczesnym uznaniu, że zastosowane środki były odpowiednie do zamierzonego celu oraz konieczne do jego realizacji).

ETPCz odwołał się również do opinii Komisji Weneckiej w sprawie „nadzoru wizyjnego prowadzonego przez podmioty prywatne w sferze publicznej i prywatnej oraz przez władze publiczne w sferze prywatnej i ochrony praw człowieka”[33], w której potwierdzono — w szczególnych przypadkach i w oparciu o wskazane przesłanki — dopuszczalność zastosowania tej postaci nadzoru[34].

Rozstrzygnięcie to wywołało duże zainteresowanie i — choćby ze względu na to, że było odmienne od wcześniejszego rozstrzygnięcia w tej sprawie[35], jak i innych wyroków ETPCz oraz TSUE[36] — spotkało się z artykulacją szeregu komentarzy[37]. Nie mogło być inaczej, ponieważ potwierdziło w istocie (oczywiście

[33] *Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection Adopted by the Venice Commission at Its 71st Plenary Session*, *CLD-AD(2007)027-e*, European Commission for Democracy through Law (Venice Commission), 1–2.06.2007, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)027-e.

[34] Wskazano tam między innymi, że „niejawny nadzór powinien być dozwolony, przy czym wyłącznie tymczasowo, jeżeli okaże się to konieczne ze względu na brak odpowiednich alternatyw” — *ibidem*, s. 7.

[35] Wyrok ETPCz z 9 stycznia 2018 r., skargi nr 1874/13 i 8567/13; zob. też komentarz: *ETPC: Ukryty monitoring kasjerek w supermarkecie skutkował naruszeniem ich prywatności*, Biuletyn Informacji Publicznej RPO, 15.01.2018, https://bip.brpo.gov.pl/pl/content/etpc-ukryty-monitoring-kasjerek-w-supermarkecie-w-prawo-do-prywatnosci (dostęp: 25.11.2022).

[36] ETPCz przyjmował wcześniej, że ukryty monitoring, a więc monitoring pracowników bez informowania ich o fakcie nagrywania, jest niedopuszczalny i narusza art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności. Por. wyrok w sprawie *Copland przeciwko Zjednoczonemu Królestwu* z 2007 r., skarga nr 62617/00. Monitoring więźnia w celi musi być szczegółowo określony przepisami prawa — wyrok ETPCz z 27 sierpnia 2019 r. w sprawie *Izmestiew przeciwko Rosji*, skarga nr 74141/10. Zob. szerzej: J. Sieńczyło-Chlabicz, *Ochrona prawa do prywatności w Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, Karcie Praw Podstawowych oraz w prawie krajowym*, [w:] *Rozprawy cywilistyczne. Księga pamiątkowa dedykowana Profesorowi Edwardowi Drozdowi*, red. M. Pecyna, J. Pisuliński, M. Podrecka, Warszawa 2013, s. 25 n.

[37] Zob. np.: A. Sobczyk, *Lopez Ribalda i inni przeciwko Hiszpanii a dopuszczalność niejawnej kontroli pracowników w Polsce*, Sobczyk & Współpracownicy, 7.02.2020, https://sobczyk.com.pl/lopez-ribalda-a-dopuszczalnosc-niejawnej-kontroli-pracownikow-w-polsce/ (dostęp: 25.11.2022); M. Barański, *Ukryty monitoring w zakładzie pracy w kontekście wyroku Europejskiego Trybunału Praw Człowieka z dnia 17 października 2019 r. (López Ribalda i inni v. Hiszpania, skargi nr 1874/13 i 8567/13)*, „Monitor Prawa Pracy” 2020, nr 3, s. 26; A. Grzelak, *Stosowanie monitoringu wizyjnego w relacjach pracowniczych — López Ribalda i Inni przeciwko Hiszpanii, skargi nr 1874/13 i 8567/13, wyrok z dnia 17 października 2019* r., [w:] *Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Komentarz Orzeczniczy za rok 2019*, red. J. Kosonoga, Warszawa 2020 r., s. 224 n.; Z. Góral, A. Tyc, *Glosa do wyroku Europejskiego Trybunału Praw Człowieka z 17 października 2019 r. w sprawie López Ribalda i inni* vs. *Hiszpania, nr skarg 1874/13 i 8567/13*, „Przegląd Sejmowy” 28, 2020, nr 3 (158), s. 255–262. Zob. też np.: wyrok ETPCz z 16 grudnia 1992 r. w sprawie *Niemietz przeciwko Niemcom*, skarga nr 13710/88; wyrok ETPCz z 16 kwietnia 2002 r. w sprawie *Société Colas Est i in. przeciwko Francji*; wyrok ETPCz z 28 stycznia 2003 r. w sprawie *Peck prze-*


© for this edition by CNS

pod określonego rodzaju warunkami) dopuszczalność stosowania przez pracodawców pewnego rodzaju form ukrytego monitoringu, służącego przetwarzaniu informacji dotyczących konkretnych osób, w celu pozyskania dowodów na ich sprzeczne z prawem i interesem pracodawcy (przedsiębiorcy) zachowania (w tym przypadku dopuszczanie się przez kilkunastu pracowników kradzieży mienia).

Mając na względzie oczywisty fakt, że ochrona prywatności obejmuje swym zakresem działalność zawodową jednostki, w tym oczywiście różne aspekty aktywności (zachowania się) osoby w miejscu wykonywanej pracy[38], jak i to, że definiowanie zakresu i charakteru ochrony prywatności wymaga każdorazowo uwzględnienia specyfiki konkretnej sytuacji (ochrona taka nie jest absolutna), w tym również tego, jakie (także równorzędne) wartości pozostają względem siebie w kolizji, charakter i istota rozstrzygnięcia Wielkiej Izby ETPCz nie powinny budzić zbytniego zaskoczenia. Jest ono bowiem w istocie dowodem obiektywnej oceny konkretnej sytuacji faktycznej dokonanej przez kompetentny do tego organ i w konsekwencji potwierdzeniem, że ochrona konkretnych dóbr (praw) przeważa nad ochroną innych, które ze względu na obiektywnie zastosowany mechanizm ważenia okazały się być *summa summarum* mniejszej wartości. Mechanizm ważenia stosowany był i jest przez ETPCz w wielu przypadkach rozstrzygania konkretnych spraw, także w odniesieniu do ochrony wynikającej z treści art. 2 Konwencji[39].

Oczywiście z perspektywy systemowej uwzględniającej obowiązujące przepisy unijne, jak i krajowe (ustawowe), praktyka stosowania ukrytego monitoringu musi budzić szczególne zainteresowanie oraz problemy interpretacyjne. Mając bowiem na względzie treść przepisów kodeksu pracy, czy postanowień rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[40] (dalej:

---

*ciwko Zjednoczonemu Królestwu*, skarga nr 44647/98; wyrok TSUE w sprawie *Volker und Markus Schecke* z 9 listopada 2010 r., C-92/09; wyrok ETPCz z 16 lutego 2000 r. w sprawie *Amann przeciwko Szwajcarii*, skarga nr 27798/95; wyrok ETPCz z 4 maja 2000 r. w sprawie *Rotaru przeciwko Rumunii*, skarga nr 28341/95.

[38] Zob. np.: wyrok ETPCz z 16 grudnia 1992 r. w sprawie *Niemietz przeciwko Niemcom*, skarga nr 13710/88; wyrok ETPCz z 16 kwietnia 2002 r. w sprawie *Société Colas Est i in. przeciwko Francji*, skarga nr 37971/97; wyrok ETPCz z 28 stycznia 2003 r. w sprawie *Peck przeciwko Zjednoczonemu Królestwu*, skarga nr 44647/98; wyrok TSUE w sprawe *Volker und Markus Schecke* z 9 listopada 2010 r., C-92/09. Zob. wyrok ETPCz z 16 lutego 2000 r. w sprawie *Amann przeciwko Szwajcarii*, skarga nr 27798/95; wyrok ETPCz z 4 maja 2000 r. w sprawie *Rotaru przeciwko Rumunii*, skarga nr 28341/95.

[39] Zob. np. wyrok ETPCz z 10 lipca 1984 r. w sprawie *McCann i inni przeciwko Zjednoczonemu Królestwu*, skarga nr 10042/82; Wyrok ETPCz z 22 marca 2001 r. w sprawie *Streletz, Kessler i Krenz przeciwko Niemcom*, skargi nr 34044/96, 35532/97, 44801/98.

[40] RODO uchyla i zastępuje dyrektywę 95/46/WE w obszarze sektorów prywatnego i publicznego w państwach członkowskich. Konieczne staje się jednocześnie podkreślenie, że obok RODO przyjęta została dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez wła-


© for this edition by CNS

RODO), pojawiać się musi kwestia oceny legalności działań pracodawcy, który decyduje się na zastosowanie ukrytego monitoringu[41]. Ze swej istoty ta forma „inwigilacji" nie może być przecież znana temu, kto poddany zostaje obserwacji, w przeciwnym bowiem razie nie byłoby możliwe osiągnięcie celu, któremu w ocenie pracodawcy ma ona służyć.

Z drugiej strony zastosowanie ukrytego monitoringu przez polskiego pracodawcę nie znajduje należytego umocowania w treści art. $22^2$ kodeksu pracy (jak i w sumie pozostałych przepisów), trudno też określić, w jaki sposób działając legalnie (już jako administrator) mógłby należycie wywiązać się wobec swoich pracowników (ale nie tylko, bo może to dotyczyć również innych osób statusu takiego nie posiadających) z nałożonego na nie niego przez RODO obowiązku informacyjnego, co musi automatycznie prowadzić do nieuzasadnionego ograniczenia możliwości realizacji praw przez osobę, której dane są przetwarzane (art. 15 n. RODO). Aktualnie obowiązujące przepisy nie tworzą po stronie standardowego pracodawcy pozytywnie i czytelnie zdefiniowanych uprawnień (w tym procedury) legalizujących prowadzenie tak zwanych ukrytych czynności operacyjnych[42].

Mając powyższe na uwadze, nie budzi wątpliwości, że każdy przypadek stosowania przez pracodawcę ukrytego monitoringu musi być traktowany jako ingerencja w sferę gwarantowanej konstytucyjnie, i potwierdzanej w różnego rodzaju aktach prawnych, autonomii informacyjnej jednostki. Co do zasady też ingerencja taka, ze względu na brak odpowiedniego umocowania w przepisach rangi ustawy, traktowana będzie wyjściowo jako działalnie potencjalnie sprzeczne z potwierdzonymi systemowo jednostce (pracownikowi) gwarancjami (wolnościami i prawami). Może też w istotny sposób pozostawać *a contrario* do prawidłowego wywiązywania się z obowiązków prawnych nałożonych na administratora danych przez przepisy prawa unijnego (RODO), i to w zakresie szerszym podmiotowo niż to ma miejsce na gruncie aktualnie obowiązującej regulacji konstytucyjnej (art. 51 Konstytucji RP).

Wielka Izba ETPCz potwierdziła, że w pewnych — wyjątkowych — sytuacjach pracodawca, wykazując konieczność i niezbędność podjętych działań, które przyjmują postać wdrożenia ukrytego monitoringu wizyjnego, może się

---

ściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (tak zwana dyrektywa policyjna), Dz.Urz.UE L 119 z 4.05.2016 r.

[41] Zob. też: *Wytyczne EROD Nr 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo*, *wersja 2.0 przyjęta 29.01.2020 r.*, European Data Protection Board, 29.01.2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl.pdf

[42] Zob. E. Rutynowska, *Komunikat FOR 2/2022: Kontrola operacyjna: czym jest, czym być powinna i jak się ma do prawa do prywatności*, Forum Obywatelskiego Rozwoju, 24.01.2022, https://for.org.pl/pliki/artykuly/8066_komunikatfor22022kontrola-operacyjnaczym-jest-czym-byc-powinna-i-jak-sie-ma-do-prawa-do-prywatnosci.pdf (dostęp: 25.11.2022). Pomijam kwestię zlecenia prowadzenia różnego rodzaju działań inwigilujących przez odrębnego administratora, na przykład detektywa.


© for this edition by CNS

(potencjalnie) uwolnić od zarzutu naruszenia gwarantowanego systemowo prawo do prywatności.

Pracodawca, wdrażając konkretne rozwiązania techniczne (jak i technologiczne), nie może działać arbitralne i dowolnie definiować okoliczności uzasadniające konieczność czy niezbędność ich zastosowania. Samo wykazanie przez niego braku alternatywnych rozwiązań prowadzących do osiągnięcia zamierzonego celu (z uwzględnieniem rodzaju i charakteru już wcześniej zastosowanych — na przykład jawnego monitoringu wizyjnego) jest już samo w sobie procesem wymagającym wcześniejszego przygotowania obiektywnej analizy ryzyka (również z perspektywy nowowdrażanego procesu służącego przetwarzaniu danych i przeprowadzenia oceny skutków dla ochrony danych). Ocena taka służy wykazaniu, że zastosowane dotychczas realne i efektywne standardowo środki nie doprowadziły do osiągnięcia zamierzonych efektów i w zasadzie nie istnieją żadne inne metody alternatywne (o mniejszym stopniu ingerencji), które taki skutek mogłyby zapewnić. W dalszej kolejności konieczne staje się wykazanie przez niego, że dołożył należytej staranności w zakresie przetwarzania danych utrwalonych za pomocą stosowanych urządzeń. Oznacza to nie tylko niezbędność sprecyzowania, w jakim czasookresie monitoring ma być stosowany (ocena incydentalności), kto i w jakim zakresie ma zapewniony dostęp do danych, jakie zostaną wdrożone mechanizmy definiujące ograniczony podmiotowo dostęp do danych poddanych archiwizacji (z uwzględnieniem ewentualności prowadzenia sporów sądowych) czy zakresu i celu wykorzystywania przetwarzanych danych, ale przede wszystkim obiektywne wykazanie, że ze względu na specyfikę sytuacji faktycznej (z uwzględnieniem kryteriów podmiotowego i przedmiotowego)[43] i już wcześniej zastosowanych środków (o których należycie poinformowano), nie wyeliminowano praktyk, których skutki stanowią naruszenie gwarantowanych przedsiębiorcy (pracodawcy) praw — na przykład również chronionego konstytucyjnie prawa własności i innych praw majątkowych (art. 64 Konstytucji RP).

[43] Jak stwierdziła Wielka Izba ETPCz w uzasadnieniu: „Zatem, o ile Trybunał nie może przyjąć twierdzenia, że, ogólnie rzecz biorąc, najmniejsze podejrzenie o sprzeniewierzenie lub jakiekolwiek inne nadużycie ze strony pracowników mogłoby usprawiedliwić wprowadzenie przez pracodawcę niejawnego nadzoru wizyjnego, o tyle istnienie uzasadnionego podejrzenia, że popełniono poważne uchybienie i rozmiar strat stwierdzonych w niniejszej sprawie może stanowić poważne uzasadnienie. Dzieje się tak tym bardziej w sytuacji, gdy sprawne funkcjonowanie przedsiębiorstwa zagrożone jest nie tylko w związku z podejrzeniem niewłaściwego postępowania jednego pracownika, lecz podejrzeniem dotyczącym wspólnego działania kilku pracowników, ponieważ tworzy to ogólną atmosferę braku zaufania w miejscu pracy — wyrok Wielkiej Izby ETPCz z 17 października 2019 r. w sprawie *López Ribalda i inni przeciwko Hiszpanii*, skargi nr 1874/13 i 8567/13, Trybunał Konstytucyjny, 22.12.2021, s. 43–44, https://trybunal.gov.pl/fileadmin/content/dokumenty/orzeczenia-etpc/2019/LOPEZ_RIBALDA_I_INNI_przeciwko_HISZPANII__Skargi_nr_187413_i_856713__wyrok_z_17.10.2019r.pdf (dostęp: 25.11.2022). Istotne oczywiście było też wzięcie pod uwagę charakteru (publicznego) miejsca wykonywania pracy przez pracowników.


© for this edition by CNS

Pytaniem podstawowym pozostaje jednak to, czy w polskim porządku prawnym tego rodzaju rozwiązanie rzeczywiście nie prowadzi do deprecjacji prawa do prywatności i to nie tylko pracowników, lecz również innych osób trzecich. Pamiętać bowiem trzeba, że:

> kolizja praw i zasad na poziomie konstytucyjnym nie może prowadzić w ostatecznym wyniku do pełnej eliminacji jednego z praw pozostających w konflikcie. Problemem wymagającym rozstrzygnięcia jest zawsze w takim wypadku znalezienie pewnego punktu równowagi, balansu dla wartości chronionych przez Konstytucję i wyznaczenie obszaru stosowania każdego z praw[44].

Dlatego też warto pozostać świadomym tego, że wyrok Wielkiej Izby ETPCz nie rozwiązał wszystkich istotnych wątpliwości interpretacyjnych. Z jednej strony potwierdził brak naruszeń gwarantowanych konwencyjnie praw, w tym prawa do prywatności (art. 8 Konwencji), jednak z drugiej strony nie wykluczył możliwości skutecznego dochodzenia przez osobę, której dane są (były) przetwarzane, gwarantowanych jej praw, szczególnie w kontekście braku należytego dopełnienia przez pracodawcę (i jednocześnie administratora) nałożonych na niego obowiązków prawnych[45]. Ponadto nie wyeliminował zasadności stosowania standardu potwierdzonego choćby w innym wydanym przez ten organ wyroku, *Liberty i inni przeciwko Wielkiej Brytanii*[46], w odniesieniu do stwierdzenia braku jasnej i dostępnej dla wiedzy publicznej informacji o sposobie przetwarzania, selekcjonowania oraz niszczenia zgromadzonych danych. Może to w praktyce oznaczać, że rozstrzygnięcie krajowego organu ochrony będzie inne niż sądu, który orzekać będzie w odrębnym postępowaniu.

Paradoksalnie w wyroku Wielkiej Izby w sprawie *López Ribalda i inni przeciwko Hiszpanii* z 2019 roku potwierdzono, że można skutecznie odseparować płaszczyznę ochrony prywatności jednostki od płaszczyzny poszanowania prawa do ochrony jej danych osobowych[47]. Trybunał nie stwierdził bowiem naruszenia art. 8 Konwencji, pomimo że w sposób oczywisty pracodawca nie wywiązał się należycie ze swoich obowiązków jako administrator danych.

---

[44] Zob. np. wyrok TK z 20 marca 2006 r., K 17/05.

[45] Tak też A. Sobczyk, *Lopez Ribalda i inni przeciwko Hiszpanii…*

[46] Wyrok Wielkiej Izby z 1 lipca 2008 r., skarga nr 58243/00.

[47] Trybunał stwierdził, że „Skarżące mogły zatem złożyć skargę do Urzędu Ochrony Danych dotyczącą niewywiązania się przez pracodawcę z obowiązku uprzedniego powiadomienia zgodnie z wymogami art. 5 tejże Ustawy. Urząd uprawniony był do prowadzenia dochodzeń w sprawie domniemanego naruszenia prawa oraz do nakładania kar finansowych na osobę odpowiedzialną. Mogły również skierować sprawę do sądów powszechnych w celu uzyskania zadośćuczynienia z tytułu rzekomego naruszenia praw wynikających z Ustawy o ochronie danych osobowych. Trybunał zauważa w tym względzie, że o ile orzecznictwo przywołane przez Rząd (zob. par. 49 powyżej) rzeczywiście dotyczy sytuacji, która nie jest identyczna z sytuacją w niniejszej sprawie, prawo do uzyskania zadośćuczynienia za szkody spowodowane naruszeniem Ustawy o ochronie danych osobowych zostało wyraźnie przewidziane w art. 19 tejże Ustawy i nie ma powodu, by obecnie kwestionować skuteczność tego środka".


© for this edition by CNS

Fundamentalne więc jest stwierdzenie Trybunału, zgodnie z którym pracodawca mógł uchylić się od jednego z nałożonych na niego obowiązków (obowiązek informacyjny) ze względu na ochronę istotnych interesów publicznych lub prywatnych. Zasadniczą cechą legalizującą działanie przedsiębiorcy (pracodawcy) w przedmiotowym zakresie staje się więc dająca się obiektywnie zweryfikować adekwatność zastosowanych środków (w tym rozwiązań, technik itp.) do stopnia zagrożenia gwarantowanych mu praw przy jednoczesnym dążeniu do jak najszybszego przywrócenia normalnego funkcjonowania zakładu pracy lub przedsiębiorstwa (zasada proporcjonalności). Konieczne jest również wykazanie, że ich zastosowanie było konieczne, a zagrożenia nie można było uniknąć zwykłymi środkami właściwymi dla funkcjonowania tego konkretnego pracodawcy (z uwzględnieniem specyfiki jego funkcjonowania, charakteru obowiązków pracowniczych, cech miejsca świadczenia pracy i faktycznych okoliczności, które zaistniały w określonym czasie) i — co najważniejsze — wykazanie istotnego interesu publicznego lub prywatnego.

## ZAKOŃCZENIE

W mojej ocenie, podobnie jak w przypadku istoty rozwiązań zawartych w Dyrektywie Parlamentury Europejskiego i Rady (UE) 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii, interes publiczny[48] musi być rozumiany szeroko, także w odniesieniu do pracodawcy będącego przedsiębiorcą. W kontekście wyeliminowania negatywnych praktyk (w tym czynów przestępczych) go naruszających, nie może on być traktowany wyłącznie jako dotykający prywatnego obszaru działania podmiotu niepublicznego. W istocie chodzi tu przecież o ochronę praworządności jako dobra wspólnego, a nie wyłącznie interesu przedsiębiorcy (pracodawcy), którego dotykają negatywne skutki działań (bezczynności) różnego rodzaju osób. Istotne jest również wzięcie pod uwagę, że pracownicy tworzący załogę również tworzą wspólnotę. Ochrona tego interesu wspólnotowego musi zostać uwzględniona, i to nie wyłącznie w rozumieniu interesu prywatnego.

Trudno też będzie każdemu pracodawcy efektywnie odwoływać się do mechanizmu ważenia konstytucyjnych wolności i praw pod kątem stwierdzenia, że w konkretnym przypadku nie doszło do naruszeń prawa do ochrony danych osobowych. W praktyce bowiem rola i znaczenie art. 51 Konstytucji RP są niewątpliwie modyfikowane przez bezpośrednio stosowane przepisy rozporządzenia unijnego, które jasno i czytelnie konkretyzują nie tylko określone obowiązki administratora (także będącego podmiotem niepublicznym), ale i charakter konse-

[48] Zob. szerzej: M. Jabłoński *et al*., *Sygnalista a ochrona danych osobowych*, Toruń 2022, s. 8 n.


© for this edition by CNS

kwencji, które mogą być wynikiem nienależytego ich wykonania. Potwierdzają też każdemu uprawnionemu wprost, jakie prawa mu przysługują, definiując jednocześnie odpowiednie procedury ich dochodzenia.

Nie budzi oczywiście wątpliwości, że każdy pracodawca, który będzie stosował ukryty monitoring (w szczególności zaś przedsiębiorca), może skutecznie podejmować próbę uwolnienia się od zarzutu naruszenia prawa do prywatności konkretnych osób, wykazując spełnienie przesłanek i kryteriów skonkretyzowanych w wyroku ETPCz w sprawie *López Ribalda i inni przeciwko Hiszpanii*. Nie można jednak zagwarantować, że ocena jego działań podejmowanych jako administratora danych zostanie oceniona pozytywnie przez krajowy organ ochrony (Prezesa Urzędu Ochrony Danych Osobowych), jak i tego, że ewentualne roszczenia kierowane przez uprawnioną osobę na podstawie art. 82 RODO zostaną w każdym przypadku uznane za bezpodstawne.

W aktualnie istniejącej sytuacji normatywnej trudno zakładać, że pracodawcy powołując się na wyrok Wielkiej Izby ETPCz zaczęli hurtowo stosować różnego rodzaju postaci ukrytego monitoringu. Uważam, że mają świadomość tego, iż rozstrzygnięcie to nie stanowi swoistego „mechanizmu systemowej legalizacji" w odniesieniu do ukrytego monitoringu wizyjnego. Dlatego też brak odpowiednich i konkretnych rozwiązań prawodawczych prowadzić będzie do kreowania „szarej strefy", w której tego rodzaju praktyki jak najbardziej mogą mieć miejsce.

## THE USE OF HIDDEN VIDEO MONITORING AGAINST EMPLOYEES: CONTENTIOUS AND AMBIGUOUS ISSUES

Summary

The fundamental issue raised in this article comes down to an attempt at identifying the question of protection of the informational autonomy of the individual in the context of the employer's use of covert video monitoring. The analysis is carried out from the point of view of the compliance of the practice in question with constitutional standards, including the constitutional weighting mechanism, and in correlation with the position of the Grand Chamber of the ECHR expressed in the judgment in the case *López Ribalda and Others v. Spain*.

Keywords: hidden video surveillance, protection of individual freedoms and rights, protection of personal data, resolution of conflicts of freedoms and rights, data controller, judgment of the ECHR in the case of *López Ribalda and others v. Spain*

## BIBLIOGRAFIA

Banaszak B., *Prawa jednostki i systemy ich ochrony*, Wrocław 1995.

Barański M., *Ukryty monitoring w zakładzie pracy w kontekście wyroku Europejskiego Trybunału Praw Człowieka z dnia 17 października 2019 r. (López Ribalda i inni v. Hiszpania, skargi nr 1874/13 i 8567/13)*, „Monitor Prawa Pracy" 2020, nr 3.


© for this edition by CNS

Dąbrowska O., *Kryteria dopuszczalności stosowania monitoringu w miejscu pracy oraz związane z tym obowiązki pracodawcy w świetle reformy ochrony danych osobowych*, „Prawo Mediów Elektronicznych" 2019, nr 1.

*ETPC: Ukryty monitoring kasjerek w supermarkecie skutkował naruszeniem ich prywatności*, Biuletyn Informacji Publicznej RPO, 15.01.2018, https://bip.brpo.gov.pl/pl/content/etpc-ukryty-monitoring-kasjerek-w-supermarkecie-w-prawo-do-prywatnosci.

Garlicki L., *Komentarz do art. 31 Konstytucji RP*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 3, red. L. Garlicki, Warszawa 2003.

Góral Z., Tyc A., *Glosa do wyroku Europejskiego Trybunału Praw Człowieka z 17 października 2019 r. w sprawie López Ribalda i inni* vs. *Hiszpania, nr skarg 1874/13 i 8567/13*, „Przegląd Sejmowy" 28, 2020, nr 3 (158).

Grzelak A., *Stosowanie monitoringu wizyjnego w relacjach pracowniczych. López Ribalda i Inni przeciwko Hiszpanii, skargi nr 1874/13 i 8567/13 wyrok z dnia 17 października 2019* r., [w:] *Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Komentarz Orzeczniczy za rok 2019*, red. J. Kosonoga, Warszawa 2020.

Grzybowski K., *Autonomia informacyjna jednostki a zgoda na przetwarzanie przez pracodawcę danych osobowych*, „Przegląd Sejmowy" 28, 2020, nr 6 (161).

Jabłoński M., *RODO a dostęp do informacji publicznych. Kwestie dyskusyjne na tle kształtującej się praktyki orzeczniczej sądów administracyjnych*, [w:] *Konstytucjonalizm polski. Refleksje z okazji jubileuszu 70-lecia urodzin i 45-lecia pracy naukowej Profesora Andrzeja Szmyta*, red. A. Gajda, K, Grajewski, A. Rytel-Warzocha, P. Uziębło, M.M. Wiszowaty, Gdańsk 2020.

Jabłoński M., Jarosz-Żukowska M., *Adresaci konstytucyjnych wolności i praw*, [w:] R. Balicki, M. Bernaczyk, O. Halub-Kowalczyk, M. Jabłoński, S. Jarosz-Żukowska, M. Kłopocka-Jasińska, A. Ławniczak, M. Masternak-Kubiak, A. Śledzińska-Simon, J. Węgrzyn, K. Wygoda, *Konstytucja i prawo konstytucyjne. Zarys wykładu*, Wrocław 2021.

Jabłoński M., Kornobis-Romanowska D., Wygoda K., *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017.

Jabłoński M., Radziszewski T., Wasiak D., Wygoda K., *Sygnalista a ochrona danych osobowych*, Toruń 2022.

Jabłoński M., Węgrzyn J., *Prawo do bycia zapomnianym*, Wrocław 2021.

Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice*, Wrocław 2002.

Jabłoński M., Wygoda K., *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej. Aspekty praktyczne,* Warszawa 2021.

Jarosz-Żukowska S., *Konstytucyjne przesłanki dopuszczalności ograniczeń prawa własności*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje*, red. L. Garlicki, A. Szmyt, Warszawa 2003.

Kalisz A., *Rozwiązywanie kolizji norm i zasad w kontekście praw człowieka*. *Uwagi teoretyczno-prawne*, [w:] *Wolność wypowiedzi* versus *wolność religijna. Studium z zakresu prawa konstytucyjnego, karnego i cywilnego*, red. A. Biłgorajski, Warszawa 2015.

Kuba M., *Komentarz do art. 22² k.p.*, [w:] *Kodeks pracy. Komentarz*, t. 1. *Art. 1–93*, red. K.W. Baran, Warszawa 2022.

*Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection Adopted by the Venice Commission at Its 71st Plenary Session*, *CLD-AD(2007)027-e*, European Commission for Democracy through Law (Venice Commission), 1–2.06.2007, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)027-e.

Rutynowska E., *Komunikat FOR 2/2022: Kontrola operacyjna: czym jest, czym być powinna i jak się ma do prawa do prywatności*, Forum Obywatelskiego Rozwoju, 24.01.2022, https://for.org.pl/pliki/artykuly/8066_komunikatfor22022kontrola-operacyjnaczym-jest-czym-byc-powinna-i-jak-sie-ma-do-prawa-do-prywatnosci.pdf.


© for this edition by CNS

Safjan M., *O różnych metodach oddziaływania horyzontalnego praw podstawowych na prawo prywatne*, „Państwo i Prawo" 2014, nr 2.

Sakowska-Baryła M., *Ochrona danych osobowych a dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2022.

Sieńczyło-Chlabicz J., *Ochrona prawa do prywatności w Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, Karcie Praw Podstawowych oraz w prawie krajowym*, [w:] *Rozprawy cywilistyczne. Księga pamiątkowa dedykowana Profesorowi Edwardowi Drozdowi*, red. M. Pecyna, J. Pisuliński, M. Podrecka, Warszawa 2013.

Skunarowska-Drzewiecka E., *Komentarz do art. 22² k.p.*, [w:] *Kodeks Pracy. Komentarz*, red. K. Walczak, Warszawa 2020.

Sobczyk A., *Lopez Ribalda i inni przeciwko Hiszpanii a dopuszczalność niejawnej kontroli pracowników w Polsce*, Sobczyk & Współpracownicy, 7.02.2020, https://sobczyk.com.pl/lopez-ribalda-a-dopuszczalnosc-niejawnej-kontroli-pracownikow-w-polsce/.

Szurgacz S., *System kamer to nie tylko kwestia prywatności*, Kancelarie RP, 23.01.2020, https://kancelarierp.pl/system-kamer-to-nie-tylko-kwestia-prywatnosci/.

Wiśniewski L., *Wolności i prawa osobiste w Konstytucji RP z 1997 r. i w prawie międzynarodowym*, Poznań 1998.

*Wytyczne EROD Nr 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo*, *wersja 2.0 przyjęta 29.01.2020 r.*, European Data Protection Board, 29.01.2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl.pdf.


© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.3

MACIEJ JAKUB ZIELIŃSKI
ORCID: 0000-0003-2250-6582
Uniwersytet im. Adama Mickiewicza w Poznaniu

# POLSKI MODEL REGULACJI MONITORINGU SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ NA TLE PORÓWNAWCZYM*

Abstrakt: W artykule podjęto próbę rekonstrukcji polskiego modelu regulacji dotyczącej monitoringu służbowej poczty elektronicznej. W ocenie autora, model ten wyznaczają przede wszystkim przesłanki zastosowania tej formy kontroli pracowników. Inkorporują one bowiem idee węzłowe dla kontroli udostępnionych pracownikom narzędzi komunikacji elektronicznej; można z nich też dekodować istotne wskazówki dotyczące dopuszczalnych form monitorowania i samej istoty tego monitoringu. Analizując polski model regulacji monitoringu służbowej poczty elektronicznej, autor sięgnął po argumenty natury komparatystycznej, mając na uwadze fakt, że unormowania dotyczące tytułowej problematyki zostały wprowadzone do polskiego porządku prawnego w celu dostosowania go do wymogów jednolitych dla całej Unii Europejskiej przepisów o ochronie danych osobowych.

Słowa kluczowe: monitoring, kontrola pracowników, tajemnica korespondencji, poczta elektroniczna

## WPROWADZENIE

Monitoring poczty elektronicznej to jedna z najbardziej kontrowersyjnych form kontroli pracowników[1]. Może bowiem (przynajmniej potencjalnie) w dotkliwy dla pracownika sposób ingerować w tajemnicę komunikacji, gwarantowaną na poziomie Konstytucji RP i aktów prawa międzynarodowego, oraz naruszać dobra osobiste pracownika chronione na podstawie stosowanych odpowiednio przepisów kodeksu cywilnego (art. 23 i 24 k.c. w związku z art. 300 k.p.). Poszanowanie tych ostatnich przez pracodawcę stanowi zaś jedną z podstawowych zasad prawa pracy (art. $11^1$ k.p.). Regulacja tego zagadnienia w polskim prawie pracy

* Opracowanie stanowi uzupełnioną wersję referatu wygłoszonego podczas Ogólnopolskiej Konferencji Naukowej „Monitoring w zakładzie pracy — aspekty prawne i organizacyjne" we Wrocławiu w dniu 10 czerwca 2022 r.

[1] M. Kuba, *Komentarz do art.* $22^2$, [w:] *Kodeks pracy. Komentarz*, t. 1. *Art. 1–93,* red. K.W. Baran, Warszawa 2022, Nb. 2.1.


© for this edition by CNS

jest stosunkowo młoda, gdyż została wprowadzona do kodeksu pracy na mocy ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych[2], która weszła w życie 25 maja 2018 roku. Przed tą datą, mimo braku stosownego unormowania, przyjmowano dopuszczalność stosowania monitoringu poczty elektronicznej, rozpatrując tę kwestię wyłącznie z punktu widzenia przepisów o ochronie danych osobowych[3]. W wyroku z 13 lutego 2014 roku, I OSK 2436/12[4], Naczelny Sąd Administracyjny uznał, że monitoring aktywności pracownika na udostępnionych mu urządzeniach komunikacji elektronicznej jest dopuszczalny, o ile spełnia wymogi zgodności z prawem, usprawiedliwionego celu, proporcjonalności i transparentności. W judykacie tym podkreślono, że pracownicy muszą mieć świadomość tego, że są poddawani monitoringowi, a pracodawca powinien szczegółowo określić zasady monitoringu i zapoznać z nimi pracowników.

*De lege lata* wymagania związane ze stosowaniem monitoringu poczty elektronicznej uregulowane są zarówno w przepisach kodeksu pracy, jak i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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)[5], co nie może dziwić. Omawiana forma kontroli pracownika prowadzi bowiem do gromadzenia przez pracodawcę informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych (danych osobowych). Choć kodeks pracy jedynie częściowo określa warunki, jakie pracodawca musi spełnić, by zapewnić zgodność z prawem przetwarzania danych osobowych pracownika zebranych w ramach przedmiotowej formy kontroli, jednocześnie kompleksowo określa przesłanki jej stosowania. Zgodnie z art. $22^3$ § 1 k.p. są nimi „niezbędność do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy". Przepis stosuje się odpowiednio do pracy do innych form monitoringu, w tym także do monitoringu aktywności pracownika w Internecie ($22^3$ § 3 k.p.).

W doktrynie rzadko analizuje się szczegółowo przesłanki zawarte w art. $22^3$ § 1 k.p. Zwykle wskazuje się, że użycie spójnika „oraz" oznacza, iż obie one muszą zostać spełnione jednocześnie[6]. Podnosi się też wątpliwości co do tego, czy omawiana forma monitoringu może być adekwatnym środkiem zapewnia-

[2] Dz.U. z 2019 r. poz. 1781.

[3] Por. M. Gorbunow, *Monitoring w świetle nowelizacji Kodeksu pracy z 10.5.2018 r.*, „Monitor Prawa Pracy" 2019, nr 10, s. 23; M. Kuba, *Monitoring poczty elektronicznej pracownika — refleksje na tle nowych regulacji prawnych*, „Praca i Zabezpieczenie Społeczne" 2019, nr 11, s. 29.

[4] Wyrok NSA z 13 lutego 2014 r., I OSK 2436/12, Lex nr 1449889; z glosą Agnieszki Stępień — A. Stępień, *Prawo pracownika do prywatności w miejscu pracy — glosa*, „Informacja w Administracji Publicznej" 2015, nr 4, Legalis.

[5] Dz.Urz.UE L 119 z 4.05.2016 r., s. 1, dalej jako RODO.

[6] E. Maniewska, K. Jaśkowski, *Kodeks pracy. Komentarz*, Warszawa 2019, s. 198; M. Kuba, *Komentarz do art. $22^2$*, Nb. 3.2.


© for this edition by CNS

nia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy[7]. Część autorów z dezaprobatą odnosi się do faktu, że w katalogu przesłanek konieczności monitoringu poczty elektronicznej pracownika ustawodawca nie uwzględnił ochrony informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę[8]. Nie wyczerpuje to jednak problematyki dopuszczalności stosowania przedmiotowego monitoringu.

Jak się wydaje, zarówno na gruncie prawa polskiego, jak i obcych porządków prawnych, to właśnie przesłanki stosowania monitoringu wyznaczają model regulacji tej formy kontroli (rozumiany jako „układ twierdzeń, które ujęte razem oddają strukturalne własności analizowanej instytucji prawnej oraz relacje pomiędzy nimi")[9]. Przesłanki te inkorporują bowiem pewne idee obejmujące węzłowe problemy kontroli udostępnionych pracownikom narzędzi komunikacji elektronicznej, które z kolei wyznaczają określony kierunek stosowania i interpretacji norm prawnych dotyczących tej instytucji prawnej. Można z nich dekodować istotne wskazówki dotyczące zarówno dopuszczalnych form kontroli pracownika, jak i samej istoty monitoringu. Tę ostatnią próbuje się w nauce polskiej uchwycić przez pryzmat używanych przez ustawodawcę pojęć[10], co — jak zostanie wykazane w niniejszym opracowaniu — nie jest drogą właściwą.

W analizie polskiego modelu regulacji monitoringu służbowej poczty elektronicznej pomocne mogą okazać się argumenty natury komparatystycznej. Należy bowiem zauważyć, że wprowadzenie unormowań dotyczących tej formy kontroli pracowników podyktowane było wejściem w życie RODO[11], przewidującego jednolite dla całej Unii Europejskiej zasady ochrony danych osobowych. Choćby z tego powodu nie sposób w omawianym zakresie uciec od analizy rozwiązań funkcjonujących w innych państwach członkowskich Unii Europejskiej. Nie chodzi przy tym o drobiazgową charakterystykę wszystkich z nich. Ponieważ monitorowanie pracowników jest kwestią dość złożoną, która może być rozpatrywana na wielu płaszczyznach, jego opis wymaga wprowadzenia pewnych uogólnień wyrażających to, co na tle poszczególnych przepisów wydaje się najważniejsze i najogólniejsze.

---

[7] M. Kuba, *Monitoring poczty elektronicznej pracownika…*, s. 31.

[8] *Ibidem*; także J. Jarguz, *Komentarz do art. 22³*, [w:] *Kodeks pracy. Regulacje COVID-19 w prawie pracy. Komentarz*, red. A. Sobczyk, Warszawa 2020, Nb. 1 oraz D. Dörre-Kolasa, *Komentarz do art. 22³ k.p.*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2020, Nb. 1.

[9] Por. K. Płeszka, *Uzasadnianie decyzji interpretacyjnych przez ich konsekwencje*, Kraków 1996, s. 30 i powołana tam literatura.

[10] J. Jarguz, *Komentarz do art. 22³*, Nb. 2.

[11] Świadczy o tym chociażby zbieżność dat początkowych stosowania RODO i obowiązywania art. 22³ k.p.


© for this edition by CNS

## PRAWNOPORÓWNAWCZY KONTEKST PROBLEMATYKI MONITORINGU POCZTY ELEKTRONICZNEJ

Analiza rozwiązań dotyczących dopuszczalności stosowania monitoringu poczty elektronicznej, które obowiązują w państwach Unii Europejskiej wskazuje, że są one dość zróżnicowane. W niektórych państwach albo w ogóle brakuje unormowań przewidujących przesłanki stosowania takiej formy monitoringu, albo regulacja prawna w tym przedmiocie jest bardzo skąpa, zaś oceny dopuszczalności ingerencji w prywatność pracownika dokonuje się na gruncie ogólnych zasad prawa. Przykładowo: w prawie włoskim, które nie normuje przypadków, w jakich pracodawca może stosować monitoring poczty elektronicznej, jego dopuszczalność analizuje się z punktu widzenia zasad minimalizacji i proporcjonalności[12], mając na uwadze, że co do zasady zawartość wiadomości elektronicznej objęta jest ochroną prywatności[13]. Do zasady minimalizacji ingerencji odwołują się także regulacje belgijskie, stanowiące, z jednej strony, że kontrola danych komunikacji elektronicznej w sieci nie może prowadzić do ingerencji w życie prywatne pracownika, a z drugiej — że w sytuacji, gdy takie monitorowanie to prowadzi do ingerencji w życie prywatne pracownika, ingerencja ta musi być ograniczona do minimum[14].

Opisane powyżej (i analogiczne) rozwiązania pozostawiają jednak spory margines niepewności co do zakresu możliwej ingerencji w prywatność pracownika, co wydaje się szczególnie widoczne na gruncie prawa francuskiego. W systemie tym regulacja prawna dotycząca monitorowania działań pracowników jest dość skąpa. Artykuł L.432-2-1 kodeksu pracy ustanawia wymogi w zakresie informowania i konsultowania rady zakładowej przed podjęciem decyzji o wdrożeniu środków lub technik monitorowania pracowników. Zwykle jako przepisy służące rekonstruowaniu zasad prowadzenia monitoringu wskazuje się również na art. L.121-8 kodeksu pracy, który stanowi, że żadne informacje dotyczące pracownika osobiście nie mogą być zbierane przez urządzenie, o którym pracownik nie został uprzednio poinformowany, oraz z art. L120-2, zgodnie z którym niedopuszczalne jest ograniczanie praw osób oraz wolności indywidualnych i zbiorowych, jeżeli nie jest uzasadnione charakterem obowiązków pracownika i proporcjonalne

[12] Zob. nakaz włoskiego Urzędu Ochrony Danych Osobowych z dnia 15 kwietnia 2021 r. przeciwko Clear Channel Italia S.p.A., znak: 9670738 [ordinanza ingiunzione del Garante per la protezione dei dati personali nei confronti di Clear Channel Italia S.p.A. — 15 aprile 2021 (9670738)], *Ordinananza ingiunzione — 15 aprile 2021*, Garante per la Protezione dei Dati Personali, 15.04.2021, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9587637 (dostęp: 30.09.2022).

[13] Wyrok Sądu Konstytucyjnego nr 281 z dnia 17 lipca 1998 r., ECLI:IT:COST:1998:281.

[14] Zob. art. 6 układu zbiorowego pracy nr 81 z dnia 26 kwietnia 2002 r., zawartego w ramach Krajowej Rady Pracy, dotyczącego ochrony prywatności pracowników w zakresie kontroli danych komunikacji elektronicznej w sieci [Convention collective de travail n° 81 du 26 avril 2002, conclue au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau].


© for this edition by CNS

do zamierzonego celu. Przepisy te dalekie są od precyzji, a dowodów na prawdziwość tej tezy dostarcza orzecznictwo Sądu Kasacyjnego. Początkowo przyjmowano w nim, że pracodawca nie może (bez naruszenia prawa do prywatności) odczytywać oznaczonych jako prywatne wiadomości wysyłanych i otrzymywanych przez pracownika dzięki narzędziu komputerowemu udostępnionemu mu do pracy, i to nawet w przypadku, gdy pracodawca zabronił korzystania z niego w celach innych niż zawodowe[15]. W kolejnych orzeczeniach podejście to łagodzono, wskazując, że w wyjątkowych przypadkach pracodawca może uzyskać dostęp do treści cyfrowych podlegających ochronie ze względu na prywatność pracownika, o ile temu ostatniego zapewniona obecność przy zapoznawaniu się z tymi treściami[16]. W konsekwencji gwarancje prywatności w zakresie odnoszącym się do monitorowania poczty elektronicznej przypominają prawo do uczestniczenia w przeszukaniu mieszkania[17].

W znacznej części państw członkowskich Unii Europejskiej dopuszczalność monitoringu poczty elektronicznej uzależnia się od istnienia określonych zasad wykorzystania służbowego sprzętu elektronicznego dla celów prywatnych. Przykładowo: prawo hiszpańskie zobowiązuje pracodawcę do ustalenia — we współdziałaniu z przedstawicielami pracowników — kryteriów korzystania z urządzeń cyfrowych z poszanowaniem minimalnych standardów ochrony prywatności pracownika i zgodnie z zasadami współżycia społecznego (art. 87 ust. 3 ustawy organicznej 3/2018 z dnia 5 grudnia o ochronie danych osobowych i gwarancji praw cyfrowych)[18]. Jednocześnie ustawa organiczna nr 3/2018 przewiduje, że dostęp pracodawcy do treści urządzeń cyfrowych, w odniesieniu do których zezwolił na ich wykorzystanie do celów prywatnych, wymaga dokładnego określenia dozwolonych zastosowań oraz ustanowienia gwarancji ochrony prywatności pracowników takich jak, w stosownych przypadkach, określenie okresów, w których urządzenia mogą być wykorzystywane do celów prywatnych (art. 87 ust. 3). Dostęp pracodawcy do skrzynki poczty elektronicznej udostępnionej pracownikowi może być więc realizowany wyłącznie w ramach kontroli przestrzegania obowiązków pracowniczych oraz w celu zagwarantowania, że wspomniane urządzenia są używane z należytą starannością[19]. W orzecznictwie przyjmuje się przy tym,

[15] Wyrok Sądu Kasacyjnego [Cour de Cassation] z dnia 2 października 2001 r., n° 99-42.942, Société Nikon France c/a M. Frédéric Onof.

[16] Wyrok Sądu Kasacyjnego [Cour de Cassation] z dnia 17 maja 2005 r., n° 03-40.017, M. Philippe Klajer c/a Société Cathnet-Science.

[17] Por. dotyczący przeszukania szafy pracownika wyrok Sądu Kasacyjnego [Cour de Cassation] z dnia 11 grudnia 2001 r., n° 99-43.030, FS-P N° Lexbase: A6554AXZ, z omówieniem J. Savatier, *Commentaire de l'arrêt de la Cour de cassation, chambre sociale, du. 19 décembre 2007, n° 06-43.918, Bull. 2007 V n° 216*, „Droit social" 2002, nr 3, s. 352.

[18] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE-A-2018-16673.

[19] P. Martín Molina, *Cuestiones relevantes de la nueva Ley Orgánica de Protección de Datos Personales y Garantía de los derechos Digitales: Los derechos digitales*, „Actualidad Civil" 2018, nr 12.


© for this edition by CNS

że pracodawca ma możliwość wprowadzenia bezwzględnego zakazu używania udostępnionych mu urządzeń dla celów prywatnych[20]. W doktrynie akcentuje się natomiast potrzebę zapewnienia pracownikowi, choćby w minimalnym zakresie, możliwości użytkowania sprzętu udostępnionego przez pracodawcę dla celów niezwiązanych z wykonywaniem obowiązków pracowniczych[21].

W prawie czeskim dopuszczalność stosowania monitoringu poczty elektronicznej została *expressis verbis* powiązana z ustawowym zakazem wykorzystywania takiej poczty do użytku osobistego bez zgody pracodawcy. Paragraf 316 ust. 1 zd. 1 czeskiego kodeksu pracy[22] zakazuje pracownikom wykorzystywania do celów osobistych środków produkcji i pracy (w tym technik komputerowych i urządzeń telekomunikacyjnych) należących do pracodawcy bez jego zgody. Drugie zdanie tego przepisu wprost wskazuje, że monitoring służy egzekwowaniu przestrzegania tego zakazu. Jak wskazuje się w orzecznictwie, ten ostatni przepis zezwala jedynie na taki sposób monitorowania, który jest niezbędny do stwierdzenia, czy pracownik przestrzega zakazu wykorzystywania powierzonego mu sprzętu dla celów prywatnych. Zakaz ten ma charakter bezwzględny, a pracodawca może ustalić zgodę na wykorzystanie poczty elektronicznej dla celów prywatnych w dowolnym zakresie (od pełnej zgody bez żadnych ograniczeń czasowych i przedmiotowych, poprzez zgodę tylko w określonym zakresie, na określony czas lub obejmującą konkretny materiał, aż do zgody na jednorazowe użycie sprzętu dla celów prywatnych)[23].

Podobnie na gruncie prawa austriackiego przyjmuje się, że wprowadzenie monitoringu poczty elektronicznej jest dozwolone, jeżeli istnieje uzasadnienie dla stosowania takiej formy monitoringu, a pracodawca wprowadził zakaz korzystania z kont poczty elektronicznej dla celów prywatnych[24]. Również w Niemczech zdaje się dominować stanowisko, zgodnie z którym monitorowanie poczty elektronicznej możliwe jest tylko wówczas, gdy pracodawca wydał zakaz jej używania dla celów służbowych, i to głównie w celu monitorowania przestrzegania

[20] Wyroki Trybunału Konstytucyjnego [Tribunal Constitucional] nr 170/2013 z dnia 7 października 2013 r., sygn. 2907-2011, ES:TC:2013:170 i nr 39/2016 z dnia 3 marca 2016 r., BOE-A-2016-3405 oraz wyrok Sądu Najwyższego [Tribunal Supremo] de z dnia 6 października 2011, sygn. 4053/2010, ECLI: ES:TS:2011:8876.

[21] M. Miñarro Yanini, *La «Carta de los derechos digitales» de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación*, „Revista de Trabajo y Seguridad Social" 2019, nr 430, s. 28.

[22] Czes. Zákon č. 262/2006 Sb.Zákon zákoník práce, Sbírka zákonů České republiky, částka 84, s. 3188–3189.

[23] Wyrok Sądu Najwyższego Republiki Czeskiej [Nejvyšší soud ČR] z dnia 16 sierpnia 2012 r. sygn. 21 Cdo 1771/2011, ECLI:CZ:NS:2012:21.CDO.1771.2011.1.

[24] Wyrok Wyższego Sądu Krajowego w Wiedniu [Oberlandesgericht Wien] z dnia 29 czerwca 2005, sygn. 8 Ra 54/05b i 8 Ra 55/05z, ARD 5633/9/2005.


© for this edition by CNS

tego zakazu. Zarówno w doktrynie[25], orzecznictwie[26], jak i praktyce działania krajowych organów nadzoru nad ochroną danych osobowych[27], przyjmuje się bowiem, że pracodawcy, którzy dozwalają pracownikom na korzystanie ze służbowej poczty elektronicznej dla celów prywatnych są uważani za dostawców usług telekomunikacyjnych i z tego tytułu polegają ograniczeniom wynikającym z obowiązku tajemnicy telekomunikacyjnej (*Fernmeldegeheimnis*). W aktualnym stanie prawnym problematykę tej ostatniej reguluje ustawa o ochronie danych w telekomunikacji i telemediach (*Telekommunikation-Telemedien-Datenschutz-Gesetz*)[28]. Paragraf 3 ust. 3 tejże ustawy stanowi, że osobom zobowiązanym do zachowania tajemnicy telekomunikacyjnej zabrania się poznawania treści lub szczegółowych okoliczności telekomunikacji poza przypadkiem, gdy jest to konieczne do świadczenia usług telekomunikacyjnych lub do obsługi ich sieci telekomunikacyjnych lub ich systemów telekomunikacji, w tym ochrony ich systemów technicznych.

W państwach członkowskich Unii Europejskiej można także spotkać rozwiązania przewidujące wręcz kazuistyczne zasady zapoznawania się przez pracodawcę z treścią wiadomości elektronicznych wysyłanych na (lub odbieranych z) adresu poczty elektronicznej przydzielonego przez pracodawcę na użytek służbowy. Fińska ustawa nr 759 z dnia 13 sierpnia 2004 roku o prywatności w miejscu pracy[29] w § 18 przyznaje pracodawcy prawo do pobierania i otwierania wiadomości elektronicznych wysyłanych na adres poczty elektronicznej przydzielony na użytek służbowy pracownika lub wiadomości poczty elektronicznej wysyłanych przez pracownika z takiego adresu, ale tylko wtedy, gdy pracodawca wdrożył niezbędne środki w celu ochrony wiadomości e-mail wysyłanych na nazwisko pracownika lub przez pracownika. Omawiana ustawa określa też przesłanki zapoznania się z wiadomościami elektronicznymi pod nieobecność pracownika oraz na wypadek jego śmierci. Zgodnie z § 19 pracodawca jest uprawniony do sprawdzenia — na podstawie informacji o nadawcy, odbiorcy lub tytule wiadomości — czy do pracownika wysłano jakieś wiadomości w okresie jego nieobecności lub czy pra-

[25] A. Auer-Reinsdorff, I. Conrad, *Handbuch IT- und Datenschutzrecht*, München 2016, s. 206; S. Brink, S. Wirtz, *Kontrolle des Arbeitgebers bei (unerlaubter) Internetnutzung der Beschäftigten,* „Arbeitsrecht Aktuell" 2016 z. 11–12, s. 255 n.

[26] Wyrok Krajowego Sądu Pracy dla Berlina-Brandenburgii [Landesarbeitsgericht Berlin-Brandenburg] z dnia 14 stycznia 2016 r. sygn. 5 Sa 657/15 — Rn. 81, BeckRS 2016, 67048) oraz Heskiego Krajowego Sądu Pracy [Hessischen Landesarbeitsgericht] z dnia 21 września 2018 r., sygn. 10 Sa 601/18, openJur 2019, 31896.

[27] Wytyczne organów nadzorczych ds. ochrony danych dotyczące zgodnego z przepisami o ochronie danych osobowych korzystania z poczty elektronicznej i innych usług internetowych w miejscu pracy [Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz], Datenschutzkonferenz, 10.02.2016, https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf (dostęp: 07.03.2022).

[28] Telekommunikation-Telemedien-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045).

[29] Laki yksityisyyden suojasta työelämässä, SDK 861/2022.


© for this edition by CNS

cownik bezpośrednio przed jego nieobecnością wysłał lub otrzymał wiadomości, wymagające od pracodawcy podjęcia określonych działań. Jest to dopuszczalne, jeżeli: 1) pracownik wykonuje zadania samodzielnie w imieniu pracodawcy, a pracodawca nie posiada systemu ewidencjonowania lub innego poznawania prowadzonych przez pracownika spraw i czynności niezbędnych do ich załatwiania; 2) ze względu na zadania pracownika i sprawy będące w toku oczywiste jest, że wiadomości w wyżej wymienionych sprawach zostały wysłane lub odebrane; 3) zgoda pracownika nie może być uzyskana w rozsądnym terminie, a sprawa nie może być rozwiązana bez zwłoki. Przedmiotowa ustawa reguluje także możliwość uzyskania dostępu do wiadomości wysyłanych na adres (lub z adresu) służbowej poczty elektronicznej w razie śmierci pracownika lub trwałego uniemożliwienia mu wykonywania obowiązków i niemożności uzyskania jego zgody. W takim przypadku, o ile odzyskanie wiadomości nie prowadzi do jej otwarcia, wymagane jest sporządzenie protokołu, który należy dostarczyć pracownikowi bez zbędnej zwłoki, zaś informacje o nadawcy lub odbiorcy wiadomości lub informacje zawarte w nagłówku nie mogą być przetwarzane w szerszym zakresie niż jest to konieczne w celu pobrania wiadomości. Z kolei osoby przetwarzające informacje nie mogą ujawniać tych informacji osobom trzecim w trakcie trwania stosunku pracy lub po jego zakończeniu. W omawianych okolicznościach pracodawca może zapoznać się z treścią wiadomości tylko wówczas, gdy na podstawie informacji o nadawcy lub odbiorcy wiadomości elektronicznej lub tytułu wiadomości jest oczywiste, że wiadomość wysłana do pracownika lub przez pracownika wymaga od pracodawcy podjęcia określonych działań w celu zakończenia negocjacji związanych z jego działalnością obsługi klientów lub zabezpieczenia jego działalności, a brak jest możliwości skontaktowania się z nadawcą lub odbiorą wiadomości (§ 20).

Powyższy przegląd rozwiązań obowiązujących w poszczególnych krajach Unii Europejskiej, jakkolwiek niekompletny, pozwala na sformułowanie wniosku co do istnienia w zasadzie trzech modeli prawnej regulacji dotyczącej monitoringu poczty elektronicznej. W modelu pierwszym dopuszczalność prowadzenia takiego monitoringu limituje się zasadą proporcjonalności ingerencji w prywatność pracownika. Tego typu podejście pozostawia spory margines niepewności co do dopuszczalnego zakresu monitorowania poczty elektronicznej pracownika, co doskonale obrazuje orzecznictwo francuskiego Sądu Kasacyjnego. Model drugi wiąże dopuszczalność stosowania kontroli poczty elektronicznej z przestrzeganiem ustanowionych (przez pracodawcę lub przepisy powszechnie obowiązującego prawa) zasad jej wykorzystania. W modelu tym dopuszczalność monitorowania poczty elektronicznej uzależniona jest od istnienia sformalizowanych, czy to na poziomie ustawowym, czy zakładowym, zasad wykorzystania udostępnionych mu narzędzi pracy. Kontrola poczty w takim układzie służy uzyskiwaniu informacji o tym, czy pracownik przestrzega ustanowionych zasad wykorzystania udostępnionych mu narzędzi pracy. Z kolei w modelu trzecim


© for this edition by CNS

ustawodawca normuje niezwykle szczegółowo i kazuistycznie zarówno dopuszczalne formy kontroli, jak i przesłanki zastosowania każdej z nich.

## PRÓBA REKONSTRUKCJI POLSKIEGO MODELU PRAWNEJ REGULACJI DOPUSZCZALNOŚCI MONITORINGU PRACOWNICZEJ POCZTY ELEKTRONICZNEJ

Przechodząc do rekonstrukcji polskiego modelu prawnej regulacji monitoringu pracowniczej poczty elektronicznej: należy uznać, że wpisuje się on w ten wzorzec, który dopuszczalność stosowania kontroli poczty elektronicznej uzależnia od istnienia zasad jej wykorzystania. Wskazują na to ustawowe przesłanki stosowania omawianej formy monitoringu wysłowione w art. $22^3$ § 1 k.p. Analiza językowa tego przepisu pozwala stwierdzić, że celem kontroli pracowniczej poczty elektronicznej jest z jednej strony zapewnienie takiej organizacji pracy, która umożliwia pełne wykorzystanie czasu pracy, a z drugiej — zapewnienie właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. W obu przypadkach mamy do czynienia z pewnymi wzorcami postępowania, z którymi pracodawca zamierza porównywać zachowania pracownika. Wskazuje na to zresztą użycie przez ustawodawcę pojęcia „kontrola" w odniesieniu do możliwych działań podejmowanych przez pracodawcę w odniesieniu do służbowej poczty elektronicznej w razie zaistnienia omawianych przesłanek. W języku potocznym kontrola oznacza porównanie stanu faktycznego ze stanem wymaganym[30]. W języku prawniczym chodzi o porównanie działań określonego podmiotu z założonym wzorcem według wybranego kryterium[31].

Pojęcie organizacji pracy nie zostało zdefiniowane w przepisach kodeksu pracy, choć ustawodawca posługuje się nim kilkakrotnie: jako elementem podlegającym uwzględnieniu przy ustalaniu norm pracy (art. 83 § 2), przesłanką wydłużenia okresów rozliczeniowych (art. 129 § 2) i przedmiotem obowiązkowej konsultacji pracodawcy z pracownikami lub ich przedstawicielami w zakresie dotyczącym bezpieczeństwa i higieny pracy (art. $237^{11a}$ § 1 pkt 1 k.p.). W języku potocznym organizacja to albo „grupa ludzi zjednoczonym wspólnym planem, programem, poglądami, zadaniami" albo „sposób, system zorganizowania

[30] *Kontrola*, [hasło w:] *Słownik języka polskiego*, t. 1, red. M. Szymczak, Warszawa 1983, s. 1001.

[31] J. Boć, *Prawo Administracyjne*, Wrocław 2010, s. 376–383; J. Korczak, *Nadzór i kontrola nad działalnością samorządu terytorialnego*, [w:] *System prawa administracyjnego*, t. 2. *Konstytucyjne podstawy funkcjonowania administracji publicznej*, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2012, s. 243–246, 251–262; M. Stahl, *Akty nadzoru jako prawna forma działania administracji*, [w:] *System prawa administracyjnego*, t. 5. *Prawne formy działania administracji*, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2013, s. 334–357.


© for this edition by CNS

czegoś”[32]. W naukach o zarządzaniu terminu „organizacja” używa się trojako: w sensie rzeczowym, atrybutywnym lub czynnościowym[33]. Rzeczowe ujęcie organizacji obejmuje „rzeczy zorganizowane”, czyli konkretne grupy ludzi lub podmioty, takie jak przedsiębiorstwa, stowarzyszenia, partie oraz zespoły pracownicze. Organizacja w znaczeniu atrybutywnym oznacza pewien szczególny rodzaj stosunków części do siebie i do złożonej z nich całości, polegających na tym, że części współprzyczyniają się do powodzenia całości. Natomiast organizacja w znaczeniu czynnościowym to pewien rodzaj zorganizowanego działania ukierunkowanego na osiągnięcie założonych celów, przy czym chodzi tu o samą czynność organizowania[34]. W tym kontekście nie powinno ulegać wątpliwości, że pojęcie „organizacji pracy” użyte w art. $22^3$ § 1 k.p. zostało użyte w znaczeniu atrybutywnym, jako rodzaj stosunków zachodzących pomiędzy materialnymi i niematerialnymi składnikami zakładu pracy a pracownikami, polegających na tym, że poszczególne elementy współprzyczyniają się do zapewnienia efektywności procesu świadczenia pracy. Chodzi więc o taki sposób ukształtowania sposobu świadczenia pracy, który pozwala na wykorzystanie całości czasu pracownika na realizację powierzonych mu obowiązków, eliminując zarówno przestoje w tym zakresie, jak i okresy niewykonywania pracy w tym czasie z przyczyn leżących po stronie pracownika.

Przy takim założeniu, dla wprowadzenia monitoringu pracodawca musi przedsięwziąć określone środki umożliwiające pełne wykorzystanie czasu pracy, czyli zorganizować pracę w taki sposób, aby to było możliwe, co jest zresztą jego obowiązkiem wynikającym z art. 94 pkt 2 k.p. Tylko bowiem w przypadku wprowadzenia określonych zasad organizacji procesu świadczenia pracy możliwe będzie porównywanie zachowań pracownika z ustalonym wzorcem, czego środkiem — jak wskazano powyżej — ma być monitoring przewidziany w art. $22^3$ § 1 k.p. Chodzi tu przede wszystkim o wprowadzenie pewnych zakazów dotyczących sposobu wykorzystywania czasu pracy wynikającego z jego rozkładu (na przykład wykorzystywania tego czasu do załatwiania spraw prywatnych poza wyznaczonymi przerwami). W pojęciu „organizacji czasu pracy umożliwiającej pełne wykorzystanie czasu pracy” mieszczą się także zakazy odnoszące się do zachowań o charakterze dyskryminacyjnych (w tym noszących znamiona molestowania lub molestowania seksualnego), mobbingowych, bądź stanowiących naruszenie zasad współżycia społecznego. Monitoring poczty elektronicznej może więc służyć kontroli przestrzegania ciążących na pracownikach obowiązków powstrzymywania się od takich zachowań[35].

[32] *Organizacja*, [hasło w:] *Słownik języka polskiego*, t. 2, red. M. Szymczak, Warszawa 1984, s. 540.

[33] H. Halma *et al.*, *Podstawy teoretyczne organizacji i zarządzania*, Katowice 1983, s. 17 n.

[34] J. Zieleniewski, *Organizacja zespołów ludzkich*, Warszawa 1972, s. 33.

[35] Podobnie, jak się wydaje, D. Dörre-Kolasa, *Komentarz do art. $22^3$ k.p.*, Nb. 7.


© for this edition by CNS

Drugą przesłanką wprowadzenia monitoringu służbowej poczty elektronicznej jest zapewnienie właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Nie ulega wątpliwości, że w ramach przysługujących mu kompetencji kierowniczych pracodawca ma prawo ustalić zasady wykorzystywania narzędzi pracy udostępnionych pracownikowi w celu wykonywania obowiązków pracowniczych. Wydaje się, że skoro monitoring ma służyć kontroli zachowań pracownika w zakresie dotyczącym użytkowania udostępnionych mu narzędzi pracy, to warunkiem stosowania takiej formy monitoringu jest ustanowienie przez pracodawcę przejrzystych zasad użytkowania tych narzędzi. Postulat ten spełnia na przykład zakaz wykorzystywania poczty elektronicznej do celów niezwiązanych z wykonywaniem obowiązków, co z jednej strony umożliwia stosowanie kontroli poczty elektronicznej w celu ustalenia, czy zakaz ten jest przestrzegany, a z drugiej — pozbawia pracownika uzasadnionego oczekiwania prywatności, które limituje zakres dopuszczalnej ingerencji w prywatność pracownika[36]. Ograniczeniu zakresu uzasadnionego oczekiwania prywatności służy zresztą odesłanie w art. $22^3$ § 3 k.p. do odpowiedniego stosowania art. $22^2$ § 6–10 k.p., które nakazują określenie celów, zakresu i sposobu zastosowania monitoringu w układzie zbiorowym pracy lub w regulaminie pracy albo — jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy — w obwieszczeniu, a także informowania o tym pracowników.

Abstrahując od problemów dotyczących ustalenia, czy i w jakim zakresie ewentualny monitoring naruszałby w takim przypadku tajemnicę korespondencji i inne dobra osobiste pracownika, pracodawca może także poprzestać na zakazie przesyłania za pomocą poczty elektronicznej materiałów zawierających informacje, których ujawnienie mogłoby narażać pracodawcę na szkodę. Niewątpliwie taki zakaz wpisywałby się w pojęcie „właściwego użytkowania udostępnionych pracownikowi narzędzi pracy", co oznacza, że kontrola poczty służbowej może służyć także sprawdzeniu, czy pracownik przestrzega zasad wykorzystywania omawianego narzędzia pracy przy przesyłaniu informacji poufnych[37]. W tym kontekście ewentualne uwzględnienie w katalogu przesłanek monitoringu służbowej poczty elektronicznej pracownika okoliczności dotyczącej ochrony omawianych informacji stanowiłoby *superfluum* naruszające podstawowe zasady legislacji[38].

[36] Zob. szerzej: M.J. Zieliński, *Obowiązek zachowania prywatności pracownika*, [w:] *System prawa pracy*, t. 3. *Indywidualne prawo pracy. Część szczegółowa*, red. K.W. Baran, M. Gersdorf, K. Rączka, Warszawa 2021, s. 172, 222 n.

[37] Podobnie, choć z nieco innym uzasadnieniem: D. Dörre-Kolasa, *Komentarz do art. $22^3$ k.p.*, Nb. 2. Odmiennie, niesłusznie, J. Jarguz, *Komentarz do art. $22^3$ k.p.*, Nb. 1.

[38] Chybiony jest zatem argument J. Jarguz, jakoby z faktu, że ustawodawca wyodrębnił przesłankę ochrony informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę przy monitoringu wizyjnym, można było wnioskować, że pominięcie jej przy innych formach monitoringu i zawarcie tego samego zakresu znaczeniowego pod inną przesłanką byłoby niespójne i niekonsekwentne (J. Jarguz, *Komentarz do art. $22^3$ k.p.*, Nb. 1).


© for this edition by CNS

Cele odnoszące się do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy muszą być spełnione łącznie, przy czym nie zawsze muszą być realizowane w tym samym momencie. Jak się wydaje, użycie przez ustawodawcę spójnika „oraz" stanowi wyraz konieczności ustanowienia przez pracodawcę zasad wykorzystania poczty elektronicznej w czasie pracy i poza nim. W przypadku istnienia określonego wzorca zachowania pracownika, zgodność z którym podlega kontroli, monitoring może dotyczyć tego, czy pracownik wykorzystuje czas pracy dla celów innych niż wykonywanie obowiązków pracowniczych, oraz tego, czy korzysta z narzędzi służbowych w sposób niezgodny z ustanowionymi przez pracodawcę zasadami poza tym czasem.

Co przy tym istotne, niezbędność dla osiągnięcia celów wymienionych w art. $22^3$ § 1 k.p. nie ma charakteru absolutnego i nie może być utożsamiana z warunkiem *sine qua non*. Jak się wydaje, każdorazowo musi być relatywizowana zasadą proporcjonalności, która w najszerszym zakresie odnosi się wprawdzie do działalności państwa, w tym zwłaszcza tej prawotwórczej (art. 31 ust. 2 Konstytucji RP, art. 52 ust. 1 zd. 2 Karty Praw Podstawowych Unii Europejskiej[39] i art. 8 ust. 2 Konwencji o ochronie praw człowieka i podstawowych wolności sporządzonej w Rzymie dnia 4 listopada 1950 roku[40]), ale odgrywa także doniosłą rolę w sferze stosowania prawa. Jak podkreślił Sąd Najwyższy w wyroku z dnia 17 września 2014 roku, I CSK 439/13[41], zasada proporcjonalności oznacza obowiązek ograniczania w najmniejszym możliwym stopniu sfery prawnej drugiej strony stosunku prawnego przy wykonywaniu przysługującego komuś prawa albo uprawnienia. Przenosząc to grunt oceny dopuszczalności monitoringu, pracodawca powinien tak dobrać formy monitoringu, aby z jednej strony mogły one doprowadzić do zakładanego celu (kontrola przestrzegania przez pracodawcę ustanowionych przezeń zasad odnoszących się do organizacji pracy i do wykorzystywania narzędzi pracy), a z drugiej strony były one najmniej dotkliwe dla pracownika[42]. W tym kontekście należy przyznać rację Dominice Dörre-Kolasie, która opowiada się za rozróżnieniem pomiędzy monitorowaniem samego przepływu komunikatów w ra-

[39] Dz.Urz.UE. C 303 z 14.12.2007 r. z późn. zm., s. 1.

[40] Dz.U. z 1993 r. Nr 61, poz. 284 z późn. zm., dalej jako EKPCz.

[41] Wyrok SN z dnia 17 września 2014 r., I CSK 439/13, OSNC 2015/7–8, poz. 93.

[42] Por. odnoszące się do szerokiego rozumienia zasady proporcjonalności jako ogólnej zasady prawa Unii Europejskiej wyroki Trybunału Sprawiedliwości UE: z dnia 12 lipca 2001 r., C-189/01, *H. Jippes, Afdeling Groningen van de Nederlandse Vereniging tot Bescherming van Dieren i Afdeling Assen en omstreken van de Nederlandse Vereniging tot Bescherming van Dieren przeciwko Minister van Landbouw, Natuurbeheer en Visserij*, ECLI:EU:C:2001:420, pkt 81; z dnia 7 lipca 2009 r., C-558/07, *The Queen, na wniosek S.P.C.M. SA, C.H. Erbslöh KG*, *Lake Chemicals and Minerals Ltd i Hercules Inc. przeciwko Secretary of State for the Environment, Food and Rural Affairs*, ECLI:EU:C:2009:430, pkt 41, z dnia 9 marca 2010 r., C-379/08 i C-380/08, *Raffinerie Mediterranee (ERG) SpA, Polimeri Europa SpA i Syndial SpA przeciwko Ministero dello Sviluppo economico i innym* i *ENI SpA przeciwko Ministero Ambiente e Tutela del Territorio e del Mare i innym*, ECLI:EU:C:2010:127, pkt 86 i przytoczone tam orzecznictwo.


© for this edition by CNS

mach poczty elektronicznej a kontrolowaniem ich treści, zaś zastosowanie tego ostatniego powinno być zastrzeżone do sytuacji, w których pracodawca posiada już podejrzenie dotyczące naruszania przez pracownika przepisów prawa[43].

W świetle powyższych uwag można stwierdzić, że w polskim modelu regulacji monitoringu poczty elektronicznej pracownika, by uznać taki monitoring za pozostający w zgodności z dyspozycją art. $22^3$ § 1 k.p., nie tylko pożądane[44], ale wręcz konieczne jest, aby pracodawca sprecyzował reguły, które powinny być stosowane przez pracowników podczas prowadzenia korespondencji służbowej, w tym zwłaszcza w czasie pracy, jak również zasady właściwego użytkowania służbowego sprzętu, który jest do tego przeznaczony. Istota omawianej formy monitoringu polega bowiem na sprawdzeniu, czy pracownik przestrzega ustalonych przez pracodawcę zasad odnoszących się do organizacji pracy oraz właściwego wykorzystania narzędzi służbowych. W tym kontekście w pełni zasadne wydaje się rezygnacja przez ustawodawcę z uszczegółowiania, co należy rozumieć przez pojęcie „właściwego wykorzystania narzędzi pracy"[45]. W omawianym ujęciu „właściwe wykorzystanie" oznacza bowiem wykorzystanie zgodnie z zasadami ustalonymi przez pracodawcę w ramach przysługujących mu uprawnień kontrolnych.

Ustanowienie zasad wykorzystywania służbowej poczty elektronicznej, w tym także dla celów niezwiązanych z wykonywaniem obowiązków pracowniczych, wyznacza też granice uzasadnionego oczekiwania prywatności przez pracownika. Wzorem orzecznictwa amerykańskiego[46], w orzecznictwie Europejskiego Trybunału Praw Człowieka zapadłym na gruncie art. 8 ust. 1 EKPCz, statuującego prawo do ochrony życia prywatnego i rodzinnego, przyjmuje się, że to właśnie to oczekiwanie wyznacza granice dopuszczalnej ingerencji pracodawcy w tajemnicę korespondencji i inne dobra osobiste pracownika[47]. W takim ujęciu wynikający z art. $22^3$ § 2 k.p. zakaz naruszania przez monitoring poczty elektronicznej tajemnicy korespondencji oraz innych dóbr osobistych pracownika nie ma charakteru absolutnego[48]. Nie odnosi się do jakichkolwiek naruszeń, ale do naruszeń bezprawnych.

Należy odnotować, że *lege non distinguente* monitoringiem będzie każda forma kontroli przestrzegania przez pracownika ustalonej organizacji pracy i zasad wykorzystywania narzędzi pracy. Nie sposób w tym zakresie zgodzić się ze sfor-

[43] D. Dörre-Kolasa, *Komentarz do art. $22^3$ k.p.*, Nb. 7.

[44] Tak *ibidem*, Nb. 2.

[45] Postulat taki zgłosiła Joanna Jarguz — J. Jarguz, *Komentarz do art. $22^3$ k.p.*, Nb. 1.

[46] Wyrok amerykańskiego Sądu Najwyższego [Supreme Court] z dnia 18 grudnia 1967 r. *Kaatz przeciwko Stanom Zjednoczonym*, 389 U.S. 347 (1967). Zob. szerzej: A. Czubik, *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Kraków 2013, s. 155–157.

[47] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 5 września 2017 r., skarga nr 61496/08, *Bărbulescu przeciwko Rumunii*, pkt 73.

[48] Podobnie, choć z inną argumentacją M. Nałęcz, *Komentarz do art. $22^3$*, [w:] *Kodeks pracy. Komentarz*, red. W. Muszalski, K. Walczak, Warszawa 2021, Nb. 3. Odmiennie, jak się wydaje, M. Kuba, *Komentarz do art. $22^2$*, Nb. 3.2. Por. też J. Jarguz, *Komentarz do art. $22^3$ k.p.*, Nb. 3; D. Dörre-Kolasa, *Komentarz do art. $22^3$ k.p.*, Nb. 6.


© for this edition by CNS

mułowanym przez Joannę Jarguz poglądem, że nie stanowią monitoringu poczty elektronicznej jednorazowe lub powtarzające się, ale nie w stałej konfiguracji, czynności kontrolne pracodawcy polegające czy to na weryfikacji poszczególnych maili, czy też na pobieżnym przeglądzie jej zawartości[49]. Autorka wniosek taki wywodzi z argumentu natury językowej, a mianowicie znaczenia słowa „monitoring", które oznacza w języku polskim „stałą obserwację i kontrolę jakichś procesów lub zjawisk", albo „stały nadzór nad jakimś obiektem chronionym"[50]. Należy jednak zauważyć, że sformułowanie „monitoring poczty elektronicznej" zostało umieszczone w nawiasie, co oznacza, że stanowi definiendum tak zwanej definicji nawiasowej, o której mowa w § 150 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 roku w sprawie „Zasad techniki prawodawczej"[51]. Zgodnie z tym przepisem, jeżeli dane określenie ma być używane w ustalonym znaczeniu tylko w obrębie zespołu przepisów, jego definicję zamieszcza się w bezpośrednim sąsiedztwie tych przepisów. W tym kontekście nieuzasadnione jest formułowanie wniosków o istocie monitoringu na podstawie definiendum tego zwrotu (wszak jest to wyrażenie definiowane przez inne wyrażenie). Uwagę należy raczej skupić raczej na definiensie, w którym wskazano, że monitoring stanowi kontrolę służbowej skrzynki elektronicznej, bez wskazania, czy chodzi o kontrolę incydentalną, czy stałą. Jakiekolwiek rozróżnienie w tym kontekście naruszałoby zatem dyrektywę wykładni *quod lege non distinguente nec nostrum est distinguere*.

## PODSUMOWANIE

Powyższe rozważania prowadzą do kilku zasadniczych wniosków. Po pierwsze, zarówno na gruncie prawa polskiego, jak i obcych porządków prawnych, to przesłanki stosowania monitoringu wyznaczają model tej formy kontroli pracowników. Określają jednocześnie kierunki stosowania i interpretacji norm prawnych odnoszących się do tego zagadnienia. Można też z nich dekodować istotne wskazówki dotyczące zarówno dopuszczalnych form omawianej kontroli, jak i samej istoty przedmiotowego monitoringu. Po drugie, w porządkach prawnych państw członkowskich Unii Europejskiej można zrekonstruować trzy modele prawnej regulacji monitoringu poczty elektronicznej. W modelu pierwszym dopuszczalność prowadzenia takiego monitoringu limituje się zasadą proporcjonalności ingerencji w prywatność pracownika. Tego typu podejście pozostawia spory margines niepewności co do dopuszczalnego zakresu monitorowania poczty elektronicz-

[49] J. Jarguz, *Komentarz do art. 22³ k.p.*, Nb. 2.

[50] *Monitoring*, [hasło w:] Słownik języka polskiego PWN, https://sjp.pwn.pl/sjp/monitoring;2568296.html (dostęp: 3.10.2022). Podobne podejście prezentuje P. Fajgielski, *Monitoring systemów teleinformatycznych a ochrona danych osobowych*, „Monitor Prawniczy" 2022, nr 21, dodatek *Wpływ technologii i technik informatycznych na ochronę danych osobowych*, s. 4.

[51] Dz.U. z 2016 r. poz. 283.


© for this edition by CNS

nej pracownika. Model drugi wiąże dopuszczalność stosowania kontroli poczty elektronicznej z przestrzeganiem ustanowionych — czy to przez pracodawcę, czy przepisy powszechnie obowiązującego prawa — zasad jej wykorzystania. W modelu tym dopuszczalność monitorowania poczty elektronicznej uzależniona jest od istnienia sformalizowanych na poziomie ustawowym lub zakładowym zasad wykorzystania udostępnionych mu narzędzi pracy. Kontrola poczty w takim układzie służy uzyskiwaniu informacji o tym, czy pracownik przestrzega ustanowionych zasad wykorzystania udostępnionych mu narzędzi pracy. Z kolei w modelu trzecim ustawodawca normuje (niezwykle szczegółowo i kazuistycznie) zarówno dopuszczalne formy kontroli, jak i ich przesłanki zastosowania każdej z nich. W tym kontekście polski model regulacji monitoringu poczty elektronicznej wpisuje się w ten wzorzec, który dopuszczalność stosowania tej formy kontroli uzależnia od istnienia zasad jej wykorzystania. Wskazują na to ustawowe przesłanki stosowania omawianej formy monitoringu wysłowione w art. $22^3$ § 1 k.p. W konsekwencji dla uznania takiego monitoringu za pozostający w zgodności z dyspozycją art. $22^3$ § 1 k.p. konieczne jest, aby pracodawca sprecyzował reguły, które powinny być stosowane przez pracowników podczas prowadzenia korespondencji służbowej, w tym zwłaszcza w czasie pracy. Istota omawianej formy monitoringu polega bowiem na sprawdzeniu, czy pracownik przestrzega ustalonych przez pracodawcę zasad odnoszących się do organizacji pracy oraz właściwego wykorzystania narzędzi służbowych. Ustanowienie zasad wykorzystywania służbowej poczty elektronicznej, w tym także dla celów niezwiązanych z wykonywaniem obowiązków pracowniczych, wyznacza też granice uzasadnionego oczekiwania prywatności przez pracownika i tym samym — granice dopuszczalnej ingerencji pracodawcy w tajemnicę korespondencji i inne dobra osobiste pracownika.

## THE POLISH REGULATORY MODEL FOR THE MONITORING OF BUSINESS E-MAIL IN A COMPARATIVE PERSPECTIVE

Summary

The article attempts to reconstruct the Polish regulatory model for the monitoring of business e-mail. In the author's opinion, this model is primarily determined by the premises for the application of this form of employee control. They incorporate nodal ideas for the control of electronic communication tools made available to employees; and can also be used to decode important indications about the acceptable forms of such monitoring and the very essence of it. While analyzing the Polish regulatory model of business e-mail monitoring, the author uses arguments of a comparative nature, bearing in mind that the regulations concerning their subject matter have been introduced into the Polish legal system in order to adapt it to the requirements of provisions on the protection of personal data which are of uniform for the entire European Union.

Keywords: monitoring, employee control, privacy of correspondence, electronic mail


© for this edition by CNS

## BIBLIOGRAFIA


Auer-Reinsdorff A., Conrad I., *Handbuch IT- und Datenschutzrecht*, München 2016.

Boć J., *Prawo Administracyjne*, Wrocław 2010.

Brink S., Wirtz S., *Kontrolle des Arbeitgebers bei (unerlaubter) Internetnutzung der Beschäftigten,* „Arbeitsrecht Aktuell" 2016, z. 11–12.

Burke P., *Historia i teoria społeczna*, Warszawa-Kraków 2000.

Czubik A., *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Kraków 2013.

Dörre-Kolasa D., *Komentarz do art. 22³ k.p.*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2020.

Fajgielski P., *Monitoring systemów teleinformatycznych a ochrona danych osobowych*, „Monitor Prawniczy" 2022, nr 21, dodatek *Wpływ technologii i technik informatycznych na ochronę danych osobowych*.

Gorbunow M., *Monitoring w świetle nowelizacji Kodeksu pracy z 10.5.2018 r.*, „Monitor Prawa Pracy" 2019, nr 10.

Halma H., Gros U., Wójcik M., Żurek K., *Podstawy teoretyczne organizacji i zarządzania*, Katowice 1983.

Jarguz J., *Komentarz do art. 22³*, [w:] *Kodeks pracy. Regulacje COVID-19 w prawie pracy. Komentarz*, red. A. Sobczyk, Warszawa 2020.

Korczak J., *Nadzór i kontrola nad działalnością samorządu terytorialnego*, [w:] *System prawa administracyjnego*, t. 2. *Konstytucyjne podstawy funkcjonowania administracji publicznej*, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2012.

Kuba M., *Komentarz do art. 22²*, [w:] *Kodeks pracy. Komentarz*, t. 1. *Art. 1–93*, red. K.W. Baran, Warszawa 2022.

Kuba M., *Monitoring poczty elektronicznej pracownika — refleksje na tle nowych regulacji prawnych*, „Praca i Zabezpieczenie Społeczne" 2019, nr 11.

Maniewska E., Jaśkowski K., *Kodeks pracy. Komentarz*, Warszawa 2019

Miñarro Yanini M., *La «Carta de los derechos digitales» de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación*, „Revista de Trabajo y Seguridad Social" 2019, nr 430.

Martín Molina P., *Cuestiones relevantes de la nueva Ley Orgánica de Protección de Datos Personales y Garantía de los derechos Digitales: Los derechos digitales*, „Actualidad Civil" 2018, nr 12.

Nałęcz M., *Komentarz do art. 22³*, [w:] *Kodeks pracy. Komentarz*, red. W. Muszalski, K. Walczak, Warszawa 2021.

*Nowy leksykon PWN*, red. B. Petrozolin-Skowrońska, Warszawa 1998.

Płeszka K., *Uzasadnianie decyzji interpretacyjnych przez ich konsekwencje*, Kraków 1996.

Savatier J., *Commentaire de l'arrêt de la Cour de cassation, chambre sociale, du. 19 décembre 2007, n° 06-43.918, Bull. 2007 V n° 216*, „Droit social" 2002, nr 3.

*Słownik języka polskiego*, t. 1, red. M. Szymczak, Warszawa 1983.

*Słownik języka polskiego*, t. 2, red. M. Szymczak, Warszawa 1984.

Stahl M., *Akty nadzoru jako prawna forma działania administracji*, [w:] *System prawa administracyjnego*, t. 5. *Prawne formy działania administracji*, red. R. Hauser, Z. Niewiadomski, A. Wróbel Warszawa 2013.

Stępień A., *Prawo pracownika do prywatności w miejscu pracy — glosa*, „Informacja w Administracji Publicznej" 2015, nr 4.

Zieleniewski J., *Organizacja zespołów ludzkich*, Warszawa 1972.

Zieliński M.J., *Obowiązek zachowania prywatności pracownika*, [w:] *System prawa pracy*, t. 3. *Indywidualne prawo pracy. Część szczegółowa*, red. K.W. Baran, M. Gersdorf, K. Rączka, Warszawa 2021.



© for this edition by CNS

# FORMY MONITORINGU W ZAKŁADZIE PRACY

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.4

TOMASZ BAKALARZ
ORCID: 0000-0002-7499-1260
Uniwersytet Wrocławski

# MONITORING POCZTY ELEKTRONICZNEJ A TAJEMNICA KORESPONDENCJI PRACOWNIKA

Abstrakt: W 2018 roku dodano do ustawy Kodeks pracy przepisy szczególne dotyczące monitoringu, w tym monitoringu służbowej poczty elektronicznej. Przyjęte rozwiązania spotkały się z krytyką doktryny w zakresie ich adekwatności co do założonych celów. Przedmiotem niniejszego tekstu jest wykładnia przepisu art. $22^3$ § 2 k.p. w kontekście systemowym, podjęta dla wykazania, że kategoryczne zastrzeżenie, iż legalny monitoring nie może naruszać tajemnicy korespondencji pracownika, istotnie utrudnia realizację celów monitoringu założonych przez ustawodawcę.

Słowa kluczowe: tajemnica korespondencji, ochrona dóbr osobistych, monitoring poczty elektronicznej

## WPROWADZENIE

Umożliwienie pracodawcy dostępu do komunikacji elektronicznej prowadzonej przez pracownika, jak każdy przejaw kontroli, stanowi ingerencję w sferę wolności i prywatności jednostki. Niezależnie, czy komunikacja odbywa się w ramach stosunków służbowych czy prywatnych, poddanie jej kontroli oddziałuje na sferę osobistą, wymusza określone zachowania, autocenzurę czy utrzymanie formy komunikacji właściwej dla poziomu kultury organizacyjnej. Tym samym kontrola wyznacza granicę wolności, a często również — choćby pośrednio — wywiera wpływ na sam proces komunikacji.

Z perspektywy prawnej każdy dysponuje wolnością i ochroną tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej wyznaczony (art. 49 Konstytucji RP). Powyższa gwarancja zakłada nie tylko obowiązek powstrzymywania się organów państwa od ingerencji w tę wolność ponad to, co jest konieczne w świetle Konstytucji — szczególnie przy uwzględnieniu kryteriów przyjętych w art. 31 ust. 3 Konstytucji RP —


© for this edition by CNS

ale również obowiązek ochrony wolności komunikowania się przed zagrożeniami wynikającymi dla niej z działania podmiotów prywatnych[1].

Oczekiwania wobec systemu prawnego, gwarantującego poszanowanie wolności komunikowania się i tajemnicy korespondencji, są spełniane między innymi przez wyraźne uznanie, że tajemnica korespondencji (*per se*, jak i jako pochodna prywatności) stanowi dobro osobiste (art. 23 k.c.) i podlega ochronie prawnej (art. 24, 448 k.c.). Tym samym podkreślono jej znacznie jako społecznie aprobowanej wartości niemajątkowej, stanowiącej wyraz poszanowania dla indywidualności i godności osoby. Takie ujęcie tajemnicy korespondencji rodzi ryzyko traktowania jej jako swoistego społecznego fetyszu, której kontrola lub jakakolwiek w nią ingerencja budzi sprzeciw bądź etyczne wątpliwości.

Wątpliwości tych nie unikniemy w przypadku korespondencji prowadzonej przez pracownika w trakcie świadczenia pracy. Zagadnienie kontroli (monitoringu) środków komunikacji pracowniczej jest powszechnie podejmowane tak w literaturze fachowej, jak i w opracowaniach poradnikowych. Jest więc zagadnieniem „pracowniczego życia codziennego", które doczekało się szczególnej regulacji ustawowej.

Ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych[2], przepisem art. 111, dodano do kodeksu pracy przepis art. $22^3$ w brzmieniu:

> § 1. Jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej). § 2. Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. § 3. Przepisy art. $22^2$ § 6–10 stosuje się odpowiednio. § 4. Przepisy § 1–3 stosuje się odpowiednio do innych form monitoringu niż określone w § 1, jeśli ich zastosowanie jest konieczne do realizacji celów, określonych w § 1.

Monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Kontrola służbowej poczty elektronicznej pracownika, prowadzona przez pracodawcę w celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, nie może ingerować w treści wiadomości ani wpływać na wszystkie okoliczności procesu porozumiewania się pracownika. Pojawia się wątpliwość, czy tak interpretowany przepis nie wyklucza jednak skutecznej kontroli.

[1] M. Florczak-Wątor, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Lex/el. 2021, art. 49.

[2] Dz.U. z 2018 r. poz. 1000.


© for this edition by CNS

## ZAKRES PRZEDMIOTOWY TAJEMNICY KORESPONDENCJI JAKO DOBRA OSOBISTEGO

Tajemnica korespondencji służy zapewnieniu poufności porozumiewania się z adresatem indywidualnie wybranym przez formułującego komunikat i obejmuje treści przeznaczone wyłącznie dla adresata. Zabezpiecza przed każdą ingerencją w proces komunikowania się, w treść przekazu, jak również chroni informacje dotyczące podmiotów biorących udział w komunikacji[3].

Ochrona wolności komunikowania się (a w jej ramach tajemnicy korespondencji) obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI. W ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się ponadto ochrona przed niejawnym monitorowaniem jednostki oraz prowadzonych przez nią rozmów, nawet w miejscach publicznych i ogólnodostępnych. Nie ma znaczenia, czy wymiana informacji dotyczy życia ściśle prywatnego, czy też prowadzonej działalności zawodowej, w tym działalności gospodarczej. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której konstytucyjna ochrona byłaby wyłączona bądź samoistnie ograniczona. W każdej z tych sfer jednostka ma więc konstytucyjnie gwarantowaną wolność przekazywania i pozyskiwania informacji, w tym udostępniania informacji o sobie samej[4].

Naruszenie tajemnicy korespondencji może przybierać postać bezprawnego zapoznania się z korespondencją zaadresowaną do innej osoby, przejęcie i przywłaszczenie sobie cudzej korespondencji, zniszczenie cudzej korespondencji, uniemożliwienie dotarcia do niej adresatowi i zapoznania się z nią, rozpowszechnienie cudzej korespondencji, a nawet brak staranności po stronie nadawcy w zapewnieniu poufności przekazywanych informacji dotyczących sfery prywatności[5].

W kontekście poczty elektronicznej tajemnicą korespondencji należy objąć informacje o nadawcy i odbiorcy maila, o osobach trzecich, którym przekazano mail „do wiadomości", treść wiadomości, a także załączone do maila pliki. Ponadto, uznając, że tajemnica chroni sam proces komunikacji, poufny powinien pozostać czas nadania/odbioru poczty, a także dane identyfikujące urządzenie służące

[3] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, s. 254–255.

[4] Wyrok TK z 30.07.2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80.

[5] M. Pazdan, *Dobra osobiste i ich ochrona*, [w:] *System prawa prywatnego*, t. 1. *Prawo cywilne — część ogólna*, red. M. Safjan, Warszawa 2012, s. 1254.


© for this edition by CNS

do komunikacji. Zasadne jest również objęcie tajemnicą korespondencji poczty zaadresowanej, ale niewysłanej (w skrzynce roboczej)[6].

## ZAKRES PODMIOTOWY TAJEMNICY KORESPONDENCJI W KONTEKŚCIE ART. $22^3$ § 2 K.P.

Wątpliwości interpretacyjne związane z art. $22^3$ § 2 k.p. dotyczą między innymi odpowiedzi na pytanie, czyje wartości niematerialne są chronione przez tajemnicę korespondencji. Niezależnie, czy mówimy o korespondencji służbowej, czy prywatnej, zasadniczo jest ona kreowana i nadawana przez pracownika (osobę zatrudnioną). Pomińmy przykłady korespondencji generowanej automatycznie bądź nadawanej osobiście przez pracodawcę prowadzącego jednoosobową działalność gospodarczą czy piastuna organu pracodawcy jako jednostki organizacyjnej, niebędącego zarazem pracownikiem tejże. Nasuwa się pytanie, czy za każdym razem to rzeczywisty nadawca korespondencji i decydent co do jej treści jest beneficjentem prawa do tajemnicy korespondencji.

W świetle art. 43 k.c. nie ma wątpliwości, że dobra osobiste przynależą także osobom prawnym (szerzej: jednostkom organizacyjnym). Wyrażają one wówczas powszechnie przyjęte wartości związane z osobą prawną, umożliwiające jej funkcjonowanie w obrocie w sposób odpowiadający zakresowi jej zadań czy działalności. Dobra osobiste osoby prawnej mają mieć funkcjonalne znacznie dla działalności podejmowanej przez jednostkę organizacyjną. W orzecznictwie wyraźnie przyjmuje się, że jednym z dóbr osobistych osoby prawnej jest tajemnica korespondencji[7].

Nie jest wykluczone, że dana komunikacja elektroniczna podlega ochronie jako przedmiot dóbr osobistych osoby prawnej (pracodawcy) oraz osoby fizycznej (pracownika), szczególnie w przypadku zagrożenia ze strony osób trzecich, w tym organów władzy publicznej. Problematyczna w perspektywie art. $22^3$ § 2 k.p. w aktualnym brzmieniu może być jednak konieczność ważenia wartości w przypadku kolizji tajemnicy korespondencji, której nadawcą jest pracownik, a służy ona realizacji działalności pracodawcy.

Konieczne wydaje się wykluczenie pracownika jako beneficjenta prawa do tajemnicy korespondencji w tym zakresie, w którym komunikowanie się stanowi realizację obowiązków pracowniczych bądź, innymi słowy, działalności z upoważnienia pracodawcy. Korespondencja może być uznana za pochodzącą od podmiotu niebędącego osobą fizyczną, gdy spełnione są przesłanki skutecznej reprezentacji

[6] Za: M. Markiewicz, *Komentarz do art. 82 ustawy o prawie autorskim i prawach pokrewnych*, [w:] *Ustawy autorskie. Komentarze*, t. 2, red. R. Markiewicz, Lex/el. 2021.

[7] Wyroki SN: z 18.09.2019 r., IV CSK 297/18 oraz Lex nr 2734448 oraz z 05.04.2013 r., III CSK 198/12, OSNC 2013 nr 12, poz. 141 wraz z cytowanym tam orzecznictwem.


© for this edition by CNS

tego podmiotu (korespondencja pochodzi od piastunów organów lub osób przez nich upoważnionych do prowadzenia korespondencji)[8]. Komunikacja służbowa skierowana do podmiotu zewnętrznego (kontrahenta, klienta, organu władzy publicznej) będzie służyła działalności mocodawcy (pracodawcy). Jeśli będzie stanowiła efekt czynności pracowniczych, to musi być potraktowana w myśl art. 22 § 1 k.p. jako realizowana na rzecz pracodawcy. Uznanie pracownika za dysponenta tajemnicy korespondencji przez siebie wytworzonej w ramach obowiązków pracowniczych blokuje możliwość realizacji przez pracodawcę uprawnień kontrolnych bądź dyrektywnych, a w szczególności weryfikację czy praca świadczona przez pracownika jest wykonywana sumiennie i starannie oraz zgodnie z poleceniem przełożonych.

Magdalena Kuba trafnie przyjmuje więc, że nie sposób traktować pracodawcy jako osobę trzecią w procesie komunikacji, o ile tylko sam nie bierze w niej osobistego udziału. Autorka zaznacza, że pracownik, prowadząc korespondencję z klientem czy kontrahentem pracodawcy, czyni to jako przedstawiciel podmiotu, który go zatrudnia, nie zaś jako osoba prywatna[9].

W świetle powyższego interpretacja przepisu art. $22^3$ § 2 k.p. w zakresie terminu „tajemnica korespondencji […] pracownika" powinna uwzględniać zakres podmiotowy prawa, wykluczając tę korespondencję, którą pracownik prowadzi w ramach wykonywania obowiązków służbowych. Chodzi tu zwłaszcza o korespondencję prowadzoną z podmiotami zewnętrznymi w ramach świadczonej przez pracodawcę działalności, ale także komunikację wewnętrzną dotyczącą poleceń lub innych form kierowania pracownikami. Wyodrębnienie korespondencji prowadzonej przy wykonywaniu obowiązków pracowniczych ułatwia podział na korespondencję służbową i prywatną.

Wydaje się zasadne, aby od korespondencji służbowej odróżnić jednak także tę komunikację, którą pracownik prowadzi ze współpracownikami, załogą zakładu pracy czy przedstawicielami organizacji związkowych. Może ona nie dotyczyć wykonywania pracy umówionego rodzaju na rzecz pracodawcy, jednocześnie sprzyjając interesowi zakładu pracy (sygnalizowanie naruszeń przepisów prawa pracy związkom zawodowym) bądź służąc budowaniu koleżeńskiej atmosfery (co korespondowałoby z obowiązkiem pracodawcy wyrażonym w art. 94 pkt 10 k.p.). Tak rozumianą korespondencję można nazwać „zakładową", w stosunku do której nie sposób odmówić pracownikowi prawa do zachowania jej w tajemnicy.

Błędne jest zaś zapatrywanie przenoszące uprawnienia cywilnoprawne pracodawcy do urządzeń technicznych (własność komputera, telefonu) oraz usług telekomunikacyjnych na zakres podmiotowy tajemnicy korespondencji. Choć to pracodawca jest podmiotem zamawiającym usługi w zakresie szeroko rozumianej komunikacji, a pracownik jest jedynie użytkownikiem zakupionych przez

[8] M. Pazdan, *Dobra osobiste i ich ochrona*, s. 1253.

[9] M. Kuba, *Prawne formy kontroli pracownika w miejscu pracy,* Warszawa 2014, s. 342–343.


© for this edition by CNS

pracodawcę usług, to jednak z uwagi na ochronę dóbr osobistych pracownika nie można wywieść z powyższego faktu prawa dostępu do informacji przetwarzanych w toku organizowanej przez pracodawcę komunikacji służbowej[10]. Udostępnienie pracownikowi oprogramowania oraz indywidualnego adresu poczty elektronicznej musi odbywać się z poszanowaniem przez pracodawcę dóbr osobistych pracownika (art. $11^1$ k.p. oraz art. $22^3$ § 2 k.p.).

## KORESPONDENCJA SŁUŻBOWA VS. KORESPONDENCJA PRYWATNA

Kodeks pracy dopuszcza stosowanie przez pracodawcę monitoringu służbowej poczty elektronicznej. Chodzi więc o oddanie do używania pracownikowi konta poczty elektronicznej, stworzonego zgodnie z umową o świadczenie usług udostępniania kont pocztowych, której stroną jest pracodawca, a w ramach której dochodzi do nadania adresu elektronicznego, przypisanie mu określonej przestrzeni dyskowej na serwerach oraz umożliwienie korzystania w celach: odbierania, wysyłania, zapisywania, przechowywania i usuwania wiadomości poczty elektronicznej.

Jest wysoce prawdopodobne, że pracownik posiada również prywatną pocztę elektroniczną dostępną przy wykorzystaniu urządzeń technicznych i oprogramowania własnego bądź pracodawcy. Co oczywiste, prywatne konto pocztowe użytkowane przez pracownika na komputerze/telefonie służbowym nie może być uznane za służbową pocztę elektroniczną.

Kontrola pracownika w zakresie wykorzystywania infrastruktury technicznej pracodawcy do korzystania z prywatnej poczty elektronicznej może spełniać przesłanki „innych form monitoringu", zgodnie z art. $22^3$ § 4 k.p. Chodzi tu w szczególności o monitoring sposobu wykorzystania przez pracownika dostępu do Internetu.

Mimo powszechnej dostępności usługowej i technicznej poczty elektronicznej nadal dostrzega się ryzyko wykorzystania służbowej poczty elektronicznej do prywatnych celów pracownika. Jednoznaczne rozdzielenie korespondencji prywatnej od służbowej, wysyłanej lub odbieranej za pośrednictwem konta służbowego, możne jednak nastręczać trudności, szczególnie wówczas, gdy kwalifikacji dokonuje się *ex ante* — przed zapoznaniem się z treścią korespondencji.

W literaturze przedstawia się sposoby oznaczenia korespondencji, której nadawca — pracownik — miałby nadać status prywatny. Proponuje się między innymi specjalne oznaczenia dla wiadomości prywatnych, na przykład FYI (*for your information*)[11] bądź wyraźne wpisywanie w temacie maili prywatnych słowa

[10] Odmienne zdanie ma M. Kuba — *ibidem*, s. 343.

[11] M. Kuba, *Monitoring poczty elektronicznej pracownika — refleksje na tle nowych regulacji prawnych*, „Praca i Zabezpieczenie Społeczne" 2019, nr 11, s. 34.


© for this edition by CNS

„prywatne" czy litery „P", z ewentualnym dodaniem określonej barwy[12]. Sugeruje się nawet, by pracodawca zakładał pracownikom dwa konta pocztowe — do komunikacji służbowej i prywatnej[13]. Wszystkie te rozwiązania wydają się jednak mało praktyczne[14] i niewystarczające dla uzyskania pewności pracodawcy o legalności procesu monitoringu poczty służbowej.

W doktrynie pojawiają się również głosy, że wystarczającym zabezpieczeniem przed ewentualnym zapoznaniem się z korespondencją prywatną na służbowym koncie pocztowym jest wprowadzenie zakazu używania do celów prywatnych służbowej skrzynki poczty elektronicznej[15].

## BEZPRAWNE NARUSZENIE TAJEMNICY KORESPONDENCJI PRACOWNIKA

Kontrola korespondencji prywatnej pracownika związana z wglądem w jej treść, weryfikacją adresata lub odbiorcy oraz czasu prowadzenia korespondencji stanowi zagrożenie dóbr osobistych osoby korzystającej z wolności komunikacji (bez względu na kwalifikację tej osoby jako pracownika — ochrona dóbr osobistych ma charakter powszechny). Kontroli tej, zgodnie z art. 24 § 1 k.c., należy przypisać domniemanie bezprawności.

Wśród okoliczności wyłączających bezprawność zagrożenia lub naruszenia dóbr osobistych podaje się między innymi działanie w ramach porządku prawnego (na podstawie przepisu), zgodę uprawnionego bądź wykonywanie własnego prawa podmiotowego.

Należy zauważyć, że treść przepisu art. $22^3$ § 2 k.p. wyklucza powołanie się na działanie w ramach porządku prawnego w celu uchylenia bezprawności monitoringu poczty objętej tajemnicą korespondencji pracownika. Tym samym kontrola naruszająca tajemnicę prywatnej korespondencji pracownika jest *a priori* sprzeczna z porządkiem prawnym. Tej oceny nie może zmienić uprzedzenie pracownika o podejmowanym monitoringu, nie mogą tego zrobić też przyjęte przez pracodawcę akty wewnętrzne organizujące sposób korzystania z poczty służbowej.

---

[12] K. Łapiński, *Wybrane aspekty dotyczące stosowania monitoringu w miejscu pracy,* „Radca Prawny. Zeszyty Naukowe" 2020, nr 1, s. 54.

[13] *Working Document on the Surveillance of Electronic Communications in the Workplace 5401/01/EN/Final/ WP 55. Adopted on 29 May 2002*, European Commision, 29.05.2002, s. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (dostęp: 11.10.2022).

[14] Tak trafnie M.J. Zieliński, *Prawna problematyka monitoringu w relacjach pracowniczych*, [w:] *System prawa pracy*, t. 3. *Indywidualne prawo pracy. Część szczegółowa,* red. K.W. Baran, M. Gersdorf, K. Rączka, Warszawa 2021, s. 227.

[15] *Ibidem*. Tak również M. Kuba, *Monitoring poczty elektronicznej pracownika…*, s. 34.


© for this edition by CNS

W tej perspektywie niewykonanie przez pracownika umownego obowiązku powstrzymania się od korzystania ze służbowego konta poczty elektronicznej do celów prywatnych bądź obowiązku oznaczania korespondencji prywatnej może rodzić jedynie odpowiedzialność pracowniczą, to jest stanowić podstawę do odpowiedzialności porządkowej (jako nieprzestrzeganie dyscypliny pracy) bądź w skrajnych przypadkach podstawę rozwiązania stosunku pracy. Jednak zastosowanie sankcji wobec pracownika za nieprzestrzegania powyższych obowiązków wymagałoby ingerencji w tajemnicę korespondencji (między innymi w zakresie informacji o nadawcy/odbiorcy poczty). Wówczas pracodawca byłby w stanie ustalić, że pracownik wysyła i odbiera maile prywatne niezgodnie z obowiązkiem powstrzymania się od takich praktyk, bądź że pracownik błędnie oznacza maile jako prywatne[16]. Tym samym kontrola wykonania obowiązku pracowniczego mającego gwarantować poszanowanie dóbr osobistych pracownika prowadziłaby do bezprawnego ich naruszania.

W kontekście regulaminowego bądź umownego zastrzeżenie zakazu korzystania z urządzeń służbowych do celów prywatnych warto wspomnieć o tak zwanym „rozsądnym oczekiwaniu prywatności" — kryterium wykorzystywanym przez Europejski Trybunał Praw Człowieka w ocenie standardu ochrony prywatności (art. 8 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności)[17]. W świetle wyroku *Barbulescu v. Rumunia*[18] otwarte pozostaje pytanie, czy — a jeśli tak, to w jakim zakresie — restrykcyjne przepisy pracodawcy o zakazie komunikacji prywatnej przy użyciu urządzeń służbowych pozostawiły pracownikowi możliwość uzasadnionego oczekiwania prywatności. Odpowiedź na nie wymagała jednak szczegółowych ustaleń faktycznych niezbędnych dla właściwego ważenia interesów pracodawcy i pracownika według zaproponowanego przez Trybunał testu proporcjonalności (pkt 121 wyroku). Dostrzec jednak należy, że „rozsądne oczekiwanie poszanowania prywatności" należy w pierwszej kolejności odnieść do uregulowań prawnych obowiązujących w danym państwie-stronie Konwencji. Trybunał strasburski zauważył, że w momencie wydawania wyroku w sprawie *Barbulescu* większość państw członkowskich Rady Europy (w tym Rumunia) nie uregulowało kwestii korzystania przez pracowników z prawa do poszanowania ich życia prywatnego i korespondencji w miejscu pracy w sposób wyraźny. Przyjął zarazem, że państwom należy przyznać szeroki margines oceny potrzeby ustanowienia ram prawnych regulujących warunki, na jakich pracodawca może regulować elektroniczne formy komunikacji pracowników o charakterze niesłużbowym w miejscu pracy, przy jednoczesnym zapewnieniu odpowiednich i wystarczających zabezpieczeń przed nadużyciami.

[16] Choćby czyniąc to w złe wierze, w celu przesłania informacji objętych tajemnicą pracodawcy.

[17] Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie 4 listopada 1950 r., Dz.U. z 1993 r. Nr 61, poz. 284.

[18] Wyrok ETPCz z 05.09.2017 r., *Bărbulescu vs. Rumunia*, skarga nr 61496/08.


© for this edition by CNS

Wprowadzenie art. $22^3$ k.p. stwarza nową sytuację normatywną, w której należy oceniać spełnienie konwencyjnego standardu ochrony prywatności. Kwestia uprzedzenia pracownika, do której nawiązuje Trybunał strasburski w proponowanym teście proporcjonalności, nie może być tu decydująca. Wynika to z wykładni art. $22^3$ § 2 k.p. w związku z art. $22^3$ § 3 i art. $22^2$ § 7 k.p. Wyrażony w art. $22^2$ § 7 k.p. obowiązek uprzedzenia pracownika o monitoringu jako kryterium jego legalności nie zastępuje ani nie łagodzi obowiązku poszanowania tajemnicy korespondencji. Innymi słowy: monitoring, o którym pracownik został uprzedzony przez pracodawcę, nie może naruszać tajemnicy korespondencji pracownika.

Kontrola prywatnej korespondencji pracownika nie może być też usprawiedliwiona przez wykonywanie prawa podmiotowego pracodawcy, gdyż działalność ta wykracza poza treść uprawnienia wywodzonego z art. $22^3$ § 1 k.p.

Ewentualną okolicznością uchylającą bezprawność mogłaby być zgoda pracownika. Nasuwa się pytanie, czy w celu minimalizowania ryzyka bezprawnej kontroli korespondencji prywatnej pracownika pracodawca może uzyskać zgodę pracownika na naruszenie tajemnicy jego korespondencji znajdującej się na służbowej skrzynce pocztowej.

Pracownik może swobodnie dysponować swymi dobrami osobistymi: prawem do prywatności i tajemnicą korespondencji. Akcentując osobisty (ściśle związany z osobą uprawnionego) charakter tych dóbr, można przyjąć, że wyrażenie zgody to wyraz autonomii uprawnionego, stanowiącej jeden z przejawów chronionej konstytucyjnie przyrodzonej i niezbywalnej godności człowieka (art. 30 Konstytucji RP)[19]. Zgoda staje się aktem woli stanowiącym wyraz świadomości uprawnionego co do przysługującego mu prawa oraz zamiaru zamanifestowania na zewnątrz skorzystania z tego prawa[20].

Zgoda uprawnionego będzie okolicznością wyłączającą bezprawność wówczas, gdy będzie zgodna z prawem (przy czym przepis art. $22^3$ § 2 k.p. nie może być uznany za przepis zabraniający wyrażenia zgody) oraz zasadami współżycia społecznego. O ile uprawniony dysponuje niezbędną swobodą, udzielona przez niego zgoda może być wyrazem jego woli. Na ocenę zakresu swobody pracownika w wyrażeniu zgody na naruszenie jego dóbr osobistych niewątpliwie wywiera wpływ podporządkowanie właściwe stosunkowi pracy, a wraz z nim uprawnienia sankcyjne przysługujące pracodawcy. Nie należy jednak pomijać faktu, że swobodne nawiązanie stosunku pracy prowadzi do samoistnego ograniczenie sfer objętych dobrami osobistymi, a w szczególności wolności w aspekcie podporządkowania co do miejsca i czasu pracy czy realizacji poleceń pracodawcy zgodnych z umową i ustawą. Ograniczenie wolności komunikowania się czy tajemnicy korespondencji odbywa się w celu zabezpieczenia prawidłowego wywiązania się

[19] B. Janiszewska, [w:] *Kodeks cywilny. Komentarz*, t. 1. *Część ogólna*, cz. 1. *Art. 1–55(4)*, red. J. Gudowski, Warszawa 2021, s. 510.

[20] Por. wyroki SN: z 12.12.2006 r., II CSK 280/06, Lex nr 232817 oraz z 24.06.2015 r., II PK 207/14, Lex nr 1794313.


© for this edition by CNS

z dobrowolnie przyjętych obowiązków pracowniczych. Stanowi proporcjonalny i adekwatny środek ochrony interesu pracodawcy, a zarazem pozostawia pracownikowi, jako użytkownikowi poczty, możliwość współdecydowania o przedmiocie kontroli.

Przy przyjęciu założenia, że zgoda pracownika nie będzie miała charakteru blankietowego, będzie ograniczona do konkretnych czynności pracodawcy podjętych w znanym pracownikowi celu oraz zostanie wyrażona przed podjęciem kontroli skrzynki mailowej, jej udzielenie należałoby uznać za dopuszczalne. Fakt uprzedzenia o monitoringu z równoczesnym jednoznacznym wypowiedzeniem się pracownika co do przeprowadzenia kontroli poczty służbowej daje podstawy do przyjęcia, że pracownik powinien rozsądnie decydować o czynnościach wykonywanych za pośrednictwem tej poczty bez „oczekiwania poszanowania prywatności". Co istotne, zgoda dotyczyłaby jedynie tajemnicy korespondencji rozumianej w sposób wcześniej przyjęty, nie zaś innych dóbr osobistych pracownika, choćby pozostających w związku z tajemnicą. Bezprawne byłoby naruszenie prywatności pracownika, choćby przez wykorzystanie informacji prywatnych pracownika uzyskanych w wyniku monitoringu poczty służbowej, przy podejmowaniu decyzji kadrowych.

## USTAWOWE CELE MONITORINGU POCZTY SŁUŻBOWEJ

Zgodnie z art. $22^3$ § 1 k.p. monitoring służbowej poczty elektronicznej jest uzasadniony, gdy jest niezbędny do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy.

Wskazany jako pierwszy cel dyscyplinujący, pozwalający na kontrolę pełnego wykorzystania czasu pracy, może być zrealizowany jedynie przy naruszeniu tajemnicy korespondencji pracownika, jeśli kontrola ta miałaby się sprowadzać do sprawdzenia, czy pracownik nie korzysta z poczty służbowej dla celów pozazawodowych. Zakreślony cel wydaje się absurdalny, gdy sprowadzić go do monitoringu częstotliwości korzystania z poczty w zakresie korespondencji służbowej. Innymi słowy: nie można efektywnie zrealizować założonego celu bez naruszenia tajemnicy korespondencji pracownika.

Warto również dostrzec, że zapewnienie właściwej płynności pracy i pełnego wykorzystania czasu pracy wymaga nie tyle monitoringu służbowej poczty elektronicznej, co monitoringu wykorzystania Internetu za pośrednictwem urządzenia służbowego. Przykładowo: większym zagrożeniem dla efektywności pracy pracownika jest korzystanie z komunikatora internetowego czy prywatnego konta e-mail niż marginalne (z racji powszechnej dostępności środków komunikacji elektronicznej)


© for this edition by CNS

korzystanie ze skrzynki służbowej[21]. Założony przez ustawodawcę cel monitoringu z art. $22^3$ § 1 k.p. wymagać będzie więc głównie innych form monitoringu (art. $22^3$ § 3 k.p.), aniżeli kontroli służbowej poczty elektronicznej pracownika.

Drugi cel monitoringu można osiągnąć bez pozyskiwania treści wiadomości przez skanowanie systemów w ramach poszukiwania zagrożeń sieciowych lub też sprawdzanie wywiązywania się z zasad dotyczących bezpiecznego korzystania z komputera[22]. Przyjęte metody techniczne nie muszą ingerować w zakres tajemnicy korespondencji, a co najwyżej uniemożliwiać wykorzystanie danego urządzenia do komunikacji prywatnej, na przykład przez blokadę adresów e-mail lub domen internetowych. Maciej Chakowski i Przemysław Ciszek wskazują, że dochodzi wówczas tylko do „badania stanu technicznego" korespondencji[23]. Inaczej należałoby jednak traktować te procesy techniczne, które polegałyby na filtrowaniu korespondencji za pomocą słów kluczowych, na przykład podyktowanych względami ochrony tajemnicy przedsiębiorstwa. Wówczas niechybnie badanie korespondencji wymuszałoby wgląd w jej treść, choćby w sposób zautomatyzowany[24].

W literaturze trafnie dostrzeżono, że wśród uzasadnień podjęcia monitoringu brakuje kwestii ochrony tajemnicy pracodawcy lub innych tajemnic prawnie chronionych. Przychylić się należy do postulatów o rewizję przepisu art. $22^3$ k.p. i uzupełnienie dopuszczalności kontroli właśnie o wskazaną sferę, co wydaje się szczególnie adekwatne w kontekście innych ustawowych celów monitoringu (na przykład monitoringu wizyjnego, gdzie w art. $22^2$ § 1 k.p. ustawodawca uzasadnia kontrolę zapewnieniem bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji, a także zachowaniem w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę)[25].

Usprawiedliwienia dla kontroli prywatnej korespondencji pracownika podejrzanego o naruszenie obowiązków pracowniczych z art. 100 § 2 pkt 4 i 5 k.p. można poszukiwać w instytucji nadużycia prawa podmiotowego. Jak wskazywał Stefan Grzybowski,

> zagrożenie lub naruszenie dobra osobistego przez działanie podjęte w obronie zasługującego na ochronę interesu nie będzie działaniem bezprawnym, jeżeli sprzeciwienie się takiemu działaniu i żądanie ochrony prawnej byłoby sprzeczne z zasadami współżycia społecznego, a zatem nie stanowiłoby wykonywania prawa osobistego (art. 5 k.c.)[26].

---

[21] O nieadekwatności środków kontroli do ustawowych celów: M. Kuba, *Monitoring poczty elektronicznej pracownika…*, s. 31.

[22] M. Wujczyk, *Prawo pracownika do ochrony prywatności*, Warszawa 2012, s. 314.

[23] M. Chakowski, P. Ciszek, *Tajemnica korespondencji pracownika a ochrona tajemnicy handlowej pracodawcy*, „Monitor Prawa Pracy" 2007, nr 1, s. 26.

[24] M. Markiewicz, *Cywilnoprawna ochrona korespondencji*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2012, nr 115, s. 98.

[25] M. Kuba, *Monitoring poczty elektronicznej pracownika…*, s. 31.

[26] Cyt. za: M. Pazdan, *Dobra osobiste i ich ochrona*, s. 1280.


© for this edition by CNS

Zasadami tymi będą między innymi zasada lojalnej współpracy czy uczciwości, której przeciwieństwem będzie dochodzenie roszczeń służących jedynie zatajeniu działań niezgodnych z prawem.

## WNIOSKI KOŃCOWE

Zasada poszanowania dóbr osobistych, w tym tajemnicy korespondencji pracownika jest zasadą podstawową prawa pracy w myśl art. $11^1$ k.p., obowiązującą niezależnie od przepisu art. $22^3$ § 2 k.p. Rzeczywistość normatywna wykreowana przez art. $22^3$ § 2 k.p. nie rozwiązuje licznych problemów na styku kontroli pracodawcy i tajemnicy korespondencji pracownika, a wręcz rzeczywistość tę komplikuje. Przepis ten można uznać za *superfluum* ustawowe i choć nadmiar regulacji prawnej jest zjawiskiem powszechnym, uzasadnionym względami informacyjno-porządkowymi, to jednak w przypadku przepisu art. $22^3$ § 2 k.p. w obecnym brzmieniu można pokusić się o stwierdzenie, że mamy do czynienia z niezgodnością prakseologiczną.

Zakładając, że skuteczna kontrola pełnego wykorzystania czasu pracy przez monitoring służbowej poczty elektronicznej wymaga ingerencji w zakres tajemnicy korespondencji pracownika (informacji o częstotliwości wykorzystywania skrzynki służbowej w celach niezawodowych), kategoryczne limitowanie legalnie podjętego monitoringu ochroną tajemnicy korespondencji uniemożliwia bądź istotnie utrudnia realizację ustawowego celu. Norma zakazująca naruszeń tajemnicy korespondencji pracownika niweczy osiągnięcie celu normy zezwalającej na podjęcie monitoringu.

Dopuszczalność naruszenia tajemnicy korespondencji pracownika w przypadku monitoringu służbowej poczty elektronicznej stanowi usprawiedliwione ograniczenie wolności komunikowania, niezbędne i proporcjonalne do ochrony praw i wolności osób trzecich (art. 31 ust. 3 Konstytucji RP), takich jak swoboda działalności gospodarczej, prawo własności czy poszanowanie wolności komunikowania się pracodawcy. Jest uzasadnione w ujęciu systemowym i celowościowym, nie będąc zarazem nadmiernym ograniczeniem wolności osobistych. Na tych podstawach zasadna wydaje się rewizja art. $22^3$ § 2 k.p.

## MONITORING OF BUSINESS E-MAIL AND THE CONFIDENTIALITY OF EMPLOYEE CORRESPONDENCE

Summary

In 2018, the Labor Code was supplemented with regulations on employee monitoring, including monitoring of business e-mail. The adopted solutions were criticized with regards their of adequacy in relation to the assumed legal goals. The subject of this text is a systematic interpretation of Art. $22^3$


© for this edition by CNS

§ 2 of the Labor Code, which prohibits violating the confidentiality of the employee's correspondence and other personal rights. The author proves that the prohibition of violating the confidentiality of correspondence during the control of a business e-mail account makes it difficult or even impossible to achieve the monitoring goals set by the legislator.

Keywords: confidentiality of correspondence, protection of personal rights, monitoring of e-mail

## BIBLIOGRAFIA

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.

Chakowski M., Ciszek P., *Tajemnica korespondencji pracownika a ochrona tajemnicy handlowej pracodawcy*, „Monitor Prawa Pracy" 2007, nr 1.

Florczak-Wątor M., [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. P. Tuleja, Lex/el. 2021.

Janiszewska B., [w:] *Kodeks cywilny. Komentarz*, t. 1. *Część ogólna*, cz. 1. *Art. 1–55(4)*, red. J. Gudowski, Warszawa 2021.

Kuba M., *Monitoring poczty elektronicznej pracownika — refleksje na tle nowych regulacji prawnych,* „Praca i Zabezpieczenie Społeczne" 2019, nr 11.

Kuba M., *Prawne formy kontroli pracownika w miejscu pracy*, Warszawa 2014.

Łapiński K., *Wybrane aspekty dotyczące stosowania monitoringu w miejscu pracy*, „Radca Prawny. Zeszyty Naukowe" 2020, nr 1.

Markiewicz M., *Cywilnoprawna ochrona korespondencji*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2012, nr 115.

Markiewicz M., [w:] *Ustawy autorskie. Komentarze*, t. 2, red. R. Markiewicz, Lex/el. 2021.

Pazdan M., *Dobra osobiste i ich ochrona*, [w:] *System prawa prywatnego*, t. 1 *Prawo cywilne — część ogólna*, red. M. Safjan, Warszawa 2012.

Wujczyk M., *Prawo pracownika do ochrony prywatności*, Warszawa 2012.

Zieliński M.J., *Prawna problematyka monitoringu w relacjach pracowniczych*, [w:] *System prawa pracy*, t. 3. *Indywidualne prawo pracy. Część szczegółowa*, red. K.W. Baran, M. Gersdorf, K. Rączka, Warszawa 2021.


© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.5

DOMINIKA DÖRRE-KOLASA
ORCID: 0000-0002-4134-741X
Uniwersytet Jagielloński

# PRZETWARZANIE DANYCH OSOBOWYCH PRACOWNIKÓW W RAMACH TAK ZWANYCH INNYCH FORM MONITORINGU

Abstrakt: Powszechna dostępność nowych technologii pozwala pracodawcom na stosowanie dotychczas niewystępujących w środowisku pracy rodzajów monitorowania aktywności pracowników. Co więcej — upowszechnienie się pracy zdalnej, w połączeniu z pojawieniem się nowej regulacji w kodeksie pracy, w naturalny sposób zwiększa zainteresowanie pracodawców procesami przetwarzania danych na temat aktywności pracowników *online*, jak również danych o lokalizacji. Technologie wykorzystywane w ramach innych form monitoringu mogą być bardzo skuteczne w wykrywaniu naruszeń obowiązków pracowniczych, ochronie informacji poufnych czy też służyć zwiększaniu efektywności pracy, lecz jednocześnie stwarzają poważne zagrożenia dla ochrony prywatności i danych osobowych. Aplikacje służące do cyfrowej analizy danych mogą bowiem działać w sposób niezauważalny dla użytkowników urządzeń, przez co zagrażają ich prywatności bardziej niż na przykład kamery CCTV. W związku z tym uzasadniona jest ponowna rewizja oceny skutków dla ochrony danych oraz baczna analiza podejmowanych działań z uwzględnieniem zasad wynikających zarówno z kodeksu pracy, jak i RODO. Skorzystanie przez pracodawców z danych pozyskanych w sposób niezgodny z przepisami może się spotkać z poważnymi konsekwencjami prawnymi.

Słowa kluczowe: monitoring, praca zdalna, GPS, kontrola pracowników, inne formy monitoringu

## UWAGI WPROWADZAJĄCE

Ustawą[1] z dnia 10 maja 2019 roku wprowadzono do kodeksu pracy przepisy dotyczące różnych rodzajów monitoringu, to jest monitoringu wizyjnego (art. $22^2$ k.p.), monitoringu poczty elektronicznej (art. $22^3$ § 1 k.p.) oraz innych form monitoringu (art. $22^3$ § 4 k.p.). Skorzystano w ten sposób z przewidzianej w RODO możliwości uszczegółowienia w przepisach krajowych zasad ochrony praw i wolności jednostek w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem.

[1] Ustawa o ochronie danych osobowych z dnia 10 maja 2019 r., Dz.U. z 2018 r. poz. 1000.


© for this edition by CNS

Zgodnie z art. 88 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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)[2] — dalej: RODO — 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.

Zawarta w kodeksie pracy regulacja dotycząca monitoringu jest zatem tą „bardziej szczegółową regulacją" w stosunku do przepisów RODO, która precyzuje ten aspekt przetwarzania danych osobowych w kontekście zatrudnienia. Nie można jednak zapominać, że do przetwarzania danych osobowych w ramach każdej z form monitoringu powinny być stosowane nie tylko przepisy kodeksu pracy, ale także przepisy RODO. Podejmując decyzję o wprowadzeniu monitoringu, jak również dokonując okresowej oceny jego funkcjonowania, należy mieć na uwadze zwłaszcza zasady przetwarzania danych osobowych określone w art. 5 RODO, a więc: zasadę rzetelności i legalności (zgodności z prawem), zasadę ograniczenia celu, zasadę minimalizacji danych, zasadę prawidłowości (poprawności danych), zasadę ograniczenia przechowywania, zasadę integralności i poufności (bezpieczeństwa danych) oraz zasadę rozliczalności.

Zgodnie z zasadami przetwarzania danych osobowych, które powinny być przez pracodawców stosowane niezależnie od stosowanej technologii[3], dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu"). Dane te powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

[2] Dz.Ur.UE. L 119 z 4.05.2016 r. ze zm., s. 1.

[3] *Opinia 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy, WP 249*, Archiwum GIODO, 21.02.2018, https://archiwum.giodo.gov.pl/pl/file/13179 (dostęp: 24.10.2022).


© for this edition by CNS

W k.p. ustawodawca dokonał dychotomicznego podziału dopuszczalnych form monitoringu, przyporządkowując do nich określone cele, które mogą uzasadniać wprowadzenie „szczególnego nadzoru" czy też „kontroli". Elementem, który pojawia się w obydwu przypadkach, jest uzależnienie decyzji pracodawcy o wprowadzeniu monitoringu od tego, czy ocenił podjęte działania jako niezbędne do osiągnięcia tych celów. Zarówno art. $22^2$, jak i art. $22^3$ k.p. rozpoczynają się od sformułowań „jeżeli jest to niezbędne do zapewnienia". Oznacza to, że decyzji o wprowadzeniu, czy też kontynuowaniu stosowanego wcześniej monitoringu powinna bezwzględnie towarzyszyć ocena, czy monitoring jest niezbędny do osiągnięcia wskazanych w przepisach celów. Wydaje się, że ową niezbędność można rozumieć szerzej niż tylko niemożność osiągnięcia tych celów bez zastosowania monitoringu. W mojej ocenie mieści się w tym zakresie również racjonalność działania, która jest uzasadniona pod względem organizacyjnym i kosztowym.

Stosując monitoring, pracodawca przetwarza dane osobowe pracowników na podstawie art. 6 ust. 1 lit. f RODO, to jest do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, z wszystkimi tego konsekwencjami.

Zamieszczenie regulacji dotyczącej monitoringu w przepisach k.p. z jednoczesnym wskazaniem na wyraźnie ustalone cele, które ustawodawca uznaje za wynikające z prawnie uzasadnionych interesów, nie zwalnia pracodawcy z obowiązku przeprowadzenia tak zwanego testu równowagi. Test ten składa się z trzech części[4]. W ramach części pierwszej należy ustalić, czy istnieje cel, dla którego podstawą prawną przetwarzania danych może być prawnie uzasadniony interes. Częścią drugą testu powinna być ocena niezbędności przetwarzania danych dla realizacji tego celu. W części trzeciej należy ocenić, czy nie jest spełniona przesłanka o charakterze negatywnym w postaci występowania w danym stanie faktycznym interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej. W przypadku spełnienia tego warunku nie będzie można powołać się na przepis art. 6 ust. 1 lit. f RODO jako uzasadnienia dla przetwarzania danych osobowych. Należy wskazać, że zgodnie z zasadą rozliczalności fakt przeprowadzenia testu równowagi powinien być udokumentowany celem wykazania, że pracodawca przed wprowadzeniem określonej formy monitoringu dokonał weryfikacji, czy nie sprzeciwia się temu ochrona praw i wolności osób, które mają być w ten sposób kontrolowane. Co więcej: należy rozważyć, jakie środki powinny być wdrożone aby zapewnić ograniczenie ewentualnego ryzyka naruszenia praw i wolności podmiotów danych. Warto o tym przypominać, gdyż praktyka pokazuje, że wielu pracodawców trwa w mylnym przeświadczeniu, że skoro ustawodawca włączył

[4] Więcej na ten temat M. Więckowska, *Przetwarzanie danych na podstawie prawnie uzasadnionego interesu*, „ABI Expert" 2018, nr 3, s. 10–14.


© for this edition by CNS

przepisy o monitoringu do kodeksu pracy, to nie ma potrzeby dokonywać analizy zgodności tego procesu z przepisami RODO, a co za tym idzie, w ogóle nie przeprowadzają oceny skutków dla ochrony danych.

## INNE FORMY MONITORINGU W PRZEPISACH K.P.

Na podstawie § 4 art. $22^3$ k.p. przepisy dotyczące monitoringu służbowej poczty elektronicznej mają odpowiednie zastosowanie do innych form monitoringu, jeśli ich wdrożenie jest niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. W pozostałych przypadkach, w których prowadzony monitoring służy innym celom wynikającym z prawnie uzasadnionych interesów pracodawcy nietożsamych z celami wskazanymi w art. $22^3$ k.p., przepis ten nie znajduje zastosowania. Tylko wówczas, gdy inne formy monitoringu są prowadzone w celach, o których mowa w § 1 art. $22^3$ k.p., pracodawca jest zobowiązany zamieścić w układzie zbiorowym pracy, regulaminie lub obwieszczeniu informację o celu, zakresie oraz sposobie zastosowania monitoringu, jak również zastosować się do obowiązków informacyjnych poprzedzających wprowadzenie tej formy kontroli pracowników (przepisy art. $22^2$ § 6–10 k.p. stosuje się odpowiednio). Podobnie jak w odniesieniu do monitoringu służbowej poczty elektronicznej inne formy monitoringu nie mogą naruszać dóbr osobistych pracowników (art. $22^3$ §2 w związku z art. $22^3$ § 4 k.p.).

## OBOWIĄZKI INFORMACYJNE PRACODAWCY WZGLĘDEM PRACOWNIKÓW

Do obowiązków pracodawcy należy poinformowanie pracowników o wprowadzeniu monitoringu w sposób przyjęty u danego pracodawcy nie później niż dwa tygodnie przed jego uruchomieniem oraz przekazanie każdemu nowemu pracownikowi przed dopuszczeniem go do pracy informacji o celu, zakresie oraz sposobie zastosowania monitoringu. W mojej ocenie treść tej informacji powinna być zindywidualizowana, a nie stanowić jedynie powtórzenia zapisów zawartych w regulaminie pracy lub układzie zbiorowym. Powinna odnosić się w szczególności do tych form monitoringu, którym ten konkretny pracownik jest (lub będzie) poddawany. Uważam również, że informacja ta powinna być w miarę potrzeby aktualizowana. Pozostaje to w interesie obydwu stron. W sytuacji gdy pracodawca będzie chciał uczynić użytek z danych osobowych pozyskanych dzięki określonej formie monitoringu, o której pracownik nie został należycie poinformowany, może spotkać się z zarzutem naruszenia zarówno przepisów RODO, jak


© for this edition by CNS

i przepisów cywilnych o ochronie dóbr osobistych, w tym przypadku prawa do prywatności. Istnieje też cały szereg orzeczeń Europejskiego Trybunału Praw Człowieka, w których silnie akcentowane jest, że każda forma ingerencji w prywatność wymaga właściwego poinformowania o prowadzonych działaniach. Jedynie tytułem przykładu można wskazać, na kanwie wyroku ETPCz *Bărbulescu przeciwko Rumunii*[5] z 5 września 2017 roku, że pracownikowi należy wskazać różnicę między monitorowaniem przepływu informacji (to jest weryfikacją czy lub jak często korzysta ze skrzynki służbowej do celów prywatnych) a monitorowaniem treści korespondencji. Monitorowanie treści informacji jest oczywiście bardziej inwazyjne, dlatego też wymaga poważniejszego, bardziej pogłębionego uzasadnienia. Pracownikowi każdorazowo należy zapewnić odpowiednie gwarancje, zwłaszcza gdy czynności monitorowania będą miały charakter inwazyjny. Gwarancje te w szczególności powinny zapewniać, że pracodawca nie ma dostępu do treści komunikacji, chyba, że pracownik został z wyprzedzeniem poinformowany o takiej ewentualności.

## OKRES RETENCJI DANYCH

Na zakończenie uwag ogólnych godzi się zaakcentować, że do innych form monitoringu, takich jak monitoring poczty elektronicznej, nie znajduje zastosowania trzymiesięczne ograniczenie przechowywania danych, które ustawodawca przewidział wyłącznie odnośnie nagrań z tak zwanego monitoringu wizyjnego, polegającego na nadzorze nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (art. $22^2$ § 3 k.p.). Brak takiego ustawowego ograniczenia stanowi groźną pokusę dla pracodawców, aby zgromadzone w ramach innych form monitoringu dane osobowe przechowywać „na wszelki wypadek", gdyby na przykład wystąpiła potrzeba uzasadnienia rozwiązania umowy o pracę. Należy w tym miejscu raz jeszcze podkreślić, że zgodnie z zasadą ograniczenia przechowywania dane osobowe mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Jeżeli tym celem jest zapewnienie organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, wydaje się być oczywistym, że okres przechowywania danych nie może być nieograniczony. Wyrażam pogląd, że pracodawca może go ustanowić w dowolny sposób, na przykład odnosząc się do obowiązujących u niego okresów rozliczeniowych czy też okresów oceny pracowniczej. W sytuacji, gdy dane pozyskane z monitoringu staną się podstawą określonych czynności prawnych wobec pracownika oczywistym jest, że okres przechowywania tych da-

[5] Wyrok ETPCz z 05.09.2017 r., *Bărbulescu vs. Rumunia*, skarga nr 61496/08.


© for this edition by CNS

nych będzie podlegał automatycznemu wydłużeniu, przynajmniej do okresu przedawnienia roszczeń pracowniczych.

## STOSOWANE W PRAKTYCE INNE FORMY MONITORINGU

Jak trafnie zauważono w opinii Grupy Roboczej art. 29 z dnia 8 czerwca 2017 roku, „przyjęcie nowych technologii informacyjnych w miejscu pracy pod względem infrastruktury, aplikacji i urządzeń inteligentnych pozwala na stosowanie nowych rodzajów systematycznego i potencjalnie inwazyjnego przetwarzania danych w miejscu pracy”[6]. Coraz bardziej zaawansowane technologicznie formy przetwarzania danych, w szczególności takie jak te odnoszące się do danych osobowych na temat korzystania z usług online lub danych dotyczących lokalizacji, są znacznie mniej widoczne dla pracowników niż inne tradycyjne formy przetwarzania, takie jak jawne monitorowanie kamerami CCTV. W takich przypadkach szczególnego znaczenia nabiera właściwe spełnienie obowiązku informacyjnego przez pracodawcę gdyż pracownicy mogą nie być świadomi tego, że są w ten sposób monitorowani, ani tym bardziej faktu, jaki zakres ich danych osobowych jest pozyskiwany dzięki tym metodom kontroli. Na długo przed pandemią koronawirusa Grupa Robocza dostrzegła, ze coraz bardziej zacierają się granice między domem a pracą. Gdy pracownicy pracują zdalnie (na przykład z domu) możliwe jest monitorowanie ich czynności poza fizycznym środowiskiem pracy[7]. Ten aspekt monitoringu będzie bez wątpienia stanowił dla pracodawców największe wyzwanie wobec ukończenia prac legislacyjnych oraz wprowadzenia pracy zdalnej do kodeksu pracy i zastąpienia nią istniejącej obecnie telepracy.

## INNE FORMY MONITORINGU A PRACA ZDALNA

Z uwagi na upowszechnienie się w ostatnim czasie pracy zdalnej, nadzwyczaj aktualne stały się uwagi Grupy Roboczej dotyczące korzystania przez pracowników z ICT (*information and communication technologies*) poza miejscem pracy. Chodzi o technologie informacyjno-telekomunikacyjne gromadzące, przetwarzające i przesyłające informacje w formie elektronicznej. Możliwości oferowane przez te technologie mogą stwarzać realne ryzyko dla życia prywatnego pracowników, ponieważ w wielu przypadkach systemy monitorowania istniejące w miejscu pracy zostają w praktyce rozszerzone na sferę domową pracowników w przypadku, gdy korzystają oni z tego rodzaju urządzeń w domu[8]. Pracodawca udostępnia

[6] *Opinia 2/2017 Grupy Roboczej art. 29…*, s. 3
[7] *Ibidem*, s. 4–5.
[8] *Ibidem*, s. 18.


© for this edition by CNS

pracownikowi sprzęt ICT lub oprogramowanie, które — po jego zainstalowaniu w domu lub na należących do pracownika urządzeniach — pozwala mu uzyskać taki sam poziom dostępu do sieci, systemów i zasobów pracodawcy, jakim dysponowałby wówczas, gdyby znajdował się w miejscu pracy, w zależności od stopnia wdrożenia odpowiednich rozwiązań. Praca zdalna może zatem stwarzać dla pracodawcy szczególnego rodzaju ryzyko spowodowane tym, że pracownicy dysponujący dostępem do jego infrastruktury nie podlegają jednocześnie analogicznym środkom bezpieczeństwa jak te, które są stosowane w pomieszczeniach należących do pracodawcy.

Zagrożenia te zdaje się dostrzegać polski prawodawca, wskazując w nowelizacji kodeksu pracy[9] na konieczność określenia przez pracodawcę procedur ochrony danych osobowych na potrzeby wykonywania pracy zdalnej oraz przeprowadzenia, w miarę potrzeby, instruktażu i szkolenia w tym zakresie. W porozumieniu lub regulaminie dotyczącym pracy zdalnej mają zostać określone zarówno zasady kontroli wykonywania pracy przez pracownika wykonującego pracę zdalną, jak również zasady kontroli przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji, w tym procedury ochrony danych osobowych. Zgodnie z treścią wprowadzonej regulacji pracodawca będzie zobligowany dostosować sposób przeprowadzania kontroli do miejsca wykonywania pracy zdalnej i jej rodzaju. Wykonywanie czynności kontrolnych nie będzie mogło naruszać prywatności pracownika wykonującego pracę zdalną i innych osób ani utrudniać korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem.

Pracodawcy mają obecnie do dyspozycji cały szereg rozwiązań technologicznych, w tym oprogramowania umożliwiające ciągłe rejestrowanie naciśnięć klawiszy lub ruchów myszy, przechwytywanie ekranu (w losowych albo regularnych odstępach czasu), rejestrowanie uruchamianych aplikacji oraz czasu korzystania z nich, a także włączanie kamer internetowych. Należy podkreślić, iż zadeklarowanie przez pracodawcę, że przetwarzanie danych osobowych za pomocą wybranego narzędzia jest mu niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy nie jest wystarczające dla stwierdzenia, iż odbywa się ono zgodnie z prawem. Pomijając wielokrotnie już wspominany obowiązek informacyjny, koniecznym będzie ograniczenie ryzyka związanego z pracą zdalną w sposób proporcjonalny. Jak wskazuje Grupa Robocza art. 29, prawdopodobieństwo, że uzasadniony interes pracodawcy będzie wystarczający

[9] Rządowy projekt ustawy o zmianie ustawy — Kodeks pracy oraz niektórych innych ustaw, druk sejmowy 2335. W dniu 16 stycznia 2023 r. ustawę uchwaloną w dniu 1 grudnia 2022 r., po odrzuceniu poprawek Senatu przekazano do podpisu Prezydenta — *Przebieg prac przed skierowaniem projektu do Sejmu*. *Rządowy projekt ustawy o zmianie ustawy — Kodeks pracy oraz niektórych innych ustaw*, Sejm Rzeczpospolitej Polskiej, 14.06.2022, https://www.sejm.gov.pl/sejm9.nsf/PrzebiegProc.xsp?nr=2335 (dostęp: 23.01.2023). Po jej opublikowaniu w Dzienniku Ustaw przepisy dotyczące pracy zdalnej wejdą w życie w terminie dwóch miesięcy.


© for this edition by CNS

do uzasadnienia stosowania metod takich jak permanentne rejestrowanie klawiszy naciskanych przez pracownika lub wykonywanych przez niego ruchów myszą jest bardzo niewielkie.

## APLIKACJE BIUROWE

Pracowników, bez względu na to czy znajdują się w miejscu pracy czy też poza nim, można monitorować z uwagi na fakt, że korzystają oni z aplikacji internetowych udostępnionych im przez pracodawcę, które przetwarzają dane osobowe. Za Grupą Roboczą art. 29 można wskazać, tytułem przykładu, na aplikacje biurowe takie jak edytory dokumentów, kalendarze, wewnętrzne portale społecznościowe bazujące na technologii przetwarzania w chmurze. Gdyby pracodawca zdecydował się na zezwolenie pracownikom na wykorzystywanie tych narzędzi do celów prywatnych, niezbędnym będzie zapewnienie im możliwości wyznaczenia określonych przestrzeni prywatnych, do których pracodawca będzie mógł uzyskać dostęp wyłącznie w wyjątkowych okolicznościach. Ma to szczególne znaczenie w przypadku kalendarzy, które oprócz organizacji czasu pracy są często wykorzystywane również do planowania prywatnych spotkań. Jeżeli praktyka taka będzie uznawana przez pracodawcę za dopuszczalną, wówczas powinna być zapewniona funkcjonalność pozwalająca na określanie zakresu podmiotowego osób, które będą miały dostęp do prywatnych wpisów pracownika z poziomu użytkownika.

## KOMUNIKACJA ELEKTRONICZNA

Monitorowanie treści szeroko rozumianej komunikacji elektronicznej pracowników (na przykład połączeń telefonicznych, przeglądanych zasobów internetowych, komunikatów natychmiastowych, połączeń za pośrednictwem telefonii internetowej itp.) uznawane jest za główne zagrożenie dla prywatności pracowników, a co za tym idzie — pracodawcy powinni podchodzić do niego ze szczególną ostrożnością, mając na uwadze rzeczywistą niezbędność prowadzonych działań do zmierzonych celów. W ocenie Grupy Roboczej w sytuacji, w której niedozwolone metody korzystania z usług łączności można zwalczać, blokując określone strony internetowe, powinno się tego dokonywać. Jeżeli w danym przypadku można zablokować strony internetowe zamiast wprowadzać ciągłe monitorowanie całej komunikacji, należy wybrać to rozwiązanie, aby zapewnić zgodność z wymogiem pomocniczości[10].

[10] *Opinia 2/2017 Grupy Roboczej art. 29…*, s. 17.


© for this edition by CNS

## MONITORING GPS

Zgodnie z kodeksem pracy (art. $22^3$ § 4) monitoring GPS pojazdów służbowych, jak każda inna forma monitoringu, może być prowadzony wówczas, gdy jest on niezbędny do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Narzędziem pracy będzie w tym przypadku samochód służbowy. We wszystkich sytuacjach, w których samochód służbowy nie stanowi narzędzia pracy pracownika, będąc tym samym jednym z benefitów (na przykład dla kadry menadżerskiej), a stosowany w tych samochodach monitoring GPS miałby na celu wyłącznie umożliwienie zlokalizowania pojazdów w dowolnym momencie (na przykład w przypadku zgłoszenia jego kradzieży), nie będziemy mieć do czynienia z monitoringiem, o którym mowa w art. § 4 art. $22^3$ k.p. Pracodawca korzystający z rozwiązań GPS instalowanych w pojazdach będzie mógł gromadzić nie tylko dane o pojeździe, lecz także o konkretnym pracowniku, który korzysta z pojazdu służbowego. Dane takie mogą obejmować nie tylko informacje o lokalizacji pojazdu (a tym samym o położeniu pracownika) zgromadzone przez podstawowe systemy śledzenia GPS, ale — w zależności od zastosowanej technologii — również wiele innych informacji, w tym informacje o stylu jazdy.

## KORZYSTANIE Z SAMOCHODU SŁUŻBOWEGO DO CELÓW PRYWATNYCH A MONITORING GPS

W przypadkach, gdy pracodawca dopuszcza możliwość korzystania z pojazdu służbowego do celów prywatnych, Grupa Robocza art. 29 rekomenduje, aby pracownikowi zostało umożliwione skorzystanie z opcji tymczasowego wyłączenia mechanizmu śledzenia położenia pojazdu, na przykład w przypadku gdy będzie to uzasadnione szczególnymi okolicznościami mogącymi wystąpić w godzinach pracy, jak chociażby wizyta lekarska. W ten sposób pracownik może z własnej inicjatywy chronić określone dane dotyczące lokalizacji, traktując je jako dane prywatne. Wydaje się jednak, że rekomendowane przez Grupę Roboczą art. 29 rozwiązanie będzie w praktyce technicznie niemożliwe lub znacznie utrudnione. Co więcej, mogłoby ono prowadzić do sytuacji, w której pracownik, po zakończeniu czynności należącej do sfery prywatnej (której podjęcie w godzinach pracy jest konieczne), zapomniałby ponownie włączyć urządzenia, przez co właściwy cel takiego monitoringu byłby niemożliwy do zrealizowania. Nie ulega jednak wątpliwości, że decydując się na tę formę monitoringu, pracodawcy powinni wziąć pod uwagę przede wszystkim to, czy pracownik pracuje w podstawowym czy zadaniowym systemie czasu pracy. Może to bowiem mieć istotne znaczenie dla


© for this edition by CNS

zorganizowania procesów monitoringu GPS służbowego samochodu pracownika z uwzględnieniem sytuacji wyjątkowych, o których była mowa powyżej.

W niektórych przypadkach pracownicy mogą również korzystać z samochodów służbowych poza godzinami pracy w celach prywatnych, w zależności od treści polityki regulującej sposób korzystania z tych pojazdów czy też indywidualnych uzgodnień pomiędzy pracownikiem a pracodawcą. W ocenie Grupy Roboczej art. 29 jest mało prawdopodobne, aby zaistniała podstawa prawna monitorowania lokalizacji pojazdów pracowników poza uzgodnionymi godzinami pracy. Jednak w przypadku wystąpienia takiej konieczności należy rozważyć możliwość wdrożenia środków, które byłyby proporcjonalne do istniejącego ryzyka. W celu zapobieżenia kradzieży samochodu może to oznaczać na przykład odstąpienie od rejestrowania położenia samochodu poza godzinami pracy, o ile nie opuści on szeroko wyznaczonego obszaru (danego regionu lub wręcz państwa). Ponadto informacje o położeniu byłyby w takim przypadku ujawniane wyłącznie na zasadzie „zbitej szyby" — pracodawca mógłby aktywować „widoczność" danej lokalizacji i uzyskać wgląd w dane, które zostały już zgromadzone przez system, po opuszczeniu określonego obszaru przez pojazd. Pracodawca musi również wyraźnie poinformować pracowników o fakcie zainstalowania urządzenia śledzącego w samochodzie służbowym oraz o tym, że urządzenie to rejestruje wszystkie ruchy wykonywane przez nich w trakcie korzystania z pojazdu (a także o tym, że — w zależności od zastosowanej technologii — ich styl jazdy również może być monitorowany). Informacje takie powinny być umieszczone w widocznym miejscu w każdym samochodzie, w zasięgu wzroku kierowcy[11].

## REJESTRATORY DANYCH NA TEMAT ZDARZEŃ

Rejestratory danych na temat zdarzeń zapewniają pracodawcy techniczną możliwość przetwarzania znacznych ilości danych osobowych pracowników, którzy prowadzą pojazdy firmowe. Urządzenia takie są coraz częściej instalowane w pojazdach w celu rejestrowania obrazu, a potencjalnie również dźwięku. Z reguły jednak takie systemy zapewniają możliwość zapisywania danych tylko w przypadku, gdy ocenią, że miało miejsce zdarzenie oceniane przez system za krytyczne (takie jak gwałtowny manewr kierowcy, nieoczekiwane hamowanie, a w każdym razie — wypadek), a w przeciwnym razie dane są nadpisywane. Można jednak wybrać również opcję stałego rejestrowania danych. Zgromadzone w ten sposób informacje mogą zostać później wykorzystane do obserwowania i analizowania stylu jazdy danej osoby w celu jego udoskonalenia. Ponadto wiele tych systemów wykorzystuje GPS do śledzenia lokalizacji pojazdu w czasie rzeczywistym; systemy te zapewniają również możliwość przechowywania innych szczegóło-

[11] *Ibidem*, s. 23.


© for this edition by CNS

wych informacji związanych z jazdą (takich jak informacje o prędkości pojazdu) w celu ich dalszego przetwarzania. Tego rodzaju urządzenia są powszechnie stosowane, w szczególności przez organizacje prowadzące działalność w sektorze transportu lub zarządzające dużymi flotami pojazdów. Co do zasady, stosowanie rejestratorów danych na temat zdarzeń można będzie uznać za zgodne z prawem wyłącznie w przypadku konieczności przetwarzania danych osobowych pracownika gromadzonych przez te rejestratory w prawnie uzasadnionym celu i w przypadku zgodności przetwarzania z zasadami proporcjonalności i pomocniczości.

Bez wątpienia dla dokonania takiej oceny będzie miało znaczenie, czy zastosowanie rejestratora zdarzeń będzie służyło działaniom prewencyjnym pracodawcy w celu zapewnienia większego bezpieczeństwa pasażerów (co ma szczególne znaczenie w przypadku podmiotów świadczących usługi transportowe) czy działaniom mającym na celu wykrycie pracowników, którzy przekraczają dozwoloną prędkość podczas prowadzenia pojazdów służbowych, przez co stwarzają większe ryzyko ponoszenia przez pracodawcę kosztów związanych z mandatami drogowymi, w celu ich zdyscyplinowania. Nie da się zaprzeczyć, że niezależnie od tego, jaki cel przyświeca pracodawcy, skutek w postaci podniesienia poziomu bezpieczeństwa i tak wystąpi. Niemniej jednak cel w postaci zapewnienia bezpieczeństwa — czy to pracowników, czy innych uczestników ruchu drogowego — powinien być nadrzędny nad celem ekonomicznym pracodawcy w postaci uniknięcia ponoszenia kosztów wynikających z użytkowania pojazdów niezgodnie z przepisami prawa o ruchu drogowym. Gdyby się zatem okazało, że pracodawca deklarując, iż celem monitoringu GPS jest kontrola właściwego użytkowania narzędzia pracy w postaci samochodu, przez co rozumiane jest stosowanie się do reguł ruchu drogowego, a w rzeczywistości dane z monitoringu służą wyłącznie monitorowaniu częstotliwości kończących się mandatami naruszeń, będziemy mieć do czynienia z przetwarzaniem niezgodnym z celem.

Prowadzenie monitoringu GPS z uwzględnieniem rejestratora zdarzeń w nadrzędnym celu, jakim jest bezpieczeństwo może być również niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Ważne jest jednak, aby komunikacja kierowana do pracowników była pełna, a przekaz zrozumiały.

## ZDALNE MONITOROWANIE STANU ZDROWIA PRACOWNIKÓW

Producenci technologii już od dłuższego czasu oferują rozwiązania pozwalające na monitorowanie stanu zdrowia. Obecnie coraz większym zainteresowaniem cieszą się one również wśród pracodawców upatrujących w nich sposobu na zwiększenie bezpieczeństwa pracowników. Monitoring wizyjny nie zawsze jest wystarczającym narzędziem, gdyż nie obejmuje on wszystkich miejsc na te-


© for this edition by CNS

renie zakładu, a przede wszystkim wymaga permanentnej obserwacji w czasie rzeczywistym. Nagrania z monitoringu są wykorzystywane przede wszystkim do analizy zdarzeń wypadkowych już po fakcie, w celu zbadania ich przyczyn i ograniczenia zagrożenia w przyszłości.

Proponowane pracodawcom urządzenia do noszenia na ciele pracowników (w postaci zegarka, breloczka czy opaski na nadgarstek) samodzielnie monitorują ich stan i aktywność, a w razie zagrożenia przesyłają sygnał na przykład do centrali ratownictwa medycznego pracodawcy. Urządzenia te, dzięki wbudowanemu lokalizatorowi, pozwalają też szybko dotrzeć do pracownika w celu udzielenia mu pomocy medycznej. Z korzystaniem z tej formy ochrony życia i zdrowia pracowników łączy się jednak poważne ryzyko pozyskania przez pracodawcę nadmiarowej liczby danych osobowych dotyczących zdrowia pracowników, a zatem danych szczególnej kategorii. Co więcej, literalne brzmienie art. $22^3$ k.p. wskazywałoby na niemożność stosowania innych form monitoringu w celach innych niż wymienione w tym przepisie, wśród których nie znajdziemy bezpieczeństwa pracowników. Jak już jednak zostało wskazane w uwagach wstępnych, uregulowanie monitoringu w kodeksie pracy nie jest równoznaczne z zakazem prowadzenia go w celach innych niż wymienione w k.p., o ile spełniona będzie którakolwiek z przesłanek legalizujących przetwarzanie danych osobowych. W przypadku danych dotyczących zdrowia, katalog przesłanek uchylających zakaz przetwarzania tych danych zawarty jest w art. 9 RODO. Zgodnie z art. 9 ust. 2 lit. b RODO zakaz przetwarzania danych szczególnej kategorii nie znajduje zastosowania wówczas, gdy przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą. Dyskusyjne jest, czy dozwolone przepisami powinno być przetwarzanie danych, czy też wystarczy, aby dozwolone przepisami było wypełnianie obowiązków i wykonywanie uprawnień, do realizacji których niezbędne jest przetwarzanie danych. Opowiadam się za drugą ze wskazanych powyżej wykładni, ponieważ przyjęcie pierwszej oznaczałoby zakwestionowanie przetwarzania danych w ramach całego szeregu regulacji przewidzianych w przepisach prawa pracy, które nie referują wprost do danych osobowych, a tym samym nie przewidują w swej treści odpowiednich zabezpieczeń praw podstawowych i interesów osoby, której dane dotyczą. Dla przykładu można wskazać na przetwarzanie przez pracodawcę danych dotyczących chorób zawodowych pracownika, przetwarzanie danych o zdrowiu członków rodziny pracownika na potrzeby przyznania świadczeń socjalnych, przetwarzanie danych osobowych o przynależności związkowej w celu dokonania potrącenia składki członkowskiej, czy też udzielenia zwolnienia od pra-


© for this edition by CNS

cy zawodowej na czas pełnienia funkcji w zarządzie organizacji związkowej czy też wykonania czynności doraźnej.

Ochrona życia i zdrowia pracowników stanowi jeden z podstawowych obowiązków pracodawcy. Zgodnie z art. 207 k.p. § 2 pracodawca jest zobowiązany chronić zdrowie i życie pracowników przez zapewnienie bezpiecznych i higienicznych warunków pracy przy odpowiednim wykorzystaniu osiągnięć nauki i techniki. W szczególności pracodawca jest obowiązany reagować na potrzeby w zakresie zapewnienia bezpieczeństwa i higieny pracy oraz dostosowywać środki podejmowane w celu doskonalenia istniejącego poziomu ochrony zdrowia i życia pracowników, biorąc pod uwagę zmieniające się warunki wykonywania pracy.

Zdarzają się takie sytuacje, w których — z uwagi na szczególne ryzyko związane z funkcjonowaniem zakładu pracy czy też odosobnieniem miejsca pracy — w razie wypadku nie zawsze na miejscu jest osoba, która będzie w stanie udzielić pomocy pracownikowi. W mojej ocenie stosowanie urządzeń monitorujących stan zdrowia pracowników czy też pozwalających na zlokalizowanie ich w okresie bezruchu uprawdopodobniających zasłabnięcie będzie wówczas uzasadnione, z tym jednak zastrzeżeniem, że dostęp pracodawcy do danych o stanie zdrowa powinien być ściśle ograniczony do tego celu. Jak wiadomo, w zależności od zaawansowania technologicznego, tego rodzaju urządzenia niejednokrotnie posiadają wiele funkcjonalności. Zliczają liczbę kroków wykonywanych przez pracowników, rejestrują tętno, monitorują ich nawyki senne. Gromadzone przez te urządzenia dodatkowe dane dotyczące zdrowia powinny być jednak dostępne wyłącznie dla pracowników. Co więcej, dane dotyczące zdrowia pracowników mogą być również przetwarzane przez podmiot, który wyprodukował dane urządzenie lub który oferuje określoną aplikację do zainstalowania na smartfonie, zatem przy dokonywaniu wyboru urządzenia lub usługi pracodawca powinien ocenić politykę ochrony prywatności danego producenta lub usługodawcy, aby upewnić się, że nie doprowadzi ona do niezgodnego z prawem przetwarzania danych dotyczących zdrowia pracowników.

## INNE FORMY MONITORINGU A PROFILOWANIE I ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI

Zgodnie z definicją zamieszczoną w art. 4 pkt 4 RODO „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.


© for this edition by CNS

Aby przetwarzanie danych osobowych mogło zostać uznane za profilowanie, niezbędnym jest łączne wystąpienie następujących trzech elementów:

— profilowanie musi stanowić zautomatyzowaną formę przetwarzania;

— profilowaniu muszą podlegać dane osobowe; oraz

— celem profilowania musi być ocena czynników osobowych osób fizycznych.

Zgodnie z wytycznymi Grupy Roboczej art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE (WP 251)[12] profilowanie oznacza gromadzenie informacji o danej osobie (lub grupie osób fizycznych) i ocenę ich cech lub wzorców zachowania w celu zakwalifikowania ich do określonej kategorii lub grupy, w szczególności do celów analizy lub prognozy takich aspektów, jak wykazywane przez dane osoby zdolności do wykonania danego zadania, zainteresowania lub ustalania prawdopodobnych zachowań. Istotą profilowania jest tworzenie profilu osoby na podstawie różnorodnych informacji, które jej dotyczą. Sporządzenie profilu osobowego pozwala na dokonywanie ocen, analiz i prognoz odnoszących się do tej osoby[13].

W przypadku innych form monitoringu mamy co do zasady do czynienia z zautomatyzowaną formą przetwarzania danych osobowych. Jak jednak wynika z powyższego, aby w jego ramach dochodziło do profilowania, pracodawca musiałby oceniać czynniki osobowe osób fizycznych. Z profilowaniem możemy mieć na przykład do czynienia wówczas, gdy analiza GPS pojazdu prowadzonego przez pracownika pozwala na określenie jego stylu jazdy, szybkości relacji na bodźce zewnętrzne czy też, w przypadku pozyskiwania danych o jakości snu pracownika, poziomie zmęczenia w poszczególnych dniach i godzinach, co umożliwiają urządzenia do monitowania stanu zdrowia pracowników.

Zgodnie z art. 22 ust. 1 RODO osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Samo zastosowanie zautomatyzowanego przetwarzania danych osobowych nie podlega żadnym dodatkowym ograniczeniom. Konieczność stosowania art. 22 RODO pojawia się dopiero wówczas, gdy w wyniku zautomatyzowanego przetwarzania danych — bez jakiegokolwiek udziału czynnika ludzkiego — miałyby zostać podjęte decyzje wywołujące wobec podmiotu danych określone skutki prawne lub w podobny sposób istotnie na nią wpływające. Zgodnie z wytycznymi Grupy Roboczej art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE (WP 251), jeżeli ostateczna de-

[12] *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, WP 251*, Urząd Ochrony Danych Osobowych, 5.12.2020, https://www.uodo.gov.pl/data/filemanager_pl/908.pdf (dostęp: 24.10.2022).

[13] P. Fajgielski, *Komentarz do art. 4 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 117.


© for this edition by CNS

cyzja zostaje podjęta przez człowieka po przeprowadzeniu oceny i uwzględnieniu innych czynników, taka decyzja nie opiera się wyłącznie na zautomatyzowanym przetwarzaniu:

> Aby można było uznać, że ma miejsce udział człowieka, administrator musi zapewnić, że jakikolwiek nadzór nad decyzją jest znaczący, a nie stanowi tylko symbolicznego gestu. Powinno być to prowadzone przez kogoś, kto ma władzę i kompetencje do zmiany decyzji. W ramach analizy należy wziąć pod uwagę wszystkie istotne dane[14].

Powyższe uwagi na temat profilowania i zautomatyzowanego podejmowania decyzji nie są czysto teoretyczne. Artykuł 13 ust. 2 lit. f oraz art. 14 ust. 2 lit. g RODO nakładają bowiem na administratora (a więc pracodawcę) szczególne obowiązki informacyjne w tym zakresie. Nakazują one podanie osobie, której dane dotyczą, istotnych informacji o zasadach podejmowania takich decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Zautomatyzowane podejmowanie decyzji, w tym profilowanie, jest także objęte prawem dostępu przysługującego osobie, której dane dotyczą (art. 15 ust. 1 lit. h). Szczególny nacisk na profilowanie został położony w art. 21 RODO, który reguluje prawo do sprzeciwu.

Co więcej art. 35 ust. 3 lit. a RODO wprowadza obowiązkową ocenę skutków dla ochrony danych w przypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, gdy opiera się ona na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną. Konieczność dokonania oceny skutków dla ochrony danych osobowych zachodzi w przypadku jakichkolwiek decyzji, przy podejmowaniu których wykorzystywano profilowanie.

Dla jasności należy wskazać, że w przypadku innych form monitoringu zawsze będziemy mieć do czynienia z zautomatyzowanym przetwarzaniem danych a niekiedy może mieć też miejsce profilowanie. Wówczas, gdy na podstawie informacji pozyskiwanych za pomocą monitoringu pracodawcy będą tworzyć profile pracowników biorąc pod uwagę określone cechy osobiste (na przykład akceptacja ryzyka, szybkość reagowania na różnego rodzaju bodźce zewnętrzne, zdolność koncentracji w poszczególnych sekwencjach czasowych w dobie pracowniczej, umiejętność adaptacji do nowych sytuacji itp.) będziemy mieli do czynienia z profilowaniem, czy wreszcie z podejmowaniem decyzji w wyniku zautomatyzowanego przetwarzania danych bez udziału czynnika ludzkiego (na przykład o ograniczeniu pracownikowi prawa do korzystania z samochodu służbowego dla celów prywatnych z uwagi na określony profil kierowcy stwarzający większe ryzyko wypadku, czy też wyłączenie możliwości pracy nocnej pracowników, którzy nie posiadają zdolności adaptacji do zmiany pory snu i pracy, co wpływa na ich szybkość reakcji).

[14] *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji…*, s. 20–21.


© for this edition by CNS

## PODSUMOWANIE

Prowadzenie monitoringu pracowników za pomocą narzędzi opartych na nowoczesnych technologiach i usługach łączności elektronicznej może z jednej strony przynieść pozytywny skutek dla efektywności czynności kontrolnych pracodawcy, a z drugiej — niesie za sobą poważne ryzyka w zakresie prywatności i innych dóbr osobistych pracowników. Poczucie permanentnej inwigilacji zdecydowanie zmniejsza poczucie komfortu pracy i zaufanie pracowników do pracodawcy. Z całego szeregu dostępnych na rynku narzędzi należy zatem wybierać te, które są niezbędne do osiągnięcia celu. Zgodnie z art. 25 RODO pracodawca ma obowiązek uwzględniać ochronę danych już w fazie projektowania (*privacy by design*) oraz w drodze realizacji zasady domyślnej ochrony danych (*privacy by default*), a decyzję o ich wprowadzeniu powinna poprzedzać analiza oceny skutków dla ochrony danych. Zasada *privacy by design* wymaga w szczególności, aby już w fazie projektowania administrator brał pod uwagę zagrożenia dla prywatności i je eliminował. Zagadnienia dotyczące prywatności powinny być uwzględniane w całym cyklu technologicznym, z naciskiem na fazę projektowania określonej technologii, a następnie na etapie jej wdrażania, korzystania z niej oraz usuwania danych. Stosowanie się do powyższego wymaga przemyślanych decyzji o wprowadzeniu określonych rozwiązań technologicznych pozwalających na monitorowanie pracowników, dokładnej analizy funkcjonalności oferowanych przez rynek narzędzi, a także przejrzystej i wyczerpującej komunikacji z pracownikami.

## PROCESSING OF EMPLOYEES' PERSONAL DATA IN THE FRAMEWORK OF SO-CALLED OTHER FORMS OF MONITORING

Summary

The widespread availability of new technologies allows employers to use types of employee activity monitoring that were previously non-existent in the work environment. Moreover, the popularization of remote work, in conjunction with the appearance of a new regulation in the Labor Code, naturally increases the employers' interest in the processing of data on employee online activity as well as location data. Technologies used in the context of other forms of monitoring, on the one hand, can be very effective in detecting violations of employee duties, protecting confidential information, in increasing the efficiency of work, but on the other hand, they pose serious risks to the protection of privacy and personal data. This is because digital data analysis applications can operate unnoticed by device users, thus posing greater threats to their privacy than, for example, CCTV cameras. Therefore, a re-examination of the data protection impact assessment and a careful analysis of the measures taken, taking into account the principles under both the Labor Code and the RODO, is warranted. Employers' use of data obtained in a non-compliant manner could face serious legal consequences.

Keywords: monitoring, remote working, GPS, employee control, other forms of monitoring


© for this edition by CNS

## BIBLIOGRAFIA

Fajgielski P., *Komentarz do art. 4 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

*Opinia 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy, WP 249*, Archiwum GIODO, 21.02.2018, https://archiwum.giodo.gov.pl/pl/file/13179.

Więckowska M., *Przetwarzanie danych na podstawie prawnie uzasadnionego interesu*, „ABI Expert" 2018, nr 3.

*Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679, WP 251*, Urząd Ochrony Danych Osobowych, 5.12.2020, https://uodo.gov.pl/pl/10/10.


© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.6

TOMASZ RADZISZEWSKI
ORCID: 0009-0004-8290-427X

# WYBRANE ASPEKTY FUNKCJONOWANIA MONITORINGU WIZYJNEGO W ŚWIETLE REGULACJI DOTYCZĄCYCH SZKÓŁ I INNYCH PLACÓWEK OŚWIATOWYCH

Abstrakt: Opracowanie porusza tematykę funkcjonowania nadzoru wizyjnego na gruncie krajowego porządku prawnego, a w szczególności jego silnej fragmentacji, która jest jednym z głównych problemów związanych z jego funkcjonowaniem. W pracy pojawia się teza, że sfragmentowany zakres normowań stanowi znaczne utrudnienie dla podmiotów wykorzystujących ten środek ochrony, ale co ważniejsze, nie tworzy spójnej całości, pozostawiając w pewnym zakresie nieuregulowanymi między innymi kwestię ochrony praw osób, których wizerunki są obserwowane, rejestrowane lub przetwarzane w sposób umożliwiający identyfikację ich tożsamości, w tym osób przebywających w otwartej i zamkniętej przestrzeni przeznaczonej do użytku publicznego, a także zagadnienie obowiązków administratora monitoringu wykorzystywanego w celach prywatnych, w ramach którego monitorowaniu podlega otwarta przestrzeń publiczna.

Praca na podstawie węzłowej analizy regulacji związanych z funkcjonowaniem monitoringu wizyjnego w szkołach i innych placówkach oświatowych może dać asumpt do dalszych rozważań na temat komplementarności porządku prawnego związanego ze stosowaniem nadzoru wizyjnego do możliwości tych podmiotów, kształtowanych na drodze szybkiego rozwoju technologii informacyjnych.

Słowa kluczowe: monitoring wizyjny, ochrona prywatności, bezzałogowe statki powietrzne, podstawy prawne monitoringu

## 1. PERSPEKTYWA ANALIZY

Należy niewątpliwie wskazać, że istnieje potrzeba systemowego uregulowania problematyki funkcjonowania monitoringu wizyjnego, który w ocenie PUODO jest „inwazyjną formą przetwarzania danych osobowych i jako taki powinien podlegać szczególnej weryfikacji przez administratora potrzeby jego stosowania i konieczności zabezpieczenia oraz kontroli przez organy kontrolne”[1]. Inwazyj-

[1] *Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego*, Archiwum Urzęd Ochrony Danych Osobowych, 15.06.2018, https://archiwum.uodo.gov.pl/pl/file/1200 (dostęp: 12.12.2022).


© for this edition by CNS

ność tego środka ochrony należy tłumaczyć, mając na uwadze istnienie zagrożeń związanych z nadmierną ingerencją w konstytucyjnie chronione prawa jednostki, między innymi do prywatności[2], ochrony informacji z nią związanych[3], w które siła i zakres ingerencji powinny być definiowane zgodnie z zasadą proporcjonalności ujętą w art. 31 ust. 3 Konstytucji RP i z poszanowaniem konstytucyjnej zasady legalizmu[4].

Rozwój społeczeństwa informacyjnego (trzeciej fali)[5], spowodował, że systemy monitoringu stały się coraz bardziej powszechnym narzędziem wykorzystywanym dla dodatkowego zabezpieczania przestrzeni publicznej i prywatnej. Tendencja obejmowania różnorodnych obszarów i miejsc użyteczności publicznej monitoringiem, a także oczekiwania związane z ich rolą na rzecz zapewniania bezpieczeństwa mają charakter postępujący, w przeciwieństwie do porządku prawnego, który ewidentnie nie nadąża za rozwojem tego rodzaju technologii informacyjnych.

Zgodnie z wyrażonym w opublikowanej w 2014 roku przez Najwyższą Izbę Kontroli informacji o wynikach kontroli w zakresie funkcjonowania miejskiego monitoringu wizyjnego jest on

> powszechnie wykorzystywanym — dotyczy to wszystkich miast wojewódzkich oraz ponad 85% miast powiatowych — narzędziem dla dodatkowego zabezpieczenia przestrzeni publicznej. W Polsce brak jest kompleksowych unormowań zasad instalowania i prowadzenia systemów monitoringu przez instytucje państwowe, samorządowe oraz podmioty prywatne. Stan ten, wobec praw i wolności obywatelskich zagwarantowanych w Konstytucji RP, w tym prawa do ochrony prywatności, ochrony danych osobowych, wymaga wprowadzenia rozwiązań rangi ustawowej, dotyczących budowy i funkcjonowania systemów monitoringu wizyjnego[6].

Krajowy porządek prawny obejmujący swym zakresem zasady i tryb instalowania i wykorzystywania monitoringu wizyjnego odnosi się jedynie do wysublimowanych aspektów jego stosowania. Dokonując w tym zakresie węzłowej

---

[2] Artykuł 47 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483) — dalej Konstytucja RP.

[3] *Ibidem*, art. 51.

[4] *Ibidem*, art. 47.

[5] Pojęcie społeczeństwa informacyjnego ma swoje korzenie w japońskiej kulturze ekonomicznej (*jōhōka shakai*). W roku 1963 pojęcia tego użył japoński socjolog Tadao Umesao w publikacji *Teoria społeczeństwa informacyjnego* [*Jōhō sangyō-ron*], dotyczącej teorii społeczeństwa opartego na przemyśle informatycznym, gdzie scharakteryzował zmiany zaistniałe w strukturach społecznych pod wpływem rozwijającej się techniki informacyjnej. Według Heidi i Alvina Tofflerów „społeczeństwo informacyjne" jest tak zwanym „społeczeństwem trzeciej fali", w którym wszelkie działania muszą i powinny opierać się na świadomym kontrolowaniu bezpieczeństwa ogólnego przez nadzorowanie bezpieczeństwa informacji — gromadzonej, wykorzystywanej i udostępnianej otoczeniu. Szerzej na ten temat T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 33.

[6] *Informacja o wynikach kontroli. Funkcjonowanie miejskiego monitoringu wizyjnego (LLU — 4101-01-00/2013 nr ewid. 181/2013/P/13/154/LLU)*, Najwyższa Izba Kontroli, 1.05.2014, https://www.nik.gov.pl/kontrole/P/13/154/LKI/ (dostęp: 14.12.2022).


© for this edition by CNS

analizy należy wskazać, że podstawy prawne w zakresie utrwalania wizji (a w niektórych przypadkach również dźwięku) posiadają:

1. podmioty państwowe i samorządowe na podstawie:

a) art. 9a ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jedn. Dz.U. z 2022 r. poz. 559 ze zm.) — obraz;

b) art. 4b ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (tekst jedn. Dz.U. z 2022 r. poz. 1526 ze zm.) — obraz;

c) art. 60a ustawy z dnia 5 czerwca 1998 roku o samorządzie województwa (tekst jedn. Dz.U. z 2022 r. poz. 2094 ze zm.) — obraz;

d) art. 5a ustawy z dnia 16 grudnia 2016 roku o zasadach zarządzania mieniem państwowym (tekst jedn. Dz.U. z 2021 r. poz. 1933 ze zm.) — obraz;

2. podmioty prywatne na podstawie:

a) art. 15b ustawy z dnia 19 listopada 2009 roku o grach hazardowych (tekst jedn. Dz.U. z 2022 r. poz. 888 ze zm.) — obraz i dźwięk;

b) art. 11 ustawy z dnia 20 marca 2009 roku o bezpieczeństwie imprez masowych (tekst jedn. Dz.U. z 2017 r. poz. 1160 ze zm.) — obraz i dźwięk;

c) art. 25 ust. 8a ustawy z dnia 14 grudnia 2012 roku o odpadach (tekst jedn. Dz.U. z 2022 r. poz. 699 ze zm.) — obraz;

3. podmioty ochrony zdrowia, zatrudnienia i szkolnictwa na podstawie:

a) art. 222 ustawy z dnia 26 czerwca 1974 roku Kodeks pracy (tekst jedn. Dz.U. z 2022 r. poz. 1510 ze zm.) — obraz;

b) art. 108a ustawy z dnia 14 grudnia 2016 roku — Prawo oświatowe (tekst jedn. Dz.U. z 2022 r. poz. 1082 ze zm.) — obraz;

c) art. 18e ustawy z dnia 19 sierpnia 1994 roku o ochronie zdrowia psychicznego (tekst jedn. Dz.U. z 2017 r. poz. 882 ze zm.) — obraz i dźwięk;

d) art. 23a ustawy z dnia 15 kwietnia 2011 roku o działalności leczniczej (tekst jedn. Dz.U. z 2018 r. poz. 160 ze zm.) — obraz;

4. organy ścigania i sądy na podstawie:

a) art. 15 i art. 19 ustawy z dnia 6 kwietnia 1990 roku o Policji (tekst jedn. Dz.U. z 2021 r. poz. 1882 ze zm.) — obraz i dźwięk;

b) art. 9ca ustawy z dnia 12 października 1990 roku o Straży Granicznej (tekst jedn. Dz.U. z 2022 r. poz. 1061 ze zm.) — obraz, ponadto art. 9e, 9f, 9g tejże w ramach realizacji czynności operacyjno-rozpoznawczych, art. 11 tejże — obraz i dźwięk;

c) art. 14 i art. 17 (kontrola operacyjna) ustawy z dnia 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz.U. z 2022 r. poz. 1900 ze zm.) — obraz i dźwięk;

d) art. 23 i art. 27 (kontrola operacyjna) ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (tekst jedn. Dz.U. z 2022 r. poz. 557 ze zm.) — obraz i dźwięk;

e) art. 29 i art. 31 (kontrola operacyjna) ustawy z dnia 9 czerwca 2006 roku o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (tekst jedn. Dz.U. z 2017 r. poz. 1978 ze zm.) — obraz i dźwięk;


© for this edition by CNS

f) art. 17, art. 18b, art. 31, art. 32 i art. 33 (czynności operacyjno-rozpoznawcze) ustawy z dnia 24 sierpnia 2001 roku o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jedn. Dz.U. z 2021 r. poz. 1214 ze zm.) — obraz i dźwięk;

g) art. 76, art. 117, art. 118 i art. 119 (czynności operacyjno-rozpoznawcze) ustawy z dnia 16 listopada 2016 roku o Krajowej Administracji Skarbowej (tekst jedn. Dz.U. z 2022 r. poz. 813 ze zm.) — obraz i dźwięk;

h) art. 121 ustawy z dnia 9 czerwca 2022 roku o wspieraniu i resocjalizacji nieletnich (Dz.U. z 2022 r. poz. 1700) — obraz i dźwięk;

i) art. 11 ustawy z dnia 29 sierpnia 1997 roku o strażach gminnych (tekst jedn. Dz.U. z 2021 r. poz. 1763 ze zm.) — obraz i dźwięk;

j) art. 20g ustawy z dnia 21 marca 1985 roku o drogach publicznych (tekst jedn. Dz.U. z 2022 r. poz. 1693 ze zm.) — obraz;

k) art. 157 ustawy z dnia 17 listopada 1964 roku — Kodeks postępowania cywilnego (tekst jedn. Dz.U. z 2021 r. poz. 1805 ze zm.) — obraz i dźwięk;

l) art. 147 ustawy z dnia 6 czerwca 1997 roku — Kodeks postępowania karnego (tekst jedn. Dz.U. z 2022 r. poz. 1375 ze zm.) — obraz i dźwięk.

Wprawdzie przytoczone powyżej regulacje nie wyczerpują wszystkich przepisów związanych z uprawnieniami do rejestracji obrazu i dźwięku, jednak wskazują one na szereg istotnych obszarów, w stosunku do których ustawodawca podjął decyzję o wprowadzeniu regulacji o charakterze szczególnym. Niemniej już przedstawiony wachlarz rozwiązań legislacyjnych *prima facie* wskazuje na mnogość powstających w różnym czasie regulacji, posiadających potencjał kolizyjny i pewien zakres niedoregulowania, zwłaszcza w sferze życia społecznego[7]. Stąd pojawiają się problemy związane na przykład ze stosowaniem monitoringu wizyjnego do celów prywatnych (na prywatnych posesjach, tak w zabudowie indywidualnej, jak i zarządzanej przez wspólnoty mieszkaniowe — na przykład placach zabaw, klatkach schodowych, parkingach, piwnicach itp.).

Innymi słowy, przedstawiona fragmentaryczność regulacji związanych z funkcjonowaniem nadzoru wizyjnego nie tworzy spójnej całości, a sprowadza się do funkcjonowania regulacji, na mocy których istnieje obowiązek wykorzystywania[8], dopuszczalność[9] lub wykluczenie jego stosowania[10], przy jednoczesnym

[7] Wyjątek stanowią tu regulacje związane z zapewnieniem bezpieczeństwa imprez masowych (ustawa o bezpieczeństwie imprez masowych), systemu kontroli gier w kasynie gry (ustawa o grach hazardowych) czy stosowaniem rejestracji obrazu w miejscach detencji Policji (rozporządzenie Ministra Spraw Wewnętrznych w sprawie pomieszczeń przeznaczonych dla osób zatrzymanych lub doprowadzonych w celu wytrzeźwienia, pokoi przejściowych, tymczasowych pomieszczeń przejściowych i policyjnych izb dziecka, regulaminu pobytu w tych pomieszczeniach, pokojach i izbach oraz sposobu postępowania z zapisami obrazu z tych pomieszczeń, pokoi i izb).

[8] Przykładowo na gruncie regulacji związanych z organizacja imprez masowych, składowaniem odpadów niebezpiecznych.

[9] Mowa między innymi o porządku prawnym w zakresie prawa pracy lub prawa oświatowego.

[10] Dotyczy regulacji stanowiących kategoryczny zakaz prowadzenia monitoringu w określonych kategoriach pomieszczeń, między innymi na gruncie prawa pracy.


© for this edition by CNS

uregulowaniu wybranych aspektów stosowania monitoringu wizyjnego. Mimo że tego rodzaju rozwiązanie funkcjonuje w części innych państw Unii Europejskiej, trudno jednak w aktualnych warunkach uznać je za optymalne. Do głównych przyczyn tego stanu rzeczy należy powszechność stosowania monitoringu wizyjnego, jak i zwiększające się możliwości techniczne, które powodują, że monitoring wizyjny coraz częściej wymaga wnikliwej analizy dopuszczalności jego stosowania, chociażby ze względu na jego coraz większe możliwości ingerowania w prywatności jednostki. Bezpośrednio przyczyniają się do tego chociażby ich coraz lepsze parametry wizyjne. Zwiększa się rozdzielczość uzyskiwanego obrazu[11], możliwości przybliżenia[12], czułość przetwornika obrazu w złych warunkach oświetleniowych[13], pojawiają się nowe technologie wizyjne pozwalające na osiąganie obrazowania w podczerwieni[14], a kwestią czasu jest przejście technologii wykorzystywanych w tak zwanych *full-body scanners*, potocznie nazywanych „nagimi skanerami", do użytku komercyjnego, wychodząc poza obszar bezpieczeństwa, na przykład na lotniskach[15]. Nie bez znaczenia dla poziomu inwazyjności monitoringu wizyjnego pozostaje również fakt stosowania do realizacji jego celów rozwiązań mobilnych, na przykład w postaci bezzałogowych statków powietrznych[16], które są wyposażane w teleobiektywy pozwalające uzyskać materiał wizyjny z odległości przekraczającej 150 m[17].

[11] Dziś przestaje dziwić stosowanie matryc światłoczułych w aparatach fotograficznych smartfonów na poziomie 200 MP.

[12] Nawet w urządzeniach konsumenckich takich jak smartfony osiągane jest dziesięciokrotne przybliżenie optyczne i kilkusetkrotne cyfrowe.

[13] Obecnie można mówić o rozkwicie tak zwanej fotografii obliczeniowej, która opierając się na sztucznej inteligencji i przeznaczonym do obróbki obrazu procesorom pozwala uzyskać znakomite pod względem ilości szczegółów zdjęcia w scenerii nocnej.

[14] Na rynku dostępne są już urządzenia konsumenckie umożliwiające nagrywanie obrazu stanowiącego namiastkę termowizji.

[15] Urządzenia tego typu funkcjonują zazwyczaj w oparciu o technologię radiowych fal milimetrowych o bardzo wysokiej częstotliwości lub w oparciu o zjawisko rozproszenia wstecznego promieniowania rentgenowskiego.

[16] Pojęcie „bezzałogowego statku powietrznego" (BSP) zostało wprowadzone do porządku prawnego UE rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (Dz.Urz.UE L 212/1 z 22.08.2018 r.), tak zwanym rozporządzeniem bazowym 2018/1139. Zgodnie z art. 3 pkt 30 tegoż „bezzałogowy statek powietrzny" oznacza każdy statek powietrzny wykonujący operację lub przeznaczony do wykonywania operacji samodzielnie lub będąc pilotowanym zdalnie bez pilota na pokładzie.

[17] Odległość ta wskazana jest jako parametr wymagany podczas wykonywana operacji w kategorii A3, podczas której pilot musi utrzymywać bezzałogowy statek powietrzny w odległości co najmniej 150 m w poziomie od terenów mieszkaniowych, użytkowych, przemysłowych lub rekreacyjnych, a operacje te muszą być wykonywane na obszarze, na którym pilot może oczekiwać, że


© for this edition by CNS

W tym miejscu warto poczynić węzłową uwagę, która dotyczy dekodowania terminu „urządzenia umożliwiającego rejestrację obrazu" (monitoringu wizyjnego) w doktrynie i orzecznictwie, w których używane przez ustawodawcę pojęcie jest stosowane zamienne z pojęciem CCTV (*closed-circuit television*)[18]. Wydaje się zasadnym, zwłaszcza w świetle przywołanych powyżej rozwiązań technicznych służących nadzorowi wizyjnemu, uznanie tego zabiegu za błędne i nadto zawężające perspektywę tego rodzaju nadzoru, w świetle możliwości (jednak prawnie dopuszczalnych), jakie posiadają obecnie podmioty zainteresowane tego rodzaju rozwiązaniem.

W praktyce funkcjonowania między innymi podmiotów publicznych lub realizujących zadania publiczne (państwowych jak i samorządowych) czy szerokorozumianych podmiotów prywatnych, każdorazowe wprowadzenie monitoringu (z wyłączeniem sytuacji, gdy mają zastosowanie regulacje nakładające obowiązek stosowania tego rozwiązania) wymaga analizy dopuszczalności jego stosowania, które wiążą się z realizacją określonych celów wskazanych na gruncie regulacji o charakterze szczególnym. Dlatego przykładowo przy podejmowaniu decyzji o wprowadzeniu do placówki oświatowej monitoringu, w celu do zachowania równowagi pomiędzy zagwarantowaniem praw jednostce (uczniów, nauczycieli i innych pracowników szkoły, a także rodziców i osób odwiedzających placówkę) a ogólnym interesem szkoły, przedmiotowa analiza powinna obejmować również konsultacje z przedstawicielami uczniów, rodziców i nauczycieli, co potwierdza, że kierownik podmiotu jest związany nie tylko przeprowadzoną we własnym zakresie analizą spełnienia podanych przez ustawodawcę przesłanek określających cel stosowania monitoringu, ale też stanowiskiem określonych grup zainteresowania.

## 2. WĘZŁOWA ANALIZA PROBLEMATYKI NADZORU WIZYJNEGO W SZKOŁACH I INNYCH PLACÓWKACH OŚWIATOWYCH

Dopiero wejście w życie ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych[19] wprowadziło do porządku prawnego zmianę w zakresie dopuszczalności stosowania monitoringu wizyjnego w placówkach oświatowych[20]. W wy-

w normalnych okolicznościach w czasie przeprowadzania operacji nie będzie ona stwarzać zagrożenia dla osób postronnych. Podczas tego rodzaju operacji można stosować drony klasy C2, C3, C4, przy czym te dwa ostanie mogą posiadać maksymalną masę startową (MTOM) do 25 kg.

[18] Funkcjonująca obiegowo definicja CCTV wskazuje, że jest to pewnego rodzaju telewizja zamkniętego obwodu, telewizyjny system dozorowy zbudowany najczęściej z kamer, rejestratora cyfrowego (DVR) lub sieciowego (NVR, charakterystycznego dla kamer IP), monitorów, switchy, okablowania, oprogramowania.

[19] Na podstawie art. 154 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2018 r. poz. 1000 ze zm.) — dalej u.o.d.o.

[20] Zakres podmiotowy regulacji dot. stosowania monitoringu wizyjnego na gruncie Ustawy z dnia 14 grudnia 2016 r. — Prawo oświatowe (tekst jedn. Dz.U. z 2021 r. poz. 1082 ze zm.) — dalej


© for this edition by CNS

niku tej nowelizacji wprowadzono do prawa oświatowego art. 108a, pozwalający dyrektorom szkół oraz innych placówek oświatowych na wprowadzenie szczególnego nadzoru (w postaci środków technicznych umożliwiających rejestrację obrazu bez dźwięku) nad pomieszczeniami szkoły lub placówek bądź terenem wokół nich. Przy czym zasady stosowania nadzoru wizyjnego (również dźwiękowego)[21] w młodzieżowych ośrodkach wychowawczych stanowią regulację odrębną na gruncie ustawy o wspieraniu i resocjalizacji nieletnich.

Funkcjonowanie nadzoru wizyjnego w szkołach i placówkach ma służyć zapewnieniu bezpieczeństwa uczniów i pracowników i/lub ochronie mienia szkoły lub placówki. Ponadto w art. 108a ust. 2 upos ustawodawca *expressis verbis* wyjaśnił kwestie dopuszczalności stosowania monitoringu w celach związanych z oceną jakości pracy personelu, czyniąc to działanie niedopuszczalnym.

Wydaje się zasadnym stwierdzenie, że wprowadzenie nadzoru wizyjnego w szkole i innych placówkach oświatowych, w porównaniu do innych podmiotów mogących stosować tego rodzaju zabezpieczenie[22], stanowi z punktu widzenia organizacyjnego największe wyzwanie, mając na uwadze realizację obowiązków o charakterze organizacyjnym nałożonych przez ustawodawcę na te podmioty w związku z projektowaniem i wdrożeniem systemu monitoringu wizyjnego.

Sama decyzja dyrektora szkoły (czy kierownika innego rodzaju placówki oświatowej) w przedmiocie wprowadzenia monitoringu wizyjnego nie może zależeć wyłącznie od pozytywnego wyniku testu niezbędności stosowania tego rozwiązania w celu zapewnienia (adekwatnego do istniejącego wachlarza zagrożeń) poziomu bezpieczeństwa uczniów, pracowników i innych osób przebywających na terenie szkoły (placówki) czy też mienia. Podjęcie przedmiotowej decyzji musi być poprzedzone uzgodnieniami z organem prowadzącym oraz konsultacjami z radą pedagogiczną, radą rodziców i samorządem uczniowskim, przy czym regulacje w tym zakresie nie wskazują na tryb i zasady prowadzenia tego rodzaju działań. Ponadto, jak wskazuje art. 108a ust. 9 upos, warunkiem *sine qua non* w ramach procesu wdrożenia nadzoru wizyjnego w szkole lub innej placówce oświatowej jest uprzednie przeprowadzenie uzgodnień z organem prowadzącym szkołę lub placówkę w zakresie zastosowania odpowiednich środków techniczno-

prawo oświatowe lub upos, obejmuje szkoły, przedszkola (zob. art. 4 pkt 1 tejże), placówki oświatowo-wychowawcze (w tym szkolne schroniska młodzieżowe), placówki kształcenia ustawicznego oraz centra kształcenia zawodowego, placówki artystyczne, poradnie psychologiczno-pedagogiczne, młodzieżowe ośrodki wychowawcze, młodzieżowe ośrodki socjoterapii, specjalne ośrodki szkolno-wychowawcze oraz specjalne ośrodki wychowawcze dla dzieci i młodzieży wymagających stosowania specjalnej organizacji nauki, placówki zapewniające opiekę i wychowanie uczniom w okresie pobierania nauki poza miejscem stałego zamieszkania, biblioteki pedagogiczne.

[21] Możliwość nagrywania dźwięku posiadają zakłady lecznicze dysponujące warunkami wzmocnionego lub maksymalnego zabezpieczenia, o których mowa w art. 121 zd. 2 ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich (Dz.U. z 2022 r. poz. 1700) — dalej ustawa o wspieraniu i resocjalizacji nieletnich lub uwrn.

[22] Z wyłączeniem podmiotów realizujących czynności operacyjno-rozpoznawcze.


© for this edition by CNS

-organizacyjnych w celu ochrony przechowywanych nagrań wizyjnych i zawartych w nich danych osobowych uczniów, pracowników i innych osób, w stosunku do których nagrania z monitoringu mogą służyć ich identyfikacji.

W kontekście funkcjonowania młodzieżowych ośrodków wychowawczych, okręgowych ośrodków wychowawczych, zakładów poprawczych i schronisk dla nieletnich, decyzję o zainstalowaniu monitoringu wizyjnego podejmuje samodzielnie kierownik podmiotu. Przy czym, jeśli nadzór dotyczy zakładów leczniczych dysponujących warunkami wzmocnionego lub maksymalnego zabezpieczenia, w gestii kierownika podmiotu pozostaje decyzja dotycząca rejestracji dźwięku. Co warte podkreślenia, ustawodawca konstruując przepisy dotyczące monitoringu wskazał, że do wyłącznej kompetencji dyrektora ośrodka, zakładu lub schroniska albo kierownika zakładu leczniczego należy decyzja o rodzaju urządzeń i środków technicznych służących do rejestrowania, utrwalania i odtwarzania obrazu lub dźwięku z monitoringu w świetle celów jego funkcjonowania, którymi są zapewnienie bezpieczeństwa i porządku wewnętrznego ośrodka, zakładu lub schroniska. Wydaje się zasadnym stwierdzenie, że w tych okolicznościach ustawodawca (w minimalnym zakresie) dostrzegł (z punktu widzenia odpowiedzialności kierownika podmiotu) konieczność przeprowadzenia analizy w zakresie potrzeb i możliwości zastosowania określonego rodzaju urządzeń i środków technicznych, nie tylko finansowych i prawnych, a spełniających również rolę ochronną wobec jednostki przed nadmierną ingerencją w jej wolności i prawa.

Bez wątpienia kwestia wyboru określonych zabezpieczeń w szkole lub innej placówce oświatowej powinna być poparta wynikami szacowania ryzyka związanego z przetwarzaniem danych osobowych w ramach procesu monitorowania, które należy traktować jako dane wejściowe w procesie projektowania zabezpieczeń[23]. Wydaje się również zasadnym, aby w ramach postępowania z ryzykiem rozważyć kwestie opracowania i udostępniania dokumentu operacyjnego, na przykład w postaci regulaminu funkcjonowania monitoringu wizyjnego w szkole lub innej placówce, odnoszącego się między innymi do: zasad udostępniania nagrań, opisu przestrzeni monitorowanej poprzez wskazanie punktów monitoringu na obszarze monitorowanym oraz pomieszczeń i obszarów nieobjętych nadzorem, zasad oceny funkcjonowania monitoringu i jego wpływu na podniesienie poziomu bezpieczeństwa. Co również istotne, jeśli zastosowanie monitoringu wizyjnego wiązałoby się z wysokim ryzykiem dla realizacji wolności i praw osób nim objętych, wówczas niezbędnym byłoby przeprowadzenie w myśl art. 35 RODO oceny skutków dla ochrony danych. W tych okolicznościach cenną wskazówką zasadności przeprowadzenia przedmiotowej oceny jest publikowany przez PUODO ko-

[23] Zob. art. 25 ust. 1 RODO. Szerzej P. Litwiński, [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych Komentarz*, red. P. Litwiński, Warszawa 2018, s. 455 n.; K. Wygoda, *Art. 25. Domyślna ochrona danych*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 287 n.


© for this edition by CNS

munikat w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[24], z którego wynika, że przeprowadzenie przedmiotowej oceny nie jest wymagane dla monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa.

Dyrektor szkoły czy kierownik innej placówki oświatowej, podejmując decyzję o wdrożeniu nadzoru wizyjnego. musi również mieć na uwadze wprowadzone ustawą (art. 108a ust. 3) ograniczenia związane z obszarem nadzorowania, którego rozszerzenie wymaga pogłębionej refleksji, aby wykazać *explicite*, że monitoring w pomieszczeniach, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, pomieszczeniach, w których udzielana jest uczniom pomoc psychologiczno-pedagogiczna, pomieszczeniach przeznaczonych do odpoczynku i rekreacji pracowników, pomieszczeniach sanitarno-higienicznych, gabinetach profilaktyki zdrowotnej, a także szatniach i przebieralniach jest niezbędny ze względu na istniejące zagrożenia dla bezpieczeństwa uczniów i pracowników lub znajdującego się tam mienia i zapewnia nienaruszalność godności oraz innych dóbr osobistych tak uczniów i pracowników, jak i innych osób pojawiających się w monitorowanej przestrzeni. Co istotne, ustawodawca wskazuje na konieczność stosowania w tych okolicznościach rozwiązań anonimizujących[25] (na przykład sprzętowo-aplikacyjnych: filtrów, algorytmów zniekształcających, obiektywów itp.), uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Ponadto, co nie mniej ważne z perspektywy kodeksu pracy, zastosowanie monitoringu wizyjnego w pomieszczeniach sanitarnych wymaga akceptacji (poprzez wyrażenie 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”[26].

Spójnie z regulacjami dotyczącymi stosowania nadzoru wizyjnego, na przykład na gruncie kodeksu pracy[27], nagrania zawierające dane osobowe mogą być przetwarzane w terminie do trzech miesięcy od dnia powstania nagrania (o ile regulacja o charakterze szczególnym, na przykład do czasu prawomocnego zakończenia postępowania, nie stanowi inaczej)[28].

---

[24] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. z 2018 r. poz. 827).

[25] Zob. art. 108a ust. 3 upos.

[26] Zob. art. $22^2$ § 2 kodeksu pracy.

[27] *Ibidem*, art. $22^2$ § 3.

[28] Zgoła inne ramy czasowe przetwarzania nagrań zostały ustalone na gruncie ustawy o ochronie zdrowia psychicznego, która nakłada na kierownika podmiotu realizującego działalność leczniczą w zakresie ochrony zdrowia psychicznego, obowiązek przechowywania nagrań co najmniej 12 miesięcy od dnia ich zarejestrowania, nie dłużej jednak niż przez 13 miesięcy, o ile nie zostaną one zabezpieczone jako dowód w sprawie w przypadku toczącego się postępowania (zob. art. 18e ust. 6 ustawy o ochronie zdrowia psychicznego), natomiast przepisy wykonawcze wydane w dele-


© for this edition by CNS

Odrębną, ale nie mniej istotną kwestię stanowi polityka informacyjna w zakresie realizacji nadzoru wizyjnego, która powinna być realizowana zarówno w stosunku do uczniów i pracowników szkoły lub innej placówki oświatowej, jak i innych osób pojawiających się w monitorowanej przestrzeni. Tutaj ustawodawca wprowadził obowiązki informowania o wprowadzeniu monitoringu na co najmniej czternaście dni przed jego planowanym uruchomieniem[29] oraz oznaczania stref monitorowania „w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż dzień przed jego uruchomieniem"[30], pozostawiając jednocześnie w gestii kierownika podmiotu sposób informowania o wprowadzanym nadzorze wizyjnym. Powinno się to jednak odbyć w sposób zwyczajowo przyjęty do przekazywania tego typu informacji w danej szkole lub placówce, z wyjątkiem sytuacji obejmowania obowiązków służbowych, wówczas przedmiotowy obowiązek informacyjny powinien być zrealizowany w stosunku do obejmującego obowiązki w sposób pisemny[31].

Wydaje się zasadnym twierdzenie, że w sytuacji zmiany obszaru monitorowanego (na przykład poprzez dodanie, przeniesienie lub demontaż kamer) dyrektor szkoły lub innej placówki oświatowej powinien poprzednio podane informacje dotyczące monitoringu zaktualizować i również przekazać zainteresowanym stronom w sposób zwyczajowo przyjęty w danej szkole lub placówce.

Możliwymi sposobami informowania o celach, zakresie oraz sposobie zastosowania monitoringu jest umieszczenie odpowiednich przepisów „w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy"[32], czy też w statucie szkoły, który (co podkreśla jego wagę) jest przyjmowany przez radę pedagogiczną. Dobrą praktyką wydaje się umieszczanie informacji o celach i zasadach funkcjonowania monitoringu wizyjnego w regulaminach konkretnych obiektów należących do szkoły lub innej placówki oświatowej, podobnie jak publikowanie przedmiotowych informacji w serwisach internetowych, mediach społecznościowych oraz podejmowanie rozmów z rodzicami w ramach rutynowych spotkań.

---

gacji art. 25 ust. 8a ustawy z dnia 14 grudnia 2012 r. o odpadach (tekst jedn. Dz.U. z 2022 r. poz. 699 ze zm.) oraz rozporządzenie Ministra Środowiska z dnia 29 sierpnia 2019 r. w sprawie wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów (Dz.U. z 2019 r. poz. 1755) wskazują, że pojemność nośnika umożliwiającego przechowywanie zarejestrowanego obrazu powinna być dostosowana do jego przechowywania przez co najmniej miesiąc od daty dokonania zapisu, a zarejestrowany obraz powinien podlegać skasowaniu po upływie miesiąca od daty dokonania jego zapisu (zob. § 4 pkt 2 tegoż).

[29] Zob. art. 108a ust. 6 prawa oświatowego.

[30] *Ibidem*, art. 108a ust. 8.

[31] Więcej na temat zasad informowania o wdrożeniu i funkcjonowaniu nadzoru wizyjnego: J. Wezgraj, *Monitoring wizyjny a ochrona danych osobowych — wymagania rodo, przepisy sektorowe oraz wytyczne UODO*, Wrocław 2019, s. 316 n.

[32] Zob. art. $22^2$ §6 kodeksu pracy.


© for this edition by CNS

Na koniec należy poruszyć w sposób węzłowy kwestię niezbędności stosowania monitoringu w świetle wskazanych ustawowo celów jego funkcjonowania. Bez wątpienia przymiot niezbędności nadzoru wizyjnego powinien podlegać okresowej ocenie przez cały jego „cykl życia", a do tego powinna służyć określona przez szkołę lub inną placówkę oświatową metodyka oceny, zawierająca między innymi obiektywne kryteria oceny jego skuteczności w realizacji przyjętych celów jego funkcjonowania. Nie wydaje się błędem, aby przedmiotowa metodyka lub inna regulacja wewnętrzna odnosiły się również do prowadzenia cyklicznej oceny w formule zbliżonej do uzgodnień z organem prowadzącym szkołę lub placówkę w zakresie projektowania i stosowania odpowiednich środków techniczno-organizacyjnych, o których mowa w art. 108a ust. 9 upos, jako elementu cyklicznego przeglądu zarządzania tym środkiem bezpieczeństwa. Można uznać za uzasadnione podjęcie analogicznych działań w kontekście oceny niezbędności nadzoru wizyjnego z uczestnictwem grup zainteresowania, to jest przedstawicieli rodziców, uczniów i rady pedagogicznej.

## 3. O NADZORZE WIZYJNYM — *DE LEGE FERENDA*

Jednym z głównych problemów związanych z funkcjonowaniem nadzoru wizyjnego jest silna fragmentacja regulacji z nim związanych, która nie tworzy spójnej całości, pozostawiając w pewnym zakresie nieuregulowanymi między innymi kwestie ochrony praw osób, których wizerunki są obserwowane, rejestrowane lub przetwarzane w sposób umożliwiający identyfikację ich tożsamości, w tym osób przebywających w otwartej i zamkniętej przestrzeni przeznaczonej do użytku publicznego. Poza obszarem regulacji prawnych znajduje się również zakres obowiązków administratora monitoringu wykorzystywanego w celach prywatnych, w ramach którego monitorowaniu podlega otwarta przestrzeń publiczna. W tym kontekście, wykorzystując pewnego rodzaju analogię, należy krytycznie ocenić brak precyzyjnych regulacji na gruncie prawa oświatowego w zakresie określania obszaru podlegającego monitorowaniu. Prawodawca wskazuje wyłącznie, że jest możliwy szczególny „nadzór nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring)"[33], nie precyzując pojęcia „terenu wokół szkoły", co budzi wątpliwości zarówno w kontekście zakresu ingerencji w prywatność i prawo do ochrony danych chociażby osób poruszających się wzdłuż ogrodzenia posesji, na której znajduje się szkoła lub inna placówka oświatowa, jak i z perspektywy ochrony dzieci w drodze do szkoły[34].

[33] Zob. art. 108a ust. 1 prawa oświatowego.

[34] Na przykład kwestie zasięgu monitoringu zostały uregulowane na gruncie przepisów wykonawczych do ustawy o odpadach. Jak wskazuje § 2 ust. 2 pkt 3 rozporządzenia w sprawie wizyjnego


© for this edition by CNS

Niewątpliwie ważnym dla realizacji wolności i praw osobistych jest, aby system monitoringu wizyjnego działał proporcjonalnie w stosunku do przyjętych celów, a zarządzający nim dokładał wszelkich starań, żeby system ten w jak najmniejszym stopniu ingerował w prywatność obserwowanych osób. Z tego punktu widzenia należy wyraźnie wskazać, że działania ustawodawcy nie stwarzają warunków, w których administrator monitoringu lub kierownik podmiotów, w imieniu i na rzecz których działa administrator, byłby obligowany do analizy adekwatności parametrów monitorowania, tak aby unikać sytuacji nadmiernego ingerowania w prywatność, na przykład poprzez stosowanie kamer wysokiej rozdzielczości w sytuacji, gdy wystarczyłoby zastosowanie monitoringu prowadzącego detekcję wkroczenia na teren chroniony, na którym prowadzone są patrole pracowników ochrony. Przyjęcie regulacji ustanawiających obowiązek analizy adekwatności parametrów monitorowania mogłoby zapewnić wyeliminowanie tak zwanej nadmierności technologicznej — na przykład w postaci kamer o wysokiej rozdzielczości, rejestrujących barwny obraz i posiadających możliwości realizacji wielokrotnych zbliżeń obrazu w sposób mogący ingerować w intymność jednostki — w sytuacji, gdy nie da się tego usprawiedliwić kwestiami bezpieczeństwa ludzi i mienia. Oczywiście z punktu widzenia RODO administrator danych osobowych, stosując monitoring wizyjny pozwalający na przykład na utrwalenie znaków szczególnych lub obrazu wskazującego na stan zdrowia, może spotkać się z zarzutem przetwarzania danych osobowych w zakresie nieadekwatnym do celu, łamiąc przy tym wyrażoną w art. 5 ust. 1 lit. c RODO zasadę adekwatności i niezbędności. Zasadnym wydaje się jednak wprowadzenie do porządku prawnego odpowiedzialności karnej[35] oraz imperatywu dostosowania technologii monitorowania do właściwych celów związanych z realizacją nadzoru wizyjnego. Obawy dotyczące skutków stosowania nadmiernych technologii monitorowania wiążą się ściśle z możliwością wykorzystywania dynamicznie rozwijanych technologii bezzałogowych statków powietrznych (BSP), o których mowa w art. 3 pkt 1 rozporządzenia delegowanego Komisji (UE) 2019/945[36], które umożliwiają

systemu kontroli miejsca magazynowania lub składowania odpadów: „system kontroli zapewnia rejestrację obrazu obejmującą: […] 3) pas zewnętrzny otaczający magazynowane lub składowane odpady o szerokości 5 m, a w przypadku gdy podmiot obowiązany do prowadzenia systemu kontroli posiada tytuł prawny do pasa o szerokości mniejszej niż 5 m — pas zewnętrzny otaczający magazynowane lub składowane odpady w zakresie, w jakim podmiot obowiązany do prowadzenia systemu kontroli posiada tytuł prawny do tego pasa".

[35] Na temat sankcji zob. *Projekt założeń do projektu ustawy o monitoringu wizyjnym*, Rządowy Proces Legislacyjny, 7.07.2014, https://legislacja.rcl.gov.pl/docs//1/200701/200707/200708/dokument119053.pdf, (dostęp: 19.12.2022), dotyczący między innymi prowadzenia w sposób nieuprawniony monitoringu w otwartej przestrzeni publicznej, zamkniętej przestrzeni przeznaczonej do użytku publicznego lub przestrzeni prywatnej osób trzecich, dokonywania automatycznej identyfikacji osób w sposób nieuprawniony, udostępniania obrazu lub nagrań osobom nieupoważnionym, czy też wykonywania kopii nagrań w celach niezgodnych z przeznaczeniem.

[36] Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich (Dz.Urz.UE L 152/1 z 11.06.2019 r.) — dalej rozporządzenie delegowane.


© for this edition by CNS

skryte podejście oraz realizację nagrań wizyjnych o wysokiej jakości z odległości przekraczającej 150 m w poziomie od terenów mieszkaniowych, użytkowych, przemysłowych lub rekreacyjnych, w zasięgu widoczności wzrokowej pilota lub obserwatora w odległości nie większej niż 120 m od najbliższego punktu powierzchni ziemi[37]. Tymczasem prawodawca UE, mimo że zwraca uwagę na konieczność poszanowania prywatności w ramach operacji powietrznych z wykorzystaniem BSP, to w kontekście klasyfikowania operacji i posiadanych uprawnień do ich wykonywania posługuje się wagą i odległościami w ramach wykonywania tych operacji przez BSP od zgromadzeń ludzi, terenów mieszkaniowych, użytkowych, przemysłowych lub rekreacyjnych, co w kontekście miniaturyzacji i jakości podzespołów optycznych użytych do budowy nawet konsumenckich BSP i związanych z tym zagrożeń dla prywatności przestaje mieć znaczenie.

Przyjęcie w zakresie prowadzenia monitoringu wizyjnego regulacji o charakterze systemowym mogłoby zapewnić wzmocnienie instrumentów służących gwarancji przestrzegania konstytucyjnych wolności i praw, przy jednoczesnym wdrożeniu skutecznych i wyważonych zasad stosowania nadzoru wizyjnego na rzecz zapewnienia bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia. Tymczasem z trudnych do zaakceptowania powodów proces prawotwórczy mający na celu przyjęcie regulacji rangi ustawowej dotyczącej monitoringu wizyjnego został zastopowany w 2014 roku i do tej pory prac nie wznowiono. Należy podkreślić, że niniejsze opracowanie, traktując problematykę monitoringu w szkołach i innych placówkach oświatowych nawet w sposób węzłowy, wskazuje na potencjalne wątpliwości i problemy interpretacyjne na gruncie przywołanych wcześniej regulacji.

## SELECTED ASPECTS OF THE FUNCTIONING OF VIDEO SURVEILLANCE IN LIGHT OF REGULATIONS CONCERNING SCHOOLS AND OTHER EDUCATIONAL INSTITUTIONS

Summary

The study discusses the functioning of video surveillance on the basis of the national legal order, in particular its strong fragmentation, which is one of the main problems related to its functioning. The paper presents a thesis that the fragmented scope of standards is a significant impediment for entities using this protection measure, but more importantly, it does not create a coherent whole, leaving, to some extent, unregulated issues, e.g. of protection of the rights of persons whose images are observed, registered or processed in a way that allows identification of their identity, including

[37] Parametr dotyczy warunków realizacji operacji powietrznych z użyciem BSP w kategorii otwartej w podkategorii A3, o której mowa w załączniku *Operacje z użyciem bezzałogowych systemów powietrznych w kategorii „otwartej" i „szczególnej"*, cz. A. *Operacje z użyciem bezzałogowych systemów powietrznych w kategorii „otwartej"* do rozporządzenia wykonawczego Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz.Urz.UE L 152/45 z 11.06.2019 r.) — dalej rozporządzenie wykonawcze.


© for this edition by CNS

persons staying in an open and enclosed space intended for public use, as well as the issue of the obligations of the administrator of monitoring used for private purposes, under which an open public space is subject to monitoring.

Work on the basis of a key analysis of regulations related to the functioning of video surveillance in schools and other educational institutions may give rise to further considerations on the complementarity of the legal order related to the use of video surveillance with the capabilities of these entities, shaped by the rapid development of information technologies.

Keywords: video surveillance, privacy protection, unmanned aerial vehicles, legal grounds for monitoring

## BIBLIOGRAFIA

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Kraków 1999.

*Informacja o wynikach kontroli. Funkcjonowanie miejskiego monitoringu wizyjnego (LLU — 4101-01-00/2013 nr ewid. 181/2013/P/13/154/LLU)*, Najwyższa Izba Kontroli, 1.05.2014, https://www.nik.gov.pl/kontrole/P/13/154/LKI/.

Litwiński P., [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych Komentarz*, red. P. Litwiński, Warszawa 2018.

*Projekt założeń do projektu ustawy o monitoringu wizyjnym*, Rządowy Proces Legislacyjny, 7.07.2014, https://legislacja.rcl.gov.pl/docs//1/200701/200707/200708/dokument119053.pdf.

Wezgraj J., *Monitoring wizyjny a ochrona danych osobowych – wymagania rodo, przepisy sektorowe oraz wytyczne UODO*, Wrocław 2019.

*Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego*, Archiwum Urzęd Ochrony Danych Osobowych, 15.06.2018, https://archiwum.uodo.gov.pl/pl/file/1200.

Wygoda K., *Art. 25. Domyślna ochrona danych*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.


© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.7

DARIUSZ WASIAK
ORCID: 0000-0001-6057-7475
Wyższa Szkoła Bankowa we Wrocławiu

# PREWENCYJNY MONITORING TRZEŹWOŚCI PRACOWNIKÓW. ZARYS PROBLEMATYKI

Abstrakt: Jak wskazuje projektodawca ustawy z dnia 7 czerwca 2022 roku o zmianie ustawy — Kodeks pracy oraz niektórych innych ustaw, podstawowym celem podjęcia próby zmodyfikowania obecnego systemu prawa pracy, jak i jego pochodnych (w szczególności w zakresie wykonywania umów innych niż w oparciu o prawo pracy) była potrzeba stworzenia podstaw prawnych dla pracodawcy do wprowadzenia i przeprowadzania przez niego prewencyjnej kontroli pracowników na obecność alkoholu lub środków działających podobnie do alkoholu w ich organizmach. Mowa tu o prewencji, która rozciąga się również na możliwość rozszerzenia zakresu monitorowania prywatnych zachowań pracowników, w tym wykonujących zadania w ramach umowy zlecenia lub o dzieło, w sferze objętej regulacją ustawy z dnia 26 października 1982 roku o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi. Dlatego też nowe uprawnienie może być realizowane wyłącznie po uprzednim wykazaniu przez pracodawcę niezbędności takich działań oraz zapewnieniu skutecznej ochrony określonym dobrom, jak i po efektywnym dopełnieniu obowiązków informacyjnych w tym zakresie. Realizacja danych uprawnień nie może bowiem w żadnym razie rodzić jakichkolwiek naruszeń godności oraz innych dóbr osobistych poddanego kontroli pracownika (w szerokim ujęciu), w tym również jego prawa na gruncie regulacji ochrony danych osobowych.

Słowa kluczowe: kontrola, trzeźwość, monitoring, prewencja, środki odurzające, prawo pracy, niezbędność, ochrona, dobra osobiste, prawo ochrony danych osobowych, bezpieczeństwo

## UWAGI WPROWADZAJĄCE

W polskim porządku prawnym, pomimo wielu, niekiedy skrajnie spornych wykładniczo poglądów i stanowisk doktryny, w tym przy udziale kancelarii prawnych[1], do dnia wejścia (planowanych na pierwszy kwartał 2023 roku) w życie zmian[2] nakreślonych projektem ustawy z dnia 7 czerwca 2022 roku o zmianie usta-

[1] Na przykład Rycak Kancelaria Prawa Pracy i HR, która głosiła, że pracodawcy mogą poddawać pracowników prewencyjnym badaniom na zawartość alkoholu w wydychanym powietrzu.

[2] Na potrzeby poczynionych tutaj rozważań przyjmuję, że projekt ustawy wejdzie w prezentowanym poniżej zakresie — Senat nie nakreśli zmian, które mogłyby zostać przyjęte przez Sejm.


© for this edition by CNS

wy — Kodeks pracy oraz niektórych innych ustaw[3], funkcjonowały systemowo ukształtowane normy umożliwiające pracodawcy w rozumieniu art. 3 k.p.[4] monitorowanie trzeźwości pracowników, czyli osób, o których mowa w art. 2 k.p.[5] Możliwości te są jednak wciąż znacząco ograniczone i, co gorsza, obarczone błędami systemowymi. Powyższe wynika wprost z obecnego brzemienia treści art. 17 ust. 1 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi[6], który w zderzeniu między innymi z art. 207 § 1 k.p.[7] w związku z art. $22^3$ k.p.[8], jak i art. 9 ust. 1–2 ogólnego rozporządzenia o ochronie danych 2016/679 — dalej RODO[9] — wprowadził zamęt wykładniczy.

Niemniej stoję na stanowisku, że dotychczas podejmowane przez pracodawców działania prewencyjne wobec pracowników w zakresie realizowania kontroli na obecność alkoholu lub środków działających podobnie do alkoholu w ich organizmach, które oparte są wyłącznie na treściach zawartych na przykład w regulaminie pracy, o którym mowa w art. 104 k.p.[10], są realizowane z naruszeniem obowiązującego systemu prawnego.

---

[3] Dalej jako projekt ustawy. Szerzej: Projekt ustawy o zmianie ustawy — Kodeks pracy i niektórych innych ustaw, Serwis Rzeczypospolitej Polskiej, 7.06.2022, https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy--kodeks-pracy-oraz-niektorych-innych-ustaw2 (dostęp: 10.12.2022).

[4] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2022 r. poz. 1510 ze zm.), dalej jako kodeks pracy. Artykuł 3 k.p. stanowi, że: „Pracodawcą jest jednostka organizacyjna, choćby nie posiadała osobowości prawnej, a także osoba fizyczna, jeżeli zatrudniają one pracowników".

[5] Artykuł 2 k.p. stanowi, że: „Pracownikiem jest osoba zatrudniona na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę".

[6] Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (tekst jedn. Dz.U. z 2021 r. poz. 1119 ze zm.), dalej jako ustawa o wychowaniu w trzeźwości. Artykuł 17 ust. 1 ustawy o wychowaniu w trzeźwości stanowi, że: „Kierownik zakładu pracy lub osoba przez niego upoważniona mają obowiązek niedopuszczenia do pracy pracownika, jeżeli zachodzi uzasadnione podejrzenie, że stawił się on do pracy w stanie po użyciu alkoholu albo spożywał alkohol w czasie pracy. Okoliczności stanowiące podstawę decyzji powinny być podane pracownikowi do wiadomości".

[7] Artykuł 207 § 1 k.p. stanowi, że: „Pracodawca ponosi odpowiedzialność za stan bezpieczeństwa i higieny pracy w zakładzie pracy. Na zakres odpowiedzialności pracodawcy nie wpływają obowiązki pracowników w dziedzinie bezpieczeństwa i higieny pracy oraz powierzenie wykonywania zadań służby bezpieczeństwa i higieny pracy specjalistom spoza zakładu pracy, o których mowa w art. $237^{11}$ § 2".

[8] Artykuł $22^3$ § 4 k.p. stanowi, że: „Przepisy § 1–3 stosuje się odpowiednio do innych form monitoringu niż określone w § 1, jeśli ich zastosowanie jest konieczne do realizacji celów określonych w § 1".

[9] Artykuł 9 ust. 1–2 RODO stanowi, że: „1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. 2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków […]".

[10] Artykuł 104 § 1 prawa pracy stanowi, że: „Regulamin pracy ustala organizację i porządek w procesie pracy oraz związane z tym prawa i obowiązki pracodawcy i pracowników".


© for this edition by CNS

Dlatego też przyjmuję, że wprowadzenie do polskiego systemu prawnego dopuszczalności realizowania przez pracodawcę prewencyjnych kontroli — badań pracowników pod kątem zawartości alkoholu lub środków działających podobnie do alkoholu jest procesem prowadzącym do jego uszczelnienia przepisów, w szczególności w zakresie prawa pracy. Z tych względów należy również przyjąć, że podjęte działania ustawodawcze rozszerzają także uprawnienie pracodawcy do monitorowania pracowników pod kątem ich stanu trzeźwości.

W tym bowiem zakresie istotę kontroli prewencyjnej należy utożsamiać z prowadzonym monitoringiem, którego celem jest niedopuszczenie do zagrożeń mogących być następstwem alkoholu lub środków działających podobnie do alkoholu. Stąd też zakres możliwości dotychczasowego monitoringu, bazującego wyłącznie na wynikach obserwacji zachowań pracownika lub grup pracowników (przy zaangażowaniu ludzkich zmysłów), rozszerza się o sztywny miernik informacyjny, który jest niewątpliwie wypadkową nowego uprawniania pracodawcy, jak i ewentualnej choroby pracownika, predyspozycji, indywidualnie sprofilowanego modelu spędzania wolnego czasu, czy też innych okoliczności i składowych, które mogły doprowadzić lub wpłynąć na poziom zawartości alkoholu w wydychanym powietrzu poddanego kontroli pracownika w ramach podjętej wobec niego kontroli prewencyjnej.

## 1. SYSTEMOWE ZALEŻNOŚCI

Istotą jeszcze nieprzyjętego projektu ustawy nie było tylko — jak podnosi projektodawca — uposażenie pracodawcy w uprawnienie do prewencyjnej kontroli swoich pracowników pod kątem zawartości alkoholu lub środków działających podobnie do alkoholu w ich organizmach. Nowe uprawnienie w zasadzie wyszło także poza system prawa pracy. Jego kształt prezentowany w projekcie ustawy uposaża pracodawcę w możliwość podejmowania przez niego działań prewencyjnych także wobec pracowników zewnętrznych. Co ważne, również wobec osób wykonujących zadanie u pracodawcy nie tylko w oparciu o prawo pracy u innego pracodawcy, ale również współpracujących w ramach relacji zleceniodawca–zleceniobiorca lub zamawiający–wykonawca. Projekt ustawy dopuszcza bowiem przeprowadzanie takich badań prewencyjnych również wobec osób, które realizują określone zadanie oparciu o umowę zlecenia lub umowę o dzieło.

Stąd też takie ujęcie zmian systemowych w projekcie ustawy należy uznać za istotne przede wszystkim z punktu widzenia samego pracodawcy, w szczególności takiego, który realizuje swoje zadania (misje biznesowe) nie tylko w oparciu o pracowników mu podległych, ale i innych — zewnętrznych. Patrząc bowiem pragmatycznie, każdy pracodawca jest obecnie bez mała bezsilny, w szczególności wobec pracowników zewnętrznych dopóty, dopóki nie wystąpi „alkoholowe”


© for this edition by CNS

naruszenie obowiązków wynikających z umów cywilnych czy też umów pracowniczych. Pracownicy ci nie są bowiem wprost ujęci w modelu kierunkowym możliwości bezpośredniego na nich oddziaływania przez pracodawcę poza zakresem zawartych umów biznesowych, w ramach których dojdzie między innymi do wyrządzenia szkody na rzecz pracodawcy, w tym w następstwie stanu po spożyciu alkoholu lub innego środka.

Powyższe zjawisko problemowe osadzone jest przede wszystkim w zakresie odniesień zawartych w art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi i jego konotacji systemowych z prawem pracy, czy też RODO, które niestety torują drogę do rozszerzania się wykazywanej w ten sposób luki prawnej[11]. W jej ramach zrodziły się bowiem różne konstrukcje interpretacyjne tegoż przepisu. Na pozór wydaje się, że przepis ten stanowi czytelny przekaz ustawodawcy. Wskazuje wszak jasno, że tylko

kierownik zakładu pracy lub osoba przez niego upoważniona mają obowiązek niedopuszczenia do pracy pracownika, jeżeli zachodzi uzasadnione podejrzenie, że stawił się on do pracy w stanie po użyciu alkoholu albo spożywał alkohol w czasie pracy. Okoliczności stanowiące podstawę decyzji powinny być podane pracownikowi do wiadomości.

Niestety w następstwie nie tyle samej luki, co raczej nadinterpretacji przepisów, nadal dochodzi do licznych, znacząco rozszerzających i niestety błędnych interpretacji przepisów, między innymi art. 52 § 2 pkt 1[12], art. 108[13], art. 207 § 1[14] k.p., w następstwie których wyrażano stanowiska wskazujące na dopuszczalność prewencyjnego badania pracowników pod kątem zawartości alkoholu w wydychanym powietrzu. Co więcej, stanowiska takie mogły wskazywać także na dopuszczalność prowadzenia takich badań w okolicznościach mogących naruszać godność i inne dobra pracownika.

Dlatego też stanowiska, które wskazywały na dopuszczalność prowadzenia badań prewencyjnych przez pracodawcę należy uznać nie tylko za błędne, ale i obarczone wysokim ryzykiem dokonania porad, których zakres oddziaływał niekorzystnie na pracodawcę. Nie zabezpieczały one bowiem interesu pracodawcy,

[11] Z założenia niecelowe działanie ustawodawcy.

[12] Ustawowo nakreślona możliwość rozwiązania przez pracodawcę umowy o pracę bez wypowiedzenia z winy pracownika w razie ciężkiego naruszenia przez pracownika podstawowych obowiązków pracowniczych.

[13] Ustawowo nakreślona możliwość nałożenia kary porządkowej, w tym pieniężnej, na pracownika za nieprzestrzeganie przez niego ustalonej organizacji i porządku w procesie pracy, przepisów bezpieczeństwa i higieny pracy, przepisów przeciwpożarowych, a także przyjętego sposobu potwierdzania przybycia i obecności w pracy oraz usprawiedliwiania nieobecności w pracy.

[14] Ustawowo nakreślony zakres obowiązków narzuconych na pracodawcę, za które ponosi odpowiedzialność. Do obowiązków tych ustawodawca zaliczył zapewnienie bezpieczeństwa i higieny pracy w zakładzie pracy, w tym ochronę zdrowia i życia pracowników przez zapewnienie im bezpiecznych i higienicznych warunków pracy przy odpowiednim wykorzystaniu osiągnięć nauki i techniki.


© for this edition by CNS

gdyż dopuszczały do działań pracodawcy z naruszeniem obowiązującego prawa[15]. Stanowiska te, w zderzeniu z wykładnią przepisów wskazujących na możliwe uzasadnienie dla takich badań, które ustawodawca zawarł w art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, wykluczają obecnie (do czasu wejścia w życie projektowanych zmian) model interpretacyjny zezwalający na prewencyjne badanie pracowników pod kątem ustalenia zawartości alkoholu w wydychanym powietrzu[16]. Żaden dotychczasowy przepis (do czasu przyjęcia projektu) nie dopuszcza możliwości prowadzania badań prewencyjnych pracowników pod kątem zawartości alkoholu lub środków działających podobnie do alkoholu[17]. Dlatego też każde dotychczasowe zachowanie pracodawcy, które było nacechowane wyłącznie działaniami prewencyjnymi, czyli działaniami podejmowanymi między innymi bez uprzedniego posiadania informacji uzasadniających możliwość ich podjęcia w zgodzie z ustawą o wychowaniu w trzeźwości, należy uznać na naruszenie obowiązujący w tym (obecnym) czasie, norm prawnych.

Nie można bowiem odczytywać na przykład wyroku Sądu Najwyższego z dnia 23 lipca 1987 roku[18] — *nota bene* mowa tu o wyroku, który stanowi podwalinę dla późniejszej linii orzeczniczej w okresie poprzedzających nowe uprawnienia nakreślone projektem ustawy — jako przesłanki przyzwalającej na realizowanie przez pracodawcę prewencyjnych kontroli w postaci badań pracowników pod kątem zawartości alkoholu. Samo przywołanie przez sąd w jego orzeczeniu, że wynikający z przepisów prawa oraz zasad współżycia społecznego obowiązek pracownika zachowania trzeźwości w czasie pracy należy do podstawowych obowiązków pracownika i ciąży na nim nie tylko wówczas, gdy wykonuje pracę w siedzibie pracodawcy, ale również gdy przebywa on w innym miejscu w czasie przeznaczonym na wykonywanie pracy, nie stanowi podstawy do uznania, że orzeczenie to uposaża pracodawcę w możliwość, jak i podstawę prawną do realizowania prewencyjnych badań, których celem jest ustalenie poziomu alkoholu w wydychanym powietrzu. Odmienne odczytywanie stać może w sprzeczności z treścią przepisów, a dokładniej przesłanek, po spełnieniu których takie badanie można przeprowadzić bez naruszania ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, jak i k.p.

[15] Można tutaj zaryzykować tezę, że w przypadku posiadania takiej opinii przez pracodawcę może on dochodzić od osoby ją sporządzającą zwrotu poniesionych kosztów za jej opracowanie, jak i żądania pokrycia swoich kosztów w przypadku sporów z pracownikiem lub innymi osobami, które doznały uszczerbku na dobrach w następstwie stosowania rozwiązań zawartych w takiej opinii.

[16] Tekst jedn. Dz.U. z 2021 r. poz. 1119 ze zm.

[17] Pomijam tutaj działania w zakresie prowadzenia prewencyjnych badań na zawartość alkoholu realizowane przez Policję przez dekadę, pomimo braku wyraźnych podstaw ku temu. Obecnie luka została już uszczelniona.

[18] Wyrok SN z 23 lipca 1987 r., I PRN 36/87, OSNC 1989, nr 2, poz. 32.


© for this edition by CNS

## 2. PRZESŁANKI MONITOROWANIA

Nie ulega wątpliwości, że nawet obowiązujące przepisy uzbrajają pracodawcę w sposobność obserwacji — monitorowania zachowań pracowników pod kątem weryfikacji ich zachowań, także w ramach funkcji kontrolnej, którą zobowiązany jest realizować każdy pracodawca względem swoim pracowników. Chodzi o weryfikację stanu, który mógłby wskazywać, że określony pracownik lub grupa pracowników dopuściła się spożycia alkoholu lub środka działającego podobnie do alkoholu. Wynika to wprost z przywołanego już art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, jak i przepisów prawa pracy.

Na ogół podstawy prawnej do takiego działania, a właściwie podstawy do przetwarzania danych przez pracodawcę, należy upatrywać w minimalnym zakresie nie tyle nakazu prawnego, co mogłoby wynikać z treści prawa pracy, ale w prawnie uzasadnionym interesie pracodawcy, o którym mowa w art. 6 ust. 1 lit. f RODO, którego źródłem jest art. $22^3$ § 4 k.p.[19] w związku z art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.

Oczywiście „interes" ten musi zostać zawsze uprzednio przez pracodawcę wykazany i wewnętrznie uregulowany, a zasady zagrożeń dla dóbr adekwatne do realnie występujących zagrożeń. Problem jednak zawsze pozostawał w realiach możliwości stosowania art. 9 ust. 1–2 RODO w przypadku ujawnienia pracownika, który może być „po spożyciu" według obserwacji pracodawcy. Tutaj zasadnym jednak było i jest nadal, aby podstaw prawnych upatrywać w pierwszej kolejności w art. 6 RODO — jako dbałości o bezpieczeństwo pracownika, którego identyfikacja następuje dopiero po uzasadnionej obserwacji. A zatem obserwacja ustanowiona powinna być na „dbałość" o bezpieczeństwo pracownika, a dopiero na kolejnym etapie na działania oparte na niezbędności potwierdzenia ustaleń w ramach działania w zasięgu art. 9 ust. 1–2 RODO.

Istotnym założeniem jest również to, że forma monitorowania określonych zachowań nie mogła/nie może być w mojej ocenie oparta na monitoringu wizyjnym[20], a wyłącznie na obserwacji prowadzonej przez (na przykład) przedstawicieli firmy ochroniarskiej czy przełożonych lub sprawności narzędzi, których poprawne działanie uzależnione jest od pełnej predyspozycji pracownika.

Oczywiście powyższe formy monitorowania powinny zostać przed ich wprowadzeniem uprzednio ocenione na podstawie wyników przeprowadzonej wstęp-

[19] Art. $22^3$ § 4 k.p. stanowi, że: „ Przepisy § 1–3 stosuje się odpowiednio do innych form monitoringu niż określone w § 1, jeśli ich zastosowanie jest konieczne do realizacji celów określonych w § 1" , czyli gdy jest to „niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwe użytkowanie udostępnionych pracownikowi narzędzi pracy".

[20] Oczywiście ewentualne nagrania z monitoringu mogą stanowić cześć materiału dowodowego na etapie ewentualnej późniejszej weryfikacji lub dowodzenia zaistniałego zdarzenia.


© for this edition by CNS

nej analizy[21] oraz późniejszej oceny skutków, o których mowa w art. 35 RODO[22] i opisane w dostępnych regulaminach lub instrukcjach przeznaczonych dla pracowników, z którymi pracodawca zobowiązany jest zapoznać pracownika[23]. Wyniki z obiektywnie i poprawnie zrealizowanego testu wagi w rozumieniu art. 35 RODO rzutować będą na dopuszczalność, jak i niezbędność prowadzenia powyższych działań.

Stąd też dokonanie przez pracodawcę lub jego przedstawicieli[24] oceny zachowań pracownika lub grup pracowników w oparciu o dane zebrane na podstawie ludzkich zmysłów, jak i przy wsparciu urządzeń wspomagających wykonywanie powierzonej pracy, w rozumieniu między innymi art. 215[25] i art. 216 k.p.[26] należy uznać za elementy realizowanego monitoringu trzeźwości pracowników.

## 3. USZCZELNIENIE SYSTEMU

Projektodawca podnosi, że zaprojektowane przez niego zmiany zorientowane są na:

1. określenie podstaw prawnych umożliwiających pracodawcy realizację prewencyjnych kontroli trzeźwości pracowników lub kontroli na obecność środków działających podobnie do alkoholu w ich organizmach, o ile pracodawca

[21] W rozumieniu art 24, art. 25 i art. 32 RODO, szerzej: *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. D. Dörre-Kolasa, Warszawa 2017.

[22] Artykuł 35 ust. 1 RODO stanowi, że: „Jeżeli dany rodzaj przetwarzania — w szczególności z użyciem nowych technologii — ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę". Szerzej: *Dokumentacja ochrony danych osobowych ze wzorami*, red. M. Jagielski, Warszawa 2019.

[23] Artykuł $22^3$ § 3 kodeksu pracy stanowi, że: „Przepisy art. $22^2$ § 6–10 stosuje się odpowiednio".

[24] Na przykład firma ochrony, której powierzono zadania związane z zapewnieniem ochrony mienia pracodawcy.

[25] Artykuł 215 § 1 k.p. stanowi, że: „Pracodawca jest obowiązany zapewnić, aby stosowane maszyny i inne urządzenia techniczne: 1) zapewniały bezpieczne i higieniczne warunki pracy, w szczególności zabezpieczały pracownika przed urazami, działaniem niebezpiecznych substancji chemicznych, porażeniem prądem elektrycznym, nadmiernym hałasem, działaniem drgań mechanicznych i promieniowania oraz szkodliwym i niebezpiecznym działaniem innych czynników środowiska pracy".

[26] Artykuł 216 k.p. stanowi, że: „§ 1. Pracodawca wyposaża w odpowiednie zabezpieczenia maszyny i inne urządzenia techniczne, które nie spełniają wymagań określonych w art. 215. § 2. W przypadku gdy konstrukcja zabezpieczenia jest uzależniona od warunków lokalnych, wyposażenie maszyny lub innego urządzenia technicznego w odpowiednie zabezpieczenia należy do obowiązków pracodawcy".


© for this edition by CNS

jest w stanie wykazać niezbędność ich przeprowadzania w związku z ochrony określonych dóbr;

2. określenie zasad przeprowadzania takich kontroli, co uczynił zarysowo w projekcie rozporządzenia Ministra Zdrowia w sprawie badań na obecność alkoholu lub środków działających podobnie do alkoholu w organizmie pracownika[27];

a) utrzymanie regulacji obecnie obowiązującej w przypadku uzasadnionego podejrzenia, że pracownik stawił się do pracy w stanie po użyciu alkoholu lub spożywał alkohol w czasie pracy,

b) wprowadzenie regulacji nakładającej na pracodawcę taki obowiązek w przypadku uzasadnionego podejrzenia, że pracownik stawił się do pracy w stanie po użyciu środka działającego podobnie do alkoholu lub zażywał taki środek w czasie pracy,

c) wprowadzenie regulacji nakładającej na pracodawcę taki obowiązek w przypadku, gdy prewencyjna kontrola trzeźwości wykaże obecność alkoholu w organizmie pracownika lub prewencyjna kontrola na obecność środka działającego podobnie do alkoholu wykaże obecność takiego środka w organizmie pracownika;

3. określenie podstaw do przeprowadzania badania w celu ustalenia obecności alkoholu, wskazującej na stan po użyciu alkoholu albo stan nietrzeźwości, lub środka działającego podobnie do alkoholu w organizmie pracownika przez uprawniony organ powołany do ochrony porządku publicznego;

4. wprowadzenie możliwości odpowiedniego zastosowania wskazanych powyżej rozwiązań do pracodawców organizujących pracę wykonywaną przez osoby fizyczne na innej podstawie niż stosunek pracy oraz osoby prowadzące na własny rachunek działalność gospodarczą;

5. uzupełnienie katalogu przesłanek uzasadniających nałożenie na pracownika kary upomnienia, kary nagany lub kary pieniężnej o przypadki stawienia się do pracy w stanie po użyciu alkoholu lub środka działającego podobnie do alkoholu lub zażywanie takiego środka w czasie pracy[28].

Realizacja wymienionych powyżej celów nie tylko uszczelni system prawny w zakresie szeroko rozumianego prawa pracy, ale jak to już podkreślono, wyeliminuje, przynajmniej częściowo ryzyka generowane przez niewłaściwe stosowanie prawa ochrony danych osobowych, które nadal pozostaje podstawowym elementem możliwości prowadzenia prewencyjnych kontroli trzeźwości.

Nie można przy tym zarazem lekceważyć tego, że:

— możliwość nie jest tożsama z nakazem wykorzystywania uprawnień;

— wykazanie przez pracodawcę niezbędności korzystania z uprawnienia zawiera w sobie między innymi proporcjonalność i możliwość osadzoną w art. 35 RODO;

— pracodawca ma obowiązek dokonania selekcji pracowników;

[27] Projekt ustawy o zmianie ustawy — Kodeks pracy…

[28] *Ibidem*.


© for this edition by CNS

— zaistnieje niezbędność przeglądu upoważnień;

— zaistnieje niezbędność przeprowadzenia szkoleń;

— zaistnieje niezbędność przejrzenia umów cywilnych, systemów IT, jak i RCP oraz form przechowywania dokumentów;

— brak wykazania niezbędności wykorzystywania uprawnień jest tożsamy z brakiem możliwości działania na podstawie nowego uprawnienia;

— zaistnieje niezbędność zawarcia nowego uprawnienia w zakresie jego stosowania w regulaminie pracy;

— zaistnieje niezbędność zapewnienia działania w sposób zapewniający ochronę dóbr poddanych kontroli;

— firma ochrony działająca u pracodawcy może, ale nie musi prowadzić takich badań;

Wprawdzie nowe uprawnienie będzie mogło być stosowane zarówno wobec uprzednio wyselekcjonowanych pracowników, określonego pracodawcy (niezależnie od rodzaju umowy), jak i tak zwanych pracowników zewnętrznych (w ramach outsourcingu), to jednak nie wtedy, gdy dany pracodawca lub pracownik będzie chciał korzystać z przysługującego mu uprawnienia do ustalenia stanu faktycznego w zakresie poziomu zawartości alkoholu w wydychanym powietrzu, lecz dopiero wtedy, kiedy będzie on mógł je zastosować i wykorzystywać.

## 4. WNIOSKI

Usunięcie dotychczasowego problemu wynikającego z braku bezpośredniej normy, która umożliwia prowadzenie przez pracodawców działań zapobiegawczych zorientowanych na niedopuszczenie do podjęcia pracy przez ich pracowników już po przeprowadzeniu uprzednich (prewencyjnych) badań pod kątem ustalenia zawartości alkoholu lub środków działających podobnie do alkoholu w organizmach poddanych badaniu pracowników może stanowić pewne remedium na obecną bolączkę pracodawców. Z zastrzeżeniem, że przyjęcie zmian w zaprojektowanym zakresie najprawdopodobniej usunie w cień problemy, które były generowane właśnie z uwagi na brak wyraźnej podstawy prawnej do powyższych działań. Wydaje się, że dokonane zmiany powinny zminimalizować dotychczas występujące (liczne) nieprawidłowości i naruszenia, w tym na kanwie prawa ochrony danych osobowych, jak i praw i wolności, których źródłem potwierdzających jest zarówno Konstytucja RP oraz przepisy prawa cywilnego[29].

Z samej już bowiem obowiązującej jeszcze treści art. 17 ust. 1 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi wynika jasno, że badaniu na zawartość alkoholu w wydychanym powietrzu może zostać poddany

[29] W szczególności art. 23 ustawy z dnia 23 kwietnia 1971 r. — Kodeks cywilny (tekst jedn. Dz.U. z 2022 r. poz. 1360).


© for this edition by CNS

wyłącznie pracownik lub grupa pracowników, wobec których kierownik zakładu pracy lub osoba przez niego upoważniona podjęła uzasadnione podejrzenie, że stawili się oni do pracy w stanie po spożyciu alkoholu albo spożywali alkohol w czasie pracy[30]. Innymi słowy, należy przyjąć, że podstawą inicjującą możliwość przeprowadzenia takiego badania, jak i przetwarzania danych osobowych określonych pracowników stanowi (do czasu przyjęcia projektowanych zmian) wymóg niezbędności uprzedniego dokonania ustalenia, czy pracodawca lub osoba przez niego upoważniona dysponuje informacjami lub danymi, które uzasadniałyby podejrzenie, że pracownicy stawili się do pracy w stanie po spożyciu alkoholu albo spożywali alkohol w czasie pracy.

Paradoksalnie takie wstępne uzasadnienie pracodawca może uzyskać w ramach obserwacji (monitoringu) zachowań pracowników, tak przed przekroczeniem przez nich linii wejścia na teren zakładu pracy, jak i już na terenie samego zakładu lub w innym miejscu wykonywania przez nich pracy.

Nie można jednak przy tym zapominać, że badanie pod kątem ustalenia stanu trzeźwości pracownika może (do czasu przyjęcia projektowanych zmian) przeprowadzać wyłącznie uprawniony organ powołany do ochrony porządku publicznego na wyraźne żądanie kierownika zakładu pracy lub osoby przez niego upoważnionej lub też samego pracownika na jego żądanie.

Przy czym warto tutaj podkreślić, że pracodawca powinien uprzednio poinstruować takiego pracownika, chociażby w ramach organizowanych wewnętrznych szkoleń[31], w zakresie obowiązujących zasad ich przeprowadzana, z ujęciem istoty dobrowolności poddaniu się takim badaniom[32].

Ponadto wyrok Sądu Najwyższego z dnia 11 lutego 2000 roku wskazuje na model realizacji obowiązków pracodawcy w stosunku do pracownika, gdy ten stawi się do pracy w stanie nietrzeźwości, czyli w stanie, który wyklucza możliwość świadczenia przez niego pracy, jak i pozostawania przez niego w gotowości do jej świadczenia, a także nakreśla możliwy zakres działań pracodawcy[33].

[30] Artykuł 17 ust. 1 ustawy o wychowaniu w trzeźwości stanowi, że: „Kierownik zakładu pracy lub osoba przez niego upoważniona mają obowiązek niedopuszczenia do pracy pracownika, jeżeli zachodzi uzasadnione podejrzenie, że stawił się on do pracy w stanie po użyciu alkoholu albo spożywał alkohol w czasie pracy. Okoliczności stanowiące podstawę decyzji powinny być podane pracownikowi do wiadomości".

[31] Również przy uwzględnieniu obowiązków wynikających z treści art. 211 k.p.

[32] Artykuł 17 ust. 3 ustawy o wychowaniu w trzeźwości stanowi, że: „Na żądanie kierownika zakładu pracy, osoby przez niego upoważnionej, a także na żądanie pracownika, o którym mowa w ust. 1, badanie stanu trzeźwości pracownika przeprowadza uprawniony organ powołany do ochrony porządku publicznego. Zabiegu pobrania krwi dokonuje osoba posiadająca odpowiednie kwalifikacje zawodowe. Do badania stanu trzeźwości stosuje się przepisy, wydane na podstawie art. 47 ust. 2".

[33] Wyrok SN z 11 kwietnia 2000 r., I PKN 586/99, OSNP 2001, nr 18, poz. 556.


© for this edition by CNS

Należy przy tym pamiętać, że ukształtowane obecnie prawo ochrony danych osobowych[34], jako jeden z głównych „uczestników" każdego procesu, w ramach którego dochodzi do niezbędności wskazania przez pracodawcę podstaw przetwarzania danych osobowych wskazuje, że bez jego uwzględnienia dochodziło i dochodzić może nadal do naruszeń praw pracowników i innych osób.

Reasumując, projekt zmian ustawowych jest wyrazem praktycznych i niewątpliwie oczekiwanych zmian w zakresie uszczelnienia systemu, które dostrzec możemy między innymi w nowej odsłonie treści art. 17 ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi[35]. Obecne brzmienie tego przepisu należy bowiem uznać za nieefektywne. Jednakże zakładany przez projektodawcę efekt regulacji, mający zostać zobrazowany znaczącym spadkiem liczby przypadków, w których pracownicy wykonywaliby powierzone im przez pracodawcę zadania znajdując się w stanie po użyciu substancji, czy też środków, które negatywnie wpływają na jego sprawność psychofizyczną będzie znacząco mniejsze, jest formułowany raczej na wyrost. Tym samym założenia projektodawcy, że wprowadzone zmiany nie tylko uszczelnią system, ale i wpłyną na zwiększenie bezpieczeństwa pracowników, innych osób, jak i ochronę mienia, również są zbyt zachłanne, aczkolwiek słusznie zorientowane na ten cel.

Warto przy tym zauważyć, że nowe uprawnienie rozciąga się również na możliwość badania między innymi w miejscu zamieszkania, które objęte jest ochroną wynikającą z treści art. 193 kodeksu karnego[36], co już tworzy podwaliny do skrajnych interpretacji z uwagi na zderzenie się prawa do prywatności z prawem pracy w szerokim ujęciu. Pomimo tego, że nowe uprawnienie konotuje z zaprojektowanymi możliwościami realizowania przez pracownika pracy w sposób zdalny, jak i stanowiskiem sądu, że realizowanie przez pracownika obowiązku pozostawania w trzeźwości polega na przykład na pozostawaniu przez niego w gotowości do wykonywania pracy w stanie trzeźwości przez cały okres, w ramach którego pracodawca może oczekiwać (wymagać) świadczenia pracy[37].

---

[34] Stanowisko wynika z wykładni treści art. 9 ust. 1 RODO, który ustanawia główną zasadę przetwarzania danych wrażliwych, jakimi niewątpliwie są informacje pozyskiwane w ramach takich badań. Przy czym należy pamiętać, że aby móc przetwarzać dane wrażliwe, każdy pracodawca musi wykazać się w pierwszej kolejności podstawą przetwarzania danych zwykłych, które nakreślone są w treści art. 6 RODO.

[35] Zaprojektowany art. 17 ustawy o wychowaniu w trzeźwości zawarty w projekcie ustawy stanowi, że: „1. Przedsiębiorca niebędący pracodawcą organizujący pracę wykonywaną przez osoby fizyczne na innej podstawie niż stosunek pracy albo osoby fizyczne prowadzące na własny rachunek działalność gospodarczą może przeprowadzać kontrolę trzeźwości tych osób oraz kontrolę na obecność w ich organizmach środków działających podobnie do alkoholu. 2. W przypadkach, o których mowa w ust. 1, stosuje się odpowiednio art. $22^{1c}$–$22^{1f}$ ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2020 r. poz. 1320, z 2021 r. poz. 1162 oraz z 2022 r. poz. 655 i …) oraz przepisy wydane na podstawie art. $22^{1g}$ tej ustawy".

[36] Ustawa z dnia 6 czerwca 1997 r. — Kodeks karny (tekst jedn. Dz.U. z 2022 r. poz.1138 ze zm.)

[37] Wyrok SN z 23 lipca 1987 r., I PRN 36/87…


© for this edition by CNS

## PREVENTIVE MONITORING OF EMPLOYEE SOBRIETY: OUTLINE OF THE ISSUES

As stated by the drafters of the Act on Amendments to the Labor Code and Certain Other Acts of June 7, 2022, the primary purpose of the attempt to modify the current labor law system, as well as its derivatives (particularly in the performance of contracts other than under labor law) was the need to create a legal basis for the employer to introduce and carry out preventive monitoring of employees for the presence of alcohol or alcohol-like agents in their bodies. Preventive measure extend to the possibility of expanding the scope of monitoring the private behavior of employees, including those performing tasks under a civil law contract, in the sphere covered by the Act on Upbringing in Sobriety and Counteracting Alcoholism of October 26 1982. Therefore, the new entitlement can only be exercised after the employer has first demonstrated the necessity of such actions and the effective protection of certain goods, as well as the effective fulfillment of information obligations in this regard. Indeed, the exercise of the rights in question may not, under any circumstances, give rise to any violations of the dignity and other personal rights of the employee (in the broad sense) subjected to control, including his/her rights under data protection law.

Keywords: control, sobriety, monitoring, prevention, intoxicants, labor law, necessity, protection, personal rights, data protection law, security

## BIBLIOGRAFIA

*Dokumentacja ochrony danych osobowych ze wzorami*, red. D. Jagielski, Warszawa 2019.

*Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. D. Dörre-Kolasa, Warszawa 2017.


© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.8

KRZYSZTOF WYGODA
ORCID: 0000-0002-0997-5512
Uniwersytet Wrocławski

# DOPUSZCZALNOŚĆ PRZETWARZANIA DANYCH BIOMETRYCZNYCH PRZEZ PRACODAWCÓW — UJĘCIE MODELOWE I PRAKTYCZNE

Abstrakt: Artykuł jest próbą wskazania rozwiązań, które powinny być stosowane w ramach podejmowania przez pracodawców decyzji o przetwarzaniu danych biometrycznych. Łączenie przetwarzania danych biometrycznych z prowadzeniem monitoringu jest, na gruncie rozwiązań wynikających z RODO i prawa krajowego, niezwykle skomplikowane. Spełnienie wszystkich warunków koniecznych do legalizacji takiego procesu przetwarzania danych jest, przynajmniej co do zasady, możliwe jedynie w bardzo ograniczonej liczbie przypadków i każdorazowo wymaga indywidualnej analizy dopuszczalności. W orzecznictwie sądowym od niedawna podejmuje się próby reinterpretacji wcześniejszego, niezwykle restrykcyjnego podejścia do przetwarzania danych biometrycznych.

Słowa kluczowe: dane osobowe, dane biometryczne, minimalizacja danych

## UWAGI WPROWADZAJĄCE

Nie ulega wątpliwości, że każdy pracodawca, który przetwarza dane osobowe pracowników musi dostosować się nie tylko do wymogów płynących z kodeksu pracy[1] i innych norm prawa krajowego, ale również do standardów działania wynikających bezpośrednio z RODO[2].

Kolejnym aksjomatem jest uznanie pracodawcy za administratora w rozumieniu RODO — co nakłada na niego szereg obowiązków przypisanych mu w tym akcie, związanych z właściwym przygotowaniem i realizacją procesów przetwarzania danych osobowych.

[1] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn. Dz.U. z 2022 r. poz. 1510, 1700) — dalej k.p.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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 (ogólne rozporządzenie o ochronie danych).


© for this edition by CNS

Ostatnią uwagą, którą poczynić należy na wstępie, jest podkreślenie ograniczonej przydatności zgody[3] jako podstawy legalizacji procesów przetwarzania danych osobowych mających miejsce w ramach relacji pracodawca–pracownik. Zarówno doktryna, jak i orzecznictwo podkreślają

> brak równowagi sił pomiędzy pracodawcą a jego pracownikami, pracownicy mogą wyrazić dobrowolną zgodę wyłącznie w wyjątkowych okolicznościach, w których fakt wyrażenia lub niewyrażenia przez nich zgody nie pociąga za sobą żadnych negatywnych konsekwencji. Przymiot dobrowolności zakłada bowiem rzeczywistą możliwość dokonania wyboru przez osoby, których dane dotyczą, oraz sprawowania przez nie kontroli[4]

nad procesem, choćby poprzez możliwość jego zastopowania z uwagi na swobodę cofnięcia zgody w dowolnym momencie jego realizacji.

## 1. POJĘCIE DANYCH BIOMETRYCZNYCH

Zawarta w art. 4 pkt 14 RODO definicja danych biometrycznych wskazuje, że status ten uzyskają tylko takie informacje o pracowniku, które łącznie spełniają wskazane w tym przepisie warunki. Muszą być zatem takimi danymi osobowymi, które odnoszą się do określonych cech (fizycznych, fizjologicznych lub behawioralnych osoby fizycznej), na podstawie których, przy użyciu specjalnych metod technicznych, jest możliwa jednoznaczna identyfikacja osoby fizycznej lub potwierdzenie jej tożsamość. Użycie zwrotu „takie jak", poprzedzające wskazane w przepisie przykłady owych cech, jednoznacznie potwierdza, że nie mogą być one traktowane enumeratywnie, a jedynie jako najbardziej typowe czy najczęściej występujące (przynajmniej w ocenie prawodawcy). Pracodawca powinien zatem uznać, że cechy fizyczne i fizjologiczne, które będą umożliwiały identyfikację pracowników obejmować mogą na przykład linie papilarne, wygląd siatkówki lub tęczówki oka, twarzy, kształt małżowiny usznej, geometrię ręki, układ naczyń krwionośnych dłoni, głos i jego barwę. Z kolei cechy behawioralne to między innymi charakter pisma, dynamika pisania, sposób poruszania się, dialekt czy nawyki pracownika (również te odnoszące się do wykonywania zlecanych mu czynności)[5].

---

[3] Szerzej zob. np. M. Mazewski, *Prawo do wyrażenia i wycofania zgody na przetwarzanie danych*, [w:] *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 45–69.

[4] D. Dörre-Kolasa, *Pozyskiwanie danych osobowych osoby ubiegającej się o zatrudnienie i pracownika na podstawie przepisów KP*, [w:] *Ochrona danych osobowych w zatrudnieniu*, red. D. Dörre-Kolasa, Warszawa 2020, s. 81. Szerzej na ten temat zarówno we wskazanym opracowaniu, jak również A. Nerka, *Komentarz do art. 7*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 170–174.

[5] Zob. *Opinia 4/2017 w sprawie pojęcia danych osobowych, WP 136*, s. 13, European Commission, 20.06.2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf (dostęp: 3.01.2023).


© for this edition by CNS

Samo utrwalenie tego typu informacji (co w przypadku ich niektórych kategorii może mieć miejsce dość często — na przykład w związku z monitoringiem wizyjnym czy nagrywaniem rozmów) nie stanowi jednak problemu z punktu widzenia zakazu ich przetwarzania wynikającego z art. 9 RODO. Dzieje się tak, gdyż koniecznym składnikiem uznania, że mamy do czynienia z przetwarzaniem danych biometrycznych jest ich przetworzenie specjalnymi metodami technicznymi, pozwalającymi (co do zasady) na ich używanie w zautomatyzowanych systemach identyfikacyjnych (w przypadku cech behawioralnych, zamiast „prostego" mechanicznego porównania cech mogą być stosowane systemy oparte o sztuczną inteligencję, a co najmniej o samouczące się sieci neuronowe). To właśnie owo techniczne podejście do przetwarzania sprawia, że pojawiają się dane biometryczne, mimo że *de facto* dość często nie dochodzi do bezpośredniego utrwalenia samych cech czy ich pełnego obrazu, a jedynie do stworzenia czegoś w rodzaju cyfrowego wzorca porównawczego (na przykład cyfrowej mapy charakterystycznych punktów pojawiających się w liniach papilarnych czy wzorze siatkówki), który następnie służy jako profil używany przez system identyfikacji do wskazywania najlepszego dopasowania danych pojawiających się w czytniku kontrolnym z utrwalonym szablonem cech konkretnego pracownika. Można bez ryzyka pomyłki stwierdzić, że użycie metod technicznych do utrwalenia obrazu czy systemowego zapisu innych parametrów rzeczywistości, obejmujące utrwalenie pewnych cech osoby fizycznej, samo w sobie nie stanowi przetwarzania danych biometrycznych. Odnosząc się do założeń definicyjnych byłoby jedynie swego rodzaju zwykłym czy też standardowym przetwarzaniem technicznym, podczas gdy z art. 4 pkt 14 RODO wypływa konieczność podjęcia czynności mieszczących się w pojęciu „specjalnego przetwarzania technicznego" danych, które w pewnym uproszczeniu można utożsamić z dokonaniem stosownych pomiarów pozwalających na tworzenie wzorców czy profili służących do umożliwienia lub potwierdzenia jednoznacznej identyfikacji osoby fizycznej[6]. Przy czym bez realnego (lub choćby planowanego w późniejszym czasie) dokonywania owego specyficznego przetransponowania danych do postaci wzorców, służących następnie do dokonywania lub potwierdzania jednoznacznej identyfikacji, trudno mówić o przetwarzaniu danych biometrycznych. Zatem działanie monitoringu wizyjnego (nawet tego o wysokiej rozdzielczości) nie implikuje *per se* przetwarzania danych biometrycznych odnoszących się do wyglądu pracowników czy innych możliwych do zidentyfikowania przez administratora (pracodawcę) osób fizycznych. Dopiero użycie (lub co najmniej planowanie takiego wykorzystania) oprogramowania służącego do identyfikacji osób, które „wzbogaci" model i prawdopodobnie cel użу-

[6] Na te aspekty związane z wyjaśnieniem pojęcia danych biometrycznych zwraca również uwagę J. Rzymowski, *RODO — GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*, Łódź 2020, s. 541–552.


© for this edition by CNS

cia systemu monitorującego, da podstawę do stwierdzenia, że mamy do czynienia z przetwarzaniem danych biometrycznych w ramach monitoringu.

Systemy zapewniające zautomatyzowaną identyfikację powinny charakteryzować się jej wysoką skutecznością i być odporne na:

— możliwości pominięcia dokonania weryfikacji tożsamości (na przykład poprzez ominięcie bramki czy brak prawidłowego odczytu cech przez czytnik o zbyt niskiej czułości);

— występowanie nieprawidłowego rozpoznania konkretnej osoby lub brak jej rozpoznania (choćby z uwagi zbyt małą elastyczność sytemu, który w przypadku najmniejszej niezgodności z wzorcem wskazuje na brak identyfikacji, lub przeciwnie — w przypadku pokrycia się jedynie części cech dokonuje identyfikacji);

— niemożności sprawdzenia niektórych osób (choćby ze względów religijnych — zakrycie twarzy, czy zbyt słabą widoczność linii papilarnych).

Wszystko to sprawia, że procesy uwzględniające przetwarzanie danych biometrycznych wymagają uprzedniego przygotowania, co pozwala na pełne zastosowanie zasad wynikających ze stosowania art. 25 RODO i uwzględnienia zasad ochrony danych już na etapie ich projektowania, a następnie bieżącą kontrolę wdrożonego systemu w działaniu.

## 2. DANE BIOMETRYCZNE A MONITORING

Nie wchodząc w niuanse regulacji k.p. dotyczących możliwości stosowania monitoringu przez pracodawców[7], należy przyjąć dopuszczalność korzystania z tej formy przetwarzania danych osobowych. Oczywiście każdorazowe użycie monitoringu wizyjnego czy innych jego form wymaga uprzedniego przygotowania i spełnienia szeregu warunków wynikających zarówno z RODO, jak i k.p. (art. $22^2$–$22^3$ k.p.). Pracodawca, chcąc realizować swoje uprawnienia z tym związane, musi niejednokrotnie porzucić założenie jego szerokiego stosowania, gdyż nie zawsze da się to wystarczająco uzasadnić zarówno w kontekście celowości, jak i niezbędności przetwarzania. Należy bowiem pamiętać, że z uwagi na znaczącą ingerencję w prawa osób monitorowanych (zwłaszcza w prywatność) jego stosowanie (zarówno w formie monitoringu wizyjnego, jak i występującego w innej postaci) co do zasady nie jest uzasadnione nadrzędnym interesem administratora, szczególnie jeżeli cel jego zainstalowania nie jest wystarczająco konkretny. W przypadku pracodawców jest to dodatkowo limitowane wskazaniami wynikającymi z art. $22^2$ § 1 i $22^3$ § 1 k.p, które przedmiotowo zawężają zakres celów

[7] Na temat warunków i zasad stosowania monitoringu zob. np.: D. Dörre-Kolasa, *Monitoring,* [w:] *Ochrona danych w zatrudnieniu*, s. 169–204; J. Wezgraj, *Monitoring wizyjny a ochrona danych osobowych. Wymagania rodo, przepisy sektorowe oraz wytyczne UODO*, Wrocław 2019; D. Dörre-Kolasa, *Ochrona danych osobowych pracowników*, [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2022, s. 827–858.


© for this edition by CNS

uzasadniających wprowadzenie monitoringu. Powstaje więc pytanie, czy z uwagi na zakaz przetwarzania danych osobowych szczególnych kategorii włączenie w proces monitoringu przetwarzania danych biometrycznych jest w ogóle możliwe, a jeśli tak, to jaka przesłanka legalizująca takie działanie może być brana pod uwagę przez pracodawców.

Pozytywna odpowiedź na tak postawione pytania, przy uwzględnieniu uwarunkowań działalności pracodawców wynikających z niewątpliwego zawężania dopuszczalnego zakresu przetwarzanych przez nich kategorii danych pracowniczych, wynikającego z kolei z samego k.p., wydaje się dość mało prawdopodobna, nie można jej jednak całkowicie wykluczyć. Zwłaszcza w jednostkowych przypadkach pracodawców (administratorów), których specyfika działalności (wymagająca szczególnej dbałości o ograniczenia dostępu do określonych obszarów, zasobów czy informacji) może teoretycznie uzasadniać sięganie po dane biometryczne jako informacje wspierające kontrolę dostępu (w aspekcie uzyskiwania wysokiego stopnia pewności co do tożsamości, a zatem i posiadanych uprawnień przez konkretnych pracowników).

Prowadząc analizę we wskazanym wyżej kontekście, należy jeszcze raz podkreślić, że wprowadzenie monitoringu przez pracodawcę wymaga, by dostosował się on do rozwiązań wynikających z k.p. Co prowadzi do wniosku, że pracodawca musi ograniczyć się nie tylko do katalogu celów uzasadniających wprowadzenie monitoringu w prawie pracy, ale również skorelować to z celami wynikającymi pośrednio z art. 9 ust. 2 RODO — tam bowiem zawarte zostały wskazania pozwalające ograniczyć działanie zakazu przetwarzania danych biometrycznych[8]. Należy dodatkowo podkreślić, że w sytuacji korzystania z rozwiązań obejmujących użycie danych biometrycznych pojawi się dodatkowy problem kwalifikacji prawnej stosowanego monitoringu.

W przypadku wprowadzenia warstwy biometrycznej do działania systemów rejestrujących obrazy trudno będzie uznać ową hybrydę za zwykły monitoring

[8] Spośród wielu przesłanek uchylających zakaz przetwarzania tych danych, ujętych w art. 9 ust. 2 RODO, w omawianym kontekście największe możliwości dają pracodawcom cztery: „a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1; b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą; […] f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy; g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą”.


© for this edition by CNS

wizyjny (nawet jeśli rozpoznawanie cech biometrycznych i identyfikacja osoby będzie oparta wyłącznie na obrazie rejestrowanym przez kamery). Z kolei użycie specjalistycznych czytników rejestrujących/odczytujących cechy biometryczne już jednoznacznie przenosi nas do „innych form monitoringu" — co teoretycznie może dodatkowo zawężać swobodę wyboru celu dla tego typu procesu przetwarzania danych. Należy jednak zaznaczyć, że tylko szczegółowa analiza konkretnego przypadku pozwoliłaby na rozstrzygnięcie, czy mamy do czynienia z odrębnymi procesami przetwarzania danych (monitoringiem i przetwarzaniem danych biometrycznych), czy z jednym procesem bazującym na przetwarzaniu danych zwykłych i szczególnych kategorii.

Reasumując: pracodawca, który zamierza wprowadzić tego rodzaju rozwiązanie, musi bardzo ostrożnie definiować rzeczywisty cel przetwarzania — nie naruszając wiążących go norm k.p. dotyczących możliwości wdrożenia szczególnych form monitoringu (zarówno w przypadku rozszerzonego o warstwę biometryczną monitoringu wizyjnego, jak i stosowania specjalnych czujników i czytników w celach monitorowania pracowników), lub starać się odrębnie zdefiniować równoległe procesy monitorowania i przetwarzania danych biometrycznych. Przy czym z uwagi na fakt, że przetwarzane mają być dane z kategorii szczególnych, warto zbadać, czy tych samych celów nie można osiągnąć w inny — mniej ingerujący w prywatność — sposób, przy którym nie będzie konieczne przetwarzanie danych biometrycznych. Przeprowadzenie oceny ryzyka bądź analizy konieczności przetwarzania tej szczególnej kategorii danych warto oprzeć (o ile to oczywiście możliwe) na dotychczasowych działaniach podejmowanych przez administratora. W przypadku wykazania, że wcześniej stosowane środki nie gwarantowały odpowiednio wysokiego poziomu realizacji założonego celu przetwarzania, sięgnięcie po dane biometryczne może okazać się dopuszczalne (o ile sam proces uda się to odpowiednio „zalegalizować") zarówno z punktu widzenia zasady celowości, jak i minimalizacji.

## 3. UŻYCIE DANYCH BIOMETRYCZNYCH — WĄTPLIWOŚCI WYNIKAJĄCE Z ORZECZNICTWA

Jak wskazano wyżej, samo wprowadzenie przez pracodawcę monitoringu nie wydaje się być szczególnie trudne — choć bez wątpienia wymaga spełnienia kilku warunków formalnych i materialnych, które definiowane są zarówno w RODO, jak i bezpośrednio w k.p. Warunki owe odnoszą się jednak nie tylko do uzyskania podstawy legalizującej proces przetwarzania (spośród wskazanych w art. 6 i 9 RODO — odrębnie dla danych zwykłych i uzupełniająco do danych szczególnych kategorii), ale również realizacji procesu w zgodzie

z zasadami ustanowionymi w art. 5 ust. 1 RODO, które — co należy wyraźnie podkreślić — odgrywają szczególną rolę wśród norm prawnych dotyczących ochrony danych osobowych zawar-


© for this edition by CNS

tych w RODO. Przyjmuje się bowiem, że zasady te nie są jedynie postulatami odczytywanymi z całokształtu przepisów o ochronie danych osobowych, ale mają wręcz charakter normatywny — są wiążącymi normami prawa, wyznaczającymi określony sposób postępowania, mając szczególne znaczenie dla stosowania i interpretacji przepisów o ochronie danych osobowych[9].

To właśnie te reguły postrzegane są jako główna przeszkoda we wdrożeniu przetwarzania danych biometrycznych przez pracodawcę (tym bardziej, jeśli ma to być powiązane z monitoringiem). Wiąże się to z ustaleniami, które poczyniono na kanwie wcześniej obowiązujących przepisów dotyczących ochrony danych osobowych.

Zarówno dyrektywa 95/46/WE[10], jak i ustawa o ochronie danych osobowych z 1997 roku[11] zawierały podobne (choć, co należy podkreślić, nietożsame) rozwiązania prawne, ale orzecznictwo pochodzące z tamtego okresu do dziś traktowane jest jako znacząca wskazówka służąca ocenie dopuszczalności przetwarzania danych biometrycznych. Dotyczy to w szczególności wyroku NSA z 1 grudnia 2009 roku[12], którego główne tezy wskazują, że:

— ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności (wyrażona w art. 26 ust. 1 pkt 3 uodo97) jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania;

— uznanie faktu wyrażenia przez pracownika zgody na przetwarzanie jego danych (na gruncie art. 23 uodo97) za okoliczność legalizującą pobranie od pracownika innych danych niż wskazane w art. $22^1$ k.p. stanowiłoby naruszenie tegoż przepisu, gdyż powoduje jego obejście. Sama wyrażona na prośbę pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych, narusza prawa pracownika i swobodę wyrażenia przez niego woli;

— wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania (w rozumieniu art. 26 ust. 1 pkt 3 uodo97).

Takie podejście powinno jednak zostać (przynajmniej częściowo) zrewidowane w związku z przeformułowaniem zasad przetwarzania wyrażonych w art. 5

[9] Wyrok WSA w warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20, CBOSA (dostęp: 3.01.2023); z powołaniem na P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

[10] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, 23.11.1995, OJ 281/31, dalej: dyrektywa 95/46/WE.

[11] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2016 r. poz. 922. ze zm. — dalej: uodo97).

[12] Wyrok NSA z dnia 1 grudnia 2009 r., I OSK 249/09, CBOSA (dostęp 3.01.2023).


© for this edition by CNS

RODO — a zwłaszcza zasady „minimalizacji danych”[13]. Obowiązek jej stosowania bez wątpienia dotyczy administratora. Jak słusznie zauważa Arwid Mednis, jest on

niezależny od legitymowania się przesłanką legalności przetwarzania danych. Dotyczy to również przetwarzania danych osobowych na podstawie zgody. Innymi słowy, administrator przetwarzający dane na podstawie pozyskanej zgody jest nadal zobowiązany do przestrzegania zasady minimalizacji danych. Nie ulega również wątpliwości, że zasada ta, podobnie jak pozostałe wymienione w art. 5 RODO, ma charakter normatywny i jest samoistnym obowiązkiem nałożonym na administratora[14].

Należy podkreślić, że termin „minimalizacja danych” stanowi skrótowe (zaproponowane przez samego prawodawcę unijnego) określenie zasady w myśl której dane osobowe używane w procesie przetwarzania muszą być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane” (art. 5 ust. 1 lit. c RODO). Warto przy tym odnotować stanowisko WSA w Warszawie, który wskazuje, że

określenie „adekwatne” oznacza „odpowiednie, zgodne, proporcjonalne, nienadmierne” i może być traktowane jako synonim słowa „stosowne”. Adekwatność i stosowność rozumieć można jako konieczność zachowania odpowiednich proporcji zakresu danych do celów przetwarzania i przetwarzanie tylko takich danych, które są potrzebne dla realizacji określonych celów. […]

Niemniej jednak, co trzeba wyraźnie podkreślić, odczytywanie z analizowanego przepisu normy nakazującej ograniczenie danych jedynie do niezbędnego minimum i przetwarzanie tylko takich danych, bez których nie da się osiągnąć celu […], uznać należy za interpretacją zbyt daleko idącą. […]

Zdaniem Sądu, wymóg niezbędności należy odczytywać łącznie z wymogiem adekwatności i stosowności, co powinno pozwolić na uwzględnienie okoliczności i dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania[15].

Takie podejście pozwala nieco odejść od literalnego traktowania wymogów adekwatności i minimalizacji — w którym adekwatność sprowadza się do oceny przydatności (nieodzowności) występowania określonego rodzaju danych na drodze realizacji celu założonego w procesie przetwarzania, natomiast minimalizacja prowadzi do uznania, że jeśli taki założony cel można osiągnąć bez przetwarzania określonego rodzaju danych, to nie należy takich danych przetwarzać. W tym miejscu warto powołać się na podsumowanie dokonane przez A. Mednisa (którego dokonał na kanwie glosowanego orzeczenia II SA/Wa 809/20) wskazujące, że:

sąd przyznaje w uzasadnieniu, że wymogi minimalizacji i adekwatności nie są ze sobą spójne, a ich spełnienie należy oceniać łącznie, co w konsekwencji oznacza, że „nie powinno się przyznawać prymatu minimalizacji kosztem adekwatności”. Jednocześnie podkreśla, jak ważne są okoliczności konkretnej sprawy […]. Słusznie sąd odrzuca sugestię PUODO, że dane biometryczne mogą być

[13] Szerzej na temat zasady minimalizacji poza wskazanymi już publikacjami komentarzowymi zob. P. Drobek, *Komentarz do art. 5*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz ,Warszawa 2018, s. 322–344.

[14] A. Mednis, *Wykorzystanie danych biometrycznych w szkole. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20*, „Gdańskie Studia Prawnicze” 25, 2021, nr 4 (52), s. 134.

[15] Wyrok WSA w Warszawie z 7 sierpnia 2020 r., II SA/Wa 809/20, CBOSA (dostęp: 3.01.2023).


© for this edition by CNS

wykorzystywane tylko wyjątkowo, i to w takich celach, jak np. bezpieczeństwo osobowe, przemysłowe czy ochrona informacji itp. Takie ograniczenie znikąd bowiem nie wynika. Oczywiste jest, że sięganie po dane biometryczne jest daleko idącą ingerencją w sferę prywatności, niemniej nie oznacza to, że […] ich użycie będzie niedopuszczalne niezależnie od okoliczności. Słusznie zatem sąd, biorąc pod uwagę okoliczności sprawy, dopuścił możliwość weryfikacji biometrycznej[16].

## ADMISSIBILITY OF BIOMETRIC DATA PROCESSING BY EMPLOYERS: MODEL AND PRACTICAL APPROACH

Summary

The article is an attempt to indicate solutions that should be used as part of employers' decisions on the processing of biometric data. Combining the processing of biometric data with monitoring is, on the basis of the solutions resulting from the GDPR and national law, extremely complicated. Meeting all the conditions necessary to legalize such a data processing process is, at least in principle, possible only in a very limited number of cases and each time requires an individual admissibility analysis. In judicial decisions, attempts have been made recently to reinterpret the previously extremely restrictive approach to the processing of biometric data.

Keywords: personal data, biometric data, data minimization

## BIBLIOGRAFIA

Dörre-Kolasa D., *Ochrona danych osobowych pracowników*, [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2022.

Dörre-Kolasa D., *Pozyskiwanie danych osobowych osoby ubiegającej się o zatrudnienie i pracownika na podstawie przepisów KP*, [w:] *Ochrona danych osobowych w zatrudnieniu*, red. D. Dörre-Kolasa, Warszawa 2020.

Drobek D., *Komentarz do art. 5*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz Warszawa 2018.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Mazewski M., *Prawo do wyrażenia i wycofania zgody na przetwarzanie danych*, [w:] *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017.

Mednis A., *Wykorzystanie danych biometrycznych w szkole. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20*, „Gdańskie Studia Prawnicze" 25, 2021, nr 4 (52).

Nerka A., *Komentarz do art. 7*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.

*Opinia 4/2017 w sprawie pojęcia danych osobowych, WP 136*, European Commission, 20.06.2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf.

Rzymowski J., *RODO — GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*, Łódź 2020.

Wezgraj J., *Monitoring wizyjny a ochrona danych osobowych. Wymagania rodo, przepisy sektorowe oraz wytyczne UODO*, Wrocław 2019.

[16] A. Mednis, *Wykorzystanie danych biometrycznych w szkole…*, s. 135.


© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

# KONTROLA I NADZÓR NAD STOSOWANIEM MONITORINGU

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.9

PRZEMYSŁAW CZECHOWSKI
ORCID: 0009-0002-4771-4134
Główny Inspektorat Pracy w Warszawie

# ROLA INSPEKTORA PRACY W KONTROLI I NADZORZE STOSOWANIA MONITORINGU PRZEZ PRACODAWCĘ — WNIOSKI *DE LEGE LATA* I *DE LEGE FERENDA*

Abstrakt: Z uwagi na stosunkowo krótki okres obowiązywania przepisów regulujących kwestie dotyczące monitoringu u pracodawcy, problematyka związana z nadzorem i kontrolą tej sfery działań nie była dotąd szerzej poruszana w literaturze przedmiotu. Autor dokonuje analizy przedmiotowych przepisów pod kątem możliwości i zakresu kontroli ich przestrzegania przez organy Państwowej Inspekcji Pracy. W ramach prowadzonych rozważań przedstawia rodzaje środków prawnych możliwych do zastosowania w przypadku stwierdzenia przez inspektora pracy naruszeń przepisów związanych ze stosowaniem monitoringu oraz wątpliwości z tym związane. Zaprezentowane zostają również wnioski *de lege ferenda* mające na celu szybsze wyeliminowanie pojawiających się na tym polu nieprawidłowości oraz skuteczniejsze przeprowadzenie kontroli.

Słowa kluczowe: Państwowa Inspekcja Pracy, monitoring, pracodawca, kontrola, środki prawne

## WPROWADZENIE

Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz.U. z 2019 r. poz. 1871), obowiązująca od dnia 25 maja 2018 roku, za sprawą artykułu 111 wprowadziła do kodeksu pracy[1] przepisy dotyczące ramowych zasad monitorowania pracowników, to jest regulację monitoringu wizyjnego, kontroli służbowej poczty elektronicznej, a także innych, niewymienionych wprost w przepisach form monitoringu (na przykład GPS, monitoring aktywności w Internecie itp.). Jak wskazywano na etapie prac legislacyjnych, dotychczasowe stosowanie monitoringu pracowników w różnych formach odbywało się pomimo braku wyraźnej do tego podstawy, natomiast wprowadzone regulacje w postaci art. $22^2$ i $22^3$ k.p. miały przede wszystkim na celu zabezpieczenie interesu pracowników przed dowolnym korzystaniem przez pracodawców z różnych rodzajów monitoringu[2].

[1] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz.U. z 2022 r. poz. 1510 ze zm.

[2] *Pełny zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych (nr 153) oraz Komisji Sprawiedliwości i Praw Człowieka (nr 139)*, s. 20-21, Sejm Rzeczpospolitej Polskiej,


© for this edition by CNS

Treść dodanego przepisu art. $22^2$ k.p. została następnie zmieniona z dniem 4 maja 2019 roku, w którym wprowadzono w życie ustawę z dnia 21 lutego 2019 roku o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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)[3]. Ponadto swego rodzaju inspiracją dla wprowadzenia wyżej wymienionych przepisów do kodeksu pracy było RODO, w którego art. 88 europejski prawodawca, uwzględniając specyfikę przetwarzania danych osobowych w kontekście zatrudniania, przewidział możliwości wprowadzenia przez państwa członkowskie szczegółowych przepisów dotyczących przetwarzania danych osobowych w związku z zatrudnianiem, mających zapewnić ochronę praw i wolności pracowników. Na gruncie tego przepisu przedmiotowe regulacje mogą być zawarte nie tylko w przepisach prawa powszechnie obowiązującego, ale również w porozumieniach zbiorowych. Takie przepisy 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 oraz systemów monitorujących w miejscu pracy.

Przytaczana ustawa o ochronie danych osobowych wprowadziła tym samym do polskiego systemu prawnego regulacje szczególne, które dotychczas nie były skodyfikowane, aczkolwiek w różnym kształcie przyjmowane i stosowane przez pracodawców na podstawie przepisów wewnątrzzakładowych, tudzież w sformalizowanych poleceniach[4] (takich jak okólniki, instrukcje, zarządzenia, procedury). Brak było bowiem w przepisach powszechnie obowiązujących wyrażonego wprost wymogu prawnej regulacji monitoringu w miejscu pracy. Zatem dodanie do przepisów kodeksu pracy regulacji zawierających ramy dla legalnego stosowania monitoringu w miejscu pracy, postulowane wcześniej w doktrynie, przyczyniło się także do wzmożenia ochrony pracowników przed ewentualnymi naruszeniami w tym zakresie[5]. Sam fakt umiejscowienia przepisów regulujących kwestie monitorowania pracowników w kodeksie pracy dał bezpośrednią podstawę dla nadzoru i kontroli przestrzegania tych przepisów przez Państwową Inspekcję Pracy. Zgodnie bowiem z art. 1 i 10 ust. 1 pkt 1 ustawy z dnia 13 kwietnia 2007 roku

22.05.2018, https://orka.sejm.gov.pl/zapisy8.nsf/0/54CE289919420564C125829500438DA7/%24File/0309308.pdf (dostęp: 20.09.2022). Należy zauważyć, że pierwotna wersja projektu tej ustawy nie zawierała tych rozwiązań, a pojawiły się one w art. 110a projektu ustawy.

[3] Dz.U. z 2019 r. poz. 730; Dz.Urz. UE L 119 z 4.05.2016 r., dalej jako RODO.

[4] Zob. G. Orłowski, *Nielegalny legalny monitoring*, „Monitor Prawa Pracy" 2018, nr 7, s. 7.

[5] O celowości wprowadzenia regulacji pisze między innymi P. Czechowski, *Geolokalizacja pracowników — nowe wyzwania dla prawa pracy?*, „Praca i Zabezpieczenie Społeczne" 2006, nr 4, s. 10–11.


© for this edition by CNS

o Państwowej Inspekcji Pracy[6], do zadań Państwowej Inspekcji Pracy należy nadzór i kontrola przestrzegania przepisów prawa pracy, w szczególności przepisów i zasad bezpieczeństwa i higieny pracy, przepisów dotyczących stosunku pracy itp.

Kodeks pracy, jako podstawowy akt prawny regulujący stosunki pracy, w art. 9 § 1 k.p. wyjaśnia zakres desygnatów pojęcia „prawo pracy" użytego w tej ustawie wskazując, iż ilekroć w kodeksie pracy jest mowa o prawie pracy, rozumie się przez to przepisy kodeksu pracy oraz przepisy innych ustaw i aktów wykonawczych określające prawa i obowiązki pracowników i pracodawców, a także postanowienia układów zbiorowych pracy i innych opartych na ustawie porozumień zbiorowych, regulaminów i statutów określających prawa i obowiązki stron stosunku pracy. Przy czym w myśl § 2 art. 9 k.p. postanowienia układów zbiorowych pracy i porozumień zbiorowych oraz regulaminów i statutów nie mogą być mniej korzystne dla pracowników niż przepisy kodeksu pracy oraz innych ustaw i aktów wykonawczych. W tym zakresie obowiązywał dotychczas przepis art.$11^1$ k.p. stanowiący, że pracodawca jest obowiązany szanować godność i inne dobra osobiste pracownika. Z treści tego przepisu wyprowadzano między innymi obowiązek pracodawcy poszanowania prawa do prywatności. Z kolei podstawy dla stosowania różnych form monitoringu upatrywano w treści art. 22 § 1 k.p. Pracownik jest bowiem zobowiązany do wykonywania pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem.

To właśnie dążenie do zapewnienia efektywnego kierownictwa wiązało się z potrzebą stosowania monitoringu pracowników. Brak stosownych regulacji w praktyce pozbawiał organy Państwowej Inspekcji Pracy realnego wpływu na sam fakt i kształt stosowanych przez pracodawców różnych rozwiązań w tym zakresie. Stąd przyjęcie nowej regulacji w kodeksie pracy otworzyło drogę dla możliwości korygowania działań pracodawców w tym obszarze i eliminowania ewentualnych nieprawidłowości, tym samym zapewniając skuteczniejszą ochronę pracownikom poddanym monitorowaniu w ramach świadczenia pracy. Przepis art. $18^4$ § 1 k.p. stanowi bowiem wprost, że nadzór i kontrolę przestrzegania prawa pracy, w tym przepisów i zasad bezpieczeństwa i higieny pracy, sprawuje Państwowa Inspekcja Pracy, pozostając w tym względzie w korelacji z przepisami statuującymi funkcjonowanie i zadania Państwowej Inspekcji Pracy.

W związku z dodaniem przepisów art. $22^2$ i $22^3$ k.p. mogą jednak rodzić się pytania o rolę i zakres uprawnień inspektora pracy przeprowadzającego kontrolę u pracodawcy w zakresie stosowanego monitoringu[7]. Czy działanie inspektora pracy w tym zakresie może być skuteczne? Jaką formę prawną mogą przybierać stosowane przez organ Państwowej Inspekcji Pracy środki? Czy na tym polu nie

[6] Dz.U. z 2022 r. poz. 1614, dalej jako ustawa o PIP.

[7] Dodatkowo na trudności interpretacyjne w związku z brakiem konsekwencji w operowaniu przez ustawodawcę pojęciem „monitoringu" zwraca uwagę Magdalena Kuba: M. Kuba, *Monitoring pracowników na gruncie KP*, „ABI Expert" 2019, nr 3, s. 22–23 oraz M. Kuba, [w:] *Kodeks pracy. Komentarz*, t. 1. *Art. 1–93*, red. K.W. Baran, Warszawa 2022, s. 299–314.


© for this edition by CNS

występuje krzyżowanie się uprawnień pracowników Urzędu Ochrony Danych Osobowych i organów Państwowej Inspekcji Pracy? Czy współdziałanie tych instytucji dla skutecznego przeciwdziałania naruszeniom praw pracowniczych w zakresie ochrony danych osobowych i prawa do prywatności jest w tym zakresie pożądane?

## ZAKRES UPRAWNIEŃ INSPEKTORA PRACY W RAMACH KONTROLI MONITORINGU

Prawidłowe stosowanie przez pracodawców przepisów kodeksu pracy jako podstawowego źródła prawa pracy w myśl wymienionych wyżej przepisów w pełni podlega kontroli realizowanej przez organy Państwowej Inspekcji Pracy w zakresie przysługujących inspektorowi pracy uprawnień przewidzianych w ustawie o Państwowej Inspekcji Pracy. Przepisy wprowadzające przedmiotową regulację do kodeksu pracy nie przewidziały bowiem dodatkowych przepisów modyfikujących, w tym rozszerzających dotychczas ustanowione uprawnienia. Przyjęcie przedmiotowej regulacji i umiejscowienie jej w ramach przepisów kodeksu pracy oznacza, że inspektor pracy kontrolujący każdego pracodawcę ma prawo i powinność (w zależności od zakresu prowadzonej kontroli) badać problematykę związaną z prawidłowym stosowaniem monitoringu pracowniczego, w szczególności jako rozwiązania niezbędnego do zapewnienia pracownikom bezpiecznych warunków pracy. Inspektor może sprawdzić wszystkie miejsca w zakładzie pracy, w których stosowany jest monitoring. Wynika to z faktu, że w ramach swoich uprawnień kontrolnych inspektor pracy zgodnie z art. 23 ust. 1 pkt 1 i 2 ustawy o PIP ma prawo do swobodnego wstępu na teren oraz do obiektów i pomieszczeń podmiotu kontrolowanego oraz przeprowadzania oględzin tych obiektów, pomieszczeń, stanowisk pracy, maszyn i urządzeń oraz przebiegu procesów technologicznych i pracy. Realizując uprawnienie w zakresie swobodnego poruszania się, inspektor pracy kontrolujący zagadnienie monitoringu pracowniczego będzie miał możliwość ustalenia, które miejsca są monitorowane, a które nie, i czy pracodawca w sposób prawidłowy oznaczył miejsca monitorowane. Inspektor pracy ma również prawo utrwalania przebiegu i wyników oględzin, o których mowa w pkt 2, za pomocą aparatury i środków technicznych służących do utrwalania obrazu lub dźwięku (art. 23 ust. 1 pkt 7 ustawy o PIP). Tym samym inspektor pracy może wykonać zdjęcia na monitorowanym terenie i zarejestrować sposób oznakowania miejsc monitorowanych w formie fotografii, które następnie mogą być dołączone do protokołu kontroli.

W mojej ocenie skuteczność weryfikacji przestrzegania przepisów w tym względzie będzie uprawniała inspektora pracy do zapoznania się z obrazem rejestrowanym przez kamery, jak również przechowywanymi nagraniami, niezależnie od miejsca ich archiwizacji (w tym wykonywania tych zadań jako zleconych podmiotowi zewnętrznemu, w tym na przykład firmie ochroniarskiej). Zgodnie


© for this edition by CNS

bowiem z art. 23 ust. 1 pkt 5 ustawy o PIP inspektor pracy ma prawo żądania przedłożenia akt osobowych i wszelkich dokumentów związanych z wykonywaniem pracy przez pracowników lub osoby świadczące pracę na innej podstawie niż stosunek pracy. Pod pojęciem wszelkich dokumentów można również rozumieć zapisy wprowadzonego przez pracodawcę monitoringu. Zgodnie bowiem z definicją dokumentu zawartą w internetowej Encyklopedii PWN[8] jest nim „każdy przedmiot materialny będący świadectwem jakiegoś faktu, zjawiska lub myśli ludzkiej"; przy czym rozróżnia się dokumenty: piśmiennicze (na przykład książki czy czasopisma) i niepiśmiennicze (na przykład plany czy dokumentacja projektowo-techniczna) oraz wizualne, oglądowe (na przykład publikacje drukowane, rękopisy, fotografie czy dzieła sztuki), audialne, słuchowe (na przykład płyty gramofonowe, kompaktowe czy taśmy magnetofonowe), audiowizualne, słuchowo-oglądowe (na przykład filmy) i nośniki komputerowe (na przykład dyskietki czy dyski optyczne). Definicja ta koresponduje również z definicją legalną dokumentu zawartą w art. $77^3$ kodeksu cywilnego[9], w myśl którego dokumentem jest nośnik informacji umożliwiający zapoznanie się z jej treścią. Z kolei zgodnie z § 14 art. 115 kodeksu karnego[10] dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.

Inspektor pracy ma również możliwość wykonywania niezbędnych dla celów kontroli odpisów lub wyciągów z dokumentów, jak również zestawień i obliczeń sporządzanych na podstawie dokumentów, a w razie potrzeby żądania ich od podmiotu kontrolowanego (art. 23 ust. 1 pkt 8 ustawy o PIP). Inspektor pracy może kontrolować dokumentację związaną z monitoringiem. W celu dokonania oceny w zakresie prawidłowego zorganizowania stanowisk pracy, w tym oznaczenia miejsc monitorowanych, inspektor pracy ma prawo kontrolowania dokumentacji prowadzonej przez pracodawcę. Przepisy kodeksu pracy nakładają bowiem na pracodawcę szereg wymogów wynikających z zastosowania monitoringu. Jednym z nich jest określenie celów, dla osiągnięcia których monitoring został wprowadzony. W zależności od konkretnej formy monitoringu, polski ustawodawca przyjął różne cele poddawania pracowników kontroli. Zgodnie z art. $22^2$ § 1 k.p. pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring), jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Budzą one wątpliwości w praktyce stosowania tych przepisów, gdyż nie są one w pełni

[8] *Dokument*, [hasło w:] Encyklopedia PWN, https://encyklopedia.pwn.pl/szukaj/dokument.html (dostęp: 20.09.2022).

[9] Dz.U. z 2022 r. poz. 1360 ze zm.

[10] Dz.U. z 2022 r. poz. 1138 ze zm.


© for this edition by CNS

dostosowane do możliwości, jakie dają chociażby w zakresie ochrony osób trzecich (z uwagi na ograniczenie do bezpieczeństwa pracowników). Jak stanowi zaś art. $22^3$ §1 i 4 k.p., jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, pracodawca może wprowadzić kontrolę służbowej poczty elektronicznej pracownika (monitoring poczty elektronicznej) lub inne formy monitoringu. Ustawodawca nie przewidział tym samym przesłanki ochrony informacji jako okoliczności uzasadniającej wprowadzenie kontroli służbowej poczty elektronicznej, co zdaje się być rozwiązaniem niekorespondującym z faktycznymi możliwościami nieuprawnionego wycieku informacji[11].

Nowe przepisy określają zatem enumeratywnie, w jakich celach prowadzenie monitoringu przez pracodawców jest obecnie dopuszczalne (zob. art. 5 ust. 1 lit. b RODO, a także art. $22^2$ § 3 k.p.). Cele monitoringu mogą być przy tym jedynie uszczegółowione w stosunku do przesłanek wskazanych w art. $22^2$ § 1 i art. $22^3$ § 1 k.p. W zawartym w art. $22^3$ § 1 k.p. katalogu przesłanek dotyczących stosowania monitoringu nie uwzględniono chociażby okoliczności związanej z oceną jakości pracy pracownika (co do czasu ustawowego uregulowania miało miejsce w praktyce). Należy zatem postulować zrewidowanie treści przedmiotowych regulacji, tak aby uwzględniały w większym stopniu ustanowione w art. 5 ust. 1 RODO zasady dotyczące przetwarzania danych osobowych, zwłaszcza zasadę celowości i zasadę adekwatności. Pracodawca, decydując się na założenie monitoringu wizyjnego w zakładzie pracy, powinien określić konkretny cel (lub cele), w którym będzie on wykorzystywany. Może natomiast używać monitoringu do realizacji tylko części lub jednego z tych celów. Tym samym stosowanie kamer w celu zapewnienia bezpieczeństwa pracownikom jest możliwe tylko wówczas, jeśli taka szczególna forma monitoringu jest niezbędna do zapewnienia pracownikom właściwego poziomu bezpieczeństwa. Dlatego inspektor pracy będzie miał prawo przeanalizować, czy wprowadzenie monitoringu było działaniem zasadnym, czy pracodawca wprowadził monitoring na wyrost, bez uzasadnionej podstawy, a właściwy poziom bezpieczeństwa był zapewniony wcześniej przy użyciu mniej inwazyjnych środków technicznych. W przypadku, gdy inspektor pracy uzna, że zapewnienie bezpiecznych warunków pracy jest możliwe bez stosowania monitoringu (wizyjnego), wówczas ma prawo zakwestionować legalność jego wprowadzania.

Ustawodawca nie zamyka przy tym katalogu technologii, które mogą być wykorzystane do monitorowania pracowników. Ograniczeniem są cele, które stanowią o legalności przetwarzania. Pracodawca powinien każdorazowo rozważyć, czy technologia, którą zamierza zastosować, nie narusza dóbr osobistych pracownika lub w inny sposób nie prowadzi do naruszenia przepisów o ochronie danych osobowych. Ostatecznie każdy pracodawca powinien indywidualnie rozważyć,

[11] Zwraca na to uwagę między innymi M. Kuba, *Monitoring pracowników na gruncie KP*, s. 23.


© for this edition by CNS

czy i jakie formy monitoringu są niezbędne w jego zakładzie pracy. Decyzja ta powinna zostać poprzedzona przeprowadzeniem analizy korzyści i obowiązków, jakie wiążą się ze stosowaniem danych technologii przy poszanowaniu dóbr osobistych pracowników. Weryfikacja wskazanego celu przez inspektora pracy może być w istocie utrudniona w kontekście ustalenia nadmiarowego monitoringu[12]. Każdorazowo trzeba bowiem zweryfikować, czy celu przetwarzania nie można zapewnić w inny, mniej inwazyjny sposób. Jedynie w sytuacjach oczywistych, na przykład wtedy, gdy pracodawca zainstalował kamery w miejscu, gdzie nie ma żadnych urządzeń czy sprzętu, ani nie jest wykonywana praca, nagrywanie przechodzących przez takie miejsca osób wydaje się niczym nieuzasadnione. Oczywiście użycie przez ustawodawcę zwrotów generalnych i bliżej niesprecyzowanych może powodować trudność w wyegzekwowaniu przestrzegania tego przepisu przez organy PIP[13].

Na tym tle wydaje się, że pracodawca został wyposażony w dużą dozę swobody, i tym samym pozostawiono mu spore pole manewru w ewentualnej polemice z inspektorem pracy w zakresie zasadności wprowadzenia monitoringu mając na uwadze przesłankę „niezbędności" oraz „konieczności", jak w przypadku innych form monitoringu[14]. Należy bowiem pamiętać, że to pracodawca — a nie inspektor pracy — jest organizatorem procesu pracy i to pracodawca finalnie ponosi odpowiedzialność za stan bezpieczeństwa i higieny pracy w zakładzie pracy. Zatem to pracodawca ponosi wszelkie związane z tym ryzyko, w szczególności dotyczące możliwości wystąpienia negatywnych konsekwencji zdrowotnych związanych z nieprawidłową organizacją pracy w zakresie bezpieczeństwa. Tym samym pracodawca będzie miał prawo dowodzenia w ramach postępowania kontrolnego, że monitoring pracowniczy jest rozwiązaniem jak najbardziej niezbędnym. Musi jednak przy tym wykazać, że zapewnienie optymalnego poziomu bezpieczeństwa nie jest możliwe przy zastosowaniu wyłącznie pozostałych środków technicznych i organizacyjnych (pracownicy ochrony, systemy alarmowe itp.). Ponadto cel przetwarzania powinien być zgodny z danymi, które pracodawca faktycznie przetwarza i wykorzystuje[15]. Z drugiej strony ustawodawca nie wyposażył inspektora

[12] Zob. P. Biały, *5 błędów w przetwarzaniu danych w ramach monitoringu,* „Ochrona Danych Osobowych" 2020, nr 7–8, s. 11–12.

[13] W doktrynie podnosi się bowiem zgodnie, że organy stosujące prawo nie mogą decydować ostatecznie o treści i charakterze obowiązujących uregulowań, gdyż powinien to czynić ustawodawca, a rozstrzygnięcie kolizji wolności i praw wymaga każdorazowo przeprowadzenia testu ważenia interesów, chociażby celem wyeliminowania zarzutu arbitralności w zakresie stosowania prawa. Tak między innymi M. Jabłoński, *Miejsce Państwowej Inspekcji Pracy w systemie organów państwa — wnioski* de lege lata *i* de lege ferenda, „Przegląd Prawa i Administracji" 118, 2019, s. 69.

[14] Inspektor pracy może w przypadku wątpliwości poinformować o potencjalnych naruszeniach Prezesa Urzędu Ochrony Danych Osobowych właściwego w zakresie kontroli wszelkich naruszeń przetwarzania danych osobowych.

[15] Tak wskazuje się w poradniku RODO Urzędu Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, s. 38, Urząd Ochrony Danych


© for this edition by CNS

pracy w łatwo weryfikowalne przesłanki, które pozwoliłyby w większości przypadków kontroli do zajęcia jednoznacznego stanowiska, minimalizując margines dowolności w działaniu pracodawcy. W praktyce jednak wydaje się to zadaniem trudnym, by nie rzec niemożliwym. Wprowadzenie ograniczeń do poszczególnych sektorów lub rodzajów prowadzonej przez pracodawcę działalności mogłoby być bowiem odebrane za nieuzasadnione krępowanie pracodawców w kreatywnym podejściu do oferowanych na rynku technologii, mających z jednej strony usprawniać proces pracy, a z drugiej czynić go bardziej bezpiecznym.

Europejska Rada Ochrony Danych przyjęła 10 lipca 2019 roku Wytyczne 3/2019 (wersja 1.0) w sprawie przetwarzania danych osobowych przez urządzenia wideo, które mają na celu wyjaśnienie, w jaki sposób RODO ma zastosowanie do przetwarzania danych osobowych w przypadku korzystania z urządzeń wideo oraz zapewnienie spójnego stosowania ogólnego rozporządzenia o ochronie danych w tym zakresie. Wskazują one między innymi, że dokonując wyboru rozwiązań technicznych administrator powinien brać pod uwagę technologie przyjazne prywatności, które zwiększają bezpieczeństwo. Przykładami takich technologii są systemy umożliwiające maskowanie lub mieszanie obszarów, które nie są istotne dla obszaru objętego nadzorem[16].

Zdecydowanie łatwiejsze dla inspektora pracy w ramach prowadzonej kontroli będzie ustalenie naruszenia i następnie wyegzekwowanie przestrzegania przepisu art. $22^2$ § $1^1$ i § 2 k.p., z których pierwszy wskazuje, że monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej, a drugi dotyczy pomieszczeń sanitarnych, szatni, stołówek oraz palarni, a więc miejsc, w których pracownicy znajdują się jedynie w celu wypoczynku i regeneracji lub takich, w których obecność monitoringu narażałaby ich intymność. W przypadku pomieszczeń organizacji związkowej zakaz ten ma charakter bezwzględny. Natomiast w przypadku miejsc wskazanych w art. $22^2$ § 2 k.p. ustawodawca nadaje temu zakazowi charakter względny, przewidując odejście od niego, jeśli stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego § 1 i nie naruszy godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Do takich technik należą na przykład obniżenie jakości wykonywanych nagrań lub skierowanie kamer wyłącznie na miejsce niezwiązane ze sferą dóbr osobistych pracownika. Jak wskazuje się

Osobowych, 4.10.2018, https://uodo.gov.pl/pl/138/545 (dostęp: 20.09.2022). Inspektor pracy w trakcie kontroli może wykorzystywać wytyczne Prezesa Urzędu Ochrony Danych Osobowych celem zapewnienia spójnego podejścia organów państwowych w kontroli przestrzegania przepisów powszechnie obowiązujących.

[16] W dniu 29 stycznia 2020 r. przyjęta została wersja 2.0: *Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo. Wersja 2.0*, European Data Protection Board, 16.07.2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl.pdf (dostęp: 30.09.2022).


© for this edition by CNS

w doktrynie, wprowadzenie możliwości uchylenia zakazu monitoringu w tych pomieszczeniach, nawet przy spełnieniu wymienionych wyżej przesłanek, może budzić kontrowersje. Przynajmniej pomieszczenia sanitarne oraz szatnie z uwagi na obowiązek poszanowania godności pracowników (art. $11^1$ k.p.) powinny być pomieszczeniami, w których zakaz monitoringu jest bezwzględny[17]. Ustawodawca nie doprecyzował ponadto, w jakiej formie powinna być ewentualnie udzielona uprzednia zgoda zakładowej organizacji związkowej — a w przypadku braku jej funkcjonowania u pracodawcy zgoda przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy. Brak jest wymogu pisemności, co w przypadku kontroli może utrudnić weryfikację udzielonej zgody i skuteczne zakwestionowanie tego braku. Mimo że ograniczenia miejscowe są w przepisach sprecyzowane (abstrahując od posłużenia się w nich również pojęciami niezawierającymi definicji legalnej, jak na przykład stołówka), nie oznacza to, że w pozostałym zakresie monitoring może być stosowany z pełną swobodą (z uwagi na zasadę proporcjonalności). W treści *Wskazówek Prezesa Urzędu Ochrony Danych Osobowych* podkreślono, że kamery nie powinny być bezpośrednio skierowane na ekran komputera pracownika i umożliwiać śledzenia wykonywanych przez niego czynności na tym urządzeniu, ponieważ monitoring wizyjny nie powinien być wykorzystywany do nadzorowania wykonywania obowiązków służbowych[18]. Umiejscowienie kamer monitoringu na korytarzu w taki sposób, że widać, kto wchodzi do pomieszczenia wydzielonego dla organizacji związkowej również należy uznać za naruszenie zakazu określonego w art. $22^2$ § $1^1$ k.p. Pracodawca nie powinien mieć bowiem możliwości rozpoznawania osób wchodzących do pomieszczenia organizacji związkowej.

Inspektor pracy uprawniony jest również do zbadania, czy pracodawca na bieżąco usuwa zapisy monitoringu (w tym nagrania obrazu), uwzględniając dopuszczalny okres ich przetwarzania, wynoszący co do zasady trzy miesiące (art. $22^2$ § 3 i 4 k.p.). Może to nastąpić poprzez zapewnienie dostępu do miejsca przechowywania nagrań lub gromadzenia danych z innych form monitorowania pracowników. Okres retencji musi być przy tym adekwatny do zastosowanego środka (monitoringu) oraz okoliczności, to jest przyjętego w praktyce celu.

Przejawem respektowania wskazanej w art. 5 ust. 1 lit. a RODO zasady przejrzystości są określone w art. $22^2$ § 6–10 k.p. obowiązki informacyjne, jakie powinien spełnić pracodawca, planujący wprowadzenie monitoringu (nie tylko wizyjnego) w zakładzie pracy, a których przestrzeganie władny kontrolować jest inspektor pracy. Obowiązki te realizowane są na kilku polach. Przede wszystkim

[17] Zwracają na to uwagę między innymi M. Frąckowiak, T. Świeboda, *Ochrona danych osobowych pracownika w perspektywie RODO i przepisów dotyczących monitoringu wizyjnego stosowanego przez pracodawcę*, „Monitor Prawa Pracy" 2018, nr 7, s. 13.

[18] Zob. *Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego*, Urząd Ochrony Danych Osobowych, 10.07.2018, https://uodo.gov.pl/data/filemanager_pl/1200.pdf (dostęp: 30.09.2022).


© for this edition by CNS

— monitoring musi znaleźć swoje umocowanie w przepisach wewnątrzzakładowych. Następnie konieczne jest wystosowanie do pracowników odpowiedniego komunikatu, a w przypadku pracowników nowozatrudnianych indywidualnie oznaczonej, pisemnej informacji. Wreszcie narzędzia lub miejsca poddawane kontroli muszą być odpowiednio oznaczone. Abstrahując od powyższego, zrealizowany ma być obowiązek informacyjny określony w art. 12 i 13 RODO (art. $22^2$ § 10 k.p.). Zgodnie bowiem z art. $22^2$ § 6 k.p., kwestie dotyczące celu (celów), zakresu i sposobu zastosowania monitoringu mają być przedmiotem postanowień układu zbiorowego pracy lub regulaminu pracy, a jeśli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest zobowiązany do wprowadzenia regulaminu pracy, mają być one przedmiotem wydanego przez pracodawcę obwieszczenia. Co do zakresu monitoringu należałoby ustalić zarówno aspekt podmiotowy (kto będzie objęty monitoringiem), jak i przedmiotowy (które miejsca będą podlegały monitoringowi). Finalnie trzeba określić, jaki zakres danych będzie gromadzony dzięki zastosowaniu danej formy monitoringu. Podkreśla się, że podczas ustalania sposobu działania monitoringu należy wskazać, jakie środki mają zostać podjęte i w jaki sposób będą stosowane (między innymi czy będzie to monitoring stały, okresowy, czy krótkotrwały)[19]. Chodzi nie tylko o granice przedmiotowe, ale także czasowe, a więc o to, by pracownik nie był monitorowany w sposób ciągły, również poza godzinami swojej pracy, gdyż takie zachowanie co do zasady należałoby uznać za wyraźne naruszenie prawa do prywatności i narażenie na niebezpieczeństwo zdrowia psychicznego pracowników. Nie znajdowałoby to jednocześnie usprawiedliwienia w konieczności zapewnienia skutecznego kierownictwa po stronie pracodawcy, a potencjalnie stanowiłoby źródło naruszeń i nadużyć. Poszanowanie prawa do prywatności w relacjach pracowniczych ma istotne znaczenie, ponieważ prywatność jest ważna nie tylko dla zachowania zdrowia psychicznego pracownika, ale także dla zachowania komfortu pracy, który sprzyja prawidłowemu wykonywaniu obowiązków i rozwojowi zawodowemu pracownika[20]. Pracodawca powinien ponadto pamiętać o tym, że cel wpisany w dokumentacji musi być tożsamy z celem wykorzystywania urządzenia monitorującego i danych w ten sposób otrzymywanych. Przetwarzanie danych osobowych powinno przede wszystkim odpowiadać zasadzie ograniczenia celu z art. 5 ust. 1 lit. b RODO.

Zatem rolą inspektora pracy, który będzie kontrolował zagadnienie monitoringu, będzie dokonanie ustaleń między innymi w zakresie źródła i sposobu regulacji monitoringu w przepisach wewnątrzzakładowych, a także tego, czy pracodawca prawidłowo wypełnił w tym zakresie obowiązek informacyjny względem pracowników. Tym samym w zakładach pracy, w których posiadanie regulaminów

[19] W ten sposób prezentuje to M. Kuba, *Monitoring pracowników na gruncie KP*, s. 24.

[20] Podnoszą to między innymi M. Miłosz, J. Świątek-Rudoman, *Nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy*, „Praca i Zabezpieczenie Społeczne" 2019, nr 4, s. 33.


© for this edition by CNS

pracy jest obowiązkowe[21], kwestie dotyczące stosowania monitoringu muszą zostać wprowadzone do regulaminu. Na etapie postępowania kontrolnego inspektor pracy powinien dokonać ustaleń, czy kwestie związane z monitoringiem zostały prawidłowo uregulowane w przepisach wewnątrzzakładowych i czy w tym zakresie regulamin pracy (albo jego zmiana) został prawidłowo wprowadzony. Należy bowiem zauważyć, że wprowadzenie regulaminu pracy w przypadku funkcjonowania związku zawodowego powinno zostać uzgodnione z organizacją związkową działającą u pracodawcy. Jednak w odróżnieniu od regulaminu wynagradzania, możliwe jest wprowadzenie regulaminu pracy, w tym przepisów dotyczących monitoringu, pomimo braku zgody organizacji związkowej na zaproponowane regulacje. Może to mieć miejsce w przypadku nieuzgodnienia regulacji w ustalonym przez strony terminie, jak również nieprzedstawienia wspólnie uzgodnionego stanowiska w terminie 30 dni od dnia przekazania przez pracodawcę projektu regulaminu pracy, w przypadku funkcjonowania co do zasady więcej niż jednej zakładowej organizacji związkowej (zob. art. $104^2$ § 2 k.p. i art. 30 ust. 6 ustawy z dnia 23 maja 1991 roku o związkach zawodowych, Dz.U. z 2022 r. poz. 854). Wystąpienie nieprawidłowości w tym względzie powinno być zauważone przez inspektora pracy i opisane w protokole kontroli, a następnie stać się przyczyną dla wydania środków prawnych z uwagi na brak podstawy prawnej stosowania monitoringu przez danego pracodawcę. *De facto* zatem rozwiązania przyjęte przez pracodawcę w zakresie monitoringu mogą być dokumentem jednostronnym, to jest obwieszczeniem albo regulaminem pracy, zwłaszcza przy braku funkcjonowania zakładowej organizacji związkowej lub braku uzgodnienia tych kwestii z powodów wskazanych wyżej.

W ramach postulatu *de lege ferenda* należałoby zatem rozważyć obowiązek uprzedniego poinformowania właściwego okręgowego inspektora pracy o wprowadzeniu przez pracodawcę monitoringu (zwłaszcza wizyjnego). Celem uprzedniego zawiadomienia inspektora pracy jest umożliwienie przeprowadzenia kontroli zasadności oraz zgodności z prawem wprowadzenia określonej formy monitoringu jako narzędzia mogącego istotnie ingerować w sferę godności i innych dóbr osobistych pracownika i jednocześnie mogącego negatywnie wpływać na komfort pracy, a tym samym bezpieczeństwo pracy[22]. Zawiadomienie inspektora pracy stanowić może tym samym warunek skuteczności tej kontroli.

[21] Dotyczy to co do zasady pracodawców zatrudniających co najmniej 50 pracowników — zob. art. 104 § $1^1$ i § 3 k.p.

[22] Przykładem podobnego uregulowania jest przepis art. 150 § 1 i 2 k.p., w którym dopuszczalność stosowania okresu rozliczeniowego czasu pracy, o którym mowa w art. 135 § 2 i 3 jest możliwa po uprzednim zawiadomieniu właściwego okręgowego inspektora pracy w przypadku, gdy u pracodawcy nie działa zakładowa organizacja związkowa, a także gdy zakładowa organizacja związkowa nie wyraża zgody na ustalenie lub zmianę systemów i rozkładów czasu pracy oraz okresów rozliczeniowych czasu pracy. Innym możliwym rozwiązaniem może być następczy obowiązek powiadomienia właściwego okręgowego inspektora pracy o zawarciu umowy na czas określony, o której


© for this edition by CNS

W toku prowadzonej kontroli inspektor pracy ma także prawo zweryfikować, czy pracodawca w sposób prawidłowy wypełnił obowiązki informacyjne względem pracowników — zarówno tych, którzy byli już zatrudnieni w okresie wprowadzania monitoringu, jak i względem pracowników nowych. Stosowanie monitoringu wobec pracowników wiąże się bowiem z dodatkowymi obowiązkami informacyjnymi, które muszą zostać wypełnione zarówno przed uruchomieniem monitoringu (nie później niż dwa tygodnie przed jego uruchomieniem), jak i przed dopuszczeniem nowego pracownika do pracy. Na pracodawcy spoczywa również obowiązek odpowiedniego oznaczenia pomieszczeń i terenów objętych monitoringiem (w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych) nie później niż jeden dzień przed uruchomieniem monitoringu. Tablice informujące o zainstalowanym monitoringu powinny być widoczne i umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Ich wymiary muszą być proporcjonalne do miejsca, gdzie zostały umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer. Jednak z uwagi na to, że należy dopełnić obowiązku informacyjnego określonego w art. 13 RODO, jako niewystarczające jawi się oznaczenie obszaru objętego monitoringiem jedynie piktogramami. W mojej ocenie nie oznacza to konieczności umieszczania wszystkich informacji wskazanych w tym przepisie przy tabliczce informacyjnej. W takiej sytuacji możliwe jest zastosowanie warstwowych not informacyjnych. Wystarczające będzie umieszczenie na tablicy informacji o tym przez kogo, w jakim celu i na jakich podstawach prawnych jest prowadzony monitoring oraz danych kontaktowych inspektora ochrony danych, jeżeli został powołany. Należy także poinformować, jaki obszar obejmuje monitoring, jakie prawa ma osoba obserwowana oraz gdzie możemy zapoznać się z dodatkowymi informacjami na ten temat[23].

Zgodnie z art. $22^2$ §7 k.p. pracodawca informuje pracowników o wprowadzeniu monitoringu w sposób u niego przyjęty w zakładzie pracy. Informacja może przyjąć formę pisma skierowanego do każdego pracownika, obwieszczenia na tablicy ogłoszeń, komunikatu e-mailowego skierowanego do załogi czy informacji przekazanej za pośrednictwem zakładowego intranetu. I znów — brak określenia wymogu weryfikowalnej formy przekazywanej informacji powoduje, że kontrola wykonania tego obowiązku w ustawowym terminie, zwłaszcza u pracodawców wykorzystujących do tego celu tablicę ogłoszeń, będzie niemożliwa. Natomiast wprowadzenie monitoringu nie jest uzależnione od zgody pracownika. Oczekiwanie od pracownika zgody nie ma żadnego uzasadnienia i może być

mowa w art. $25^1$ § 4 pkt 4 k.p. wraz ze wskazaniem przyczyn zawarcia takiej umowy (obiektywnych przyczyn leżących po stronie pracodawcy) w terminie pięciu dni roboczych od dnia jej zawarcia.

[23] *Montujesz kamery w miejscy pracy. Sprawdź, o czym należy pamiętać*, Archiwum UODO, 12.08.2020, https://archiwum.uodo.gov.pl/pl/138/1634 (dostęp: 27.09.2022).


© for this edition by CNS

działaniem nadmiernym, pozostającym w opozycji do przepisów, które weszły w życie z dniem 25 maja 2018 roku[24].

Dotychczas w ramach kontroli przeprowadzanych przez organy Państwowej Inspekcji Pracy najczęściej stwierdzano nieprawidłowości w zakresie prowadzenia monitoringu pomieszczeń sanitarnych w sposób, który nie gwarantował nienaruszania godności oraz innych dóbr osobistych pracownika, jak również bez uprzedniego uzyskania zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy. Dość częstym uchybieniem był brak oznaczeń pomieszczeń i terenu monitorowanego w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych. Pracodawcy nie określali też celu, zakresu oraz sposobu zastosowania monitoringu w zakładzie. Stwierdzano brak przekazanej informacji dla pracowników o celu, zakresie oraz sposobie zastosowania monitoringu w zakładzie[25].

## ŚRODKI PRAWNE STOSOWANE PRZEZ INSPEKTORA PRACY

Z punktu widzenia możliwych do zastosowania na skutek przeprowadzonej kontroli i poczynionych w jej trakcie przez inspektora pracy ustaleń faktycznych (wskazujących na nieprawidłowości) środków prawnych na pierwszy plan wysuwa się wystąpienie i polecenie. Podstaw dla stosowania tych środków o niewładczym charakterze należy upatrywać w aktach prawa międzynarodowego. Zgodnie z art. 17 ust. 1 konwencji nr 81 Międzynarodowej Organizacji Pracy (MOP) z 11 lipca 1947 roku dotyczącej inspekcji pracy w przemyśle i handlu[26] i art. 22 ust. 1 konwencji nr 129 MOP z dnia 25 czerwca 1969 roku dotyczącej inspekcji pracy w rolnictwie[27] osoby naruszające przepisy, których stosowanie kontrolują inspektorzy pracy, podlegają natychmiastowym procedurom prawnym bez uprzedniego ostrzeżenia, jednakże ustawodawstwo krajowe może przewidzieć wyjątki w przypadkach, gdy należy udzielić uprzedniego ostrzeżenia w celu poprawienia sytuacji lub zastosowania środków zapobiegawczych. W doktrynie wskazuje się, że właśnie w tej drugiej grupie środków „pokontrolnych" należy

[24] Tak między innymi wyrok Sądu Rejonowego w Toruniu z dnia 28 grudnia 2018 r., IV P 364/18, Portal Orzeczeń Sądu Rejonowego w Toruniu, 18.03.2019, http://orzeczenia.torun.sr.gov.pl/content/$N/151025200002021_IV_P_000364_2018_Uz_2019-02-22_001 (dostęp: 30.09.2022).

[25] Informacje na temat naruszeń w zakresie przetwarzania danych osobowych przekazywane były przez poszczególne okręgowe inspektoraty pracy w związku z porozumieniem zawartym 14 grudnia 2012 r. pomiędzy Państwową Inspekcją Pracy a ówczesnym Biurem Generalnego Inspektora Ochrony Danych Osobowych: *Porozumienie pomiędzy Państwową Inspekcją Pracy a Biurem Generalnego Inspektora Ochrony Danych Osobowych w sprawie zasad współdziałania PIP i GIODO*, Państwowa Inspekcja Pracy, 14.12.2012, https://www.pip.gov.pl/pl/f/v/19359/giod0%20pip%2012.pdf (dostęp: 27.09.2022).

[26] Dz.U. z 1997 r. Nr 72, poz. 450.

[27] Dz.U. z 1997 r. Nr 72, poz. 452.


© for this edition by CNS

upatrywać podstaw prawnych dla takich form działania inspekcji, które nie posiadają charakteru władczego i wiążą się z wyodrębnianą w ramach funkcji kontroli fazą oddziaływania naprawczego[28]. Obie wspomniane wyżej konwencje przyjmują, że prawo decyzji w sprawie wyboru rodzaju środka prawnego należeć powinno do inspektora. Stosownie bowiem do art. 17 ust. 2 konwencji nr 81 i art. 22 ust. 2 konwencji nr 129, inspektorzy pracy dysponują swobodą decydowania, czy należy udzielić ostrzeżenia lub porady zamiast rozpoczęcia lub zalecenia rozpoczęcia odpowiednich procedur. Decyzja co do finalnie podjętego środka powinna wynikać z uprzednio wyważonej oceny inspektora co do wyboru najbardziej odpowiedniego w danych okolicznościach środka prawnego. Jak stwierdziła Komisja Ekspertów MOP, wybór środka karnego jest uzasadniony w przypadku ciężkiego lub umyślnego naruszenia przepisów lub też naruszeń powtarzających się. Jeżeli natomiast stwierdzone naruszenie ma charakter lekki lub nieumyślny, wynikający z niedostatecznej znajomości prawa, bardziej uzasadnione jest zastosowanie innych środków. Podkreśla się przy tym, że wybór zastosowanego środka prawnego powinien być adekwatny do stopnia zagrożenia. Uprzednie ostrzeżenie przed podjęciem procedur karnych jest pozytywnie oceniane przez Komisję Ekspertów MOP. Z art. 11 ust. 8 ustawy o Państwowej Inspekcji Pracy wynika zatem, że wystąpienie może być kierowane w razie innych naruszeń niż te, które uprawniają do wydania decyzji. Nie ulega bowiem wątpliwości, że wystąpienie w porównaniu z decyzją administracyjną jest słabszym i łagodniejszym środkiem przywracania stanu praworządności i powinno być środkiem działań inspektora pracy, przeznaczonym głównie do reagowania na lżejsze naruszenia prawa, nie wyłączając naruszeń z dziedziny bhp oraz wynagrodzenia za pracę.

Należy jednak zauważyć, że pomimo pojawienia się nowej regulacji dotyczącej stosowania monitoringu w zakładzie pracy w kodeksie pracy, ustawodawca nie zdecydował się na odrębne uregulowanie środków nadzorczo-kontrolnych przestrzegania tych przepisów. Inspektor pracy nie został wyposażony wprost w możliwość wydawania nakazów (mających charakter decyzji administracyjnych), czy wystąpień (lub poleceń) w przypadku stwierdzenia nieprawidłowości w tym zakresie[29]. Może to okazać się niewystarczające dla efektywnego zapewnienia przestrzegania nowych przepisów. W świetle orzecznictwa sądów administracyjnych wystąpienie stanowi bowiem zalecenie czy też postulat usunięcia

[28] Tak między innymi D. Makowski, *Inspekcja pracy jako instytucja państwowego nadzoru nad przestrzeganiem prawa pracy*, Łódź 2017, s. 310 n.

[29] Tytułem przykładu można wskazać na wprowadzenie do ustawy o Państwowej Inspekcji Pracy z dniem 1 stycznia 2017 r. art. 11b, stosownie do którego organy PIP są uprawnione do skierowania wystąpienia (a także polecenia) w sprawie wypłacenia wynagrodzenia w wysokości wynikającej z wysokości minimalnej stawki godzinowej. Ustawodawca poprzestał w tym przypadku na wyposażeniu organów PIP w środki związane z funkcją kontroli, nie przewidując możliwości stosowania decyzji administracyjnych (środków nadzoru). Inspektor pracy nie został zatem uprawniony do wydawania nakazu wypłaty wynagrodzenia w wysokości minimalnej stawki godzinowej.


© for this edition by CNS

naruszenia prawa przez pracodawcę[30]. Poza dyskusją pozostaje jednocześnie, że wystąpienie nie jest decyzją administracyjną (decyzjami są bowiem jedynie nakazy i zakazy wydawane w sytuacjach określonych w ustawie — zob. art. 33 ust. 1 pkt 1 ustawy o PIP)[31], jak również to, że niewykonanie wniosków pokontrolnych zawartych w wystąpieniu nie podlega egzekucji administracyjnej[32]. Pewnym usprawiedliwieniem dla takiego działania może być fakt, że niewiążący charakter wystąpienia (przeważający w literaturze przedmiotu i powszechnie przyjmowany w praktyce inspekcyjnej) nie wpływa na obniżenie skuteczności tego środka działania, aczkolwiek może mieć wpływ na jego realizację przy krytycznej postawie pracodawcy niepodzielającego stanowiska inspektora pracy. Oczywiście decyzja administracyjna również może być przedmiotem zaskarżenia, ale konieczność napisania odwołania, a następnie skargi do wojewódzkiego sądu administracyjnego jest zabiegiem daleko bardziej uciążliwym, wymagającym obsługi prawnej i poniesienia dodatkowych kosztów, często decydujących o niekwestionowaniu decyzji administracyjnych wydawanych przez inspektorów pracy.

Innym środkiem działania inspekcji może być w tym zakresie polecenie, które zostało wprowadzone ustawą z dnia 9 czerwca 2011 roku[33], mocą której zmianie uległ między innymi art. 11 pkt 8 ustawy o PIP. Jak wskazywano w uzasadnieniu do projektu ustawy zmieniającej, polecenie miało być nowym środkiem prawnym przeznaczonym do usunięcia drobnych nieprawidłowości, a celem nowelizacji zróżnicowanie i odformalizowanie przysługujących inspekcji środków działania. W przypadku polecenia, jego charakter prawny nasuwa większe wątpliwości niż wystąpienie z uwagi na dualizm regulacji. Jak stanowi art. 34 ust. 4 ustawy o PIP decyzje i polecenia, o których mowa w ust. 1a i 1b, wydaje się w celu usunięcia ujawnionych w toku kontroli uchybień, jeżeli mogą być one usunięte podczas trwania kontroli lub niezwłocznie po jej zakończeniu. Ponadto, w myśl art. 35 ust. 2 tej ustawy, do poleceń stosuje się odpowiednio ust. 1 przepisu, zgodnie z którym podmiot kontrolowany, do którego została skierowana decyzja, ma obowiązek informowania odpowiedniego organu Państwowej Inspekcji Pracy o jej realizacji z upływem terminów określonych w decyzji. Jak podkreśla się w doktrynie, podmiot kontrolowany ma obowiązek informowania o realizacji polece-

[30] Zob. np. uzasadnienie postanowienia NSA z 23.10.2008 r., I OSK 1029/08, Lex nr 500994, wyrok WSA w Poznaniu z 28.02.2014 r., II SA/Po 975/13, Lex nr 1488296.

[31] Szerzej o tym A. Jasińska-Cichoń, *Ustawa o Państwowej Inspekcji Pracy, komentarz do art. 11*, Warszawa 2008, a także K. Rączka, [w:] M. Gersdorf, J. Jagielski, K. Rączka, *Ustawa o Państwowej Inspekcji Pracy. Komentarz do art. 11*, Warszawa 2008.

[32] Stosownie do art. 2 § 1 pkt 11 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, egzekucji administracyjnej podlegają jedynie obowiązki z zakresu bhp oraz wypłaty należnego wynagrodzenia za pracę, a także innego świadczenia przysługującego pracownikowi, nakładane w drodze decyzji organów PIP.

[33] Ustawa z dnia 9 czerwca 2011 r. o zmianie ustawy o Państwowej Inspekcji Pracy oraz niektórych innych ustaw (Dz.U. z 2011 r. Nr 142, poz. 829).


© for this edition by CNS

nia, nie zaś tylko o terminie i sposobie realizacji, jak w przypadku wystąpienia[34]. Stąd można wnioskować, że polecenie jest wiążące dla kontrolowanego. Poza tym etymologia terminu „polecenie", w przeciwieństwie do wystąpienia, kojarzy się z konstrukcją rozstrzygnięcia wiążącego. W internetowym słowniku języka polskiego PWN[35] oznacza ono wypowiedź nakazującą komuś wykonanie jakiejś czynności. Jednak z drugiej strony wątpliwości budzi nieprecyzyjny sposób określenia zakresu stosowania polecenia oraz jego podobieństwo do wystąpienia, co przemawiałoby na rzecz niewładczego środka.

Na ogólną liczbę 248058 wszystkich wniosków w wystąpieniach wydanych przez inspektorów pracy w 2019 roku oraz 13773 wydanych poleceń, jedynie 1052 wniosków oraz 40 poleceń dotyczyło wniosków z zakresu monitoringu[36]. Z tej liczby zrealizowanych zostało 860 wniosków oraz 39 poleceń. W swojej podstawie prawnej miały przepis art. $22^2$ k.p. lub art. $22^3$ k.p. Podobnie odpowiednio na liczbę 189813 wniosków oraz 10863 poleceń wydanych ogółem w 2021 roku, jedynie 942 wniosków oraz 81 poleceń dotyczyło kwestii związanych z monitoringiem. Z tej liczby zostało zrealizowanych 750 wystąpień oraz 78 poleceń. Zatem proporcja ta względem ogółu wydanych przez inspektorów pracy wniosków i poleceń wydaje się być stała i oscyluje w granicach 0,3–0,5% ogółu wydanych tego rodzaju środków prawnych.

W praktyce stosowania środków prawnych przez inspektora pracy może jednak powstać wątpliwość co do dopuszczalności zastosowania nakazu w przypadku stwierdzenia naruszenia przepisów w zakresie monitoringu. Wynika to z faktu, że wspólna przesłanka wszystkich środków prawnych określonych w art. 11 ustawy o PIP, określona w jej początkowej części, dotyczy naruszenia przepisów prawa pracy lub przepisów dotyczących legalności zatrudnienia. Podnosi się jednak, że została ona rodzajowo skonkretyzowana w dalszych przepisach art. 11 tej ustawy. Przykładem może być między innymi pkt 1, przewidujący możliwość nakazania usunięcia stwierdzonych uchybień w ustalonym terminie w przypadku, gdy naruszenie dotyczy przepisów i zasad bezpieczeństwa i higieny pracy, co zdaje się sugerować, iż z uwagi na zamknięty katalog przesłanek wydanie nakazu (będącego decyzją administracyjną) może dotyczyć naruszenia tylko przepisów bhp (lub przepisów płacowych — pkt 7). Tymczasem monitoring pracowniczy został uregulowany w dziale II kodeksu pracy, który nie jest poświęcony wprost problematyce bezpieczeństwa i higieny pracy, a stosunkowi pracy. Powstaje pytanie, czy wyklucza to możliwość potraktowania tych przepisów jako mających na celu oprócz zgodnego z prawem przetwarzania danych osobowych również ukształto-

[34] Tak między innymi D. Makowski, *Inspekcja pracy jako instytucja państwowego nadzoru…*, s. 319.

[35] *Polecenie*, [hasło w:] Słownik języka polskiego PWN, https://sjp.pwn.pl/szukaj/polecenie.html (dostęp: 4.10.2022).

[36] Dane te pochodzą z wewnętrznej bazy statystycznej Departamentu Planowania, Analiz i Statystyki w Głównym Inspektoracie Pracy w Warszawie.


© for this edition by CNS

wanie bezpiecznych i higienicznych warunków pracy. Umiejscowienie tych przepisów mogło być bowiem podyktowane faktem, że monitoring wiąże się między innymi z przetwarzaniem danych osobowych, a kwestie te regulowane były dotychczas w art. $22^1$ k.p., co systemowo uzasadniało uregulowanie tego zagadnienia wśród tych przepisów[37]. Natomiast nie ulega wątpliwości, iż problematyka ta związana jest również z organizacją bezpiecznych i higienicznych warunków pracy. Tym bardziej, że sama redakcja celów, dla których osiągnięcia niezbędne jest wprowadzenie monitoringu, odwołuje się do zapewnienia bezpieczeństwa pracowników czy też właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Stąd w ocenie autora niewykluczone jest, zwłaszcza przy stosowaniu niezgodnego z prawem monitoringu wizyjnego, potraktowanie takiego naruszenia w związku z art. 207 § 2 k.p. stanowiącym o tym, że pracodawca zobowiązany jest chronić zdrowie (w tym zdrowie psychiczne) i życie pracowników przez zapewnienie bezpiecznych i higienicznych warunków pracy przy odpowiednim wykorzystaniu osiągnięć nauki i techniki. W szczególności zaś jest obowiązany organizować pracę w sposób zapewniający bezpieczne i higieniczne warunki pracy.

Abstrahując od rodzaju możliwych do zastosowania środków prawnych, należy wskazać na inny pozytywny aspekt roli inspektora pracy. Otóż prawidłowo sporządzony protokół z kontroli wraz z załącznikami może być następnie istotnym dowodem z dokumentu urzędowego w ramach postępowania sądowego w sprawie ewentualnych roszczeń pracownika z zakresu ochrony dóbr osobistych, do których stosuje się poprzez art. 300 k.p. odpowiednio przepisy kodeksu cywilnego, jeżeli nie są one sprzeczne z zasadami prawa pracy.

Wydaje się, że istotnym wzmocnieniem skuteczności kontroli inspektora pracy byłoby również wprowadzenie przepisów bezpośrednio penalizujących naruszenia pracodawcy w tym zakresie (chociażby przez rozszerzenie katalogu wykroczeń z art. 281 k.p.) . Rozwiązanie takie w jakimś stopniu korespondowałoby z sankcjami, które może zastosować prezes urzędu ochrony danych osobowych w ramach postępowania w sprawie naruszenia przepisów o ochronie danych osobowych.

## WNIOSKI KOŃCOWE

Przeprowadzona analiza przepisów, będąca w pewnym zakresie jedynie zasygnalizowaniem rodzących się wątpliwości, prowadzi do wniosku, że zarówno sposób wprowadzenia, jak i sposób funkcjonowania monitoringu u pracodawcy niewątpliwie podlega kontroli inspektorów pracy. I chociażby z tego punktu wi-

[37] Poza tym również art. 15 k.p. usytuowany w dziale pierwszym k.p. stanowi, że pracodawca jest obowiązany zapewnić pracownikom bezpieczne i higieniczne warunki pracy. O tym, iż obowiązki z zakresu bhp nie wynikają jedynie z przepisów działu X kodeksu pracy pisze między innymi T. Wyka, [w:] *Kodeks pracy. Komentarz*, t. 2. *Art. 94–304[5]*, red. K.W. Baran, Warszawa 2022, s. 1798–1820.


© for this edition by CNS

dzenia wprowadzenie regulacji do kodeksu pracy było posunięciem ze wszech miar zasadnym. Było także wyrazem potrzeby nadzoru i kontroli tej sfery organizacji pracy przez organy PIP, choć bez dostrzeżenia potrzeby zwiększenia udziału tych organów w procesie poprzedzającym zainicjowanie monitoringu przez pracodawcę. Pracodawcy powinni więc zadbać, aby były spełnione wszystkie wymogi formalne poprzedzające wprowadzenie monitoringu, jak również te, które należy dopełnić w trakcie jego funkcjonowania — związane między innymi z obowiązkami informacyjnymi względem nowo zatrudnionych pracowników. Pomimo skodyfikowania kwestii monitoringu, część nadużyć na tym polu będzie niemożliwa lub przynajmniej mocno utrudniona do wykrycia przez inspektora pracy na etapie kontroli przy zdeterminowanym działaniu pracodawcy ukierunkowanym na usuwanie dowodów niezgodnej z prawem aktywności na tym polu. Ograniczeniem efektywnej kontroli mogą być również trudności związane z weryfikacją zakresu prowadzonych przez pracodawcę innych form monitoringu, bliżej nieokreślonych przez ustawodawcę — zapewne dla zwiększenia elastyczności regulacji. W ramach próby wyeliminowania tych trudności sformułowano postulaty *de lege ferenda* mogące wzmocnić ochronę pracowników w tym zakresie, zwłaszcza w sytuacji braku działania u pracodawcy organizacji związkowej lub rozbieżności w stanowiskach w przypadku działania kilku organizacji związkowych. Uprzednie poinformowanie właściwego okręgowego inspektora pracy o zamiarze wprowadzenia monitoringu w zakładzie pracy stanowiłoby z jednej strony narzędzie dyscyplinujące dla samego pracodawcy, który musiałby liczyć się z weryfikacją przyjętych rozwiązań przez organy PIP już od początku ich uruchomienia. Informacja ta, z drugiej strony, mogłaby być również wykorzystana w realizacji tematu kontrolnego obejmującego to zagadnienie i pozwalać na szybkie ujawnienie i wyeliminowanie nieprawidłowości.

## THE ROLE OF THE LABOUR INSPECTOR IN THE CONTROL AND SUPERVISION OF THE APPLICATION OF MONITORING BY THE EMPLOYER: *DE LEGE LATA* AND *DE LEGE FERENDA* CONCLUSIONS

Summary

Due to the relatively short period of being in force of the provisions governing monitoring issues at the employer, the issues related to the supervision and control of this sphere of activities have not been discussed more widely in the literature on the subject so far. The author analyzes the provisions in question in terms of the possibility and scope of control of their compliance by the authorities of the National Labour Inspectorate. As part of the ongoing deliberations, he presents the types of legal remedies that can be used in the event of a labor inspector finding infringements of the provisions related to the use of monitoring and doubts related to it. *De lege ferenda* conclusions are also presented in order to quickly eliminate irregularities in this field and to carry out control more effectively.

Keywords: National Labour Inspectorate, monitoring, employer, control, remedies


© for this edition by CNS

## BIBLIOGRAFIA

Biały P., *5 błędów w przetwarzaniu danych w ramach monitoringu*, „Ochrona Danych Osobowych" 2020, nr 7–8.

Czechowski P., *Geolokalizacja pracowników — nowe wyzwania dla prawa pracy?*, „Praca i Zabezpieczenie Społeczne" 2006, nr 4.

Frąckowiak M., Świeboda T., *Ochrona danych osobowych pracownika w perspektywie RODO i przepisów dotyczących monitoringu wizyjnego stosowanego przez pracodawcę*, „Monitor Prawa Pracy" 2018, nr 7.

Jabłoński M., *Miejsce Państwowej Inspekcji Pracy w systemie organów państwa — wnioski de lege lata i de lege ferenda*, „Przegląd Prawa i Administracji" 118, 2019.

Jasińska-Cichoń A., *Ustawa o Państwowej Inspekcji Pracy. Komentarz,* Warszawa 2008.

Kuba M., [w:] *Kodeks pracy. Komentarz*, t. 1. *Art. 1–93*, red. K.W. Baran, Warszawa 2022.

Kuba M., *Monitoring pracowników na gruncie KP*, „ABI Expert" 2019*,* nr 3.

Makowski D., *Inspekcja pracy jako instytucja państwowego nadzoru nad przestrzeganiem prawa pracy*, Łódź 2017.

Miłosz M., Świątek-Rudoman J., *Nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy*, „Praca i Zabezpieczenie Społeczne" 2019, nr 4.

*Montujesz kamery w miejscy pracy. Sprawdź, o czym należy pamiętać*, Archiwum UODO, 12.08.2020, https://archiwum.uodo.gov.pl/pl/138/1634.

*Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, Urząd Ochrony Danych Osobowych, 4.10.2018, https://uodo.gov.pl/pl/138/545.

Orłowski G., *Nielegalny legalny monitoring*, „Monitor Prawa Pracy" 2018, nr 7.

*Porozumienie pomiędzy Państwową Inspekcją Pracy a Biurem Generalnego Inspektora Ochrony Danych Osobowych w sprawie zasad współdziałania PIP i GIODO*, Państwowa Inspekcja Pracy, 14.12.2012, https://www.pip.gov.pl/pl/f/v/19359/giod0%20pip%2012.pdf.

Rączka K., *Ustawa o Państwowej Inspekcji Pracy. Komentarz*, red. M. Gersdorf, J. Jagielski, K. Rączka, Warszawa 2008.

*Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego*, Urząd Ochrony Danych Osobowych, 10.07.2018, https://uodo.gov.pl/data/filemanager_pl/1200.pdf.

Wyka T., [w:] *Kodeks pracy, Komentarz*, t. 2. *Art. 94–304*$^{5}$, red. K.W. Baran, Warszawa 2022.


© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.10

JANUSZ KRASOŃ
Państwowa Inspekcja Pracy we Wrocławiu

# WYBRANE ZAGADNIENIA ZWIĄZANE Z KONTROLĄ MONITORINGU WIZYJNEGO W ZAKŁADZIE PRACY PROWADZONEJ PRZEZ INSPEKTORA PRACY W KONTEKŚCIE OCHRONY DANYCH OSOBOWYCH

Abstrakt: Przepisy dotyczące monitoringu wizyjnego w zakładzie pracy zawarte w prawie pracy zostały dodane do kodeksu pracy w efekcie uchwalenia RODO, stąd też korespondują z zasadami i przepisami ochrony danych osobowych. Specyfika tych przepisów wpływa na postępowanie kontrolne inspektora pracy.

Słowa kluczowe: Państwowa Inspekcja Pracy, kodeks pracy, kontrola monitoringu, RODO, pracodawca

## WPROWADZENIE

Kontrola monitoringu wizyjnego w zakładzie pracy prowadzona przez inspektora pracy jest postępowaniem wynikającym z obowiązków nałożonych przez ustawodawcę na Państwową Inspekcję Pracy w zakresie kontroli i nadzoru przestrzegania przepisów prawa pracy. Jednak z powodu istoty monitoringu jest postępowaniem niełatwym, w którym kontrolujący obarczony zostaje społecznym kontekstem przedmiotowego zagadnienia i zawiłościami natury prawnej.

Realizacja uprawnień kontrolnych pracodawcy, a monitoring jest właśnie takim uprawnieniem, wiąże się z koniecznością respektowania przez pracodawcę wielu regulacji zarówno z zakresu prawa pracy, jak i prawa cywilnego, niekiedy też prawa karnego. Wdrożony przez pracodawcę monitoring wizyjny, w zależności od jego zakresu oraz stosowanych narzędzi, może stanowić zagrożenie dla dóbr osobistych pracownika, przede wszystkim jego godności oraz prywatności. Informacje pozyskiwane w jego toku należy kwalifikować jako dane osobowe w rozumieniu przepisów o ochronie danych osobowych.

Wydaje się zasadnym, aby w przypadku omawiania postępowania kontrolnego monitoringu zakładowego prowadzonego przez inspektora pracy z jednej


© for this edition by CNS

strony omówić wymogi jakie determinują wprowadzenie tej formy kontroli pracownika w kontekście ochrony danych osobowych, z drugiej — zwrócić uwagę na trudności w zakresie dokonania przez inspektora pracy pełnej oceny, czy zastosowany w zakładzie monitoring jest zgodny z prawem.

## MONITORING WIZYJNY PRACOWNIKA A OCHRONY DANYCH OSOBOWYCH

Zgodnie z art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W następstwie stosowania monitoringu wizyjnego pracodawca gromadzi informacje o pracowniku, a więc o osobie zidentyfikowanej[1]. Wagę problematyki podkreślił Prezes Urzędu Ochrony Danych Osobowych, który w czerwcu 2018 roku opublikował na stronach internetowych Urzędu wskazówki dotyczące wykorzystywania monitoringu wizyjnego, w których stwierdził, że: „Monitoring wizyjny jest inwazyjną formą przetwarzania danych osobowych i jako taki powinien podlegać szczególnej weryfikacji przez administratora potrzeby jego stosowania i konieczności zabezpieczenia oraz kontroli przez organy kontrolne”[2].

Przepisy dotyczące monitoringu wizyjnego pracowników zostały przyjęte w wyniku reformy prawa ochrony danych osobowych, która z kolei była następstwem uchwalenia przez Parlament Europejski rozporządzenia RODO. Zgodnie z art. 88 ust. 1 RODO kraje Unii Europejskiej mogły przyjąć szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników, dotyczących między innymi rekrutacji, wykonania umowy o pracę, obowiązków prawnych, zarządzania, planowania i organizacji pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy, korzystania ze świadczeń związanych z zatrudnieniem czy celów zakończenia stosunku pracy. Przesądzono także, że regulacje krajowe muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności oraz prawnie uzasadnionych interesów i praw podstawowych. Monitoring w miejscu pracy został więc potraktowany szczególnie i uznany jako istotny w znaczeniu społecznym. Polski ustawodawca wprowadził regulacje sektoro-

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, Dz.Urz.UE L 119 z 4.05.2016 r.

[2] *Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego. Wersja 1*, Urząd Ochrony Danych Osobowych, 10.07.2018, https://uodo.gov.pl/data/filemanager_pl/1200.pdf (dostęp: 19.08.2022).


© for this edition by CNS

we dotyczące ochrony danych osobowych pracowników dokonując stosownych zmian w kodeksie pracy. Przepisy zostały dodane do k.p. na podstawie ustawy o ochronie danych osobowych[3]. Obowiązują one od 25 maja 2018 roku, przy czym art. $22^2$ w obecnym brzmieniu obowiązuje od 4 maja 2019 roku[4]. Można je zatem uznać za przepisy szczególne w rozumieniu art. 88 RODO.

Przepisy regulujące monitoring w zakładzie pracy zawarte w art. $22^2$ k.p. dają pracodawcy prawo do ich wdrożenia i precyzują wymogi niezbędne do spełnienia, a w przypadku pracodawcy-administratora określają podstawę prawną dla przetwarzania danych osobowych. Zauważyć można, że treść przywołanego artykułu koresponduje z wieloma zasadami dotyczącymi przetwarzania danych osobowych opisanymi w RODO. Poniżej opisanych zostanie kilka przykładów korelacji przepisów zawartych w art. $22^2$ k.p. z wybranymi zasadami przetwarzania danych osobowych wynikających z RODO.

Zgodnie z art. $22^2$ § 1 pracodawca może, w pewnych okolicznościach, wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu — jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Z przepisu wynika, że pracodawca ma prawo zastosować monitoring tylko i wyłącznie w celach wymienionych w tym artykule, więc mamy tu do czynienia z jednoznacznie określonym celem przetwarzania danych osobowych pracowników. Jednocześnie katalog przesłanek pozwalający na wprowadzenie monitoringu wizyjnego w zakładzie pracy jest zamknięty. Zastosowanie przez pracodawcę tej formy kontroli wobec pracowników w innych celach będzie niezgodne z prawem pracy, a także naruszy przepisy o ochronie danych osobowych.

Na podstawie art. $22^2$ § 3 k.p. pracodawca przechowuje nagrania obrazu przez okres nieprzekraczający trzech miesięcy od dnia nagrania. Regulacja odnosi się wprost do zasady ograniczenia czasowego, wedle której dane osobowe nie mogą być przechowywane w formie umożliwiającej identyfikację osób fizycznych przez okres dłuższy, niż jest to niezbędne do celów, dla których dane są przetwarzane. Mówi o tym art. 5 ust. 1 lit. e RODO. Jeśli jednak nagrania mają stanowić dowód w postępowaniu prowadzonym na podstawie przepisów prawa lub pracodawca powziął wiadomość, że mogą stanowić dowód w takim postępowaniu, okres trzech miesięcy ulega przedłużeniu do czasu prawomocnego zakończenia postępowania — art. $22^2$ § 4 k.p. Ustalenie powyższej okoliczności jako przesłan-

[3] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. z 2019 r. poz. 1781.

[4] Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 (ogólne rozporządzenie o ochronie danych), Dz.U. z 2019 r. poz. 730.


© for this edition by CNS

ki dalszego przechowywania nagrań z monitoringu należy uznać jako prawnie uzasadniony interes pracodawcy-administratora danych osobowych w rozumieniu art. 6 ust. 1 lit. f RODO. Z kolei art. $22^2$ § 5 k.p. stanowi, że po upływie okresu trzech miesięcy lub — w przypadku wskazanym w art. $22^2$ § 4 k.p. — po prawomocnym zakończeniu postępowania, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu.

Kolejną zasadą zawartą w omawianych przepisach jest zasada jawności kontroli pracownika. Pracodawca jest zobowiązany realizować powyższą zasadę wielopłaszczyznowo. Po pierwsze, informacja dotycząca monitoringu wizyjnego ma mieć charakter informacji zbiorowej, skierowanej do ogółu pracowników, bowiem zgodnie z art. $22^2$ § 7 k.p. pracodawca ma obowiązek poinformowania pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż dwa tygodnie przed jego uruchomieniem. Informacja ta ma charakter uprzedni. Po drugie, informowanie o monitoringu ma odbywać się także w trybie indywidualnym. Art. $22^2$ § 8 k.p. stanowi, że przed dopuszczeniem pracownika do pracy pracodawca przekazuje mu pisemną informację o celu, zakresie i sposobie zastosowania monitoringu.

Niezależnie od spełnienia obowiązku informacyjnego, na zasadach wskazanych w art. $22^2$ § 7–8 k.p. pracodawca ma również dokonać odpowiedniego oznaczenia terenu objętego monitoringiem, tak aby pracownik nie miał wątpliwości, która konkretnie przestrzeń jest poddana kontroli. Jak stanowi art. $22^2$ § 9 k.p., pracodawca jest zobowiązany oznaczyć pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych. Ma to uczynić nie później niż dzień przed uruchomieniem monitoringu. Poza obowiązkami o charakterze informacyjnym ustawodawca przesądza również o sposobie wdrożenia szczególnego nadzoru nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu.

W myśl art. $22^2$ § 6 k.p. cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub regulaminie pracy, a jeśli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy, kwestie te mają się znaleźć w obwieszczeniu. W zależności zatem od tego, który z powyższych wariantów znajduje zastosowanie, pracodawca uzgadnia te zagadnienia ze związkami zawodowymi albo ustala je sam.

Spełnienie przez pracodawcę ustanowionych na mocy art. $22^2$ § 7–9 k.p. obowiązków informacyjnych związanych z wdrażaniem monitoringu wizyjnego nie konsumuje jednak obowiązków pracodawcy jako administratora danych osobowych. Jak stanowi art. $22^2$ § 10 k.p., przepis art. $22^2$ § 9 k.p. nie narusza art. 12 i 13 RODO.

Warto także zauważyć, że w art. $22^2$§ 1 i 2 ustawodawca, wyznaczając jednoznacznie granice dopuszczalnego monitoringu pracownika, dodatkowo podkreślił kwestie ochrony godności i dóbr osobistych pracownika oraz zasadę wolności


© for this edition by CNS

i niezależności związków zawodowych, co wyraża się w zakazie monitoringu wizyjnego w pomieszczeniach sanitarnych, szatniach, stołówkach, palarniach i pomieszczeniach udostępnianych zakładowej organizacji związkowej, chyba że jest to niezbędne dla realizacji celu określonego w art. $22^2$ § 1 i nie narusza godności i innych dóbr osobistych pracownika. Przepisy te korespondują także z zasadami dotyczącymi przetwarzania danych osobowych określonymi w art. 5 w związku z art. 6 w związku z art. 9 RODO.

Szerszej refleksji wymaga na koniec zawarta w art. $22^2$ § 1 zasada adekwatności i proporcjonalność gromadzenia danych osobowych. Przywołany przepis nie tylko definiuje cele, dla realizacji których pracodawca może wdrożyć monitoring wizyjny, ale wprowadza dodatkowe kryterium — „pojęcie niezbędności" — którego spełnienie jest wymogiem koniecznym przy wprowadzaniu tej formy kontroli. Opisując nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy, Michał Miłosz i Justyna Świątek-Rudoman słusznie zauważają, że:

> ze względu na inwazyjność nadzoru wizyjnego jako formy przetwarzania danych osobowych monitoring może być zastosowany, jeśli zamierzonych celów nie może pracodawca osiągnąć innymi efektywnymi metodami niewymagającymi przetwarzania danych osobowych lub w mniejszym stopniu ingerującymi w prawo jednostki do prywatności i ochrony danych osobowych. Pracodawca musi ocenić, czy obszar, na jakim ma być wprowadzony monitoring wizyjny oraz parametry stosowanego systemu monitoringu (np. pole kamer, ciągły charakter monitoringu, wysoka rozdzielczość nagrań umożliwiająca odczyt monitorów komputerowych) są adekwatne do osiągnięcia zamierzonych celów i w konsekwencji ograniczyć obszar monitorowania oraz parametry systemu do niezbędnego zakresu[5].

Narzędziem przydatnym do określenia niezbędności przetwarzania danych osobowych w kontekście wdrożonego monitoringu może być ocena skutków dla ochrony danych osobowych DPIA (Data Protection Impact Assessment). DPIA to proces mający na celu scharakteryzowanie przetwarzania danych, dokonanie oceny jego niezbędności i proporcjonalności oraz wsparcie administratora w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z tego przetwarzania. Ocena skutków ma służyć ocenie ryzyka, na jakie narażone jest przetwarzanie danych osobowych, a także do wprowadzenia adekwatnych środków zaradczych ograniczających to ryzyko do poziomu akceptowalnego. Czynności, dla których przeprowadzenie oceny jest obowiązkowe, znajdują umocowanie w art. 35 ust. 4 RODO. Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Podstawą ogłoszenia Komunikatu Prezesa Urzędu Ochrony Danych Osobowych jest art. 54 ust. 1 pkt 1 w związku z art. 172 ustawy o ochronie danych osobowych. Prezes Urzędu Ochrony danych

[5] M. Miłosz, J. Świątek-Rudoman, *Nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy*, „Praca i Zabezpieczenie Społeczne" 2019, nr 4, s. 34.


© for this edition by CNS

osobowych w wydanych niewiążących wytycznych przygotował propozycję wykazu operacji, w jakich przetwarzanie danych osobowych przy użyciu monitoringu wizyjnego wymagają przeprowadzenia oceny skutków[6]. Z opublikowanego wykazu operacji wynika, że Prezes UODO nie wskazał monitoringu wewnątrzzakładowego jako operacji wymagającej dokonania oceny DPIA. Natomiast Grupa Robocza art. 29[7] w swoich zaleceniach interpretuje że ocenę skutków należy dokonać w sytuacji, kiedy przetwarzanie danych odbywa się na dużą skalę, co znaczy, że należy wziąć pod uwagę: liczbę osób, których dane dotyczą, ilość danych, czas trwania lub ciągłość przetwarzania oraz zakres geograficzny przetwarzania, a z taką sytuacją mamy do czynienia w wielu podmiotach zatrudniających pracowników. Ponadto Grupa Robocza art. 29 wskazała wśród przykładów przetwarzania, w których istnieje prawdopodobieństwo, że wymagane będzie przeprowadzenie oceny skutków dla ochrony danych sytuację, w której „przedsiębiorstwo systematycznie monitoruje działania swoich pracowników m.in. ich stanowiska pracy".

## ZAKRES KONTROLI INSPEKTORA PRACY

Nie ulega wątpliwości, że kwestie związane z monitoringiem wizyjnym w zakładzie pracy mają prawo kontrolować pracownicy Urzędu Ochrony Danych Osobowych w imieniu prezesa tego urzędu. Podstawę do tego dają art. 34, 60 i 78 u.o.d.o. Z przytoczonych przepisów wynika, że organem właściwym w sprawie ochrony danych osobowych jest prezes UODO, a także że to on przeprowadza kontrolę przestrzegania przepisów o ochronie danych oraz prowadzi postępowanie w sprawie ich naruszenia. Z drugiej strony prawo do kontroli monitoringu wchodzi w zakres uprawnień Państwowej Inspekcji Pracy. Artykuł $18^4$ k.p. i art. 10 ustawy o PIP[8] stanowi, że inspekcja pracy sprawuje nadzór i kontrolę przestrzegania prawa pracy — a więc również zamieszczonych w k.p. regulacji dotyczących monitoringu. Z powyższego wynika, że inspektor pracy kontroluje monitoring wizyjny w zakładzie pracy i ocenia, czy pracodawca dostosował się przy jego wprowadzaniu do wymogów zawartych w art. $22^2$ k.p.

---

[6] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, M.P. z 2019 r. poz. 666.

[7] *Opinia 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy, WP 249*, Archiwum GIODO, 21.02.2018, https://archiwum.giodo.gov.pl/pl/file/13179 (dostęp:19.08.2022). Grupa Robocza powołana została na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych jako niezależny podmiot o charakterze doradczym. Została rozwiązana 25 maja 2018 r., a w jej miejsce powołano Europejską Radę Ochrony Danych.

[8] Ustawa z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy, Dz.U. z 2022 r. poz. 1614.


© for this edition by CNS

Oczywistym jest, że wdrożenie monitoringu dopuszczalne jest jedynie w celu zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, dlatego też monitoring służący innym celom będzie przez inspektora pracy zakwestionowany jako niezgodny z prawem. Zdecydowanie trudniejszą kwestią będzie dla inspektora pracy rozstrzygnięcie czy wdrożenie monitoringu było niezbędne w sytuacji, kiedy pracodawca zastosował monitoring zgodnie z celami określonymi w art. $22^2$ § 1. k.p., to znaczy czy zastosowanie monitoringu było faktycznie niezbędne do zapewnienia określonego przez pracodawcę celu. W praktyce nie jest to jednak sprawa prosta. Inspektor pracy miałby bowiem ocenić, czy osiągnięcie celów nie byłoby możliwe bez wprowadzania monitoringu w sytuacji, kiedy ocena niezbędności wdrożenia tej formy kontroli pracownika leży w kompetencjach pracodawcy. Inspektor pracy ma ograniczone możliwości weryfikacji podjętej przez pracodawcę decyzji. Nie ma tu też znaczenia, czy pracodawca-administrator dokonał przed wdrożeniem monitoringu oceny skutków dla ochrony danych osobowych, czy też jej nie dokonał, bowiem inspektor pracy nie ma podstawy prawnej ani kompetencji, by rozstrzygnięcie pracodawcy w tym zakresie kwestionować lub weryfikować. Zgodnie z art. 21 ustawy o PIP postępowanie kontrolne inspektora pracy ma na celu ustalenie stanu faktycznego w zakresie przestrzegania prawa pracy. Ustalając stan faktyczny inspektor pracy musi rozstrzygnąć nie tylko, czy był on niezbędny, ale również czy wprowadzony w określonym celu monitoring służy do osiągnięcia tego celu. Zasadność uznania ochrony bezpieczeństwa pracowników za uzasadniony cel stosowania monitoringu nie budzi wątpliwości. Może je natomiast wywołać sytuacja, kiedy stan faktyczny zastosowanego monitoringu wskazuje, że nie obejmuje wyłącznie pracowników, ale głównie osoby trzecie, takie jak klienci, kontrahenci czy dostawcy, a także osoby świadczące na rzecz pracodawcy usługi lub pracę na podstawie innej niż stosunek pracy, na przykład zleceniobiorcy czy samozatrudnieni. Zdecydowanie problematycznym w ocenie będzie także monitoring zastosowany w celu bezpieczeństwa pracowników wykonujących prace o niskim ryzyku wystąpienia zdarzeń zagrażających ich bezpieczeństwu, takich jak na przykład pracownicy biurowi. W przypadku, kiedy okolicznością uzasadniającą wprowadzenie monitoringu wizyjnego w miejscu pracy jest ochrona mienia, ocena stanu faktycznego wydawałaby się z pozoru prostsza, jeśli monitoring rzeczywiście swoim zakresem chroni mienie, oraz jeśli przyjmiemy, że ochronę mienia interpretujemy zgodnie z ustawą o ochronie osób i mienia[9] i rozumiemy jako działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do wstępu osób nieuprawnionych na teren chroniony. Ustawodawca nie wskazał, o czyje mienie chodzi, należy wobec tego przyjąć, że wprowadzenie monitoringu wizyj-

[9] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, Dz.U. z 2021 r. poz. 1995.


© for this edition by CNS

nego uzasadniać będzie ochrona mienia nie tylko należącego do pracodawcy, ale również do pracowników, zleceniobiorców czy osób trzecich. W praktyce analiza stanu faktycznego może jednak stwarzać kłopoty w ocenie inspektora pracy także i w tym przypadku. Trudno jest jednoznacznie stwierdzić, czy wprowadzony w celu ochrony mienia monitoring swym zasięgiem nie obejmuje również pracowników lub głównie pracowników pod pretekstem ochrony mienia, wychodząc w ten sposób poza cel, do realizacji którego został wdrożony.

Kolejną przesłanką, której sformułowanie wywołuje trudności interpretacyjne i problemy w ustaleniu stanu faktycznego, jest kontrola produkcji. Czy należy ją rozumieć wyłącznie jako monitoring procesów produkcyjnych zapewniający ich prawidłowy przebieg, czy również jako kontrola wydajności produkcji i efektywności świadczonej pracy (popularna na przykład w magazynach, dużych halach produkcyjnych i montażowych), która potencjalnie mogłaby stanowić podstawę oceny pracownika? Opisując kryteria dopuszczalności stosowania monitoringu w miejscu pracy oraz związane z tym obowiązki pracodawcy w świetle reformy ochrony danych osobowych, Olga Dąbrowska słusznie zauważa, że:

> W opublikowanych przez Prezesa Urzędu Ochrony Danych Osobowych wskazówkach dotyczących wykorzystania monitoringu wizyjnego wyraźnie stanął on na stanowisku, że niedopuszczalne jest stosowanie monitoringu jako środka nadzoru nad jakością wykonywanej pracy. Taka interpretacja wydaje się zgodna nie tylko z literalnym brzmieniem przepisu, który wyraźnie stanowi nie o „kontroli świadczonej pracy", a „kontroli produkcji", ale również z zaleceniami Grupy Roboczej art. 29. Ostatnią przesłanką stanowiącą podstawę do wprowadzenia środków technicznych umożliwiających rejestrację obrazu jest zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. O ile cel ten nie budzi zastrzeżeń, o tyle przedmiotowa forma monitoringu nie wydaje się odpowiednia w kontekście ochrony informacji, zwłaszcza że przepisy o monitoringu nie zezwalają na nagrywanie dźwięku towarzyszącego zdarzeniom, a zgodnie z poglądem Prezesa Urzędu Ochrony Danych Osobowych stosowanie rejestracji dźwięku może zostać uznane za nadmiarową formę przetwarzania danych i wiązać się z odpowiedzialnością administracyjną, cywilną, a nawet karną[10].

Decydując się na wprowadzenie monitoringu przy użyciu kamer, pracodawca powinien mieć na względzie właściwe ich rozmieszczenie na terenie zakładu pracy. Ulokowanie kamer w miejscach, w których pracownik ma szczególne prawo oczekiwać poszanowania prywatności, jest sprzeczne z prawem. Ustawodawca przesądził w art. $22^2$ § 2 k.p. zakaz prowadzenia monitoringu w pomieszczeniach sanitarnych, szatniach, stołówkach oraz palarniach, jak również w pomieszczeniach udostępnianych zakładowej organizacji związkowej. Zakaz ten nie ma jednak charakteru bezwzględnego, co powoduje, że kontrola przestrzegania wymogów zawartych w tym przepisie może stwarzać spore problemy. W myśl komentowanego przepisu zainstalowanie środków technicznych umożliwiających

[10] O. Dąbrowska, *Kryteria dopuszczalności stosowania monitoringu w miejscu pracy oraz związane z tym obowiązki pracodawcy w świetle reformy ochrony danych osobowych*, „Prawo Mediów Elektronicznych" 2019, nr 1, s. 16.


© for this edition by CNS

rejestrację obrazu w wyżej wymienionych pomieszczeniach jest dopuszczalne, jeśli jest ono niezbędne dla realizacji celu określonego w art. $22^2$ § 1 k.p. i pod warunkiem, że nie naruszy to godności i innych dóbr osobistych pracownika. Jak wskazuje się w art. $22^2$ § 2 k.p., jest to możliwe w szczególności dzięki zastosowaniu technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Nasuwają się jednak wątpliwości, czy prowadzenie monitoringu na takich zasadach realizuje w ogóle jakiś cel, skoro istotą użytkowania narzędzi takich jak kamery jest ułatwienie ustalenia tożsamości sprawców naruszeń. Trudno sobie ponadto wyobrazić poszanowanie godności czy prywatności pracownika przy zastosowaniu kamer w miejscach takich jak toalety czy szatnie. Ocena stanu faktycznego przez inspektora pracy, a zwłaszcza rozstrzygnięcie, czy w sytuacji wdrożenia monitoringu w pomieszczeniach sanitarnych i szatniach zastosowane techniki są właściwe, może być w praktyce niemożliwe, a w każdym razie mocno subiektywne. Przesądzenie zaś, czy zastosowane techniki (niska rozdzielczość kamer itp.) są właściwe, znajduje się zdecydowanie poza kompetencjami inspektora pracy. Wydaje się, że ustawodawca dokonał zbyt daleko idącego uproszczenia włączając do tej samej kategorii pomieszczenia sanitarne i szatnie, stołówki, palarnie. Bezsprzecznie ryzyko naruszenia dóbr osobistych pracownika w przypadku pomieszczeń sanitarnych i szatni jest największe. Zdaniem Grupy Roboczej art. 29 toalety, łazienki czy szatnie to miejsca, które są przeznaczone do osobistego użytku pracowników, dlatego też nie powinny być one objęte monitoringiem wizyjnym. Druga kategoria wskazanych w art. $22^2$ § 2 k.p. pomieszczeń to stołówki i palarnie, a więc w dalszym ciągu miejsca nieprzeznaczone do wykonywania pracy. Wydaje się jednak, że ewentualne zamieszczenie kamer w tym obszarze nie jest dla pracownika tak dotkliwe, jak w przypadku pierwszej grupy pomieszczeń.

Najmniej problematyczną w postępowaniu kontrolnym inspektora pracy wydaje się ocena wykonania obowiązku jawności przetwarzania danych oraz obowiązku informacyjnego pracodawcy wobec pracowników. Wyrazem tego jest wymóg odpowiedniego formalnego uregulowania funkcjonowania monitoringu w zakładzie pracy oraz obowiązki informacyjne ciążące w tym względzie na pracodawcy. Przepisy kodeksu pracy zawarte w art. $22^2$ § 7, 8 i 9 przewidują przede wszystkim, że szczegółowe cele, zakres oraz sposób zastosowania monitoringu wizyjnego ustalany jest w układzie zbiorowym pracy lub w regulaminie pracy, a w sytuacji, gdy pracodawca nie jest obowiązany do ustalenia regulaminu pracy i nie jest objęty układem zbiorowym — uregulowanie powyższych kwestii następuje w drodze obwieszczenia. W opinii Grupy Roboczej art. 29 zalecono włączenie w proces opracowywania wewnętrznych zasad i polityk dotyczących monitoringu reprezentatywnej grupy pracowników. Zakres kontroli inspektora pracy będzie więc polegał na sprawdzeniu, czy w akcie wprowadzającym tę formę nadzoru pracodawcy wskazali cele, do jakich monitoring wizyjny będzie stosowany, czy określili obszar nim objęty, w tym również to, czy monitoring funkcjonuje jedynie w budynkach stanowiących zakład pracy, czy obejmuje również teren wokół zakładu


© for this edition by CNS

pracy. W zależności od okoliczności inspektor pracy oceni, czy konieczne będzie doprecyzowanie, w jakich budynkach lub na jakich obszarach został zastosowany monitoring. Jego zakres może być określany także w sposób negatywny przez wskazanie obszarów na terenie zakładu pracy, których monitoring nie obejmuje.

Problemów nie będzie stwarzać także kontrola obowiązku informacyjnego polegającego na udostępnieniu pracownikom wiadomości o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy we właściwym terminie i we właściwej formie pisemnej oraz czy zgodnego z przepisami oznaczenia monitorowanych pomieszczeń i teren w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych.

## PODSUMOWANIE

Dotychczasowa praktyka postępowań kontrolnych inspektorów pracy dotyczących monitoringu w zakładach pracy, prowadzonych głównie w efekcie skarg pracowników, wskazuje, że w zasadniczej mierze dokonują oni kontroli obowiązków formalnych, jakie spełnić musi pracodawca wdrażając tą formę kontroli pracowników. Większość pracodawców decydując się na zastosowanie monitoringu jako cel jego wdrożenia określa bezpieczeństwo pracowników i ochronę mienia. W tym przypadku, na co wskazano powyżej, inspektor pracy nie ma ani uprawnień, ani możliwości przy ocenie stanu faktycznego stwierdzić, czy wdrożony monitoring był niezbędny i czy zastosowany zakres jest właściwy. Ocena stanu faktycznego dotyczącego obowiązków informacyjnych i uregulowania monitoringu w aktach prawa zakładowego nie stwarza takich problemów, a stwierdzenie przez inspektora pracy naruszenia prawa nie budzi zastrzeżeń pracodawcy.

W razie stwierdzenia naruszenia przepisów prawa pracy inspektor pracy, zgodnie z art. 11 ustawy o PIP, ma uprawnienie skierowania do pracodawcy wystąpienia lub wydania polecenia, w sprawie usunięcia naruszenia przepisów prawa pracy, a także wyciągnięcia konsekwencji w stosunku do osób winnych zaistniałej sytuacji. Wystąpienie lub polecenie inspektora pracy nie jest jednak środkiem władczym, z jakim mamy do czynienia w przypadku nakazu inspektora pracy. W sytuacjach problematycznych, wychodzących poza uprawnienia inspektora pracy, dotyczących monitoringu wizyjnego, a także domniemania naruszenia przez pracodawcę przepisów o ochronie danych osobowych, inspektor wysyła stosowne zawiadomienie do Prezesa UODO. Taką możliwość daje mu podpisane porozumienie pomiędzy Państwową Inspekcją Pracy a Biurem Generalnego Inspektora Ochrony Danych Osobowych w sprawie współdziałania PIP i GIODO[11]. Dość

[11] *Porozumienie pomiędzy Państwową Inspekcją Pracy a Biurem Generalnego Inspektora Ochrony Danych Osobowych w sprawie zasad współdziałania PIP i GIODO*, Państwowa Inspekcja Pracy, 14.12.2012, https://www.pip.gov.pl/pl/f/v/19359/giod0%20pip%2012.pdf (dostęp: 13.08.2022).


© for this edition by CNS

powszechną praktyką inspektorską w przypadku braku możliwości przesądzenia, czy mamy do czynienia z naruszeniem ochrony danych osobowych, jest wysłanie przez inspektora pracy skarżącemu się pracownikowi informacji o przysługującym mu prawie zgłoszenia do Prezesa UODO skargi o naruszenie jego danych osobowych.

## SELECTED ISSUES RELATED TO THE CONTROL OF VIDEO MONITORING IN THE WORKPLACE CONDUCTED BY A LABOR INSPECTOR IN THE CONTEXT OF PERSONAL DATA PROTECTION

Summary

The provisions on video monitoring in the workplace contained in the labor law were added to the Labor Code as a result of the adoption of the GDPR, hence they correspond to the principles and provisions of personal data protection. The specificity of these provisions affects the control procedures of the labor inspector.

Keywords: National Labor Inspectorate, Labor Code, monitoring control, GDPR, employer

## BIBLIOGRAFIA

Dąbrowska O., *Kryteria dopuszczalności stosowania monitoringu w miejscu pracy oraz związane z tym obowiązki pracodawcy w świetle reformy ochrony danych osobowych*, „Prawo Mediów Elektronicznych" 2019, nr 1.

Miłosz M., Świątek-Rudoman J., *Nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy*, „Praca i Zabezpieczenie Społeczne" 2019, nr 4.

*Opinia 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy, WP 249*, Archiwum GIODO, 21.02.2018, https://archiwum.giodo.gov.pl/pl/file/13179.

*Porozumienie pomiędzy Państwową Inspekcją Pracy a Biurem Generalnego Inspektora Ochrony Danych Osobowych w sprawie zasad współdziałania PIP i GIODO*, Państwowa Inspekcja Pracy, 14.12.2012, https://www.pip.gov.pl/pl/f/v/19359/giod0%20pip%2012.pdf.

*Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego*, Urząd Ochrony Danych Osobowych, 10.07.2018, https://uodo.gov.pl/data/filemanager_pl/1200.pdf.


© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.11

ŁUKASZ PAROŃ
ORCID: 0000-0002-5865-6622
Ośrodek Szkolenia Państwowej Inspekcji Pracy im. Profesora Jana Rosnera we Wrocławiu

# DANE Z MONITORINGU JAKO ŹRÓDŁO DOWODOWE W POSTĘPOWANIU KONTROLNYM PAŃSTWOWEGO INSPEKTORA PRACY

Abstrakt: Dokonujący się postęp technologiczny powoduje zmiany w wielu obszarach naszego życia. W stosunkach zatrudnienia wykorzystywane są coraz doskonalsze sposoby monitorowania pracy świadczonej przez zatrudnionych. Przyczyny takiego działania są zrozumiałe i zostały zaakceptowane przez ustawodawcę. Jednocześnie prawodawca zezwala na stosowanie monitoringu w określonych przypadkach i z zachowaniem określonych przesłanek. Dane zgromadzone podczas monitorowania pracy są bardzo przydatne dla pracodawców. Wydaje się jednak, że te same dane mogą okazać się pomocne dla państwowych inspektorów pracy przeprowadzających kontrolę w zakresie przestrzegania przepisów prawa pracy. Umożliwiają bowiem ustalenie stanu faktycznego w sposób obiektywny i dojście do prawdy materialnej. Niniejszy artykuł jest próbą odpowiedzi w przedmiocie dopuszczalności stosowania dowodu z monitoringu w toku postępowania kontrolnego prowadzonego przez państwowego inspektora pracy.

Słowa kluczowe: kontrola państwowej inspekcji pracy, postępowanie dowodowe państwowego inspektora pracy, monitoring, dowody w postępowaniu kontrolnym

## WPROWADZENIE

Postęp technologiczny i rozwój społeczeństwa cyfrowego ściśle powiązany jest z rozwojem technik informatycznych, cyfrowych i elektronicznych. Jednym z jego przejawów jest monitoring, do którego wykorzystuje się coraz bardziej rozwinięte instrumenty techniczne. Już sam fakt, że monitoring ujmowany jest jako zjawisko polegające na „stałej obserwacji i kontroli jakichś procesów lub zjawisk[1]" może dostarczać wielu istotnych informacji. Rozwój techniki powoduje zwiększenie rodzajów i ilości gromadzonych informacji. Są one w sposób automatyczny przetwarzane i wykorzystywane dla różnych celów, najczęściej zwią-

[1] *Monitoring*, [hasło w:] Słownik języka polskiego PWN, https://sjp.pwn.pl/szukaj/monitoring.html (dostęp: 30.12.2022).


© for this edition by CNS

zanych z procesami optymalizacyjnymi w produkcji, sektorze usług czy innych obszarach aktywności człowieka. Dziedziną, w której stosowano monitoring od kilkunastu lat, było również prawo pracy, jednak zauważyć należy, że dopiero w 2018 roku[2] nastąpiło prawne uregulowanie tego problemu w stosunkach pracy. Uzasadnieniem dla takiej decyzji były niewątpliwie dwie przesłanki. Pierwszą była konieczność regulacji coraz powszechniej występującego zjawiska, którym jest monitoring, będący kwalifikowaną formą kontroli pracownika. Drugą przesłanką była potrzeba wyznaczenia granicy dopuszczalnej możliwości ingerencji pracodawcy (za którą różne formy monitoringu niewątpliwie należy uznać) w sferę godności i życia prywatnego pracownika .

Rozwój i postęp technologiczny nie może pozostawać bez wpływu na działalność organów państwowych i skuteczność ich postępowania. Uznając za bezdyskusyjną potrzebę istnienia Państwowej Inspekcji Pracy jako gwaranta przestrzegania przepisów prawa pracy[3], konieczne jest dostrzeżenie potrzeby rozwoju instrumentów dostępnych Państwowej Inspekcji Pracy dla realizacji powierzonych zadań. Stosowane przez pracodawców techniki monitoringu mogą być, jak się wydaje, wykorzystywane nie tylko przez podmioty zatrudniające. Ich zapisy mogą być podstawą do ustalenia stanu faktycznego przez organy kontrolujące prawo pracy, to jest państwowych inspektorów pracy. Celem niniejszego artykułu jest analiza dopuszczalności stosowania monitoringu jako dowodu w postępowaniu kontrolnym PIP, ze szczególnym wskazaniem oceny przydatności takiego rozwiązania. Zagadnienie to jest doniosłe praktycznie, a nie było dotychczas przedmiotem analiz i rozważań w literaturze.

## MONITORING W ZAKŁADZIE PRACY

Przepisy kodeksu pracy usankcjonowały możliwość stosowania różnych form monitoringu aktywności pracownika, wyznaczając również zasady ich stosowania. Jak zauważa Dominika Dörre-Kolasa[4], ustawodawca w celu zapewnienia ochrony praw i wolności zdecydował się na skorzystanie z przewidzianej w art. 88 RODO[5] możliwości bardziej szczegółowego uregulowania — za sprawą norm krajowych

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tekst jedn. Dz.U. z 2019 r. poz. 1781 ze zm.

[3] D. Makowski, *Państwowa Inspekcja Pracy*, [w:] *System prawa pracy*, t. 8. *Prawo rynku pracy*, red. M. Włodarczyk, Warszawa 2018, s. 1455.

[4] D. Dörre-Kolasa, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa 2018, s. 320.

[5] Rozporządzenie Parlamentu Europejskiego i RADY (UE) 2016/679 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), Dz.Urz.UE L 119 z 5.04.2016 r., s. 1.


© for this edition by CNS

— przetwarzania danych osobowych pracowników związanych z zatrudnieniem. Podkreślenia wymaga fakt, że regulacja kodeksowa w zakresie stosowanego monitoringu została podzielona na część dotyczącą monitoringu w postaci rejestracji obrazu, monitoringu poczty elektronicznej oraz innych form monitoringu. Weronika Kupny[6] zwraca uwagę na wielość form monitoringu stosowanego przez pracodawców, i to zarówno tych wymienionych przez ustawodawcę wprost, jak i takich, które mieszczą się w kategorii „innych" form, jak na przykład kontrolowanie wykazu połączeń telefonicznych, kontrolowanie aktywności pracownika w internecie czy geolokalizację. Z perspektywy omawianego tematu należy zwrócić uwagę na zakres monitoringu. Paweł Fajgielski[7] zauważa, że wprowadzając normy dotyczące monitoringu wizyjnego do ustawy z dnia 26 czerwca 1974 roku Kodeks pracy[8] (dalej k.p.), ustawodawca przesądził definitywnie o możliwości rejestracji obrazu, natomiast nie dopuścił nagrywania dźwięku lub obrazu i dźwięku, co miało zapobiegać dalej idącym formom ingerowania w sferę prywatności osób objętych zasięgiem monitoringu[9]. Podkreślenia wymaga również to, że przesłanką zastosowania monitoringu wizyjnego są enumeratywnie wskazane przypadki, to jest zapewnienie bezpieczeństwa pracowników, ochrona mienia, kontrola produkcji oraz zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Należy jednocześnie zaznaczyć, że monitoring wizyjny nie może stanowić środka kontroli pracy wykonywanej przez pracownika, co wyklucza dokonywanie ocen jakości pracy na podstawie tak zgromadzonego przez pracodawcę materiału dowodowego[10].

Monitoring wizyjny nie jest jednak jedyną kwalifikowaną formą kontroli pracownika. Ustawodawca w k.p. wskazuje również monitoring poczty elektronicznej oraz inne formy monitoringu. Podkreślić należy, że wyżej wspomniane formy monitoringu mogą znaleźć zastosowanie, jeżeli jest to niezbędne dla zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz dla właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Poczyniono jednocześnie zastrzeżenie, że monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Jak zauważa Magdalena Kuba[11], niejasność co do pojęcia monitoringu, jaki jest dopuszczal-

[6] W. Kupny, *Ochrona prywatności w miejscu pracy w erze dynamicznie rozwijających się technologii — dziś i jutro*, „Roczniki Administracji i Prawa" 18, 2018, nr 1, s. 335–353.

[7] P. Fajgielski, [w:] *Komentarz do ustawy o ochronie danych osobowych*, [w:] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, art. 111.

[8] Tekst jedn. Dz.U. z 2022 r. poz. 1510.

[9] Tak też K. Bonawenturski, *Cele, zakres oraz sposób zastosowania monitoringu wizyjnego w miejscu pracy*, „Pracownik i Pracodawca" 5, 2020, nr 1, s. 20.

[10] Tak też M. Miłosz, J. Świątek-Rudoman, *Nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy*, „Praca i Zabezpieczenie Społeczne" 2019, nr 4, s. 34.

[11] M. Kuba, *Monitoring poczty elektronicznej pracownika — refleksje na tle nowych regulacji prawnych*, „Praca i Zabezpieczenie Społeczne" 2019, nr 11, s. 29–35.


© for this edition by CNS

ny, może powodować różne sposoby jego stosowania. Monitoring poczty elektronicznej może być bowiem wykorzystywany z użyciem środków technicznych (odpowiednie oprogramowanie) lub przybrać formę kontroli realizowanej przez konkretną osobę. Autorka zauważa, że prawodawca unijny posłużył się pojęciem „systemów monitorujących w miejscu pracy", co niewątpliwie jest węższym pojęciem w stosunku do monitoringu i oznacza raczej zespół środków funkcjonujących według określonych reguł, podejmowanych w celu wykonania czynności kontrolnych w miejscu pracy.

Wydaje się jednak, że koncentrowanie uwagi na monitoringu wizyjnym i monitoringu poczty elektronicznej jest głęboko nieuzasadnione. Ustawodawca dopuścił bowiem w art. $22^3$ § 4 k.p. stosowanie również innych form monitoringu, nie wskazując przy tym konkretnych rozwiązań. Tak ogólne sformułowanie umożliwia pracodawcom podjęcie szerokiego wachlarza działań monitorujących wobec pracownika, o ile zostanie to uzasadnione „niezbędnością dla zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz dla właściwego użytkowania udostępnionych pracownikowi narzędzi pracy". W kontekście innych form monitoringu wymienić należy technologię identyfikacji radiowej (RFID), która umożliwia zarówno identyfikację jak i lokalizację pracownika. W praktyce może to umożliwić ocenę wykorzystania czasu pracy oraz ustalenia, gdzie znajduje się pracownik i czy wykonuje powierzone zadania w wyznaczonym czasie i miejscu. Zauważyć jednak należy, że w tej technologii wykorzystywane są również dane biometryczne, co nabiera szczególnego znaczenia w kontekście oceny dopuszczalności każdorazowego stosowania tej formy monitoringu[12]. Kolejną z innych form monitoringu jest monitoring pracownika w sieci komputerowej. Pracownik nierzadko korzysta ze służbowego sprzętu w godzinach pracy do przeglądania stron internetowych dla celów wyłącznie prywatnych. Jak zauważa Sebastian Ożóg[13], *cyberslacking* nie jest zjawiskiem rzadkim, a niewątpliwie należy uznać go za naruszenie prawidłowego wykonywania obowiązków pracowniczych. Monitoring taki może być wykorzystywany dla oceny stopnia świadczenia pracy w poszczególnych okresach czasu na podstawie danych pozyskiwanych ze źródeł teleinformatycznych. Krystyna Ziółkowska[14] wskazuje na stosowanie przez pracodawców programów sprawdzających każdy ruch pracownika polegający na „wejściu do internetu", odnotowania czasu takiej czynności, zarejestrowania zainstalowanych plików czy programów. Autorka dostrzega również monitoring aktywności pracownika realizowany w celu określenia wydajności ich pracy oraz wychwycenia działań niepożądanych ze strony pracownika.

[12] Szerzej na ten temat K.M. Szymorek, *Aspekty prawne kontrolowania pracowników za pomocą technologii identyfikacji radiowej (RFID)*, „Monitor Prawa Pracy" 2012, nr 10, s. 523–527.

[13] S. Ożóg, *Monitoring pracownika w sieci komputerowej*, „Polski Rocznik Praw Człowieka i Prawa Humanitarnego" 2, 2011, s. 159–170.

[14] K. Ziółkowska, *Prawo pracownika do ochrony prywatności w stosunkach pracy*, „Studia Prawnoustrojowe" 2020, nr 48, s. 286.


© for this edition by CNS

Bardzo ciekawym rozwiązaniem monitoringu aktywności pracownika jest *keylogger*, czyli kontrola liczby znaków wprowadzanych na klawiaturze komputera. Jak zauważa Arkadiusz Lach[15], stosowanie tego rodzaju instrumentu kontroli pracownika może umożliwiać ocenę szybkości wykonywania zadań lub weryfikację realizacji zadań powierzonych pracownikowi w ramach pracy zdalnej z domu. Tego rodzaju informacje stanowią cenną wskazówkę co do wykorzystywania czasu pracy przez pracownika. W praktyce powinny być wykorzystywane przez państwowych inspektorów pracy, ale i pracodawców. Mogą być bowiem źródłem informacji o nadmiernym obciążeniu ilościowym pracą i wskazywać na potrzebę rewizji przydzielonych obowiązków.

Powszechnie stosowanym sposobem monitorowania pracowników jest geolokalizacja. Moduły GPS praktykowane są w różnych rodzajach samochodów, w sprzęcie komputerowym, a nawet telefonach. Lach[16] wskazuje na stosowanie tego rozwiązania dla weryfikacji sposobu realizacji zobowiązania pracowniczego w tym znaczeniu, czy pracownik znajduje się w podróży na wyznaczonych trasach. Nie należy jednak zapominać, że moduły tego rodzaju odnotowują nie tylko miejsce, ale i czas aktywności, dodatkowo rejestrują — w przypadku samochodu — „aktywność tego urządzenia" to jest: czy jest w drodze, na postoju, czy silnik jest wyłączony lub włączony.

Kolejna forma monitoringu, niewskazana wprost w k.p., to monitoring połączeń telefonicznych realizowanych przez pracowników z telefonów służbowych. Istotne jest w takich wykazach odnotowywanie czasu dokonanego połączenia oraz czasu trwania, co może być przydatne w trakcie oceny stopnia i sposobu wykorzystania czasu pracy.

Przedstawiony powyżej zarys rodzajów monitoringu stosowanego przez pracodawców oraz powodu i uzasadnienia ich stosowania uprawnia do postawienia pytania, czy tak zgromadzone dane są przydatne w toku kontroli prowadzonej przez państwowego inspektora pracy, a przede wszystkim — czy mogą być przez niego wykorzystane. Państwowa Inspekcja Pracy (dalej PIP) została powołana do nadzoru i kontroli przestrzegania przepisów prawa pracy, bezpieczeństwa i higieny pracy, a także kontroli legalności zatrudnienia[17]. Niezwykle istotną częścią postępowania kontrolnego jest postępowanie dowodowe prowadzone przez państwowego inspektora pracy. Niektóre obszary aktywności PIP mogą skutecznnie wykorzystywać instrumenty monitoringu dla oceny przestrzegania prawa pracy, na przykład przepisów o czasie pracy, postępowania w sprawie wypadku przy pracy itp.

[15] A. Lach, *Monitorowanie pracownika po nowelizacji Kodeksu pracy*, „Monitor Prawniczy" 2018, nr 18, s. 969–974.

[16] *Ibidem*.

[17] Artykuł 1 ustawy z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy, tekst jedn. Dz.U. z 2022 r. poz. 1614, dalej pip.


© for this edition by CNS

## MONITORING JAKO ŹRÓDŁO DOWODOWE

Celem postępowania kontrolnego zgodnie z artykułem 21 pip jest ustalenie stanu faktycznego w zakresie przestrzegania prawa pracy, w szczególności przepisów i zasad bezpieczeństwa i higieny pracy, a także przepisów dotyczących legalności zatrudnienia oraz udokumentowanie dokonanych ustaleń. Przytoczona norma prawna wyraźnie wskazuje, że celem działań kontrolnych jest dokonanie ustalenia stanu faktycznego oraz jego udokumentowanie. Odbywa się w sposób opisany przepisami właściwymi dla protokołu kontroli lub notatki urzędowej. Zanim jednak nastąpi udokumentowanie ustaleń, konieczne jest przeprowadzenie rozpoznania w zakresie stanu faktycznego. Zauważyć należy, że art. 21 pip stanowi część rozdziału 4 pip, regulującego zasady postępowania kontrolnego, co należy traktować jako wyraźne wskazanie norm prawnych wyznaczających jego przebieg, tryb postępowania, etapy dochodzenia ustaleń. Artykuł 23 pip wyraźnie wskazuje, jakie czynności może podejmować państwowy inspektor pracy w toku postępowania kontrolnego. Katalog tych czynności nie wymienia jednak wprost zapisów z monitoringu, który może rejestrować szeroką gamę form aktywności pracownika. Jak zauważa Jacek Jagielski[18], art. 23 pip, określający uprawnienia państwowego inspektora pracy w zakresie prowadzonego postępowania dowodowego w toku kontroli nie ma charakteru wyczerpującego. W ocenie autora regulacja postępowania dowodowego, jak i całego postępowania kontrolnego nie jest rozwinięta. Ponadto do postępowania kontrolnego opartego wyłącznie na ustawowym reżimie prawnym pip może być stosowany posiłkowo kodeks postępowania administracyjnego (dalej k.p.a.). Podstawy prawnej dla takiego postępowania należy słusznie upatrywać w art. 12 pip, przewidującym stosowanie przepisów k.p.a. w postępowaniu przed organami PIP w sprawach nieuregulowanych. Postępowanie dowodowe w ustawie pip niewątpliwie nie zostało uregulowane w sposób wyczerpujący, co stanowi o niekompletności ustawy ustrojowej i uzasadnia posiłkowe stosowanie przepisów k.p.a. Konstatacja ta jest o tyle istotna, że umożliwia odwołanie się do reguł dowodowych określonych w k.p.a., a w szczególności art. 75 § 1 k.p.a., który bardzo szeroko ujmuje dopuszczalne dowody w postępowaniu. Wskazany przepis nakazuje dopuścić jako dowód wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem. Za dowody uznaje się w szczególności dokumenty, zeznania świadków, opinie biegłych oraz oględziny. Zaakcentować należy, że katalog dowodów w rozumieniu wskazanego artykułu ma charakter otwarty, na co wyraźnie wskazują sformułowanie „w szczególności" a przede wszystkim zwrot o dopuszczeniu wszystkiego, co może przyczynić się do wyjaśnienia sprawy[19]. Podkreślić należy, że dowód z monitoringu należy uznać za tak

[18] J. Jagielski, [w:] M. Gersdorf, J. Jagielski, K. Rączka, *Komentarz do ustawy o Państwowej Inspekcji Pracy*, Warszawa 2008, s. 94–95.

[19] Pogląd o otwartym katalogu środku dowodowych jest powszechnie akceptowany, na przykład: B. Adamiak, [w:] B. Adamiak, J. Borkowski, *Postępowanie administracyjne i sądowoadmi-*


© for this edition by CNS

zwany dowód nienazwany, co wobec dokonującego się postępu technicznego jest rzeczą zrozumiałą. Nie sposób bowiem w epoce cyfryzacji wymienić wszystkich możliwych i dostępnych dowodów, które przyczynią się do wyjaśnienia sprawy.

Rozstrzygając kwestię dopuszczalności dowodu z monitoringu w postępowaniu kontrolnym należy przywołać zasadę prawdy obiektywnej, która została wyrażona w art. 7 k.p.a., ale jest również wyrażona w art. 21 pip, na co nie zawsze zwraca się należytą uwagę. Jak zauważa Janusz Borkowski, zasada prawdy obiektywnej sformułowana w art. 7 k.p.a. stanowi o odcięciu się od poglądu o dopuszczalności orzekania na podstawie prawdy formalnej, uzyskanej reglamentowanymi środkami dowodowymi[20]. Zasada ta nie formułuje żadnych ograniczeń dowodowych poza jedną — zasadą praworządności, co oznacza, że wykluczony z postępowania jest wyłącznie dowód sprzeczny z prawem. Hanna Knysiak-Sudyka słusznie zauważa[21], że organ rozpatrujący sprawę ma obowiązek z urzędu określić, jakie dowody są niezbędne dla prawidłowego i pełnego wyjaśnienia stanu faktycznego sprawy. Autorka wskazuje na to, że ciężar dowodu w postępowaniu administracyjnym co do zasady spoczywa na organie administracji publicznej. Zasada ta nakazuje organowi być „dysponentem postępowania", jednak — co również istotne — nie wyklucza inicjatywy dowodowej strony postępowania, jeżeli chce ona z określonych faktów wywodzić skutki prawne[22]. Wskazana zasada jest silnie zakorzeniona w systemie prawnym i uznawana jest za warunek prawidłowo prowadzonego postępowania oraz jego rozstrzygnięcia[23]. Jak trafnie zauważa Emanuel Iserzon, organ narusza prawo nie tylko w przypadku wadliwej oceny prawnej stanu faktycznego, ale również i wtedy, gdy prawidłowo zastosowano prawo do fałszywie ustalonego stanu faktycznego[24]. Autor wyjątkowo celnie wskazuje, że „fakt prawotwórczy musi być ustalony w sposób obiektywny, tj. za pomocą takich środków, które mogą przekonać każdego prawidłowo myślącego człowieka o bycie danego faktu". Osiągnięciu tego celu ma służyć zasada prawdy obiek-

*nistracyjne*, Warszawa 2003, s. 211; G. Łaszczyca, [w:] *System prawa administracyjnego procesowego*, t. 2, cz. 4. *Dynamika postępowania administracyjnego ogólnego*, red. C. Martysz, Warszawa 2021, s. 537.

[20] J. Borkowski, [w:] B. Adamiak, J. Borkowski, *Postępowanie administracyjne i sądowoadministracyjne*, s. 34.

[21] H. Knysiak-Sudyka, [w:] *System prawa administracyjnego procesowego*, t. 2, cz. 3. *Czynności procesowe w postępowaniu administracyjnym ogólnym*, red. Łaszczyca, A. Matan, Warszawa 2021, s. 537.

[22] Ciężar dowodzenia nadal spoczywa na organie administracji publicznej, jakkolwiek inicjatywa dowodowa została wyraźniej również sformułowana na rzecz strony, patrz uwagi M. Grzymisławska-Cybulska, *Nowelizacja artykułów 7, 8 i 16 kpa w doktrynie i orzecznictwie sądów administracyjnych*, „Ius Novum" 7, 2013, nr 4, s. 105–121; podobnie P. Krzykowski, [w:] *Kodeks postępowania administracyjnego. Komentarz*, t. 1. *Komentarz do art. 1–60*, red. M. Karpiuk, P. Krzykowski, A. Skóra, Olsztyn 2020, s. 45.

[23] K. Jandy-Jendrośka, J. Jendrośka, *System jurysdykcyjnego postępowania administracyjnego*, [w:] *System prawa administracyjnego*, t. 3, red. T. Rabska, J. Łętowski, Wrocław 1978, s. 173.

[24] E. Iserzon, *Prawo administracyjne*, Warszawa 1968, s. 222.


© for this edition by CNS

tywnej, prawdy materialnej, czy też zasada prawdy. Zasady prawdy obiektywnej ma więc w istocie fundamentalne znaczenie dla prawidłowego przeprowadzenia postępowania wyjaśniającego, które ma umożliwić dokonanie subsumcji faktów uznanych za udowodnione pod właściwą normę prawną, a następnie umożliwić ustalenie konsekwencji prawnych tychże faktów[25]. Warto wskazać, że zasada prawdy obiektywnej wymaga dynamicznego podejścia do gromadzonego materiału dowodowego i może wymagać zmiany zakresu pozyskiwanych dowodów, ze względu na dokonane ustalenia[26]. Uwaga taka jest szczególnie istotna z perspektywy kontroli PIP, w trakcie której mogą zrodzić się wątpliwości, na przykład co do rzetelności zapisów w ewidencji czasu pracy, a prowadzony przez pracodawcę monitoring elektroniczny będzie rejestrował aktywność pracownika na komputerze czy w wewnątrzzakładowym systemie teleinformatycznym niezbędnym dla wykonywania obowiązków pracowniczych. Realizacja prawdy obiektywnej oznacza bowiem nie tylko obowiązek ustalenia stanu faktycznego, ale również obowiązek ustalenia stanu faktycznego na podstawie kompletnego, całościowo zebranego materiału dowodowego; niekompletność zgromadzonego materiału dowodowego będącego podstawą rozstrzygnięcia stanowi o niezrealizowaniu zasady prawdy obiektywnej[27]. Znaczenie prawdy obiektywnej podkreślano również w judykaturze. Trybunał Konstytucyjny w orzeczeniu z 10 czerwca 1987 roku[28], przyjął: „Jedną z naczelnych zasad postępowania administracyjnego jest zasada prawdy obiektywnej, a zatem udowodnienie każdego faktu mającego znaczenie prawne może nastąpić za pomocą wszystkich legalnych środków […]. Jakiekolwiek ograniczenie w tym przedmiocie może wynikać tylko z przepisów ustawowych". Powszechność znaczenia prawdy obiektywnej, jak słusznie zauważa Barbara Adamiak, formułuje się również w Europejskim Kodeksie Dobrej Administracji[29].

Zasada prawdy obiektywnej jest poniekąd wyrażona w art. 21 pip, który nakazuje przeprowadzenie postępowania kontrolnego w celu ustalenia stanu faktycznego. Działania państwowego inspektora pracy powinny więc koncentrować się na możliwie rzetelnym odzwierciedleniu stanu rzeczywistego w protokole kontroli lub notatce urzędowej. Jagielski słusznie dopatruje się wyrażenia tej zasady we wskazanym przepisie, akcentując, że ustalenia kontrolne powinny odzwierciedlać rzeczywisty stan rzeczy, a zasadę prawdy obiektywnej należy postrzegać

[25] J. Jendrośka, *Zasady postępowania administracyjnego*, [w:] *Księga pamiątkowa Profesora Eugeniusza Ochendowskiego*, Toruń 1999, s. 145.

[26] M. Grzeszczuk, *Zasada prawdy obiektywnej jako zasada stosowania prawa*, „Studia Iuridica Lublinensia" 25, 2016, nr 1, s. 283.

[27] A. Wróbel, [w:] M. Jaśkowska, A. Wróbel, *Kodeks postępowania administracyjnego. Komentarz*, Zakamycze 2005, s. 150–151.

[28] Orzeczenie TK z dnia 10 czerwca 1987 r., P 1/87/2, „Palestra" 1987, nr 12, s. 113.

[29] B. Adamiak, [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2005, s. 71. Aspekt ten dostrzega także R. Siuciński, *Zasada dochodzenia prawdy materialnej w postępowaniu administracyjnym w ujęciu prawnoporównawczym*, „Przegląd Prawa Publicznego" 2010, nr 10, s. 14.


© for this edition by CNS

jako najważniejszą cechę prawidłowej kontroli[30]. Zauważyć można, że nieprawidłowo ustalony stan faktyczny skutkować będzie przeprowadzeniem postępowania kontrolnego w sposób nierzetelny, a przeprowadzona kontrola nie przyniesie spodziewanych efektów w postaci eliminacji nieprawidłowości. Wskazać należy, że postępowanie kontrolne państwowego inspektora pracy cechuje obowiązek dowodzenia organu administracji, to jest zasada oficjalności. Następstwem tej zasady jest kumulacja ról procesowych organu administracji, która obejmuje inicjatywę dowodową, przeprowadzenie dowodów, zbieranie materiału dowodowego i jego ocenę oraz rozstrzygnięcie, które fakty zostały udowodnione[31]. Artykuł 23 pip formułuje szereg dowodów, które możemy kwalifikować zgodnie z systematyką dowodów jako dowody nazwane, jak na przykład dowody z zeznań świadków i oświadczeń, oględziny, dowody z dokumentów w postaci akt osobowych i innej dokumentacji z zakresu stosunku pracy. Ustawa o PIP nie formułuje jednak żadnych wskazówek co do innych możliwych dowodów z postępowania, które można byłoby określić mianem dowodów nienazwanych. Stan taki ocenić należy jako niezadowalający. Ponadto, o czym wspomniano wyżej, ustawa o PIP nie zawiera żadnych innych wskazówek w zakresie postępowania dowodowego w ogólności. Uzasadnieniem dla uwzględnienia materiału z monitoringu zakładowego w toku kontroli są także cenne uwagi Dariusza Makowskiego w kontekście zakresu postępowania dowodowego prowadzonego przez PIP[32]. Autor wskazuje bowiem, że konstrukcja art. 23 ust. 1 pip nie powinna być wykładana w ten sposób, że wskazuje na zamknięty katalog działań państwowego inspektora pracy, lecz przeciwnie. Mając na uwadze przepisy prawa międzynarodowego, to jest Konwencji nr 81[33] i 129[34] w sprawie inspekcji pracy w przemyśle i handlu oraz w rolnictwie, należy uznać że mogą być podejmowane również inne działania, niewymienione w przepisie art. 23 ust. 1 pip. Działania te stosownie do przepisów Konwencji są uzasadnione niezbędnością upewnienia się, że przepisy prawa pracy są ściśle przestrzegane w zakładach pracy. Ponadto takie dodatkowe, niewymienione działania realizują w pełni zasadę ustalenia rzeczywistego stanu faktycznego w toku prowadzonego postępowania kontrolnego i realizują zasadę prawdy obiektywnej.

[30] J. Jagielski, [w:] M. Gersdorf, J. Jagielski, K. Rączka, *Komentarz do ustawy o Państwowej Inspekcji Pracy*, s. 86–87. Zauważyć również należy, że konieczność uwzględnienia zasady prawdy obiektywnej w toku postępowania państwowego inspektora pracy dostrzega również Adrianna Jasińska-Cichoń, która wskazuja na nią przez pryzmat obowiązku stosowania zasad postępowania administracyjnego w postępowaniu przed organami PIP na podstawie art. 12 uPIP — A. Jasińska-Cichoń, *Ustawa o Państwowej Inspekcji Pracy*, Warszawa 2008, s. 70.

[31] D. Gregorczyk, [w:] *System prawa administracyjnego procesowego*, t. 2, cz. 4, s. 200.

[32] D. Makowski, *Inspekcja pracy jako instytucja państwowego nadzoru nad przestrzeganiem prawa pracy*, Łódź 2017, s. 291.

[33] Konwencja nr 81 Międzynarodowej Organizacji Pracy w sprawie inspekcji pracy w przemyśle i handlu z dnia 11 lipca 1947 r., Dz.U. z 1997 r. Nr 72, poz. 450.

[34] Konwencja nr 129 Międzynarodowej Organizacji Pracy dotycząca inspekcji pracy w rolnictwie, Dz.U. z 1997 r. Nr 72, poz. 452.


© for this edition by CNS

Wobec takiej sytuacji, kierując się art. 12 pip, ale również przesłankami art. 21 pip, należy skorzystać z przepisów k.p.a. w zakresie postępowania dowodowego. Wobec powyższego regułą postępowania kontrolnego powinno być powtórzenie w toku jego prowadzenia normy wynikającej z art. 75 § 1 k.p.a., zgodnie z którą jako dowód należy dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem. W praktyce oznacza to, że każdy środek służący wyświetleniu sprawy powinien być uwzględniony i co ważne, każdy dowód — zgodnie z k.p.a. — ma równą moc dowodzenia, chyba że ustawa stanowi inaczej[35]. Nie istnieje więc hierarchia dowodów w postępowaniu czy prymat dowodów nazwanych nad nienazwanymi. Mając na uwadze, że wyliczenie dowodów zawarte w art. 75 § 1 k.p.a. jest przykładowe, zapisy z monitoringu sprawowanego przez pracodawcę można uznać za materiał dowodowy, kwalifikując je jako dowód rzeczowy o charakterze pośrednim, nienazwanym i podstawowym. W tym kontekście należy podnieść, że zagadnienie dowodów nienazwanych będzie niewątpliwie nabierać znaczenia ze względu na postęp techniczny i społeczny[36]. Grzegorz Łaszczyca[37] wskazuje słusznie, że istota środków dowodowych o charakterze nienazwanym tkwi w ich „nowości", wynikającej z dynamicznego rozwoju nauki i techniki, szczególnie w sferze cyfrowej i informatycznej. Autor zauważa jednocześnie, co również należy podzielić, że jakkolwiek dowody te nie mogą być traktowane w sposób pośledni ze względu na równą moc środków dowodowych, to jednak wymagają one wnikliwej oceny — niekiedy bardziej krytycznej, ale nie dezawuującej. Wskazana dynamika stosowanych technik monitoringu może być obserwowana szczególnie w prawie pracy, ponieważ art. $22^3$ § 4 k.p. dopuszcza stosowanie innych form monitoringu niż wymienione w kodeksie, co oznacza że katalog tych działań jest otwarty[38]. Państwowy inspektor pracy, prowadząc postępowanie kontrolne związane z wypadkiem przy pracy powinien skorzystać z monitoringu wizyjnego, jeżeli zilustruje to przebieg zdarzenia wypadkowego. Podobnie powinien postąpić organ kontrolny, jeżeli prowadzi postępowanie kontrolne w zakresie przestrzegania przepisów o czasie pracy i nabiera wątpliwości co do rzetelności ewidencji czasu pracy — wówczas należy rozważyć możliwość skorzystania z dowodu w postaci zapisów zawartych w systemach teleinformatycznych pracodawcy, które są dość powszechne. Przypomnieć należy, że również strona postępowania kontrolnego może wystąpić z takim wnioskiem, przejawia-

[35] Przykładem jest art. 86 k.p.a. o dowodzie z przesłuchania stron.

[36] M. Błażewski, J. Bigos, *Dopuszczalność dowodów pochodzących z jawnych źródeł w postępowaniu administracyjnym*, „Folia Iuridica Universitatis Wratislaviensis" 9, 2020, nr 2, s. 253–266; M. Rudnicki, *Zagadnienie otwartości katalogu środków dowodowych w ogólnym postępowaniu administracyjnym*, „Studia Prawnicze i Administracyjne" 2013, nr 2 (4), s. 67–72.

[37] G. Łaszczyca, [w:] *System prawa administracyjnego procesowego*, t. 2, cz. 4, s. 539.

[38] Szerzej na przykład J. Woźniak, *Współczesne monitorowanie pracy. Podstawy teoretyczne i metody zastosowania*, Warszawa 2021.


© for this edition by CNS

jąc inicjatywę dowodową w tym zakresie[39]. Pominięcie tych dowodów skutkować może nieprawidłowo przeprowadzonym postępowaniem dowodowym, co będzie rzutowało na wyniki postępowania kontroli[40]. Obowiązek uwzględnienia pełnego materiału dowodowego został wyrażony w art. 77 § 1 k.p.a. Również ten przepis uzasadnia korzystanie z każdego dostępnego prawnie środka dowodowego. Jak zauważa Adamiak, zebranie całego materiału dowodowego oznacza zebranie dowodów dotyczących wszystkich mających znaczenie prawne dla sprawy faktów[41]. Z tej perspektywy uzasadnione staje się również zobowiązanie do uwzględnienia materiału dowodowego opartego na zapisach monitoringu wewnątrzzakładowego.

Należy przypomnieć, że zapisy z monitoringu mogą być traktowane jako dowody tylko jeżeli nie są sprzeczne z prawem. Ograniczeniem w wykorzystaniu zapisów monitoringu realizowanego przez pracodawcę jako źródła dowodowego w postępowaniu kontrolnym państwowego inspektora pracy będzie sprzeczność z prawem danego dowodu. Niedopuszczalnym będzie wykorzystanie informacji zawartych w monitoringu, jeżeli nie zostały spełnione wymagania ustawowe dla jego wprowadzenia. Brak przekazanej pracownikom informacji o stosowanym monitoringu wykluczy go z potencjalnych źródeł dowodowych. Ponadto monitorowanie wizyjne jest dozwolone w enumeratywnie wyliczonych przypadkach i tylko we wskazanych sytuacjach można je stosować i pozyskać te dane dla postępowania kontrolnego państwowego inspektora pracy. Warunkiem wykorzystania tych informacji w postępowaniu kontrolnym jest zgodność ich pozyskania z prawem, ściśle związana z zasadnością zastosowania monitoringu w miejscu pracy.

## PODSUMOWANIE

Postępowanie dowodowe prowadzone przez państwowego inspektora pracy powinno odzwierciedlać stan faktyczny, a nie stan przedstawiony czy wyobrażony przez stronę. Działania organu kontroli powinny nakierowane być pełnoskalowo na realizację zasady prawdy obiektywnej, co może być uwzględnione przede wszystkim wówczas, gdy zostaną wyświetlone wszystkie fakty i okoliczności istotne dla sprawy. Postępowanie dowodowe powinno obejmować również dowód z monitoringu, o ile taki jest stosowany w zakładzie pracy, jest praktykowany i ma

[39] A. Majewska, *Żądanie dowodowe strony w ogólnym postępowaniu administracyjnym*, „Annales Universitatis Mariae Curie-Skłodowska, Sectio G (Ius)" 60, 2013, nr 1, s. 93–104.

[40] Wadliwość postępowania wyjaśniającego może przybrać różne postaci: nieprzeprowadzenie postępowania w ogóle, nieprzeprowadzenie postępowania w części, przekroczenie granic swobodnej oceny dowodów, pominięcie dowodów z powodu ich nieznajomości — A. Ziółkowska, *Formy wadliwości postępowania wyjaśniającego w ogólnym postępowaniu administracyjnym*, „Samorząd Terytorialny" 2009, nr 9, s. 62–73.

[41] B. Adamiak, [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego…*, s. 402.


© for this edition by CNS

znaczenie dla sprawy. Jeżeli bowiem pracodawca może korzystać z dobrodziejstw tego systemu, oceniając zachowanie pracownika, to również państwowy inspektor pracy, dokonując oceny przestrzegania praworządności w stosunkach pracy przez pracodawcę, powinien mieć możliwość skorzystania z tego instrumentu jako środka dowodowego w postępowaniu kontrolnym. Wydaje się, że dążąc do prawdy obiektywnej, postępowanie państwowego inspektora pracy, nie może pomijać dowodu z monitoringu — o ile taki jest dostępny, albowiem wykluczałoby to dążenie do przeprowadzenia rzetelnej kontroli, odzwierciedlającej stan faktyczny w zakresie przestrzegania przepisów prawa pracy.

## VIDEO SURVEILLANCE AS AN ALTERNATIVE SOURCE OF EVIDENCE IN INSPECTIONS OF STATE LABOUR INSPECTORS

Summary

Recent technological progress leads to changes in many areas of human life. Employers use increasingly refined methods to monitor the work performed by their employees. The reasons for such actions are understandable, and they have been approved by the legislator. However, the law permits video surveillance in specific cases and provided that specific requirements are met. The data collected during video surveillance of work are highly useful for employers. It seems, though, that the same data may also be of significant use for state labour inspectors as they check compliance with the labour law. This is because such data makes it possible to objectively establish the facts and the substantive truth. This article attempts to answer the questions related to the acceptability of using video surveillance evidence in inspections carried out by state labour inspectors.

Keywords: inspection of the state labour inspectorate, evidence procedure of a state labour inspector

## BIBLIOGRAFIA

Adamiak B., [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2005.

Adamiak B., Borkowski J., *Postępowanie administracyjne i sądowoadministracyjne*, Warszawa 2003.

Błażewski M., Bigos J., *Dopuszczalność dowodów pochodzących z jawnych źródeł w postępowaniu administracyjnym*, „Folia Iuridica Universitatis Wratislaviensis" 9, 2020, nr 2.

Bonawenturski K., *Cele, zakres oraz sposób zastosowania monitoringu wizyjnego w miejscu pracy*, „Pracownik i Pracodawca" 5, 2020, nr 1.

Dörre-Kolasa D., [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa 2018.

Fajgielski P., *Komentarz do ustawy o ochronie danych osobowych*, [w:] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.

Gregorczyk D., [w:] *System prawa administracyjnego procesowego*, t. 2, cz. 4. *Dynamika postępowania administracyjnego ogólnego*, red. C. Martysz, Warszawa 2021.

Grzymisławska-Cybulska M., *Nowelizacja artykułów 7, 8 i 16 kpa w doktrynie i orzecznictwie sądów administracyjnych*, „Ius Novum" 7, 2013, nr 4.


© for this edition by CNS

Grzeszczuk M., *Zasada prawdy obiektywnej jako zasada stosowania prawa*, „Studia Iuridica Lublinensia" 25, 2016, nr 1.
Iserzon E., *Prawo administracyjne*, Warszawa 1968.
Jagielski J., [w:] M. Gersdorf, J. Jagielski, K. Rączka, *Komentarz do ustawy o Państwowej Inspekcji Pracy*, Warszawa 2008.
Jandy-Jendrośka K., Jendrośka J., *System jurysdykcyjnego postępowania administracyjnego*, [w:] *System prawa administracyjnego*, t. 3, red. T. Rabska, J. Łętowski, Wrocław 1978.
Jasińska-Cichoń A., *Ustawa o Państwowej Inspekcji Pracy*, Warszawa 2008.
Jendrośka J., *Zasady postępowania administracyjnego*, [w:] *Księga pamiątkowa profesora Eugeniusza Ochendowskiego*, Toruń 1999.
Knysiak-Sudyka H., [w:] *System prawa administracyjnego procesowego*, t. 2, cz. 3. *Czynności procesowe w postępowaniu administracyjnym ogólnym*, red. Łaszczyca, A. Matan, Warszawa 2021.
Krzykowski P., [w:] *Kodeks postępowania administracyjnego. Komentarz*, t. 1. *Komentarz do art. 1–60*, red. M. Karpiuk, P. Krzykowski, A. Skóra, Olsztyn 2020.
Kuba M., *Monitoring poczty elektronicznej pracownika — refleksje na tle nowych regulacji prawnych*, „Praca i Zabezpieczenie Społeczne" 2019, nr 11.
Kupny W., *Ochrona prywatności w miejscu pracy w erze dynamicznie rozwijających się technologii — dziś i jutro*, „Roczniki Administracji i Prawa" 18, 2018, nr 1.
Lach A., *Monitorowanie pracownika po nowelizacji Kodeksu pracy*, „Monitor Prawniczy" 2018, nr 18.
Łaszczyca G., [w:] *System prawa administracyjnego procesowego*, t. 2, cz. 4. *Dynamika postępowania administracyjnego ogólnego*, red. C. Martysz, Warszawa 2021.
Majewska A., Żądanie dowodowe strony w ogólnym postępowaniu administracyjnym, „Annales Universitatis Mariae Curie-Skłodowska, Sectio G (Ius)" 60, 2013, nr 1.
Makowski D., *Inspekcja pracy jako instytucja państwowego nadzoru nad przestrzeganiem prawa pracy*, Łódź 2017.
Makowski D., *Państwowa Inspekcja Pracy*, [w:] *System prawa pracy*, t. 8. *Prawo rynku pracy*, red. M. Włodarczyk, Warszawa 2018.
Miłosz M., Świątek-Rudoman J., *Nowe ramy prawne stosowania przez pracodawcę monitoringu wizyjnego w zakładzie pracy*, „Praca i Zabezpieczenie Społeczne" 2019, nr 4.
Ożóg S., *Monitoring pracownika w sieci komputerowej*, „Polski Rocznik Praw Człowieka i Prawa Humanitarnego" 2, 2011.
Rudnicki M., *Zagadnienie otwartości katalogu środków dowodowych w ogólnym postępowaniu administracyjnym*, „Studia Prawnicze i Administracyjne" 2013, nr 2 (4).
Siuciński R., *Zasada dochodzenia prawdy materialnej w postępowaniu administracyjnym w ujęciu prawnoporównawczym*, „Przegląd Prawa Publicznego" 2010, nr 10.
Szymorek K.M., *Aspekty prawne kontrolowania pracowników za pomocą technologii identyfikacji radiowej (RFID)*, „Monitor Prawa Pracy" 2012, nr 10.
Woźniak J., *Współczesne monitorowanie pracy. Podstawy teoretyczne i metody zastosowania*, Warszawa 2021.
Wróbel A., [w:] M. Jaśkowska, A. Wróbel, *Kodeks postępowania administracyjnego. Komentarz*, Zakamycze 2005.
Ziółkowska A., *Formy wadliwości postępowania wyjaśniającego w ogólnym postępowaniu administracyjnym*, „Samorząd Terytorialny" 2009, nr 9.
Ziółkowska K., *Prawo pracownika do ochrony prywatności w stosunkach pracy*, „Studia Prawnoustrojowe" 2020, nr 48.


© for this edition by CNS

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

# INFORMACJA DLA AUTORÓW

1. Teksty do wydania w numerze na dany rok należy przesłać najpóźniej do 31 marca.

2. Wszystkie artykuły publikowane w czasopiśmie „Przegląd Prawa i Administracji" są recenzowane.

3. O przyjęciu tekstu do wydania w Czasopiśmie Autorzy zostaną poinformowani w ciągu 30 dni za pośrednictwem poczty elektronicznej na wskazany przez nich adres.

4. Recenzje zostaną przesłane Autorom, którzy zobowiązują się do dokonania zasugerowanych w nich poprawek i korekt.

5. Teksty należy nadsyłać w formacie dokumentów programu Word lub tekstu sformatowanego RTF. Maksymalna objętość tekstu:

a) artykuł — 60 000 znaków ze spacjami;

b) recenzja — 25 000 znaków ze spacjami.

6. Szczegółowe informacje dotyczące formatowania tekstów oraz sporządzania przypisów znajdują się na stronie www.wuwr.com.pl w zakładce „Dla Autorów".

7. Teksty odbiegające od podanych standardów będą odsyłane do Autorów z prośbą o dostosowanie ich do wymogów pisma.

8. Do tekstu należy dołączyć streszczenie w języku angielskim (do 600 znaków ze spacjami).

9. Wydawnictwo zastrzega sobie prawo do dokonywania poprawek redakcyjnych tekstów.

10. Przesłanie przez Autora tekstu do Redakcji Czasopisma jest równoznaczne z jego oświadczeniem, że przysługują mu autorskie prawa majątkowe do tego tekstu, że tekst jest wolny od wad prawnych oraz że nie był wcześniej publikowany w całości lub części ani nie został złożony w redakcji innego czasopisma, a także z udzieleniem nieodpłatnej zgody na wydanie tekstu w czasopiśmie „Przegląd Prawa i Administracji" oraz jego nieograniczone co do czasu i terytorium rozpowszechnianie, w tym wprowadzenie do obrotu egzemplarzy czasopisma oraz odpłatne i nieodpłatne udostępnianie jego egzemplarzy w internecie.

11. Autorzy są zobowiązani do wykonania korekty autorskiej w ciągu 7 dni od daty jej otrzymania. Niewykonanie korekty w tym terminie oznacza zgodę Autora na wydanie tekstu w postaci przesłanej do korekty.

12. Wszystkie udostępnione przez Wydawnictwo artykuły, w formacie PDF, znajdują się na stronie www.cns.wuwr.pl.

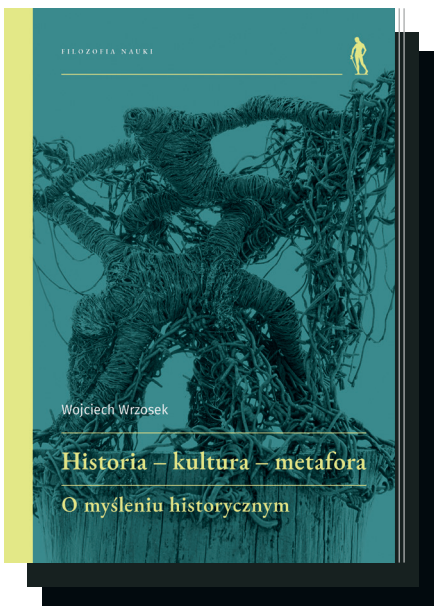
13. Autorzy nie otrzymują honorarium autorskiego za przekazane artykuły.

14. Teksty w wersji elektronicznej prosimy nadsyłać na adres Redakcji Czasopisma: mariusx@prawo.uni.wroc.pl.

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS

## Polecamy nasze nowe serie i publikacje

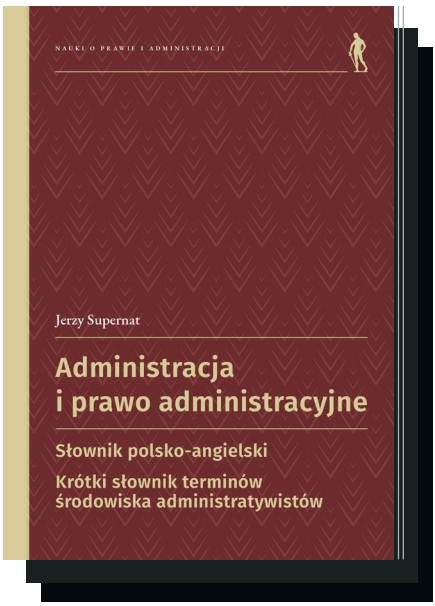


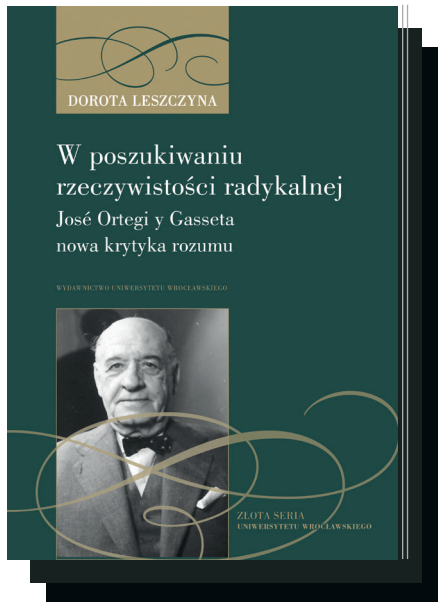




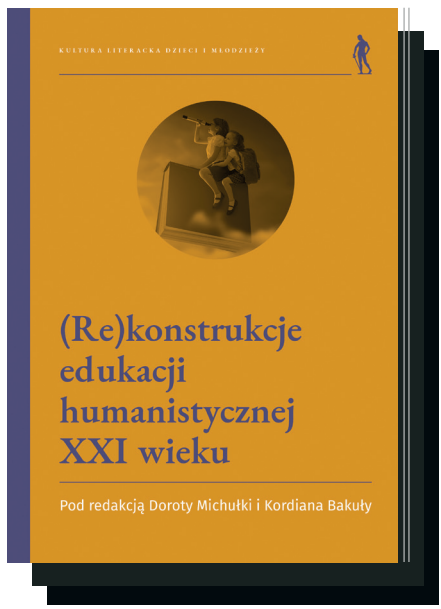

© for this edition by CNS

Wydawnictwo
Uniwersytetu
Wrocławskiego









© for this edition by CNS

Wydawnictwo
Uniwersytetu
Wrocławskiego

**Wydawnictwo Uniwersytetu Wrocławskiego sp. z o.o.**

pl. Uniwersytecki 15
50-137 Wrocław
sekretariat@wuwr.com.pl

wuwr.eu
Facebook/wydawnictwouwr

Przegląd Prawa i Administracji 132, 2023
© for this edition by CNS