PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 27 stycznia 2025 r.

DOL.413.13.2024

Pani
Izabela Leszczyna
Minister Zdrowia
Ministerstwo Zdrowia

Szanowna Pani Minister,

działając na podstawie art. 52 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[1] Prezes Urzędu Ochrony Danych Osobowych zwraca się z uprzejmą prośbą i wnioskiem o rozważenie podjęcia działań w celu **doprecyzowania przepisów dotyczących stosowania monitoringu wizyjnego w placówkach medycznych**. Analiza aktualnych regulacji prawnych podjęta przez organ nadzorczy w związku z sygnalizowanymi mu problemami w ich stosowaniu, a także przypadki zgłaszanych naruszeń przepisów o ochronie danych osobowych w tym obszarze, uzasadniają wniosek o potrzebie wprowadzenia stosownych zmian legislacyjnych w celu zapewnienia skutecznej ochrony danym osobowym oraz poszanowania prawa do prywatności i godności pacjentów i innych osób objętych takim monitoringiem.

I. Uwagi wstępne.

Stosowanie monitoringu wizyjnego w placówkach leczniczych zostało uregulowane w art. 23a ustawy o działalności leczniczej[2]. Z przepisu art. 23a ust. 1 tej

[1] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781; dalej: ustawa o ochronie danych osobowych). Zgodnie z art. 52 ust. 2 tej ustawy Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

[2] Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. 2024 r., poz. 799; dalej: ustawa o działalności leczniczej). Zgodnie z art. 23a ustawy o działalności leczniczej:
1. Kierownik podmiotu wykonującego działalność leczniczą może określić w regulaminie organizacyjnym sposób obserwacji pomieszczeń:
1) ogólnodostępnych, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pacjentów lub pracowników,

Urząd Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

tel. 22 531-03-88
fax 22 531-03-99

www.uodo.gov.pl

ustawy wynika, że kierownik podmiotu wykonującego działalność leczniczą może określić w regulaminie organizacyjnym sposób obserwacji pomieszczeń: ogólnodostępnych za pomocą urządzeń rejestrujących obraz (monitoring), jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pacjentów lub pracowników (pkt 1), w których są udzielane świadczenia zdrowotne oraz pobytu pacjentów, w szczególności pokoi łóżkowych, pomieszczeń higieniczno-sanitarnych, przebieralni, szatni, jeżeli wynika to z przepisów odrębnych (pkt 2). Ponadto, ustawą z dnia 16 czerwca 2023 r. o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[3], poprzez dodanie pkt 3 do art. 23a ust. 1 ustawy o działalności leczniczej, rozszerzono możliwość zastosowania monitoringu wizyjnego w pomieszczeniach, w których są udzielane świadczenia zdrowotne. Aktualnie – w przypadku szpitali, zakładów opiekuńczo-leczniczych, zakładów pielęgnacyjno-opiekuńczych, zakładów rehabilitacji leczniczej i hospicjów – istnieje możliwość stosowania monitoringu wizyjnego w każdym takim pomieszczeniu, jeżeli jest to konieczne w procesie leczenia pacjentów lub do zapewnienia im bezpieczeństwa. Przepis przewiduje dodatkowo konieczność spełnienia przesłanek dotyczących poszanowania intymności i godności pacjenta, a także zapewnienia ochrony danych osobowych pacjentów.

Treść art. 23a ust. 1 ww. ustawy nie jest zatem jasna, a sam pkt 3 został sformułowany bardzo ogólnie, nie precyzuje bowiem zasad i procedur stosowania monitoringu, ani wymaganych i odpowiadających *ratio legis* gwarancji dla ochrony danych osobowych poszczególnych osób objętych monitoringiem odzwierciedlających wymogi wynikające z rozporządzenia 2016/679 (w szczególności art. 5 ust. 1 lit. a, b, c, f w zw. z art. 6 ust. 3 w zw. z art. 9 ust. 2 i 3 rozporządzenia 2016/679). Regulacje szczegółowe dotyczące przetwarzania danych osobowych musi zaś cechować zupełność, przejrzystość i konkretność, zwłaszcza w odniesieniu do przetwarzania danych dotyczących zdrowia. Odesłanie – o którym mowa w art. 23a ust. 1 ustawy – do stosowania regulacji ogólnych dotyczących ochrony danych osobowych z całą pewnością nie jest wystarczające.

Wykorzystywanie monitoringu wizyjnego w podmiotach leczniczych oznacza w większości przypadków **przetwarzanie danych osobowych szczególnych kategorii, dotyczących zdrowia** (art. 9 ust. 1 rozporządzenia 2016/679). Dlatego też trzeba mieć na względzie spoczywający na ustawodawcy, w myśl przepisów rozporządzenia

---

2) w których są udzielane świadczenia zdrowotne oraz pobytu pacjentów, w szczególności pokoi łóżkowych, pomieszczeń higieniczno-sanitarnych, przebieralni, szatni, jeżeli wynika to z przepisów odrębnych,

3) w których są udzielane świadczenia zdrowotne, jeżeli jest to konieczne w procesie leczenia pacjentów lub do zapewnienia im bezpieczeństwa -w przypadku szpitali, zakładów opiekuńczo-leczniczych, zakładów pielęgnacyjno-opiekuńczych, zakładów rehabilitacji leczniczej i hospicjów

– za pomocą urządzeń umożliwiających rejestrację obrazu (monitoring), uwzględniając konieczność poszanowania intymności i godności pacjenta, w tym przekazywanie obrazu z monitoringu w sposób uniemożliwiający ukazywanie intymnych czynności fizjologicznych, potrzebę zastosowania monitoringu w danym pomieszczeniu oraz konieczność ochrony danych osobowych.

[3] Ustawa z dnia 16 czerwca 2023 r. o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U z 2023 r. poz. 1675).

2016/679, szczególny obowiązek wprowadzenia precyzyjnych i adekwatnych do ochrony danych osobowych regulacji w tym obszarze, uwzględniających nie tylko zasady wynikające z rozporządzenia 2016/679, ale i zasady wyznaczone przez art. 51 ust. 2 i art. 31 ust. 3 Konstytucji RP.

Zgodnie z art. 5 ust. 1 lit a oraz motywem 41 rozporządzenia 2016/679[4], podstawa prawna lub akt prawny będący podstawą do przetwarzania danych osobowych powinny być **jasne** i **precyzyjne**, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka. Realizacja zasady przejrzystości, o której mowa w tym przepisie, wymaga od twórcy przepisów tworzenia rozwiązań, które w sposób jasny będą wskazywały na ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących osobie, której dane będą przetwarzane.

Ponadto, w myśl art. 5 ust. 1 lit c rozporządzenia 2016/679, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Jak stanowi zaś art. 6 ust. 3 rozporządzenia 2016/679 podstawa przetwarzania, o której mowa w ust. 1 lit. c) i e), **musi być określona w prawie** Unii lub w prawie państwa członkowskiego, któremu podlega administrator i ma zawierać cel przetwarzania, a dodatkowo także **przepisy szczegółowe dostosowujące**

---

[4] Zgodnie z art. 5 ust. 1 dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania");
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").
2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").
Zgodnie z motywem 41, W przypadku gdy w niniejszym rozporządzeniu jest mowa o podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Taka podstawa prawna lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających - jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej "Trybunałem Sprawiedliwości") i Europejskiego Trybunału Praw Człowieka.

stosowanie przepisów rozporządzenia, w tym ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego **muszą służyć realizacji celu leżącego w interesie publicznym oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu**.

Dodatkowo, w przypadku przetwarzania danych szczególnych kategorii (tzw. wrażliwych) – stosownie do treści art. 9 ust. 2 lit h rozporządzenia 2016/679 – dozwolone jest ich przetwarzanie do celów (m.in.) zapewnienia opieki zdrowotnej, czy leczenia w przypadku, gdy jest to niezbędne i odbywa się na podstawie prawa Unii lub prawa państwa członkowskiego oraz z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3 rozporządzenia 2016/679, tj. z zapewnieniem zachowania tajemnicy zawodowej[5]. Obowiązek zachowania tajemnicy zawodowej przy przetwarzaniu szczególnych kategorii danych powinien być nałożony przepisami prawa i dotyczyć osób przetwarzających dane.

Z punktu widzenia standardów konstytucyjnych dotyczących prawa do ochrony danych osobowych wynikającego z art. 51 Konstytucji RP, warto podnieść, że sprawy istotne, które muszą zostać uregulowane w przepisach rangi ustawy, obejmują w szczególności **warunki dopuszczalności przetwarzania danych osobowych**[6]. W wyroku z 19 lutego 2002 r., sygn. akt U 3/01, Trybunał Konstytucyjny podkreślił, że ustawa powinna określać w sposób szczególnie precyzyjny warunki przetwarzania danych dotyczących sfery intymności jednostki. Trybunał wskazał, że w tej specyficznej materii, którą stanowi unormowanie wolności i praw człowieka i obywatela, **unormowanie ustawowe musi cechować zupełność**.

Jednocześnie, wobec braku w przepisach szczegółowych – regulujących działalność leczniczą – odpowiednich gwarancji zapewniających autonomię informacyjną podmiotów danych, **wątpliwości budzi proporcjonalność** przyjętych rozwiązań przewidujących możliwość zastosowania w bliżej nieokreślony sposób

[5] Zgodnie z art. 9 ust. 2 lit h rozporządzenia 2016/679, ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków: przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
Zgodnie z art. 9 ust. 3 rozporządzenia 2016/679 dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez - lub na odpowiedzialność - pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

[6] Zob. wyroki z 19 maja 1998 r., sygn. akt U 5/97, 30 lipca 2014 r., sygn. akt K 23/11 oraz 19 lutego 2002 r., sygn. akt U 3/01.

monitoringu wizyjnego w każdym pomieszczeniu, w którym udzielane są świadczenia zdrowotne (art. 5 ust. 1 lit. c w zw. z art. 51 Konstytucji RP w zw. z art. 31 ust. 3 Konstytucji RP).

Co istotne, wykorzystywanie monitoringu wizyjnego w podmiotach leczniczych trzeba uznać za poważną ingerencję w prawo do prywatności osób objętych monitoringiem, w szczególności pacjentów. Zgodnie z art. 20 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[7] pacjent ma prawo do poszanowania intymności i godności, w szczególności w czasie udzielania mu świadczeń zdrowotnych. Artykuł 30 Konstytucji RP stanowi zaś, że przyrodzona i niezbywalna godność człowieka jest źródłem wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych[8]. Art. 47 Konstytucji RP gwarantuje dodatkowo poszanowanie prawa do życia prywatnego.

W tym względzie również Trybunał Sprawiedliwości UE wskazał, że uregulowanie zawierające środek umożliwiający ingerencję w prawa i wolności osób fizycznych musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania takiego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, których dane osobowe są przetwarzane, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć[9].
W szczególności osoby te powinny być w stanie określić okoliczności i warunki, w jakich zakres praw przyznanych im przez wspomniane rozporządzenie może podlegać ograniczeniu**.**

Ponadto, Trybunał podkreślił, że zgodnie z art. 52 ust. 1 zdanie pierwsze Karty Praw Podstawowych UE (dalej: KPP) wszelkie ograniczenia w korzystaniu z uznanych w tym akcie praw i wolności, do których należą między innymi prawo do poszanowania życia prywatnego, zagwarantowane w art. 7 KPP, oraz prawo do ochrony danych osobowych, zapisane w art. 8 KPP, muszą być przewidziane ustawą, co oznacza w szczególności, że podstawa prawna umożliwiająca ingerencję w te prawa powinna sama określać zakres ograniczenia wykonywania danego prawa[10]. Dodatkowo, z orzecznictwa Trybunału Sprawiedliwości UE wynika, że **odstępstwa od ochrony danych osobowych i jej ograniczenia powinny być stosowane jedynie wtedy, gdy jest to absolutnie konieczne**[11].

Artykuł 51 oraz art. 31 ust. 3 Konstytucji RP również przewidują, że ograniczenia prawa do prywatności i autonomii informacyjnej jednostki powinny mieć rangę

---

[7] Zob. ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2024 r. poz. 581).

[8] Zob. wyrok TK z 16 marca 2011 r., sygn. akt K 35/08, w którym TK wskazał, że skierowany do władzy publicznej nakaz poszanowania godności człowieka z art. 30 Konstytucji RP, wymaga zaś zapewnienia „możliwie najskuteczniejszej i najszerszej" ochrony wolności i praw konstytucyjnych oraz usuwania naruszeń tych praw.

[9] Zob. podobnie wyrok z 2 marca 2021 r., Prokuratuur (Warunki dostępu do danych dotyczących łączności elektronicznej), C 746/18 przytoczone tam orzecznictwo.

[10] Zob. podobnie wyrok z 6 października 2020 r., Privacy International, C 623/17; zob. szerzej: M. Wróblewski, *Karta Praw Podstawowych Unii Europejskiej*, [w:] „System Prawa Unii Europejskiej. Tom I. Podstawy i źródła prawa Unii Europejskiej", red. S. Biernat, Warszawa 2020, s. 725-775.

[11] Zob. wyrok z 4 maja 2017 r., Rīgas satiksme, C 13/16, wyrok TSUE z 22 czerwca 2021 w sprawie C-439/19, podobnie wyrok TSUE z 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18.

ustawową, nie naruszać istoty ograniczanych wolności i praw, a także być konieczne w demokratycznym państwie prawnym dla ochrony enumeratywnie wymienionych wartości (bezpieczeństwa, porządku publicznego, ochrony środowiska, zdrowia, moralności publicznej czy też wolności i praw innych osób).

W świetle standardów europejskich i konstytucyjnych ocena proporcjonalności art. 23a ustawy o działalności leczniczej wymaga zatem ważenia dwóch wartości: interesu publicznego (interesu podmiotu leczniczego dotyczącego stosowania monitoringu w celu leczenia pacjentów lub zapewnienia im bezpieczeństwa) oraz prawa do ochrony danych osobowych i prawa do prywatności.

Niezbędnym narzędziem tzw. testu prywatności jest zaś **ocena skutków dla ochrony danych**, którą prawodawca jest zobowiązany przeprowadzić w przypadku wprowadzania rozwiązań mogących powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych dotyczących przetwarzania danych, w tym w szczególności z użyciem nowych technologii (art. 35 ust. 10 rozporządzenia 2016/679 w zw. z art. 25 ust. 1 i 2 oraz art. 36 rozporządzenia 2016/679). Jest to również ważny instrument rozliczalności, ponieważ ułatwia nie tylko przestrzeganie wymogów określonych w rozporządzeniu 2016/679, ale także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów rozporządzenia 2016/679[12].

Poniżej przedstawiono szczegółową analizę art. 23a ustawy o działalności leczniczej w kontekście przytoczonych powyżej standardów ochrony danych osobowych.

II. Uwagi szczegółowe.

1. Niedookreśloność art. 23a ustawy o działalności leczniczej w kontekście zasady legalności

Ustawodawca nie uregulował w przepisach dotyczących stosowania monitoringu wizyjnego w placówkach medycznych **zasad stosowania monitoringu, o którym mowa w art. 23a ustawy o działalności leczniczej. Pozostawił te istotne zagadnienia woli wykonawcy normy, tj. do unormowania w regulaminie organizacyjnym**, a zatem akcie pozbawionym mocy powszechnie obowiązującego źródła prawa. Przekazanie tak istotnej materii do uregulowania poza regulację ustawową, z punktu widzenia przedstawionych wyżej standardów ochrony danych osobowych, w tym zasady zgodności z prawem, budzi zasadnicze zastrzeżenia organu nadzorczego.

Jak wynika z powołanego wyżej orzecznictwa TSUE i TK warunki dopuszczalności przetwarzania danych osobowych powinny być precyzyjnie określone w normach prawnych, o właściwym poziomie regulacji. Ma to służyć temu, aby

[12] Zob. Wytyczne grupy Roboczej art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie "może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, WP248 rev.01.

wykonawcom norm wyznaczyć podstawy i granice działania, jak również aby osoby, których dane osobowe są przetwarzane, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć. To na ustawodawcy ciąży zatem obowiązek uregulowania sposobów i granic przetwarzania danych osobowych niezbędnych dla działalności podmiotu leczniczego, w tym zakres i sposób przetwarzania, a także minimalne warunki przetwarzania, odpowiednio do celów regulacji (*ratio legis*).

W wytycznych Rzecznika Praw Pacjentów odnośnie do stosowania monitoringu wizyjnego w podmiotach leczniczych[13] rekomenduje się przykładowo, aby w tzw. pomieszczeniach łóżkowych zastosowanie monitoringu było uzależnione od medycznego uzasadnienia wprowadzenia monitoringu, a w pomieszczeniach zabiegowych – bez rejestracji wizerunku. Ponadto rekomenduje się możliwość monitorowania tego rodzaju pomieszczeń, jeśli bezpieczeństwo konkretnej grupy pacjentów wskazuje na taką potrzebę. Wskazuje się także, aby podmiot leczniczy respektował prawną skuteczność sprzeciwu pacjenta wobec prowadzenia streamingu w przypadku prowadzenia działalności dydaktycznej przez podmiot leczniczy[14].

Ustawodawca nie określił jednak tych zasad, stanowiących istotne gwarancje ochrony danych osobowych oraz prywatności pacjentów w regulacji ustawowej, tj. w art. 23a ustawy o działalności leczniczej.

Brak jest również regulacji wymaganych art. 9 ust. 3 rozporządzenia 2016/679, dotyczących zapewnienia upoważnienia dla osób przetwarzających dane z monitoringu i gwarantujących zachowanie tajemnicy zawodowej. W tym kontekście należy również mieć na względzie konieczność zagwarantowania tajemnicy lekarskiej podczas udzielania świadczeń zdrowotnych w monitorowanych pomieszczeniach.

Dodatkowo z punktu widzenia konstrukcji przepisu **niejasna jest relacja pkt 2 i 3 artykułu 23a ust. 1 ustawy**, obie te normy odnoszą się bowiem do kwestii stosowania monitoringu wizyjnego w pomieszczeniach, w których są udzielane świadczenia zdrowotne. W art. 23a ust. 1 pkt 2 ustawy przewidziano możliwość funkcjonowania monitoringu w takich pomieszczeniach, jeżeli wynika to z przepisów odrębnych. Zgodnie z tymi odrębnymi regulacjami, będą to pomieszczenia zespołu porodowego, oddziału dziecięcego, psychiatrycznego, anestezjologii[15]. Pozostawienie tych regulacji,

---

[13] Monitoring wizyjny w podmiotach leczniczych. Nowy przewodnik dla kierowników placówek medycznych" Warszawa 2023: https://www.gov.pl/web/rpp/monitoring-wizyjny-w-podmiotach-leczniczych-nowy-przewodnik-dla-kierownikow-placowek-medycznych

[14] Jak wskazano w wytycznych „podmioty lecznicze, w których prowadzona jest działalność dydaktyczna, mają możliwość udostępniania w czasie rzeczywistym obrazu rejestrowanego przez system monitoringu wizyjnego, w zakresie niezbędnym do realizacji celów dydaktycznych, o których mowa w art. 36 ust. 4 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, chyba że pacjent lub jego przedstawiciel ustawowy sprzeciwią się temu".

[15] W świetle przepisów rozporządzenia Ministra Zdrowia z dnia 26 marca 2019 r. w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą (Dz. U. z 2022 r., poz. 402), kamery mogą być instalowane w następujących pomieszczeniach: 1) zespołu porodowego (załącznik nr 1 do rozporządzenia, cz. 4, ust. 4); 2) oddziału dziecięcego (załącznik nr 1 do rozporządzenia, cz. 5, ust. 7); 3) oddziału psychiatrycznego (załącznik nr 1 do rozporządzenia, cz. 8, ust. 6 pkt 2 lit. h); 4) stacji dializ – na stanowisku nadzoru pielęgniarskiego (załącznik nr 7 do rozporządzenia, ust. 3). Ponadto § 29 rozporządzenia stanowi, że w pokojach łóżkowych dopuszcza się instalację urządzeń umożliwiających obserwację pacjentów, jeżeli jest to konieczne w procesie ich leczenia i dla zapewnienia im bezpieczeństwa. Ponadto przepisy części 1

przy jednoczesnym wprowadzeniu art. 23a ust. 1 pkt 3, który umożliwia zastosowanie monitoringu w każdym pomieszczeniu, w którym są udzielane świadczenia zdrowotne budzi poważne zastrzeżenia z punktu widzenia zasady rzetelności i przejrzystości.

Materia dotycząca stosowania obserwacji pacjentów w placówkach medycznych została zawarta także w rozporządzeniu w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą[16]. Zgodnie z § 29 rozporządzenia w pokojach łóżkowych dopuszcza się instalację urządzeń umożliwiających obserwację pacjentów, jeżeli jest to konieczne w procesie ich leczenia i dla zapewnienia im bezpieczeństwa[17]. Regulacja ta jest jednak bardzo lakoniczna i nie zawiera szczegółowych wytycznych, jakie powinny zostać spełnione w przypadku wprowadzenia monitoringu.

Brak jest więc aktualnie jakichkolwiek regulacji w przepisach powszechnie obowiązujących, które określałyby zasady i warunki – standardy – stosowania monitoringu wizyjnego w placówkach medycznych.

W ocenie Prezesa UODO doprecyzowanie art. 23a ust. 1 pkt 3 ustawy o działalności leczniczej o normy wyznaczające zasady funkcjonowania monitoringu w pomieszczeniach, w których są udzielane świadczenia zdrowotne jest niezbędne w celu zapewnienia skutecznego poziomu ochrony danych osobowych i poszanowania prawa do prywatności pacjentów (jak i ewentualnych osób trzecich, np. odwiedzających pacjenta) we wszystkich podmiotach leczniczych.

2. Brak regulacji gwarantujących prawo do informacji pacjentów w kontekście zasady przejrzystości

Brak jest również odpowiednich przepisów dotyczących wypełnienia **obowiązku informacyjnego wobec pacjentów i innych osób**. Nieodłącznym elementem europejskiego prawa o ochronie danych jest natomiast, aby osoby, których dane dotyczą, były świadome faktu działania monitoringu wizyjnego. Jak wynika z wytycznych EROD w sprawie przetwarzania danych osobowych przez urządzenia wideo, osoby te – stosownie do zasady przejrzystości (art. 5 ust. 1 lit a rozporządzenia 2016/679) oraz praw wynikających z art. 12 i 13 i art. 15 rozporządzenia 2016/679 – należy szczegółowo informować o miejscach objętych monitoringiem[18]. Gwarancje w

załącznika nr 1 do rozporządzenia Ministra Zdrowia z dnia 16 lutego 2016 r. w sprawie standardu organizacyjnego opieki zdrowotnej w dziedzinie anestezjologii i intensywnej terapii (Dz. z 2023 r., poz. 332) stanowią, iż na OAiT oraz oddziałach anestezjologii w szpitalu zapewnia się możliwość obserwacji bezpośredniej lub przy użyciu kamer wyposażonych w funkcjonowanie autostartu, w szczególności możliwość obserwacji twarzy. Dodatkowo należy wskazać, że zgodnie z art. 18e ust. 2 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. z 2022 r. poz. 2123), pomieszczenie przeznaczone do izolacji wyposaża się w instalację monitoringu umożliwiającą stały nadzór nad osobą z zaburzeniami psychicznymi w nim przebywającą oraz kontrolę wykonania czynności związanych z tym rodzajem środka przymusu bezpośredniego.

[16] Rozporządzenie Ministra Zdrowia z dnia 26 marca 2019 r. w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą (Dz. U. z 2022 r. poz. 402).

[17] Zgodnie z § 29 rozporządzenia w pokojach łóżkowych dopuszcza się instalację urządzeń umożliwiających obserwację pacjentów, jeżeli jest to konieczne w procesie ich leczenia i dla zapewnienia im bezpieczeństwa.

[18] Zob. Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo

tym zakresie powinny być więc uwzględnione również w przepisach ustawy o działalności leczniczej.

Jednym z podstawowych obowiązków administratora (podmiotu leczniczego) jest **przejrzyste informowanie** osoby, której dane dotyczą i **przejrzysta komunikacja** z nią **w sprawie przetwarzania danych osobowych** (art. 12 rozporządzenia 2016/679), w myśl regulacji w nim przewidzianych.

Należy przy tym wskazać, że niedopuszczalne jest, by monitoring był prowadzony przy pomocy ukrytych kamer. Uprawnienia do prowadzenia niejawnego monitorowania mają jedynie służby porządkowe bądź specjalne prowadzące czynności na podstawie ustaw regulujących ich działalność. Stosowanie ukrytych kamer może zostać uznane za nadmiarową formę przetwarzania danych, wiązać się z odpowiedzialnością administracyjną i cywilną, a nawet karną[19].

W kontekście art. 13 rozporządzenia 2016/679 ustawodawca powinien więc zadbać o właściwe normy zobowiązujące kierowników placówek leczniczych – na wzór funkcjonujących już rozwiązań przyjętych w innych regulacjach prawnych dotyczących monitoringu wizyjnego[20] – do przekazania informacji o zastosowanym monitoringu oraz oznaczenia monitorowanych pomieszczeń w sposób widoczny i czytelny. Należy przy tym pamiętać, że obowiązek informacyjny ciążący na administratorze danych w odniesieniu do osób, których dotyczy przetwarzanie danych osobowych, jest ściśle związany z prawem do informacji, które zostało przyznane tym osobom w art. 12 i 13 i art. 15 rozporządzenia 2016/679, a także z celem rozporządzenia 2016/679, jakim jest zapewnienie skutecznej ochrony podstawowych praw i wolności osób fizycznych.

3. **Proporcjonalność przyjętych rozwiązań dotyczących stosowania monitoringu wizyjnego w placówkach medycznych**.

Dotychczasowe regulacje dotyczące stosowania monitoringu wizyjnego w pomieszczeniach, w których są udzielane świadczenia zdrowotne[21], **ograniczały możliwość zastosowania monitoringu do określonych w odrębnych przepisach przypadków**. Przykładowo, jak wskazano wyżej, zgodnie z przepisami wykonawczymi wydanymi na podstawie art. 22 ust. 3 ustawy o działalności leczniczej, kamery mogą być instalowane w pomieszczeniach zespołu porodowego, oddziału dziecięcego, psychiatrycznego, anestezjologii. Jednocześnie **ograniczenia dotyczyły możliwości nagrywania obrazu** uzyskanego z monitoringu wizyjnego. Artykuł 23a ust. 2 ustawy o

[19] Zob. Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego", czerwiec 2018 r.

[20] Zob. np. art. Art. 22^2 § 7- § 9 ustawy z dnia 26 czerwca 1974 r., Kodeks pracy (Dz. U. 2023, poz. 1465, ze zm.), art. 108a ust. 6-8 ustawy z dnia 14 grudnia 2016 r. Prawa oświatowego (Dz. U. z 2024, poz. 737, ze zm.), art. 9a ust. 5 ustawy z 8 marca 1990 r. o samorządzie gminnym (Dz.. U. z 2024, poz. 1465 ze zm.), art. 4b ust. 5 ustawy z dnia 5 czerwca 1998 o samorządzie powiatowym (Dz. U. z 2024, 107), art. 60a ust. 6 ustawy o samorządzie wojewódzkim z dnia 5 czerwca 1998 r., (Dz. U. z 2024, poz. 566) .

[21] Art. 23a ust. 1 pkt 2 ustawy o działalności leczniczej.

działalności leczniczej odnoszący się do nagrań obrazu uzyskanego z monitoringu dotyczył ust. 1, w odniesieniu do pomieszczeń ogólnodostępnych[22].

Natomiast aktualnie, zgodnie z art. 23a ust. 1 pkt 3 ustawy o działalności leczniczej, istnieje możliwość zastosowania monitoringu **w każdym** pomieszczeniu, w którym są udzielane świadczenia zdrowotne. Ponadto, zgodnie z dodanym art. 23a ust. 2 i 3 ustawy o działalności leczniczej nagrania obrazu uzyskane w wyniku monitoringu zawierające dane osobowe podmiot wykonujący działalność leczniczą ma możliwość przetwarzać bez żadnych ograniczeń w odniesieniu do pomieszczeń, w których jest instalowany, wyłącznie do celów, dla których zostały zebrane i przechowując przez okres nie dłuższy niż 3 miesiące od dnia nagrania (23a ust. 2). Po upływie okresu, o którym mowa w ust. 2, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej (art. 23a ust. 3).

Proporcjonalność przyjętego w art. 23a ust. 1 pkt 3 ustawy o działalności leczniczej rozwiązania budzi więc wątpliwości Prezesa UODO. Stosownie bowiem do zasad ograniczenia celu i minimalizacji danych[23], wynikających z art. 5 ust. 1 lit b i c rozporządzenia 2016/679, zastosowanie monitoringu wizyjnego może mieć miejsce jedynie w przypadku gdy cel, tj. leczenie pacjentów lub zapewnienie bezpieczeństwa pacjentów, uzasadnia obserwację osób i jeżeli jest to niezbędne do tego celu.

W wytycznych dotyczących stosowania monitoringu wizyjnego Europejska Rada Ochrony Danych (EROD) wskazuje na różne ryzyka związane ze stosowaniem urządzeń monitorujących, w tym na ryzyko wykorzystania monitoringu niezgodnie z przeznaczeniem, ryzyko nieprawidłowego działania urządzeń oraz związanych z tym uprzedzeń. EROD podkreśla przy tym, że mając do czynienia z monitoringiem wizyjnym zawsze należy dokładnie przeanalizować ogólne zasady określone w rozporządzenia 2016/679 (art. 5 rozporządzenia 2016/679)[24].

W ocenie EROD, monitoring wizyjny nie jest domyślnie niezbędny, gdy istnieją inne środki umożliwiające osiągnięcie założonego celu. W przeciwnym razie dojść może do ryzykownych zmian w zakresie norm kulturowych, prowadzących do zaakceptowania braku prywatności jako warunku podstawowego.

Oznacza to, że monitoring wizyjny może być wprowadzany wyłącznie wtedy, kiedy inne, mniej inwazyjne metody zapewniania bezpieczeństwa pacjentom są niewystarczające[25].

Tymczasem konstrukcja aktualnych regulacji krajowych może być interpretowana jako zezwalająca na zastosowania monitoringu wizyjnego w każdym pomieszczeniu, w którym są udzielane świadczenia zdrowotne (nie tylko w szpitalach, ale także np. hospicjach). Ustawodawca nie przewidział przy tym – jak wskazano już wyżej –

---

[22] Zob. Kodeks postępowania dla sektora ochrony zdrowia, Warszawa, 2023 r. (s. 28; https://uodo.gov.pl/pl/426/1110

[23] Zgodnie z art. 5 ust. 1 lit. b i c rozporządzenia 2016/679 dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

[24] Zob. str. 5,6 Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo Wersja 2.0 przyjęta w dniu 29 stycznia 2020 r.

[25] Zob. też wskazówki Prezesa UODO dotyczące wykorzystywania monitoringu wizyjnego https://uodo.gov.pl/data/filemanager_pl/1200.pdf

żadnych regulacji zapewniających poszanowanie prawa do ochrony danych osobowych, czy prywatności pacjenta, odsyłając jedynie do generalnych przesłanek i ogólnych przepisów.

Aktualne regulacje mogą być dodatkowo interpretowane jako zezwalające na stosowanie monitoringu wizyjnego wraz z funkcją nagrywania obrazu. Wydaje się, jednocześnie, że skoro art. 23a ust. 1 ustawy przewiduje możliwość obserwacji pomieszczeń „za pomocą urządzeń umożliwiających rejestrację obrazu", to wykluczona powinna być taka interpretacja tych przepisów, która pozwoliłaby nie tylko na nagrywanie obrazu, ale i dźwięku.

Co ważne, przy tak istotnej ingerencji w prawo do prywatności pacjenta i prawa do autonomii informacyjnej jednostki, wątpliwości budzi również **uzależnienie podjęcia decyzji o zastosowaniu monitoringu od swobodnej woli kierownika podmiotu leczniczego.** To ustawodawca powinien określić w jakich sytuacjach i z uwzględnieniem jakich rozwiązań dopuszczalne jest zastosowanie tak inwazyjnej formy zapewnienia bezpieczeństwa pacjentów, jeśli podmiot leczniczy przyjmuje takie rozwiązanie.

Adekwatne przepisy przewidujące stosowanie monitoringu w miejscu pracy, czy w placówkach edukacyjnych, zapewniają zaangażowanie przedstawicieli osób obserwowanych w proces decyzyjny dotyczący instalowania i funkcjonowania monitoringu. Przykładowo, Kodeks pracy[26] przewiduje przeprowadzenie konsultacji z pracownikami, zaś przepisy Prawa oświatowego[27] z organem prowadzącym szkołę oraz społecznością szkolną (radą pedagogiczną, radą rodziców i samorządem uczniowskim).

Powyższe regulacje przewidują również istotne zasady i warunki instalowania monitoringu takie jak: wskazanie pomieszczeń wykluczonych z monitorowania (sale dydaktyczne, wychowawcze, pomieszczenia sanitarne, stołówki), konieczność zastosowania technik uniemożliwiających rozpoznanie osób w sytuacji zainstalowania monitoringu w niektórych takich pomieszczeniach, czy też ustalają gwarancje ochrony praw osób monitorowanych, takie jak np. obowiązki informacyjne, czy szczególne regulacje np. o braku podstaw do uznania monitoringu jako środka nadzoru nad jakością wykonywania pracy.

Regulację wynikającą z art. 23a ustawy o działalności leczniczej trudno więc aktualnie pogodzić również z regulacjami wynikającymi z Kodeksu pracy, które gwarantują poszanowanie prawa do prywatności i ochrony danych osobowych pracowników zatrudnionych w podmiotach leczniczych (por. też wyrok Europejskiego Trybunału Praw Człowieka z 17 października 2019 roku López Ribalda i Inni przeciwko Hiszpanii [Wielka Izba], skargi nr 1874/13 i 8567/13, w którym Trybunał odniósł się do zasad i kryteriów stosowania monitoringu wizyjnego w miejscu pracy)[28].

---

[26] Zob. art. 22^2 ustawy z dnia 26 czerwca 1974 r., Kodeks pracy (Dz. U. 2023 r. poz. 1465, ze zm.),
[27] Art. 108a ust. 3 ustawy z dnia 14 grudnia 2016 r. Prawa oświatowego (Dz. U. z 2024 r. poz. 737 ze zm.).
[28] Jak wskazał ETPC, „pracodawca może zastosować środki nadzoru wideo w miejscu pracy. Kryteria te należy stosować, biorąc pod uwagę specyfikę stosunku pracy oraz rozwój nowych technologii, które mogą umożliwiać podejmowanie środków coraz bardziej ingerujących w życie prywatne pracowników. W tym kontekście, aby zapewnić proporcjonalność środków nadzoru wideo w miejscu pracy, sądy krajowe powinny uwzględnić następujące czynniki przy dokonywaniu wyważenia różnych konkurujących interesów:

Ustawodawca nie zapewnił także właściwych gwarancji w odniesieniu do tożsamych **praw osób odwiedzających** pacjenta. W wytycznych Rzecznika Praw Pacjenta słusznie rekomenduje się przy tym wyznaczenie pokojów odwiedzin lub innych obszarów kontaktu pacjenta z bliskimi.

Wobec braku precyzyjnych przepisów zapewniających właściwe gwarancje dla skutecznej ochrony danych osobowych, w ocenie Prezesa Urzędu Ochrony Danych Osobowych, aktualne regulacje przyzwalające na daleko idącą swobodę w stosowaniu monitoringu mogą więc prowadzić do nadmiernej, nieproporcjonalnej ingerencji w prawo do autonomii informacyjnej pacjenta i jego prawa do prywatności, a tym samym naruszać przepisy rozporządzenia 2026/679, a także art. 47 i art. 51 Konstytucji RP w zw. z art. 31 ust. 3 Konstytucji RP.

4. Zapewnienie gwarancji bezpieczeństwa danych przetwarzanych w związku ze stosowaniem monitoringu wizyjnego.

Dodatkowo, przepisy nie przewidują **żadnych gwarancji ani minimalnych kryteriów** zapewniających pogodzenie celów regulacji z wymogami z rozporządzenia 2016/679 w odniesieniu do **stosowania środków zabezpieczenia danych**, w szczególności zapewniających ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, uniemożliwiających ich utratę lub bezprawne rozpowszechnienie, a także uniemożliwiających dostęp do danych osobom nieuprawnionym (art. 5 ust. 1 lit. f rozporządzenia 2016/679).

W obliczu wyzwań, jakie niesie za sobą **rozwój nowych technologii**, ustawodawca powinien natomiast przyjąć w przepisach rozwiązania odpowiadające gwarancjom wymaganym mocą art. 9 ust. 3 i 4 rozporządzenia 2016/679 w związku z art. 24 tego aktu. Na projektodawcy ciąży dodatkowo obowiązek wynikający z art. 32 rozporządzenia 2016/679 wdrożenia odpowiednich środków technicznych i

---

- czy pracownika powiadomiono o możliwości wprowadzenia przez pracodawcę środków nadzoru wideo i o zastosowaniu takich środków: chociaż w praktyce pracowników można powiadomić na różne sposoby – w zależności od konkretnych faktycznych okoliczności każdej sprawy, powiadomienie powinno co do zasady być jasne co do charakteru monitoringu i nastąpić przed jego zastosowaniem;
- zakres monitoringu prowadzonego przez pracodawcę i stopień ingerencji w prywatność pracownika: w tym względzie należy uwzględnić zakres prywatności w miejscu podlegającym monitorowaniu wraz ze wszelkimi ograniczeniami co do czasu i obszaru oraz liczby osób mających dostęp do wyników;
- czy pracodawca przedstawił uprawnione powody uzasadniające monitoring i jego zakres: im bardziej ingerujący monitoring, tym poważniejsze uzasadnienie jest wymagane;
- czy było możliwe wprowadzenie systemu monitoringu opartego na mniej ingerujących metodach i środkach: w tym względzie należy dokonać oceny w świetle konkretnych okoliczności każdej sprawy, czy cel, do którego dążył pracodawca, można było osiągnąć bez ingerowania w prywatność pracowników w takim zakresie;
- konsekwencje monitoringu dla podlegających mu pracowników: należy uwzględnić, w szczególności, wykorzystanie przez pracodawcę wyników monitoringu oraz to, czy wyniki te zostały wykorzystane do uzyskania zadeklarowanego celu tego środka;
- czy pracownikowi zapewniono odpowiednie gwarancje, zwłaszcza gdy funkcjonowanie monitoringu pracodawcy ma charakter ingerujący: gwarancje takie mogą przyjąć postać m.in. przekazania zainteresowanym pracownikom oraz przedstawicielom personelu informacji o zainstalowaniu i zakresie monitoringu, zadeklarowania takiego środka niezależnemu organowi lub istnienia możliwości złożenia skargi.” .

organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający planowanemu aktem prawnym ryzyku przetwarzania.

Zapewnienie ochrony danych wiąże się nierozerwalnie z analizą ryzyka oraz wymogiem uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, a także – w przypadkach, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – dokonaniem oceny skutków dla ochrony danych (art. 35 ust. 1 i 10, art. 25 ust. 1 i 5 rozporządzenia 2016/679).

Przeprowadzenie **oceny skutków** na etapie projektowania rozwiązań przyjętych w art. 23a ustawy o działalności leczniczej niewątpliwie pozwoliłoby uniknąć wskazywanych, z punktu widzenia zasady legalności i proporcjonalności, zastrzeżeń pod adresem tych regulacji.

Ponadto, konieczne jest zapewnienie wysokich standardów bezpieczeństwa danych w związku z wykorzystywaniem urządzeń monitorujących. Implementacja systemów rejestracji obrazu wiąże się niewątpliwie z szeregiem wyzwań technicznych i organizacyjnych. Wdrażanie takiego rozwiązania wymaga odpowiednich środków technicznych, w tym zapewniających integrację danych, takich jak szyfrowanie danych, mechanizmy kontroli dostępu, rejestrowanie poszczególnych operacji oraz procedury aktualizacji i reakcji na incydenty bezpieczeństwa.

Obecne środowisko technologiczne, ze względu na dynamicznie zmieniające się zagrożenia, wymaga podejścia z dużą ostrożnością do uznawania jakichkolwiek systemów za w pełni bezpieczne. Jak zwracano uwagę w ww. opinii EROD dotyczącej monitoringu wizyjnego, „przy funkcjonowaniu monitoringu należy mieć na względzie konieczność ustanowienia zabezpieczenia, aby uniknąć wykorzystania danych niezgodnie z przeznaczeniem w zupełnie innych – dla osób, których dane dotyczą – i nieoczekiwanych celach (np. w celach marketingowych, monitorowania wyników pracownika itd.). Ponadto zauważono, że obecnie wdraża się wiele narzędzi służących wykorzystaniu utrwalonych wizerunków i przekształceniu tradycyjnych kamer w inteligentne kamery. Ilość danych generowanych przez nagrania wideo, w połączeniu z tymi narzędziami i technikami zwiększają ryzyko ich wtórnego wykorzystania (bez względu na to, czy są związane z celem pierwotnie przypisanym systemowi) lub nawet ryzyko związane z wykorzystaniem danych niezgodnie z przeznaczeniem. Oprócz kwestii prywatności istnieją również ryzyka związane z ewentualnym nieprawidłowym działaniem tych urządzeń oraz związanych z tym uprzedzeń. Badacze zauważają, że oprogramowanie wykorzystywane do identyfikacji, rozpoznawania i analizy twarzy działa inaczej w zależności od wieku, płci i pochodzenia etnicznego osoby identyfikowanej. Algorytmy działają w oparciu o zróżnicowane dane demograficzne, w związku z tym uprzedzenia związane z rozpoznawaniem twarzy stwarzają ryzyko pogłębienia uprzedzeń wśród społeczeństwa. Dlatego też administratorzy danych muszą również zapewnić, aby przetwarzanie danych biometrycznych pochodzących z monitoringu wizyjnego podlegało regularnej ocenie jego znaczenia i skuteczności zastosowanych zabezpieczeń”.

Dlatego w ocenie Prezesa UODO – stosownie do treści zasady integralności i poufności, a także rozliczalności (art. 5 ust. 1 lit f oraz ust. 2 rozporządzenia 2016/679)

– należy zapewnić w projektowanych przepisach gwarancje bezpieczeństwa adekwatne do ryzyk przetwarzania, obejmujące przeprowadzanie regularnych testów bezpieczeństwa, aktualizacji i monitorowania potencjalnych zagrożeń.

5. Przypadki naruszeń przepisów dotyczących stosowania monitoringu wizyjnego w podmiotach leczniczych oraz problemy w ich stosowaniu

Problemy związane ze stosowaniem przepisów ustawy przez podmioty lecznicze są aktualne oraz prowadzą do naruszenia przepisów dotyczących ochrony danych osobowych.

Problematyka wykorzystywania monitoringu wizyjnego jest przedmiotem częstych pytań i skarg wpływających do UODO, a także przedmiotem decyzji wydawanych przez Prezesa UODO. W pismach kierowanych do UODO niejednokrotnie pojawiają się pytania dotyczące zarówno legalności, jak i zasad oraz procedur stosowania monitoringu wizyjnego[29]. Ponadto regulacje dotyczące stosowania monitoringu wizyjnego były niejednokrotnie przedmiotem opinii PUODO na etapie procesu legislacyjnego (zob. też m.in. opinia PUODO w związku z wykorzystywaniem monitoringu w zakładach leczniczych dla nieletnich, czy w ośrodkach wychowawczych / zakładach poprawczych/schroniskach dla nieletnich)[30]. Problematyka ta została już poddana wybiórczej regulacji w związku z przyjmowaniem w 2018 r. nowej ustawy o ochronie danych osobowych, w przepisach Kodeksu pracy, Prawa oświatowego, czy też ustaw samorządowych[31].

Warto też przypomnieć powtarzające się **zastrzeżenia i wnioski Najwyższej Izby Kontroli** w związku z przeprowadzonymi kontrolami w placówkach leczniczych.

W wynikach kontroli z 2018 r. dotyczących „ochrony intymności i godności pacjentów w szpitalach" stwierdzono, że w większości badanych szpitali nie zagwarantowano pełnej ochrony przetwarzania danych osobowych, uzyskanych z monitoringu wizyjnego[32]. Wskazywano na dużą ilość montowanych kamer, a także instalowanie ich w niedozwolonych pomieszczeniach, bez podstawy prawnej[33]. Zdaniem NIK, dyrektorzy szpitali przed zainstalowaniem monitoringu wizyjnego, kierując

---

[29] Zob. sprawozdania Prezesa UODO np. za 2023 r. str. 164, 237; za 2022 r. str. 173; za 2021, str. 70.
[30] Zob. sprawozdanie UODO za 2022 r. (str. 113): opinia PUODO dot. projektu rozporządzenia w sprawie komisji do spraw środka leczniczego dla nieletnich, trybu wykonywania środka leczniczego oraz warunków zabezpieczenia zakładów leczniczych, DOL.401.411.2022; opinia PUODO dot. projektu ustawy o wspieraniu i resocjalizacji nieletnich DOL.401.379.2021
[31] Zob. art. 9a ustawy z 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 1465 ze zm), art. 4b ustawy z dnia 5 czerwca 1998 o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107), art. 60a ustawy o samorządzie wojewódzkim z dnia 5 czerwca 1998 r., (Dz. U. z 2024 r. poz. 566).
[32] Zob. informacje o kontroli NIK dostępne na stronie internetowej: https://www.nik.gov.pl/plik/id,16805,vp,19361.pdf, str. 30.
[33] „W 12 skontrolowanych szpitalach funkcjonujące systemy monitoringu wizyjnego obejmowały **łącznie 962 kamery oraz 28 atrap. Kamery instalowano w latach 2000–2017.** W 11 szpitalach, zainstalowano kamery w pomieszczeniach szpitalnych, w których, według rozporządzeń Ministra Zdrowia z 26 czerwca 2012 r. i z 16 grudnia 2016 r., nie było dopuszczone monitorowanie stanu pacjenta, tj. w gabinetach zabiegowych, salach chorych i obserwacyjnych, izolatkach, gabinetach rezonansu magnetycznego, pokoju odwiedzin oraz w punktach rejestracji pacjenta. W czterech szpitalach rejestrowano obraz z kamer znajdujących w salach chorych, izolatkach, gabinetach konsultacyjnych. W siedmiu szpitalach obraz był rejestrowany z kamer umieszczonych w punktach rejestracji pacjentów.

się zasadą gospodarności, powinni przeanalizować celowość jego wprowadzenia, określić koszty wdrożenia i funkcjonowania systemu. W żadnym ze skontrolowanych szpitali nie zrobiono tego. Nie analizowano także rozmieszczenia kamer pod kątem ingerencji monitoringu w prawo pacjentów do prywatności. Co więcej, żaden z 12 szpitali nie analizował skuteczności działania monitoringu pod kątem postawionych mu celów, takich jak poprawa bezpieczeństwa pacjentów czy też zabezpieczenie materiału dowodowego w przypadkach zarejestrowania czynów zabronionych. W większości szpitali zamontowanie kamer nie przełożyło się na poprawę bezpieczeństwa w szpitalach. W czterech szpitalach, pomimo zainstalowania monitoringu wizyjnego, liczba niebezpiecznych zdarzeń wręcz wzrosła.

Podobne wnioski wynikają z kontroli NIK z 2024 r. dotyczącej „przestrzegania praw pacjenta w systemie ochrony zdrowia". Jak wskazano, „ograniczeniem prywatności pacjenta jest nieuzasadnione, nadmierne stosowanie monitoringu wizyjnego. Z ustaleń kontroli wynikało, iż monitoringiem wizyjnym obejmowano pomieszczenia, w których obowiązujące w okresie objętym kontrolą przepisy nie przewidywały obecności kamer, a regulaminy wewnętrzne dotyczące monitoringu wizyjnego były niekiedy sporządzane nierzetelnie. Nieprawidłowości w tym zakresie stwierdzono w przypadku 18 % podmiotów"[34].

Rzecznik Praw Obywatelskich również sygnalizuje zastrzeżenia wobec przepisów regulujących monitoring wizyjny w placówkach medycznych, jako nadmiernie ingerujących w prawo do prywatności i w prawo ochrony danych osobowych pacjentów. Rzecznik zwracał uwagę na wpływające do Biura RPO skargi obywateli odnośnie do nowych regulacji, a także wskazywał na wątpliwości co do proporcjonalności przyjętych rozwiązań w znowelizowanym art. 23a ustawy o działalności leczniczej[35].

Przykłady niewłaściwego stosowania monitoringu w dotychczasowej działalności podmiotów leczniczych, których dostarczają kontrole NIK dowodzą, że monitoring był wykorzystywany nadmiernie i prowadził do naruszenia prawa do prywatności i prawa ochrony danych osobowych. Aktualne regulacje – dodatkowo poszerzające dopuszczalność stosowania monitoringu wizyjnego w podmiotach leczniczych – zostały zaś sformułowane w sposób bardzo ogólny, przez co nie zapewniają aktualnie właściwej ochrony prywatności i danych

[34] Zob. Informacje z kontroli str. 42, 43. Jako przykład wskazano, że „dopuszczono jednocześnie, aby monitoring wizyjny w okresie 30 marca 2022 r. do 5 września 2023 r. objął także izolatkę na izbie przyjęć (z użyciem jednej z 32 kamer zainstalowanych w Szpitalu), mimo braku podstawy prawnej, czym naruszono art. 23a ust. 1 pkt 2 ustawy o działalności leczniczej" (str. 43).

[35] Zob. wystąpienie RPO, przesłane do wiadomości PUODO: https://bip.brpo.gov.pl/pl/content/rpo-monitoring-pomieszczenia-swiadczenia-zdrowotne-mz-odpowiedz. Jak wskazywano w wystąpieniu: „Wnioskodawcy sygnalizują, że dodany art. 23a ust. 1 pkt 3 ustawy o działalności leczniczej pozostawia **zbyt dużą swobodę decyzyjną kierownikowi** podmiotu leczniczego w odniesieniu do zastosowania monitoringu wizyjnego w pomieszczeniu, w którym udzielane są świadczenia zdrowotne. Jednocześnie wskazują, że przepis ten **nie określa przesłanek zastosowania monitoringu** (np. przesłanki konieczności), a także nie pozostawia pacjentom możliwości odmowy wyrażenia zgody na udzielenie świadczenia zdrowotnego w pomieszczeniu monitorowanym, przez co naraża pacjentów na ryzyko naruszenia ich prawa do intymności, godności i prywatności. Wskazywane są także uwagi dotyczące **dostępu do nagrań** obrazu uzyskanego z monitoringu, który przewidziany jest aktualnie dla personelu technicznego i ochrony, a nie personelu medycznego".

osobowych pacjentów. W konsekwencji mogą prowadzić do nadmiernej ingerencji w prawo do prywatności i ochrony danych osobowych pacjenta.

Podsumowując, w opinii Prezesa UODO konieczne jest stworzenie spójnego systemu w zakresie stosowania monitoringu wizyjnego w placówkach medycznych, w miejsce rozproszonych fragmentarycznych regulacji w tym obszarze, poprzez odpowiednie uwzględnienie wskazywanych zasad i standardów ochrony danych osobowych, tak, aby uniknąć jakiejkolwiek dowolności po stronie podmiotów wykonujących działalność leczniczą i jednocześnie zagwarantować właściwą ochronę danych osobowych i prawa do prywatności osób objętych monitoringiem.

W przypadku podjęcia prac legislacyjnych przez resort zdrowia, w związku z przedstawionym powyżej zagadnieniami, Prezes Urzędu Ochrony Danych Osobowych deklaruje swoje wsparcie eksperckie celem wypracowania rozwiązań uwzględniających przepisy o ochronie danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

Do wiadomości

Pan
Marian Banaś
Najwyższe Izby Kontroli

Pan Marcin Wiącek
Rzecznik Praw Obywatelskich

Pan
Prezes Bartłomiej Łukasz Chmielowiec
Rzecznik Praw Pacjenta