GRUPA ROBOCZA ART. 29

17/PL

WP 249

Opinia 2/2017 na temat przetwarzania danych w miejscu pracy

Przyjęta w dniu 8 czerwca 2017 r.

Spis treści

1. Streszczenie

Niniejsza opinia stanowi uzupełnienie wcześniejszych publikacji Grupy Roboczej Art. 29, tj. *opinii 8/2001 w sprawie przetwarzania danych osobowych w związku z zatrudnieniem* (WP 48)[1] i *dokumentu roboczego z 2002 r. w sprawie nadzoru komunikacji elektronicznej w miejscu pracy* (WP 55)[2]. Od czasu publikacji tych dokumentów przyjęto szereg nowych technologii, które umożliwiają bardziej systematyczne przetwarzanie danych osobowych pracowników w miejscu pracy, co stanowi poważne wyzwanie dla ochrony prywatności i danych.

W niniejszej opinii dokonano nowej oceny równowagi między prawnie uzasadnionymi interesami pracodawców a uzasadnionymi oczekiwaniami pracowników w zakresie ochrony prywatności poprzez opis zagrożeń, jakie niosą ze sobą nowe technologie, i przeprowadzenie oceny proporcjonalności szeregu scenariuszy, w których można je wykorzystać.

Chociaż opinia dotyczy przede wszystkim dyrektywy o ochronie danych, przeanalizowano w niej dodatkowe obowiązki nakładane na pracodawców na mocy ogólnego rozporządzenia o ochronie danych. Ponownie przedstawiono w niej również stanowisko i wnioski zawarte w opinii 8/2001 i dokumencie roboczym WP 55, mianowicie, że przy przetwarzaniu danych osobowych pracowników:

- pracodawcy powinni zawsze pamiętać o podstawowych zasadach ochrony danych, niezależnie od stosowanej technologii;
- treść komunikacji elektronicznej wychodzącej z lokalu przedsiębiorstwa jest objęta taką samą ochroną praw podstawowych co komunikacja analogowa;
- istnieje małe prawdopodobieństwo, aby zgoda stanowiła podstawę prawną do przetwarzania danych w miejscu pracy, chyba że pracownicy mogą odmówić przetwarzania danych bez negatywnych konsekwencji;
- niekiedy można powołać się na wykonanie umowy i prawnie uzasadnione interesy, pod warunkiem że przetwarzanie danych jest bezwzględnie konieczne ze względów prawnych i zgodne z zasadą proporcjonalności i pomocniczości;
- pracownicy powinni otrzymywać skuteczne informacje o prowadzonym monitoringu; oraz
- międzynarodowe przekazywanie danych pracowników powinno się odbywać tylko wówczas, gdy zapewniony jest odpowiedni stopień ochrony.

2. Wprowadzenie

Szybkie 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. Na przykład:

---

[1] *Opinia 08/2001 Grupy Roboczej Art. 29 w sprawie przetwarzania danych osobowych w związku z zatrudnieniem*, WP 48, z dnia 13 września 2001 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] Grupa Robocza Art. 29, *dokument roboczy w sprawie nadzoru komunikacji elektronicznej w miejscu pracy*, WP 55, z dnia 29 maja 2002 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

- technologie wspomagające przetwarzanie danych w miejscu pracy mogą być obecnie wdrażane za ułamek kosztów, jakie trzeba by było ponieść kilka lat temu, podczas gdy zdolność do przetwarzania danych osobowych przez te technologie wzrosła wykładniczo;
- nowe formy przetwarzania danych, takie jak te odnoszące się do danych osobowych na temat korzystania z usług *online* lub danych dotyczących lokalizacji z urządzenia inteligentnego, są znacznie mniej widoczne dla pracowników niż inne bardziej tradycyjne formy przetwarzania, np. jawne monitorowanie kamerami CCTV. W związku z tym powstaje pytanie, w jakim stopniu pracownicy są świadomi tych technologii, ponieważ pracodawcy mogą niezgodnie z prawem dokonywać takiego przetwarzania danych bez uprzedniego powiadomienia o tym pracowników; oraz
- coraz bardziej zacierają się granice między domem a pracą. Na przykład gdy pracownicy pracują zdalnie (np. z domu) lub podróżują w celach służbowych, możliwe jest monitorowanie czynności poza fizycznym środowiskiem pracy oraz może ono obejmować monitorowanie jednostki w kontekście prywatnym.

W związku z tym, o ile takie technologie mogą być pomocne w wykrywaniu utraty własności intelektualnej i materialnej przedsiębiorstwa lub zapobieganiu takiej utracie, w zwiększaniu wydajności pracowników i ochronie danych osobowych, za które odpowiada administrator danych, stwarzają one również poważne zagrożenia dla ochrony prywatności i danych. W rezultacie konieczna jest nowa ocena równowagi między prawnie uzasadnionym interesem pracodawcy polegającym na ochronie jego działalności a uzasadnionymi oczekiwaniami dotyczącymi ochrony prywatności osób, których dane dotyczą: tj. pracowników.

Chociaż niniejsza opinia będzie się koncentrowała na nowych technologiach informacyjnych poprzez ocenę dziewięciu różnych scenariuszy, w których można je zastosować, znajdzie się w niej również zwięzły przegląd bardziej tradycyjnych metod przetwarzania danych w miejscu pracy, w którym zagrożenia są spotęgowane w związku z postępem technologicznym.

Ilekroć w niniejszej opinii występuje termin „pracownik", Grupa Robocza Art. 29 nie zamierza ograniczać zakresu tego terminu jedynie do osób zatrudnionych na podstawie umowy o pracę uznanej za taką na mocy obowiązującego prawa pracy. W ostatnich dziesięcioleciach coraz powszechniejsze stały się nowe modele biznesowe obsługiwane przez różne stosunki pracy, w szczególności praca na podstawie umowy-zlecenia. Niniejsza opinia ma objąć wszystkie sytuacje, w których istnieje stosunek pracy, niezależnie od tego, czy opiera się on na umowie o pracę.

Należy stwierdzić, że pracownicy rzadko mogą dobrowolnie udzielić zgody, odmówić zgody lub cofnąć zgodę, z uwagi na zależność wynikającą ze stosunku pracy między pracodawcą a pracownikiem. Poza wyjątkowymi sytuacjami pracodawcy będą musieli polegać na innej podstawie prawnej niż zgoda, takiej jak konieczność przetwarzania danych ze względu na prawnie uzasadniony interes. Prawnie uzasadniony interes sam w sobie nie wystarcza jednak, aby przetwarzanie było nadrzędne wobec praw i wolności pracowników.

Niezależnie od podstawy prawnej takiego przetwarzania przed jego rozpoczęciem należy przeprowadzić analizę proporcjonalności, aby ustalić, czy przetwarzanie jest konieczne do osiągnięcia prawnie uzasadnionego celu, oraz rozważyć środki, jakie należy wdrożyć, aby zapewnić ograniczenie naruszeń praw do życia prywatnego i tajemnicy komunikacji do minimum. Może to stanowić część oceny skutków dla ochrony danych.

3. Ramy prawne

Chociaż poniższą analizę przeprowadzono głównie w odniesieniu do obecnych ram prawnych wynikających z dyrektywy 95/46/WE (dyrektywa o ochronie danych)[3], w niniejszej opinii przedstawione zostaną również obowiązki wynikające z rozporządzenia 2016/679 (ogólnego rozporządzenia o ochronie danych)[4], które weszło już w życie i zacznie mieć zastosowanie od dnia 25 maja 2018 r.

Jeżeli chodzi o proponowane rozporządzenie w sprawie prywatności i łączności elektronicznej[5], Grupa Robocza wzywa europejskich prawodawców do stworzenia szczególnego wyjątku w odniesieniu do ingerencji w urządzenia wydawane pracownikom[6]. Proponowane rozporządzenie nie zawiera odpowiedniego wyjątku od ogólnego zakazu ingerencji, a prawodawcy zazwyczaj nie mogą udzielić ważnej zgody na przetwarzanie danych osobowych swoich pracowników.

3.1 Dyrektywa 95/46/WE – dyrektywa o ochronie danych

W opinii 08/2001 Grupa Robocza Art. 29 uprzednio wskazała, że pracodawcy uwzględniają podstawowe zasady ochrony danych określone w dyrektywie o ochronie danych podczas przetwarzania danych osobowych w związku z zatrudnieniem. Rozwój nowych technologii i nowych metod przetwarzania w tym kontekście nie zmienił tej sytuacji – można stwierdzić, że zmiany te sprawiły, że *ważniejsze* jest, aby pracodawcy uwzględniali te zasady. W tym kontekście pracodawcy powinni:

- zapewnić, aby dane przetwarzano do określonych i prawnie uzasadnionych celów, które są proporcjonalne i niezbędne;
- uwzględniać zasadę ograniczenia celu, upewniając się jednocześnie, że dane są prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do prawnie uzasadnionego celu;
- stosować zasadę proporcjonalności i pomocniczości niezależnie od obowiązującej podstawy prawnej;
- jasno informować pracowników o wykorzystaniu i celach technologii monitorowania;
- umożliwiać osobom, których dane dotyczą, korzystanie z przysługujących im praw, w tym prawa dostępu i, w stosownych przypadkach, prawa do sprostowania, usunięcia lub zablokowania danych osobowych;
- aktualizować dane i nie przechowywać ich dłużej niż to konieczne; oraz

[3] 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, Dz.U. L 281 z 23.11.1995, s. 31-50, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:31995L0046

[4] Rozporządzenie Parlamentu Europejskiego i Rady 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. L 119 z 4.5.2016, s. 1-88,* http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679

[5] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE, 2017/0003 (COD), http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

[6] Zob. *opinia 01/2017 Grupy Roboczej Art. 29 na temat proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej*, WP 247, z dnia 4 kwietnia 2017 r., s. 29; http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

- zastosować wszystkie środki konieczne do ochrony danych przed nieuprawnionym wykorzystaniem i zapewnić, aby pracownicy byli wystarczająco świadomi obowiązków ochrony danych.

Bez powtarzania wcześniej udzielonych porad Grupa Robocza Art. 29 pragnie podkreślić trzy zasady, mianowicie: podstawa prawna, przejrzystość i zautomatyzowane decyzje.

3.1.1 *PODSTAWA PRAWNA (ART. 7)*

Podczas przetwarzania danych osobowych w związku z zatrudnieniem musi być spełnione co najmniej jedno z kryteriów określonych w art. 7. Jeżeli rodzaje przetwarzanych danych osobowych obejmują szczególne kategorie (przedstawione w art. 8), przetwarzanie jest zabronione, chyba że ma zastosowanie wyjątek[7,8]. Nawet jeżeli pracodawca może powołać się na jeden z tych wyjątków, podstawa prawna określona w art. 7 nadal jest wymagana, aby przetwarzanie było zgodne z prawem.

Podsumowując, pracodawcy muszą zatem wziąć pod uwagę następujące kwestie:

- w odniesieniu do większości przypadków przetwarzania danych w miejscu pracy **podstawą prawną nie może i nie powinna być zgoda pracowników** (art. 7 lit. a)) ze względu na charakter stosunków między pracodawcą i pracownikiem;
- przetwarzanie może być konieczne do **realizacji umowy** (art. 7 lit. b), w przypadkach gdy pracodawca musi przetwarzać dane osobowe pracownika w celu wywiązania się z takich zobowiązań;
- często zdarza się, że **prawo pracy może nakładać obowiązki prawne** (art. 7 lit. c)), **które wymagają przetwarzania danych osobowych**; w takich przypadkach należy wyraźnie i w sposób wyczerpujący poinformować pracownika o takim przetwarzaniu (chyba że ma zastosowanie wyjątek);
- jeżeli pracodawca próbuje powoływać się na **uzasadniony interes** (art. 7 lit. f)), cel przetwarzania danych musi być zgodny z prawem; wybrana metoda lub określona technologia musi być konieczna, proporcjonalna i wdrażana w możliwie najmniej inwazyjny sposób, a także musi umożliwiać pracodawcy wykazanie, że **wprowadzono odpowiednie środki** w celu zapewnienia równowagi z podstawowymi prawami i wolnościami pracowników[9];
- operacje przetwarzania muszą być również zgodne z **wymogami przejrzystości** (art. 10 i 11), a pracownicy powinni zostać wyraźnie i dokładnie poinformowani

[7] Zgodnie z częścią 8 opinii 08/2001; np. art. 8 ust. 2 lit. b) zawiera wyjątek, zgodnie z którym przetwarzanie danych jest konieczne do wypełniania obowiązków i szczególnych uprawnień administratora danych w dziedzinie prawa pracy, o ile jest to dozwolone przez prawo krajowe przewidujące odpowiednie środki zabezpieczające.

[8] Należy zauważyć, że w niektórych państwach istnieją specjalne środki, których pracodawcy muszą przestrzegać, aby chronić życie prywatne swoich pracowników. Portugalia jest przykładem państwa, w którym istnieją specjalne środki, a podobne środki mogą być stosowane również w kilku innych państwach członkowskich. Z powyższych względów wnioski zawarte w pkt 5.6 i przykłady przedstawione w pkt 5.1 i 5.7.1 niniejszej opinii nie mają zatem zastosowania do Portugalii.

[9] *Opinia 06/2014 Grupy Roboczej Art. 29 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE*, WP 217, przyjęta dnia 9 kwietnia 2014 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_pl.pdf

o przetwarzaniu ich danych osobowych[10], w tym o istnieniu technologii monitorowania; oraz
- należy przyjąć **odpowiednie środki techniczne i organizacyjne** mające zapewnić bezpieczeństwo przetwarzania (art. 17).

Najistotniejsze kryteria na mocy art. 7 wyszczególniono poniżej.

- **Zgoda (art. 7 lit. a))**

Zgodnie z dyrektywą o ochronie danych „zgoda" oznacza konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych. Aby zgoda była ważna, musi również istnieć możliwość jej odwołania.

W swojej opinii 8/2001 Grupa Robocza Art. 29 już wcześniej zaznaczyła, że jeżeli pracodawca musi przetwarzać dane osobowe swoich pracowników, błędem jest założenie na wstępie, że przetwarzanie można usankcjonować, uzyskując zgodę pracowników. W przypadkach gdy pracodawca twierdzi, że zgoda jest wymagana, a niewyrażenie zgody przez pracownika prowadzi do rzeczywistej lub potencjalnej szkody (która może być wysoce prawdopodobna w związku z zatrudnieniem, zwłaszcza gdy dotyczy to pracodawcy śledzącego zachowanie pracownika), zgoda taka nie jest ważna, ponieważ nie jest i nie może być dobrowolnie udzielona. W odniesieniu do większości przypadków przetwarzania danych pracowników podstawą prawną takiego przetwarzania nie może i nie powinna być zgoda pracowników, a zatem konieczna jest inna podstawa prawna.

Ponadto nawet w przypadkach, w których zgodę można uznać za ważną podstawę prawną takiego przetwarzania (tj. jeżeli można bez wątpienia stwierdzić, że zgoda jest dobrowolna), musi ona stanowić konkretne i świadome wskazanie przez pracownika. Domyślne ustawienia urządzeń lub zainstalowanie oprogramowania, które ułatwia elektroniczne przetwarzanie danych osobowych, nie może kwalifikować się jako zgoda wyrażona przez pracowników, ponieważ zgoda wymaga aktywnego oświadczenia woli. Braku działania (tj. braku zmian w ustawieniach domyślnych) nie można na ogół uznać za wyraźną zgodę na takie przetwarzanie[11].

- **Realizacja umowy (art. 7 lit. b))**

Stosunki pracy często opierają się na umowie o pracę zawartej między pracodawcą a pracownikiem. Przy wypełnianiu obowiązków wynikających z tej umowy, takich jak wypłacanie pracownikowi wynagrodzenia, pracodawca jest zobowiązany do przetworzenia pewnych danych osobowych.

- **Zobowiązania prawne (art. 7 lit. c))**

Często zdarza się, że prawo pracy nakłada na pracodawcę obowiązki prawne, które wymagają przetwarzania danych osobowych (np. do celów obliczenia wysokości podatku

[10] Zgodnie z art. 11 ust. 2 dyrektywy o ochronie danych administrator danych jest zwolniony z obowiązku przekazywania informacji osobie, której dane dotyczą, w przypadkach, w których zapis lub gromadzenie danych jest wyraźnie określone w prawie.

[11] Zob. także opinia *15/2011 Grupy Roboczej Art. 29 w sprawie definicji zgody*, WP 187, z dnia 13 lipca 2011 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_pl.pdf, s. 24.

i zarządzania wynagrodzeniami). W takich przypadkach prawo takie stanowi podstawę prawną przetwarzania danych.

- **Uzasadniony interes (art. 7 lit. f))**

Jeżeli pracodawca chce powołać się na podstawę prawną wskazaną w art. 7 lit. f) dyrektywy o ochronie danych, cel przetwarzania danych musi być uzasadniony, a wybrana metoda lub określona technologia, za pomocą której prowadzone jest przetwarzanie, musi być konieczna z punktu widzenia uzasadnionego interesu pracodawcy. Przetwarzanie danych musi być również proporcjonalne do potrzeb biznesowych, tj. celu, który ma zostać osiągnięty. Przetwarzanie danych w miejscu pracy należy prowadzić w sposób jak najmniej inwazyjny i tak, by było ukierunkowane na konkretny obszar ryzyka. Ponadto, jeżeli pracodawca powołuje się na art. 7 lit. f), pracownik zachowuje prawo sprzeciwu wobec przetwarzania z ważnych i uzasadnionych przyczyn zgodnie z art. 14.

Aby móc powołać się na art. 7 lit. f) jako podstawę prawną przetwarzania, konieczne jest wprowadzenie szczególnych środków łagodzących w celu zapewnienia właściwej równowagi między uzasadnionym interesem pracodawcy a podstawowymi prawami i wolnościami pracowników[12]. Środki takie, w zależności od formy monitorowania, powinny obejmować ograniczenia w monitorowaniu, aby zagwarantować nienaruszalność prywatności pracownika. Tego rodzaju ograniczenia mogą być następujące:

- geograficzne (np. monitorowanie prowadzone jest tylko w określonych miejscach; należy zakazać monitorowania obszarów wrażliwych takich jak miejsca kultu religijnego oraz np. strefy sanitarne i pomieszczenia socjalne);
- ukierunkowane na dane (np. nie należy monitorować osobistych plików elektronicznych i komunikacji); oraz
- czasowe (np. kontrola wyrywkowa zamiast ciągłego monitorowania).

3.1.2 *PRZEJRZYSTOŚĆ (ART. 10 I 11)*

Wymogi dotyczące przejrzystości określone w art. 10 i 11 mają zastosowanie do przetwarzania danych w miejscu pracy; pracownicy muszą być informowani o istnieniu technologii monitorowania, o celach przetwarzania danych osobowych oraz o wszelkich kwestiach niezbędnych do zagwarantowania rzetelnego przetwarzania.

Wraz z wprowadzeniem nowych technologii potrzeba utrzymania przejrzystości staje się jeszcze bardziej widoczna, ponieważ technologie te umożliwiają gromadzenie i dalsze przetwarzanie dużych ilości danych osobowych w sposób ukryty.

3.1.3 *ZAUTOMATYZOWANE DECYZJE (ART. 15)*

[12] Aby zapoznać się z przykładem równowagi, którą należy osiągnąć, zob. wyrok Europejskiego Trybunału Praw Człowieka z 2010 r. w sprawie *Köpke przeciwko Niemcom*, ECHR 1725, (http://www.bailii.org/eu/cases/ECHR/2010/1725.html), w której pracownik został zwolniony w wyniku niejawnego nadzoru wideo prowadzonego przez pracodawcę i prywatną agencję detektywistyczną. Chociaż w tym przypadku Trybunał stwierdził, że władze krajowe zachowały właściwą równowagę między uzasadnionym interesem pracodawcy (w zakresie ochrony praw własności), prawem pracownika do poszanowania życia prywatnego a interesem publicznym związanym z wymierzeniem sprawiedliwości, zauważył również, że różne interesy mogą zyskać w przyszłości różne znaczenie w wyniku postępu technologicznego.

Art. 15 dyrektywy o ochronie danych przyznaje także osobom, których dane dotyczą, prawo do nieobjęcia ich decyzją opartą wyłącznie na zautomatyzowanym przetwarzaniu, w przypadku gdy taka decyzja wywołuje skutki prawne, które ich dotyczą lub mają na nie istotny wpływ, oraz oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących ich aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, chyba że decyzja jest konieczna w celu zawarcia lub realizacji umowy, jest dozwolona przez prawo UE lub prawo państw członkowskich bądź opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3.2 Rozporządzenie 2016/679 – ogólne rozporządzenie o ochronie danych

Ogólne rozporządzenie o ochronie danych zawiera i zaostrza wymogi określone w dyrektywie o ochronie danych. Wprowadzono w nim również nowe obowiązki dla wszystkich administratorów danych, w tym pracodawców.

3.2.1 *UWZGLĘDNIANIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA*

Art. 25 ogólnego rozporządzenia o ochronie danych wymaga, aby administratorzy danych uwzględniali ochronę danych w fazie projektowania oraz domyślną ochronę danych. Na przykład: w przypadku gdy pracodawca wydaje pracownikom urządzenia, należy wybrać rozwiązania najbardziej sprzyjające zachowaniu prywatności, jeżeli wykorzystywane są technologie śledzące. Należy również wziąć pod uwagę minimalizację danych.

3.2.2 *OCENY SKUTKÓW DLA OCHRONY DANYCH*

W art. 35 ogólnego rozporządzenia o ochronie danych określono wymogi dotyczące prowadzania oceny skutków dla ochrony danych przez administratora danych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przykładem jest systematyczna, kompleksowa ocena czynników osobowych odnoszących się do osób fizycznych, która opiera się 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.

Jeżeli w ocenie skutków dla ochrony danych zostanie wykazane, że administrator danych nie jest w stanie w wystarczającym stopniu wyeliminować zidentyfikowanego ryzyka, tj. ryzyko szczątkowe pozostaje wysokie, wówczas przed rozpoczęciem przetwarzania administrator danych musi skonsultować się z organem nadzorczym (art. 36 ust. 1) zgodnie z wytycznymi Grupy Roboczej Art. 29 dotyczącymi oceny skutków dla ochrony danych[13].

3.2.2 „Przetwarzanie w kontekście zatrudnienia”

Art. 88 ogólnego rozporządzenia o ochronie danych stanowi, że 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 przepisy te mogą być przewidziane do celów:

[13] *Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz ustalenia, czy przetwarzanie może powodować „wysokie ryzyko” dla celów rozporządzenia 2016/679*, WP 248, z dnia 4 kwietnia 2017 r., http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, s. 18.

- 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;
- wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem (na zasadzie indywidualnej); oraz
- zakończenia stosunku pracy.

Zgodnie z art. 88 ust. 2 przepisy te powinny 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.

W niniejszej opinii Grupa Robocza przedstawiła wytyczne dotyczące uzasadnionego wykorzystania nowej technologii w różnych sytuacjach, wyszczególniając odpowiednie i szczegółowe środki zapewniające pracownikom poszanowanie ich godności, prawnie uzasadnionych interesów i praw podstawowych.

4. Zagrożenia

Nowoczesne technologie umożliwiają śledzenie pracowników w miejscu pracy i w ich domach, za pomocą wielu różnych urządzeń takich jak smartfony, komputery osobiste, tablety, pojazdy i urządzenia do noszenia na ciele. Jeżeli nie istnieją żadne ograniczenia dotyczące przetwarzania oraz jeżeli nie jest ono prowadzone jawnie, istnieje duże ryzyko, że uzasadniony interes pracodawców w zakresie poprawy efektywności i ochrony majątku przedsiębiorstwa przerodzi się w nieuzasadnione i inwazyjne monitorowanie.

Technologie monitorowania komunikacji mogą mieć również negatywny wpływ na prawa podstawowe pracowników do organizowania się, organizowania spotkań pracowniczych oraz do komunikowania się w sposób poufny (w tym na prawo do uzyskiwania informacji). Monitorowanie komunikacji i zachowań będzie wywierało presję na pracowników, aby przestrzegali przepisów w celu uniemożliwienia wykrycia zachowań uznawanych za anomalie, podobnie jak intensywne stosowanie CCTV wpłynęło na zachowanie obywateli w przestrzeniach publicznych. Ponadto ze względu na możliwości takich technologii pracownicy mogą nie być świadomi, jakie dane osobowe są przetwarzane i do jakich celów, przy czym możliwe jest również, że nie zdają sobie sprawy z istnienia samej technologii monitorowania.

Monitorowanie internetowe różni się również od innych bardziej widocznych narzędzi obserwacji i monitorowania takich jak CCTV w tym sensie, że może odbywać się w sposób ukryty. W przypadku braku łatwo zrozumiałej i łatwo dostępnej polityki monitorowania w miejscu pracy pracownicy mogą nie zdawać sobie sprawy z istnienia i skutków stosowania

monitoringu, a w związku z tym nie są w stanie korzystać ze swoich praw. Kolejne zagrożenie wynika z „gromadzenia nadmiernej ilości" danych w takich systemach, np. w systemach gromadzących dane dotyczące lokalizacji za pośrednictwem WiFi.

Zwiększenie ilości danych generowanych w środowisku pracy, w połączeniu z nowymi technikami analizowania i zestawiania danych, może także stwarzać ryzyko dalszego przetwarzania niezgodnego z przepisami. Przykładem niezgodnego z prawem dalszego przetwarzania danych jest wykorzystywanie systemów, które zgodnie z prawem zainstalowano w celu ochrony własności, do monitorowania dostępności i wyników pracowników oraz ich przyjaznego podejścia do klientów. Inne przykłady obejmują wykorzystanie danych zgromadzonych za pośrednictwem systemu CCTV do regularnego monitorowania zachowania i wyników pracowników lub wykorzystanie danych systemu geolokalizacyjnego (takiego jak np. śledzenie za pomocą WiFi lub Bluetooth) do ciągłego śledzenia ruchów i zachowania pracownika.

W rezultacie takie śledzenie może naruszać prawa pracowników do prywatności, niezależnie od tego, czy monitorowanie odbywa się systematycznie czy sporadycznie. Ryzyko nie ogranicza się do analizy treści komunikacji. Analiza metadanych dotyczących danej osoby może zatem pozwolić na równie szczegółowe i naruszające prywatność monitorowanie życia i wzorców zachowań jednostek.

Szerokie wykorzystanie technologii monitorowania może również zmniejszyć gotowość (i liczbę kanałów służących do tego celu) pracowników do informowania pracodawców o nieprawidłowościach lub nielegalnych działaniach przełożonych lub innych pracowników, które mogą zaszkodzić działalności (zwłaszcza danym klientów) lub miejscu pracy. Często konieczne jest zapewnienie anonimowości, aby dany pracownik podjął działania i zgłosił takie sytuacje. Monitorowanie naruszające prawa pracowników do prywatności może utrudniać konieczną komunikację z odpowiednimi inspektorami. W takim przypadku ustanowione środki stosowane przez wewnętrznych demaskatorów mogą stracić na skuteczności[14].

5. Scenariusze

Niniejsza sekcja dotyczy szeregu scenariuszy przetwarzania danych w miejscu pracy, w których nowe technologie lub zmiany istniejących technologii zagrażają lub mogą zagrozić prywatności pracowników. We wszystkich takich przypadkach pracodawcy powinni rozważyć, czy:

- czynność przetwarzania jest konieczna, a jeżeli tak, jaka podstawa prawna ma zastosowanie;
- proponowane przetwarzanie danych osobowych jest sprawiedliwe wobec pracowników;
- czynność przetwarzania jest proporcjonalna do zgłaszanych obaw; oraz
- czy czynność przetwarzania jest przejrzysta.

[14] Zob. np. *opinia 1/2006 Grupy Roboczej Art. 29 w sprawie zastosowania unijnych zasad ochrony danych do wewnętrznych systemów informowania o nieprawidłowościach w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych*, WP 117, z dnia 1 lutego 2006 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_pl.pdf

5.1 Operacja przetwarzania w trakcie procesu rekrutacji

Korzystanie z mediów społecznościowych jest szeroko rozpowszechnione i stosunkowo popularnym zjawiskiem jest udostępnianie profili użytkowników w zależności od ustawień wybranych przez właściciela konta. W rezultacie pracodawcy mogą sądzić, że kontrola profili społecznościowych potencjalnych kandydatów jest uzasadniona w trakcie procesu rekrutacji. Może to również dotyczyć innych dostępnych publicznie informacji o potencjalnym pracowniku.

Pracodawcy nie powinni jednak zakładać, że tylko dlatego, iż profil społecznościowy danej osoby jest publicznie dostępny, mogą przetwarzać jej dane do własnych celów. Takie przetwarzanie wymaga podstawy prawnej tj. uzasadnionego interesu. W tym kontekście pracodawca powinien – przed przejrzeniem profilu społecznościowego – rozważyć, czy profil społecznościowy osoby ubiegającej się o pracę jest powiązany z celami biznesowymi czy prywatnymi, ponieważ może to stanowić ważne wskazanie w odniesieniu do dopuszczalności prawnej kontroli danych. Ponadto pracodawcy mogą gromadzić i przetwarzać dane osobowe osób ubiegających się o pracę w takim zakresie, w jakim gromadzenie tych danych jest konieczne i istotne dla wykonywania pracy, o którą się ubiegają.

Dane przekazane w związku z ubieganiem się o pracę powinny zwykle być niszczone po tym, gdy stanie się jasne, że oferta zatrudnienia nie zostanie przedstawiona, lub jeżeli osoba ubiegająca się o zatrudnienie jej nie zaakceptuje[15]. Dana osoba musi również zostać właściwie poinformowana o takim przetwarzaniu zanim weźmie udział w procesie rekrutacji.

Nie istnieją żadne podstawy prawne, zgodnie z którymi pracodawca mógłby wymagać od potencjalnego pracownika przyjęcia go „do grona znajomych" lub w inny sposób udostępnienia zawartości profilu.

Przykład:

Podczas rekrutacji nowych pracowników pracodawca sprawdza profile kandydatów na różnych portalach społecznościowych i dołącza informacje z tych portali (oraz wszelkie inne informacje dostępne w internecie) do procedury sprawdzającej.

Jedynie w przypadku gdy na potrzeby zatrudnienia konieczne jest dokonanie przeglądu informacji o kandydacie znajdujących się w mediach społecznościowych, np. aby móc ocenić konkretne zagrożenia związane z kandydatami na dane stanowisko, a kandydaci zostaną odpowiednio poinformowani (np. w tekście ogłoszenia o pracę), pracodawca może mieć podstawę prawną na mocy art. 7 lit. f) do przeprowadzenia przeglądu publicznie dostępnych informacji o kandydatach.

[15] Zob. także Rada Europy, *zalecenie CM/REC (2015) 5 Komitetu Ministrów dla państw członkowskich na temat ochrony danych osobowych wykorzystywanych dla celów zatrudnienia*, pkt 13.2 (1 kwietnia 2015 r., https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). W przypadkach gdy pracodawca chce zatrzymać dane na wypadek wystąpienia kolejnej możliwości zatrudnienia, osoba, której dane dotyczą, powinna zostać odpowiednio poinformowana i powinna mieć możliwość wyrażenia sprzeciwu wobec dalszego przetwarzania danych, a wówczas takie dane należy usunąć (Id.).

5.2 Operacje przetwarzania wynikające z badania przeprowadzonego pod kątem zatrudnienia

Dzięki istnieniu profili w mediach społecznościowych i rozwojowi nowych technologii analitycznych pracodawcy dysponują możliwościami technicznymi (lub mogą je uzyskać), które pozwalają im na stałe monitorowanie pracowników poprzez gromadzenie informacji na temat ich znajomych, opinii, przekonań, zainteresowań, zwyczajów, miejsc pobytu, postaw i zachowań, a zatem pozyskiwanie danych, w tym danych wrażliwych, na temat życia prywatnego i rodzinnego pracownika.

Badanie profili pracowników w mediach społecznościowych nie powinno stanowić ogólnej praktyki.

Ponadto pracodawcy powinni powstrzymać się od wymagania od pracownika lub osoby ubiegającej się o zatrudnienie dostępu do informacji, którymi dzieli się z innymi osobami za pośrednictwem sieci społecznościowych.

Przykład:
Pracodawca monitoruje na portalu LinkedIn profile byłych pracowników, którzy objęci są klauzulą o zakazie konkurencji. Celem takiego działania jest monitorowanie przestrzegania takich klauzul. Monitorowanie ogranicza się do byłych pracowników.

Dopóki pracodawca może udowodnić, że takie monitorowanie jest konieczne do ochrony jego uzasadnionych interesów, nie ma innych, mniej inwazyjnych środków oraz że byli pracownicy zostali odpowiednio poinformowani o zakresie regularnego obserwowania ich publicznych informacji, pracodawca może powołać się na podstawę prawną w postaci art. 7 lit. f) dyrektywy o ochronie danych.

Ponadto pracownicy nie powinni być zobowiązani do korzystania z profili w mediach społecznościowych zapewnianych przez ich pracodawcę. Nawet jeżeli jest to wyraźnie przewidziane w świetle ich zadań (np. rzecznik organizacji), umowa o pracę powinna zawierać warunki gwarantujące pracownikowi prawo do zachowania niepublicznego profilu „niezwiązanego z pracą", z którego mogą korzystać zamiast „oficjalnego" profilu związanego z pracodawcą.

5.3 Operacje przetwarzania wynikające z monitorowania korzystania z ICT w miejscu pracy

Tradycyjnie za główne zagrożenie dla prywatności pracowników uznano monitorowanie treści komunikacji elektronicznej w miejscu pracy (np. połączeń telefonicznych, przeglądanych zasobów internetowych, wiadomości e-mail, komunikatów natychmiastowych, połączeń za pośrednictwem telefonii internetowej itd.) W swoim dokumencie roboczym z 2001 r. w sprawie nadzoru komunikacji elektronicznej w miejscu pracy Grupa Robocza Art. 29 przedstawiła szereg wniosków dotyczących monitorowania wiadomości e-mail i korzystania z internetu. Chociaż wnioski te są nadal aktualne, należy wziąć pod uwagę postęp technologiczny, który umożliwił wprowadzenie nowych, potencjalnie bardziej inwazyjnych i wszechobecnych sposobów monitorowania. Postęp ten obejmuje m.in.:

- narzędzia ochrony przed utratą danych, które służą do monitorowania komunikacji wychodzącej w celu wykrycia potencjalnych naruszeń ochrony danych;
- zapory sieciowe następnej generacji i systemy zunifikowanego zarządzania zagrożeniami (ang. *Unified Threat Management*), które mogą zapewnić różnorodne technologie monitorowania, w tym głęboką inspekcję pakietów (ang. *Deep Packet Inspection*), przechwytywanie TLS, filtrowanie stron internetowych, filtrowanie treści, raportowanie w ramach urządzenia, informacje o tożsamości użytkownika i (jak opisano powyżej) narzędzie ochrony przed utratą danych. Takie technologie mogą być również wprowadzane pojedynczo, w zależności od pracodawcy;
- aplikacje i środki bezpieczeństwa, które obejmują rejestrowanie dostępu pracowników do systemów pracodawcy;
- technologię eDiscovery, która odnosi się do wszystkich procesów obejmujących wyszukiwanie danych w celu wykorzystania ich w charakterze dowodu;
- śledzenie aplikacji i wykorzystania urządzenia za pomocą niewidocznego oprogramowania na pulpicie lub w chmurze;
- korzystanie w miejscu pracy z aplikacji biurowych dostarczanych jako usługa w chmurze, która teoretycznie umożliwia bardzo szczegółowe rejestrowanie działań pracowników;
- monitorowanie urządzeń osobistych (np. komputerów osobistych, telefonów komórkowych, tabletów), które pracownicy przynoszą do pracy zgodnie z określoną polityką użytkowania, taką jak zasada „przynieś własny sprzęt" (ang. *Bring-Your-Own-Device*), oraz technologię zarządzania urządzeniami mobilnymi, która umożliwia dystrybucję aplikacji, danych i ustawień konfiguracyjnych oraz poprawek dla urządzeń mobilnych; oraz
- korzystanie z urządzeń do noszenia na ciele (np. urządzeń do dbania o zdrowie i sprawność fizyczną).

Możliwe jest, że pracodawca wdroży rozwiązanie monitorujące typu „wszystko w jednym", takie jak zestaw pakietów bezpieczeństwa, które umożliwiają monitorowanie wszystkich sposobów wykorzystania ICT w miejscu pracy, a nie tylko monitorowanie wiadomości e-mail lub aktywności w internecie, jak dawniej. Wnioski przyjęte w WP 55 miałyby zastosowanie do każdego systemu, który umożliwia prowadzenie takiego monitorowania[16].

Przykład:

Pracodawca zamierza wprowadzić urządzenie kontrolne TLS służące do odszyfrowywania i kontrolowania bezpiecznego ruchu w celu wykrywania wszelkich nieprawidłowości. Urządzenie jest również w stanie rejestrować i analizować całą aktywność pracownika w internecie z wykorzystaniem sieci organizacji.

Coraz częściej stosuje się szyfrowane protokoły komunikacyjne w celu ochrony przepływów danych (w tym danych osobowych) w internecie przed przechwyceniem. Rozwiązanie takie może jednak również powodować problemy, ponieważ szyfrowanie uniemożliwia

[16] Zob. także wyrok Europejskiego Trybunału Praw Człowieka z 2007 r., *Copland przeciwko Zjednoczonemu Królestwu*, 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, ECHR 253 (http://www.bailii.org/eu/cases/ECHR/2007/253.html), w którym Trybunał orzekł, że wiadomości e-mail wysłane z lokalu przedsiębiorstwa i informacje pochodzące z monitorowania aktywności w internecie mogą stanowić część życia prywatnego i korespondencji pracownika oraz że gromadzenie i przechowywanie tych informacji bez wiedzy pracownika oznaczałoby ingerencję w prawa pracownika, mimo że Trybunał nie orzekł, iż takie monitorowanie nigdy nie byłoby konieczne w demokratycznym społeczeństwie.

monitorowanie danych przychodzących i wychodzących. Urządzenie kontrolne TLS odszyfrowuje strumień danych, analizuje ich treść do celów bezpieczeństwa, a następnie ponownie zaszyfrowuje strumień.

W tym przypadku pracodawca powołuje się na uzasadniony interes – konieczność ochrony sieci oraz danych osobowych pracowników i klientów, przechowywanych w ramach tej sieci, przed nieuprawnionym dostępem lub wyciekiem danych. Monitorowanie całej aktywności pracowników w internecie stanowi jednak nieproporcjonalną reakcję naruszającą prawo do poufności komunikacji. Pracodawca powinien w pierwszej kolejności rozważyć możliwość zastosowania innych, mniej inwazyjnych metod ochrony poufności danych klientów i bezpieczeństwa sieci.

Ponieważ w niektórych przypadkach przechwytywanie danych przekazywanych za pośrednictwem protokołu TLS może okazać się bezwzględnie konieczne, urządzenie należy skonfigurować w taki sposób, aby uniemożliwić ciągłe rejestrowanie działalności pracownika, na przykład poprzez blokowanie podejrzanych danych przychodzących lub wychodzących i przekierowywanie użytkownika do portalu informacyjnego, z poziomu którego może on zwrócić się o dokonanie przeglądu takiej zautomatyzowanej decyzji. Jeżeli mimo to zachodziłaby bezwzględna konieczność zastosowania pewnej formy ogólnego rejestrowania, urządzenie można skonfigurować również w taki sposób, aby nie gromadziło danych dziennika, jeżeli urządzenie nie zasygnalizowało wystąpienia określonego zdarzenia, co pozwala ograniczyć gromadzone informacje do minimum.

Jako dobrą praktykę zaleca się, aby pracodawca zaoferował pracownikom alternatywny, niemonitorowany dostęp. Można to osiągnąć, oferując pracownikom możliwość skorzystania z bezpłatnej sieci Wi-Fi lub z samodzielnych urządzeń lub terminali (wyposażonych w odpowiednie zabezpieczenia gwarantujące poufność komunikacji), za pomocą których pracownicy będą mogli korzystać z przysługującego im prawa do wykorzystywania urządzeń w miejscu pracy do niektórych zastosowań prywatnych[17]. Ponadto pracodawcy powinni pamiętać o tym, że przechwytywanie niektórych rodzajów danych zaburza właściwą równowagę między ich uzasadnionymi interesami a prywatnością pracownika – dotyczy to na przykład prywatnych wiadomości e-mail, a także odwiedzin na portalach bankowości elektronicznej i na stronach internetowych poświęconych zdrowiu; dlatego też należy odpowiednio skonfigurować urządzenie, tak aby nie przechwytywało ono danych w przypadkach, w których takie przechwytywanie byłoby nieuzasadnione w świetle zasady proporcjonalności. Pracownikom należy udzielić szczegółowych informacji na temat rodzajów komunikacji, które są monitorowane przez urządzenie.

Należy opracować politykę określającą, kiedy można uzyskać dostęp do podejrzanych danych dziennika i kto jest uprawniony do uzyskania takiego dostępu, oraz w przystępny i trwały sposób udostępnić ją wszystkim pracownikom jako dodatkowe wytyczne w kwestii dozwolonych i niedozwolonych sposobów korzystania z sieci i urządzeń. Pozwoli to pracownikom tak zmodyfikować swoje zachowanie, aby uniknąć bycia monitorowanym

[17] Zob. sprawa z 1997 r. *Halford przeciwko Zjednoczonemu Królestwu*, ECHR 32 (http://www.bailii.org/eu/cases/ECHR/1997/32.html), w której Trybunał stwierdził, że „wykonywanie połączeń telefonicznych z lokalu przedsiębiorstwa i z domu można uznać za objęte zakresem pojęć »życia prywatnego« i »korespondencji« w rozumieniu art. 8 ust. 1 [konwencji]"; oraz sprawa z 2016 r., Barbulescu przeciwko Rumunii, ECHR 61 (http://www.bailii.org/eu/cases/ECHR/2016/61.html) dotycząca korzystania ze służbowego konta w komunikatorze internetowym w celach prywatnych, w której Trybunał uznał, że monitorowanie takiego konta przez pracodawcę było ograniczone i proporcjonalne; sędzia Pinto de Albuquerque zgłosił zdanie odrębne, opowiadając się za koniecznością znalezienia właściwej równowagi w tej kwestii.

w trakcie uprawnionego korzystania z aplikacji IT w miejscu pracy do celów prywatnych. Dobrą praktyką byłoby poddawanie takiej polityki ocenie przynajmniej raz do roku, aby ustalić, czy wybrana metoda monitorowania przynosi zamierzone rezultaty i czy te same cele można byłoby osiągnąć za pomocą innych, mniej inwazyjnych narzędzi lub środków.

Niezależnie od danej technologii lub oferowanych przez nią funkcji, na podstawę prawną w postaci art. 7 lit. f) można powołać się wyłącznie wówczas, gdy przetwarzanie danych spełnia określone warunki. Po pierwsze, pracodawcy korzystający z tego rodzaju produktów lub aplikacji muszą wziąć pod uwagę proporcjonalność wdrażanych przez siebie środków, a także to, czy w danej sytuacji można podjąć jakiekolwiek dodatkowe działania, aby ograniczyć lub zmniejszyć skalę i skutki przetwarzania danych. Przykładem dobrej praktyki w tym zakresie jest przeprowadzanie tego rodzaju analizy w ramach oceny skutków dla ochrony danych przed wprowadzeniem jakiejkolwiek technologii monitorowania. Po drugie, niezależnie od polityki ochrony prywatności, pracodawcy muszą wdrożyć politykę akceptowalnych zastosowań, w której określą dopuszczalny sposób korzystania z sieci i ze sprzętu organizacji i precyzyjnie opiszą odbywające się przetwarzanie danych, a ponadto muszą poinformować o takim wdrożeniu.

W niektórych państwach przyjęcie tego rodzaju polityki zgodnie z prawem wymagałoby uzyskania zgody samorządu pracowniczego lub podobnego organu reprezentującego pracowników. W praktyce tego rodzaju politykę często opracowują pracownicy odpowiedzialni za obsługę informatyczną. Ponieważ tego rodzaju polityka koncentruje się głównie na kwestiach związanych z bezpieczeństwem, a nie na uzasadnionych oczekiwaniach dotyczących poszanowania prywatności pracowników, Grupa Robocza Art. 29 zaleca, aby reprezentatywna próba pracowników każdorazowo uczestniczyła w ocenie konieczności monitorowania, a także logiki polityki i jej dostępności.

Przykład:

Pracodawca korzysta z narzędzia ochrony przed utratą danych do automatycznego monitorowania wychodzących wiadomości e-mail, aby zapobiegać nieuprawnionemu przekazywaniu danych zastrzeżonych (np. danych osobowych klientów) niezależnie od tego, czy takie działania są podejmowane umyślnie, czy też nie. Po uznaniu wiadomości e-mail za potencjalne źródło naruszenia ochrony danych przeprowadza się dalsze dochodzenie.

W takim przypadku pracodawca ponownie powołuje się na swój uzasadniony interes związany z koniecznością zapewnienia ochrony danych osobowych klientów i swoich aktywów przed nieuprawnionym dostępem lub wyciekiem danych. Korzystanie z takiego narzędzia ochrony przed utratą danych może jednak wiązać się ze zbędnym przetwarzaniem danych osobowych – na przykład „fałszywie dodatnie" ostrzeżenie może doprowadzić do uzyskania nieuprawnionego dostępu do wiadomości e-mail wysłanych przez pracowników zgodnie z obowiązującymi regułami (które mogą być np. wiadomościami e-mail o charakterze osobistym).

Dlatego też konieczność stosowania narzędzia ochrony przed utratą danych i jego wdrożenia powinna zostać w pełni uzasadniona, aby zapewnić właściwą równowagę między uzasadnionymi interesami pracodawcy a prawem podstawowym pracowników do ochrony ich danych osobowych. Aby pracodawca mógł powołać się na swój uzasadniony interes, powinny zostać wdrożone określone środki ograniczające ryzyko. Na przykład zasady stosowane przez system przy ustalaniu, czy daną wiadomość e-mail można uznać za stwarzającą ryzyko potencjalnego naruszenia ochrony danych, powinny być w pełni przejrzyste dla użytkowników, a w przypadku gdy system uzna, że wysyłana wiadomość e-mail może doprowadzić do naruszenia ochrony danych, nadawca tej wiadomości e-mail powinien zostać powiadomiony o tym fakcie za pomocą komunikatu ostrzegawczego przed wysłaniem wiadomości, aby umożliwić mu rezygnację z jej wysłania.

W niektórych przypadkach pracowników można monitorować nie poprzez wdrażanie określonych technologii, ale po prostu z uwagi na fakt, że korzystają oni z aplikacji internetowych udostępnionych im przez pracodawcę, które przetwarzają dane osobowe. Przykładem takich aplikacji są aplikacje biurowe bazujące na technologii przetwarzania w chmurze (np. edytory dokumentów, kalendarze, portale społecznościowe). Pracownikom należy zapewnić możliwość wyznaczenia określonych przestrzeni prywatnych, do których pracodawca będzie mógł uzyskać dostęp wyłącznie w wyjątkowych okolicznościach. Ma to znaczenie na przykład w przypadku kalendarzy, które często są wykorzystywane również do planowania prywatnych spotkań. Jeżeli pracownik określi dane spotkanie jako „Prywatne" lub zawrze odpowiednią uwagę w samym opisie spotkania, pracodawcy (i inni pracownicy) nie powinni mieć możliwości zapoznania się z opisem spotkania.

W tym kontekście wymóg pomocniczości oznacza niekiedy brak możliwości prowadzenia jakiegokolwiek monitorowania. Dotyczy to na przykład sytuacji, w której niedozwolone metody korzystania z usług łączności można zwalczać, blokując określone strony internetowe. Jeżeli w danym przypadku można zablokować strony internetowe zamiast ciągłego monitorowania całej komunikacji, należy wybrać to rozwiązanie, aby zapewnić zgodność z wymogiem pomocniczości.

Ogólniej rzecz ujmując, działaniom prewencyjnym należy przypisywać znacznie większą wagę niż działaniom mającym na celu wykrycie określonych zachowań – interesy

pracodawcy można chronić skuteczniej, zapobiegając niewłaściwemu korzystaniu z internetu, niż przeznaczając dodatkowe zasoby na wykrywanie nadużyć.

5.4 Operacje przetwarzania wynikające z monitorowania korzystania z ICT poza miejscem pracy

Korzystanie z ICT poza miejscem pracy stało się bardziej powszechne z uwagi na wzrost popularności pracy w domu, pracy zdalnej i polityki „pracy na własnym sprzęcie w miejscu pracy". Możliwości oferowane przez te technologie mogą stwarzać 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. .

5.4.1 *MONITOROWANIE PRACY W DOMU I PRACY ZDALNEJ*

Pracodawcy coraz częściej oferują pracownikom możliwość pracy zdalnej, np. z domu lub w trakcie podróży. Pojawienie się takiej możliwości należy wręcz uznać za główny czynnik odpowiedzialny za zacieranie się rozróżnienia na miejsce pracy i dom. Ogólnie rzecz biorąc, w takiej sytuacji pracodawca udostępnia pracownikowi sprzęt ICT lub oprogramowanie, które – po jego zainstalowaniu w domu pracownika lub na należących do niego 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.

Chociaż praca zdalna może być postrzegana jako rozwiązanie korzystne dla pracodawcy, może ona również narażać go na dodatkowe ryzyko. Na przykład pracownicy dysponujący zdalnym dostępem do infrastruktury pracodawcy nie podlegają środkom bezpieczeństwa fizycznego, które mogą obowiązywać w lokalu pracodawcy. Mówiąc wprost: w przypadku niewdrożenia odpowiednich środków technicznych ryzyko uzyskania nieuprawnionego dostępu do danych wzrasta i może doprowadzić do utraty lub zniszczenia informacji znajdujących się w posiadaniu pracodawcy, w tym danych osobowych pracowników lub konsumentów.

Aby ograniczyć to ryzyko, pracodawcy mogą uznać zainstalowanie pakietów oprogramowania (na miejscu albo w chmurze) umożliwiających np. rejestrowanie naciśnięć klawiszy lub ruchów myszy, przechwytywanie ekranu (w losowych albo regularnych odstępach czasu), rejestrowanie uruchamianych aplikacji (oraz czasu korzystania z tych aplikacji), a także – w przypadku kompatybilnych urządzeń – włączanie kamer internetowych i nagrywanie materiałów za ich pomocą za uzasadnione. Tego rodzaju technologie są powszechnie dostępne i można je uzyskać m.in. od osób trzecich, takich jak dostawcy usług przetwarzania w chmurze.

Metody przetwarzania wykorzystywane w ramach takich technologii są jednak nieproporcjonalne, przy czym prawdopodobieństwo, że uzasadniony interes pracodawcy będzie wystarczający do uzasadnienia stosowania metod takich jak np. rejestrowanie klawiszy naciskanych przez pracownika lub wykonywanych przez niego ruchów myszą, jest bardzo niewielkie.

W tym kontekście kluczowe znaczenie ma ograniczenia ryzyka związanego z pracą z domu lub pracą zdalną w proporcjonalny, adekwatny sposób, niezależnie od formy wykonywania takiej pracy i od wykorzystywanej w tym celu technologii, w szczególności w przypadku,

gdy granica między korzystaniem z danego urządzenia w celach związanych z pracą i w celach prywatnych jest płynna.

5.4.2 *KORZYSTANIE Z WŁASNEGO SPRZĘTU (BYOD)*

Z uwagi na coraz większą popularność konsumenckich urządzeń elektronicznych, a także biorąc pod uwagę coraz bardziej rozbudowane funkcje i możliwości tych urządzeń, pracownicy mogą zwracać się do pracodawców o umożliwienie im korzystanie w miejscu pracy z własnego sprzętu w celu wypełniania obowiązków służbowych. Jest to tak zwana praktyka BYOD, czyli przynieś własny sprzęt.

Skuteczne wdrożenie rozwiązań w zakresie korzystania z własnego sprzętu w miejscu pracy może przynieść pracownikom szereg korzyści, m.in. poprawić ich zadowolenie z pracy, podnieść ich ogólne morale, a także zwiększyć ich wydajność i elastyczność. Taki sposób wykonywania pracy z definicji wiąże się jednak z tym, że część operacji wykonywanych przez pracownika na danym urządzeniu będzie miała osobisty charakter, w szczególności o określonych porach dnia (np. wieczorami lub w weekendy). Dlatego też nie można wykluczyć, że korzystanie przez pracowników z ich własnych urządzeń doprowadzi do sytuacji, w której pracodawcy będą przetwarzali informacje na temat tych pracowników – i potencjalnie informacje na temat członków ich rodzin, którzy również korzystają z tych urządzeń – niezwiązane z działalnością prowadzoną przez dane przedsiębiorstwo.

W kontekście zatrudnienia zagrożenia dla prywatności towarzyszące korzystaniu z własnego sprzętu w miejscu pracy są najczęściej związane z technologiami monitorowania gromadzącymi identyfikatory takie jak adresy MAC lub z przypadkami uzyskania dostępu do urządzenia pracownika przez pracodawcę pod pretekstem przeprowadzenia skanowania bezpieczeństwa, tj. pod kątem obecności złośliwego oprogramowania. Jeżeli chodzi o tę ostatnią kwestię, istnieje szereg rozwiązań komercyjnych pozwalających skanować urządzenia prywatne, ale stosowanie takich rozwiązań może potencjalnie umożliwić uzyskanie dostępu do wszystkich danych przechowywanych na takim urządzeniu, dlatego też należy uważnie monitorować korzystanie z tego rodzaju środków. Na przykład co do zasady nie powinno być możliwości uzyskania dostępu do tych części urządzenia, co do których można przypuszczać, że są wykorzystywane wyłącznie do celów prywatnych (np. do folderu ze zdjęciami wykonanymi za pomocą urządzenia).

Monitorowanie lokalizacji takich urządzeń oraz danych wysyłanych i odbieranych przez te urządzenia można uznać za leżące w uzasadnionym interesie pracodawcy, który jako administrator danych jest zobowiązany do zapewnienia ochrony danych osobowych. Monitorowanie może być jednak niezgodne z prawem wówczas, gdy dotyczy osobistego urządzenia pracownika i gdy prowadzi do gromadzenia danych dotyczących także życia prywatnego i rodzinnego pracownika. Aby uniemożliwić monitorowanie prywatnych informacji, należy wdrożyć odpowiednie środki pozwalające odróżnić korzystanie z urządzenia w celach prywatnych od korzystania z niego w celach służbowych.

Pracodawcy powinni również wdrażać metody bezpiecznego przenoszenia swoich własnych danych między danym urządzeniem a ich siecią. W niektórych przypadkach urządzenie może zostać zatem skonfigurowane w taki sposób, aby przekierowywać wszystkie dane przez wirtualną sieć prywatną, aby zapewnić określony poziom bezpieczeństwa; jeżeli jednak taki środek zostanie zastosowany, pracodawca powinien również wziąć pod uwagę fakt, że oprogramowanie zainstalowane w celach związanych z monitorowaniem stanowi zagrożenie dla prywatności w czasie, gdy pracownik korzysta z urządzenia do celów osobistych. Można

korzystać z urządzeń oferujących dodatkowe zabezpieczenia, takie jak umieszczanie danych w "piaskownicy" (przechowywanie danych w określonej aplikacji).

Z drugiej strony pracodawca musi również rozważyć możliwość wprowadzenia zakazu korzystania z określonych urządzeń służbowych do celów prywatnych, jeżeli nie ma żadnej możliwości zapobieżenia monitorowaniu wykorzystania do celów prywatnych – na przykład jeżeli urządzenie oferuje możliwość uzyskania zdalnego dostępu do danych osobowych, w odniesieniu do których pracodawca pełni funkcję administratora danych.

5.4.3 *ZARZĄDZANIE URZĄDZENIAMI MOBILNYMI*

Zarządzanie urządzeniami mobilnymi umożliwia pracodawcom zdalne lokalizowanie urządzeń, wdrażanie określonych ustawień lub aplikacji oraz usuwanie danych na żądanie. Pracodawca może obsługiwać tę funkcję samodzielnie lub zlecić to zadanie osobie trzeciej. Usługi zarządzania urządzeniami mobilnymi umożliwiają również pracodawcom rejestrowanie lub śledzenie urządzenia w czasie rzeczywistym, nawet jeżeli nie zgłoszono jego kradzieży.

Ocenę skutków dla ochrony danych powinno się przeprowadzać przed wprowadzeniem jakiejkolwiek technologii tego rodzaju, jeżeli jest ona nową technologią lub jeżeli administrator danych nie jest z nią zaznajomiony. Jeżeli ocena skutków dla ochrony danych wykaże, że wdrożenie technologii zarządzania urządzeniami mobilnymi jest konieczne w danych okolicznościach, należy nadal przeprowadzić ocenę w celu ustalenia, czy przetwarzanie danych wynikające z zastosowania tej technologii jest zgodne z zasadami proporcjonalności i pomocniczości. Pracodawcy muszą zagwarantować, że dane gromadzone przy wykorzystaniu wspomnianej funkcji zdalnego określania lokalizacji będą przetwarzane w określonym celu oraz że nie będą stanowiły i nie będą mogły stanowić elementu szerzej zakrojonego programu ciągłego monitorowania pracowników. Funkcje śledzenia należy ograniczyć, nawet gdy korzysta się z nich w określonych celach. Systemy śledzenia mogą zostać zaprojektowane w taki sposób, by umożliwiały rejestrowanie danych o lokalizacji bez przedstawiania ich pracodawcy – w takiej sytuacji dane o lokalizacji powinny zostać udostępnione pracodawcy wyłącznie w przypadku zgłoszenia urządzenia lub jego utraty.

Pracownicy, których urządzenia są objęte usługami zarządzania urządzeniami mobilnymi, muszą również uzyskać wyczerpujące informacje na temat tego, jakie środki śledzenia są stosowane i jakie to ma dla nich konsekwencje.

5.4.4 *URZĄDZENIA DO NOSZENIA NA CIELE*

Pracodawcy coraz częściej rozważają możliwość wyposażenia swoich pracowników w urządzenia do noszenia na ciele, aby śledzić i monitorować stan ich zdrowia i aktywność w miejscu pracy, a niekiedy również poza nim. Ta forma przetwarzania danych wiąże się jednak z przetwarzaniem danych dotyczących zdrowia, a zatem jest zakazana na mocy art. 8 dyrektywy o ochronie danych.

Z uwagi na brak równowagi w relacjach między pracodawcami a pracownikami – tj. z uwagi na fakt, że pracownik jest uzależniony finansowo od pracodawcy – a także biorąc pod uwagę wrażliwy charakter danych dotyczących zdrowia, wysoce nieprawdopodobne jest, aby pracownik mógł udzielić prawnie wiążącej, wyraźnej zgody na śledzenie lub monitorowanie takich danych, zwłaszcza że pracownicy zasadniczo nie dysponują „swobodą" udzielania tego rodzaju zgody. Nawet jeżeli pracodawca korzysta z usług osób trzecich w celu

gromadzenia danych dotyczących zdrowia, a te osoby trzecie przekazują mu wyłącznie zbiorcze informacje na temat ogólnych zmian stanu zdrowia pracowników, taka metoda przetwarzania danych nadal byłaby niezgodna z prawem.

Ponadto, jak opisano w *opinii 05/2014 w sprawie technik anonimizacji*[18], zagwarantowanie całkowitej anonimizacji danych jest niezwykle trudne ze względów technicznych. Nawet w środowisku liczącym ponad tysiąc pracowników, z uwagi na dostępność innych danych na temat pracowników, pracodawca nadal byłby w stanie zidentyfikować poszczególnych pracowników o określonych parametrach zdrowotnych, takich jak wysokie ciśnienie krwi czy otyłość.

Przykład:

Organizacja oferuje swoim pracownikom w prezencie urządzenia do monitorowania stanu zdrowia. Urządzenia takie zliczają liczbę kroków wykonywanych przez pracowników, rejestrują tętno oraz monitorują ich nawyki senne.

Gromadzone przez te urządzenia dane dotyczące zdrowia powinny być dostępne wyłącznie dla pracowników, a nie dla pracodawcy. Wszelkie dane przekazywane między pracownikiem (będącym osobą, której dane dotyczą) a urządzeniem/usługodawcą (pełniącym funkcję administratora danych) są kwestią dotyczącą wyłącznie tych stron.

Ponieważ dane dotyczące zdrowia mogą być również przetwarzane przez podmiot komercyjny, który wyprodukował dane urządzenie lub który oferuje określone usługi pracownikom, 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.

5.5 Operacje przetwarzania związane z czasem pracy i obecnością w miejscu pracy

Systemy zapewniające pracodawcom możliwość kontrolowania osób uprawnionych do wejścia na teren ich lokalu lub uzyskania dostępu do określonych obszarów w takim lokalu mogą zapewniać również możliwość śledzenia działań pracowników. Chociaż tego rodzaju systemy istnieją już od kilku lat, nowe technologie służące do śledzenia czasu pracy pracowników i ich obecności w miejscu pracy są coraz powszechniej wykorzystywane – niektóre z tych technologii wiążą się z przetwarzaniem danych biometrycznych, podczas gdy inne umożliwiają śledzenie urządzeń mobilnych.

Chociaż systemy takie mogą stanowić istotny element ścieżki audytu pracodawcy, stwarzają one również ryzyko polegające na zapewnianiu inwazyjnego poziomu wiedzy na temat działań podejmowanych przez pracownika w miejscu pracy i kontroli nad tymi działaniami.

Przykład:

Pracodawca dysponuje serwerownią, w której przechowuje wrażliwe dane biznesowe, dane osobowe pracowników i dane osobowe klientów w postaci cyfrowej. Aby wywiązać się ze

[18] *Opinia 5/2014 Grupy Roboczej Art. 29 w sprawie technik anonimizacji*, WP 216, z dnia 10 kwietnia 2014 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_pl.pdf

spoczywających na nim zobowiązań prawnych do ochrony takich danych przed nieuprawnionym dostępem, pracodawca zainstalował system kontroli dostępu rejestrujący wejścia pracowników posiadających odpowiednie uprawnienia dostępu do tego pomieszczenia i wyjścia takich pracowników z tego pomieszczenia. W przypadku stwierdzenia zaginięcia dowolnego elementu wyposażenia, uzyskania nieuprawnionego dostępu do jakichkolwiek danych, utraty takich danych lub ich kradzieży, rejestr prowadzony przez pracodawcę umożliwi mu ustalenie osób, które uzyskiwały dostęp do pomieszczenia w określonym czasie.

O ile przetwarzanie danych jest konieczne i nie narusza prawa pracowników do poszanowania ich życia prywatnego, można uznać, że leży ono w uzasadnionym interesie pracodawcy zgodnie z art. 7 lit. f), jeżeli pracownicy zostali odpowiednio poinformowani o operacji przetwarzania. Stałego monitorowania częstotliwości i konkretnych momentów wchodzenia i wychodzenia pracowników nie można jednak uznać za uzasadnione, jeżeli zgromadzone w ten sposób dane wykorzystuje się również w innym celu, np. w ramach oceny wydajności pracowników.

5.6 Operacje przetwarzania wykorzystujące systemy monitoringu wizyjnego

Obecnie monitoring i nadzór wizyjny stwarza podobne problemy dla prywatności pracowników jak wcześniej: umożliwia stałe rejestrowanie zachowań pracownika[19]. Najistotniejsze zmiany dotyczące stosowania tej technologii w kontekście zatrudnienia są związane z możliwością łatwego uzyskania zdalnego dostępu do zgromadzonych danych (np. za pomocą smartfona); zmniejszeniem wielkości kamer (oraz poprawą ich parametrów, np. wprowadzenie możliwości rejestrowania obrazu wysokiej rozdzielczości); oraz umożliwieniem przetwarzania danych za pomocą nowych narzędzi do analizy zawartości wizji.

Dzięki możliwościom oferowanym przez narzędzia analizy zawartości wizji pracodawca może m.in. w zautomatyzowany sposób monitorować mimikę twarzy pracownika, aby wykryć odchylenia od ustalonych schematów ruchu (np. w kontekście fabryk). Takie działania w nieproporcjonalny sposób naruszają prawa i wolności pracowników, dlatego też zasadniczo uznaje się je za bezprawne. Przetwarzanie danych często może wiązać się również z profilowaniem, a także – potencjalnie – ze zautomatyzowanym procesem decyzyjnym. Dlatego też pracodawcy nie powinni stosować technologii rozpoznawania twarzy. Chociaż od tej zasady mogą istnieć pewne niszowe wyjątki, nie mogą one uzasadniać powszechnego stosowania takich technologii[20].

5.7 Operacje przetwarzania związane z pojazdami, z których korzystają pracownicy

Technologie umożliwiające pracodawcom monitorowanie należących do nich pojazdów są obecnie powszechnie stosowane, w szczególności przez organizacje prowadzące działalność w sektorze transportu lub zarządzające dużymi flotami pojazdów.

[19] Zob. odniesienie do wyroku w sprawie *Köpke przeciwko Niemcom* przywołane powyżej; ponadto należy podkreślić, że w niektórych jurysdykcjach dopuszcza się możliwość instalowania systemów takich jak systemy CCTV w celu udowodnienia, że doszło do zachowań niezgodnych z prawem; zob. wyrok Trybunału Konstytucyjnego Hiszpanii w sprawie *Bershka*.

[20] Ponadto zgodnie z ogólnym rozporządzeniem o ochronie danych przetwarzanie danych biometrycznych w celach identyfikacyjnych uznaje się za dopuszczalne wyłącznie w wyjątkowych sytuacjach wymienionych w art. 9 ust. 2.

Każdy pracodawca korzystający z rozwiązań telematycznych instalowanych w pojazdach będzie gromadził dane o pojeździe i konkretnym pracowniku korzystającym z tego pojazdu. 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, uwzględniając informacje o stylu jazdy. Niektóre technologie (np. rejestratory danych na temat zdarzeń) mogą również umożliwiać ciągłe monitorowanie zarówno pojazdu, jak i kierowcy.

Pracodawca może być zobowiązany do zainstalowania technologii śledzenia w pojazdach w celu wykazania zgodności z innymi zobowiązaniami prawnymi, np. obowiązkiem zapewnienia bezpieczeństwa pracowników kierujących tymi pojazdami. Pracodawca może również posiadać uzasadniony interes w dysponowaniu możliwością zlokalizowania pojazdów w dowolnym momencie. Nawet jeżeli pracodawcy posiadaliby uzasadniony interes w dążeniu do realizacji tych celów, powinni w pierwszej kolejności ocenić, czy przetwarzanie danych w tych celach jest konieczne i czy faktyczne wprowadzenie odpowiednich środków jest zgodne z zasadami proporcjonalności i pomocniczości. Jeżeli pracodawca dopuszcza możliwość korzystania z pojazdu do celów prywatnych, najistotniejszym środkiem, jaki może zastosować, aby zapewnić zgodność z tymi zasadami, jest zaoferowanie pracownikowi możliwości skorzystania z opcji wyłączenia: co do zasady pracownik powinien mieć możliwość tymczasowego wyłączenia mechanizmu śledzenia położenia w przypadku, gdy będzie to uzasadnione szczególnymi okolicznościami, takimi jak wizyta lekarska. W ten sposób pracownik może z własnej inicjatywy chronić określone dane dotyczące lokalizacji, traktując je jako dane prywatne. Pracodawca musi zapewnić niewykorzystywanie danych do celów, które mogą wiązać się z niezgodnym z prawem dalszym przetwarzaniem, np. do śledzenia i oceny pracowników.

Pracodawca musi również wyraźnie poinformować pracowników o fakcie zainstalowania urządzenia śledzącego w pojeździe firmowym 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 rejestrowany). Informacje takie powinny być umieszczone w widocznym miejscu w każdym samochodzie, w zasięgu wzroku kierowcy.

W niektórych przypadkach pracownicy mogą korzystać z pojazdów firmowych poza godzinami pracy, np. w celach prywatnych, w zależności od polityki regulującej sposób korzystania z tych pojazdów. Ze względu na wrażliwy charakter danych o lokalizacji jest mało prawdopodobne, aby istniała 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 np. 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.

Jak stwierdzono w *opinii 13/2011 Grupy Roboczej Art. 29 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych*[21]:

„Urządzenia monitorowania pojazdów nie są urządzeniami monitorowania pracowników. Ich funkcją jest śledzenie lub monitorowanie lokalizacji pojazdów, w których są zainstalowane. Pracodawcy nie powinni postrzegać ich jako urządzeń do śledzenia lub monitorowania zachowania lub miejsca pobytu kierowców lub innych pracowników, na przykład poprzez wysyłanie powiadomień o prędkości, z jaką porusza się pojazd".

Ponadto, jak stwierdzono w *opinii 5/2005 Grupy Roboczej Art. 29 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną*[22]:

„Przetwarzanie danych dotyczących lokalizacji może być uzasadnione, jeżeli jest częścią monitorowania przewozu ludzi lub towarów lub służy lepszemu dysponowaniu zasobami w celu świadczenia usług w rozproszonych lokalizacjach (np. planowanie operacji w czasie rzeczywistym), lub zapewnieniu bezpieczeństwa pracownikom bądź towarom czy pojazdom, za które są oni odpowiedzialni. Grupa robocza uważa natomiast przetwarzanie danych za wykraczające poza niezbędny zakres w przypadku, gdy pracownicy mogą według własnego uznania ustalać plany wyjazdów służbowych lub wówczas, gdy służy ono wyłącznie monitorowaniu ich pracy, jeżeli można to robić innymi metodami".

5.7.1 *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, w razie wypadku. Takie systemy zapewniają możliwość rejestrowania gwałtownych zmian kierunku jazdy lub wypadków, np. w reakcji na nieoczekiwane hamowanie, w przypadku wybrania opcji rejestrowania danych w okresie bezpośrednio poprzedzającym zdarzenie; można jednak wybrać również skorzystać z opcji stałego rejestrowania takich 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 szczegółowych 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. Stosowanie rejestratorów danych na temat zdarzeń można jednak 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.

[21] *Opinia 13/2011 Grupy Roboczej Art. 29 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych*, WP 185, z dnia 16 maja 2011 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_pl.pdf

[22] *Opinia 5/2005 Grupy Roboczej Art. 29 w sprawie wykorzystywania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną*, WP 115, z dnia 25 listopada 2005 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_pl.pdf

Przykład:

Przedsiębiorstwo transportowe wyposaża wszystkie swoje pojazdy w kamery wideo umieszczone w szoferce, które rejestrują dźwięk i obraz. Celem przetwarzania gromadzonych w ten sposób danych jest doskonalenie umiejętności pracowników w zakresie kierowania pojazdami. Kamery zostały skonfigurowane w taki sposób, aby zachowywały nagrania w przypadku wystąpienia określonych zdarzeń, takich jak nieoczekiwane hamowanie lub gwałtowna zmiana kierunku jazdy. Przedsiębiorstwo przyjmuje, że posiada podstawę prawną do podjęcia takich działań, ponieważ przetwarzanie danych leży w jego uzasadnionym interesie polegającym na ochronie bezpieczeństwa jego pracowników i innych kierowców zgodnie z art. 7 lit. f) dyrektywy.

Uzasadniony interes przedsiębiorstwa związany z monitorowaniem kierowców nie przeważa jednak nad prawem tych kierowców do ochrony swoich danych osobowych. Stałe monitorowanie pracowników za pomocą takich kamer stanowi poważne naruszenie ich prawa do prywatności. W tym kontekście można skorzystać z innych metod (np. zainstalować urządzenia uniemożliwiające korzystanie z telefonów komórkowych), a także wdrożyć inne systemy bezpieczeństwa, takie jak zaawansowany system hamowania awaryjnego lub system ostrzegania przed niezamierzoną zmianą pasa ruchu, które mogą być wykorzystywane do przeciwdziałania wypadkom pojazdów, w zależności od tego, który z tych systemów zostanie uznany za odpowiedniejszy. Ponadto gromadzenie takich materiałów wideo może często skutkować przetwarzaniem danych osobowych osób trzecich (takich jak przechodnie), a w przypadku takiego przetwarzania posiadanie przez przedsiębiorstwo uzasadnionego interesu nie stanowi wystarczającego uzasadnienia dla przetwarzania.

5.8 Operacje przetwarzania wiążące się z ujawnieniem danych pracowników osobom trzecim

Przedsiębiorstwa coraz częściej przekazują dane swoich pracowników klientom, aby zagwarantować sprawniejsze świadczenie stosownych usług. W zależności od zakresu świadczonych usług tego rodzaju dane mogą być stosunkowo szczegółowe (np. mogą obejmować fotografię z wizerunkiem pracownika). Z uwagi na nierównowagę sił pozycja pracowników jest jednak zbyt słaba, aby można było w ich przypadku mówić o dobrowolnym udzielaniu zgody na przetwarzanie ich danych osobowych przez ich pracodawcę, a w przypadku stwierdzenia, że takie przetwarzanie danych nie jest proporcjonalne, pracodawca nie posiada tytułu prawnego do tego rodzaju przetwarzania danych.

Przykład:

Przedsiębiorstwo kurierskie przesyła swoim klientom wiadomość e-mail zawierającą link odsyłający do strony zawierającej informacje o imieniu i nazwisku kuriera (pracownika) oraz o jego lokalizacji. Przedsiębiorstwo udostępnia również zdjęcie paszportowe kuriera. Przedsiębiorstwo wyszło z założenia, że posiada tytuł prawny do przetwarzania danych z uwagi na swój uzasadniony interes (art. 7 lit. f) dyrektywy) polegający na zapewnieniu klientowi możliwości sprawdzenia, czy dostawca jest faktycznie osobą, za którą się podaje.

Ujawnienie klientom danych dotyczących imienia i nazwiska oraz wizerunku dostawcy nie jest jednak konieczne. Z uwagi na brak innych podstaw prawnych uzasadniających takie przetwarzanie należy uznać, że przedsiębiorstwo kurierskie nie jest uprawnione do udostępniania klientom tego rodzaju danych osobowych.

5.9 Operacje przetwarzania wiążące się z międzynarodowym przekazywaniem danych kadrowych oraz innych danych dotyczących pracowników

Pracodawcy coraz częściej korzystają z aplikacji i usług w chmurze, takich jak aplikacje i usługi służące do przetwarzania danych kadrowych oraz internetowe aplikacje biurowe. Korzystanie z większości z tych aplikacji skutkuje międzynarodowym przekazywaniem danych pracowników. Jak wspomniano wcześniej w opinii 08/2001, art. 25 dyrektywy stanowi, że przekazywanie danych osobowych państwu trzeciemu spoza UE można uznać za dopuszczalne wyłącznie w przypadku, gdy państwo to zapewnia odpowiedni stopień ochrony. Niezależnie od podstawy prawnej, przekazywanie danych musi odbywać się zgodnie z przepisami dyrektywy.

Dlatego też należy zapewnić zgodność ze stosownymi przepisami dotyczącymi międzynarodowego przekazywania danych. Grupa Robocza Art. 29 podtrzymuje swoje wcześniejsze stanowisko, w którym stwierdziła, że lepszym rozwiązaniem jest poleganie na odpowiednim poziomie ochrony, a nie na odstępstwach wymienionych w art. 26 dyrektywy o ochronie danych; jeżeli podjęcie działań w tym obszarze jest uzależnione od uzyskania zgody, taka zgoda musi być konkretna, jednoznaczna i dobrowolna. Należy jednak również zapewnić, aby udostępnianie danych poza obszarem UE/EOG i późniejsze uzyskiwanie dostępu do tych danych przez inne podmioty w ramach grupy ograniczało się do minimum niezbędnego do osiągnięcia zamierzonych celów.

6. Wnioski i zalecenia

6.1 Prawa podstawowe

Treści przesyłane za pomocą łączności, o której mowa powyżej, jak również dane o ruchu związane z taką łącznością podlegają takiej samej ochronie praw podstawowych jak komunikacja „analogowa”.

Treść komunikacji elektronicznej wychodzącej z lokalu przedsiębiorstwa może być objęta zakresem pojęć „życia prywatnego” i „korespondencji” w rozumieniu art. 8 ust. 1 europejskiej konwencji praw człowieka. Zgodnie z aktualnym brzmieniem dyrektywy o ochronie danych pracodawcy mogą gromadzić dane w uzasadnionym celu – o ile przetwarzanie tych danych odbywa się na odpowiednich warunkach (tzn. jest proporcjonalne i konieczne, leży w rzeczywistym i istniejącym obecnie interesie, jest zgodne z prawem i odbywa się w konkretnym celu i w przejrzysty sposób) – wyłącznie w oparciu o określoną podstawę prawną zapewniającą im możliwość przetwarzania danych osobowych zgromadzonych lub wygenerowanych za pośrednictwem środków łączności elektronicznej.

Fakt, że pracodawca jest właścicielem środków elektronicznych, nie znosi prawa pracowników do poufności komunikacji związanej z danymi o lokalizacji i korespondencją. Śledzenie lokalizacji pracowników za pomocą ich własnych urządzeń lub urządzeń firmowych należy ograniczać do sytuacji, w których takie śledzenie jest bezwzględnie konieczne do osiągnięcia uzasadnionego celu. W przypadku pracy na własnym sprzęcie w miejscu pracy należy pamiętać o zapewnieniu pracownikom możliwości ochrony ich prywatnej komunikacji przed jakimkolwiek pracowniczym systemem monitorowania.

6.2 Zgoda; uzasadniony interes

Pracownicy praktycznie nigdy nie mogą dobrowolnie udzielić zgody, odmówić zgody ani cofnąć zgody, z uwagi na zależność wynikającą ze stosunku pracy między pracodawcą a pracownikiem. Z powodu tej nierównowagi sił pracownicy mogą udzielić dobrowolnej zgody wyłącznie w wyjątkowych okolicznościach, w których przyjęcie lub odrzucenie propozycji nie pociąga za sobą żadnych konsekwencji.

Niekiedy pracodawcy mogą powołać się na uzasadniony interes, wskazując go jako podstawę prawną podejmowanych działań, pod warunkiem że przetwarzanie danych jest bezwzględnie konieczne ze względów prawnych i zgodne z zasadami proporcjonalności i pomocniczości. Przed wdrożeniem jakiegokolwiek narzędzia monitorowania należy przeprowadzić analizę proporcjonalności, aby zbadać, czy wszystkie dane są niezbędne, czy konieczność przetwarzania danych przeważa nad ogólnymi prawami pracowników do prywatności, które przysługują im również w miejscu pracy, oraz czy w danym przypadku zachodzi potrzeba wdrożenia środków zapewniających ograniczenie skali naruszenia prawa do życia i poufności komunikacji do niezbędnego minimum.

6.3 Przejrzystość

Pracowników należy skutecznie informować o wszelkich środkach monitorowania wdrożonych w miejscu pracy, celach tego monitorowania oraz okolicznościach, w których się ono odbywa, a także działaniach, które pracownicy mogą podejmować, aby uniemożliwić gromadzenie ich danych przez technologie monitorowania. Polityka i zasady dotyczące zgodnego z prawem monitorowania muszą być przejrzyste i łatwo dostępne. Grupa Robocza zaleca włączenie reprezentatywnej grupy pracowników w proces opracowywania i oceny takich zasad i polityki, ponieważ większość działań w obszarze monitorowania może wiązać się z ingerencją w życie prywatne pracowników.

6.4 Proporcjonalność i minimalizacja danych

Przetwarzanie danych w miejscu pracy musi być proporcjonalne do ryzyka, jakie ponosi pracodawca. Na przykład niewłaściwe korzystanie z internetu można wykryć bez konieczności analizowania zawartości stron internetowych. Jeżeli takiemu niewłaściwemu korzystaniu z internetu można zapobiec (np. poprzez stosowanie filtrów sieci Web), pracodawca zasadniczo nie ma prawa do monitorowania.

Co więcej, wprowadzenie całkowitego zakazu komunikowania w celach prywatnych jest niepraktyczne, a egzekwowanie przestrzegania tego zakazu może wymagać wdrożenia nieproporcjonalnego poziomu monitorowania. Działaniom prewencyjnym należy przypisywać znacznie większą wagę niż działaniom mającym na celu wykrycie określonych zachowań – interesy pracodawcy można chronić skuteczniej, zapobiegając niewłaściwemu korzystaniu z internetu, niż przeznaczając dodatkowe zasoby na wykrywanie nadużyć.

Należy w miarę możliwości ograniczać do minimum informacje rejestrowane w ramach ciągłego monitorowania, jak również informacje ujawniane pracodawcy. Pracownicy powinni mieć możliwość tymczasowego wyłączenia mechanizmów śledzenia lokalizacji, jeżeli w danych okolicznościach będzie to uzasadnione. Rozwiązania umożliwiające np. śledzenie pojazdów mogą zostać skonfigurowane w taki sposób, aby rejestrowały dane dotyczące lokalizacji bez ujawniania ich pracodawcy.

Pracodawcy muszą pamiętać o zasadzie minimalizacji danych przy podejmowaniu decyzji o wdrożeniu nowych technologii. Informacje należy przechowywać przez jak najkrótszy czas

wymagany zgodnie z wyznaczonym okresem zatrzymywania. Informacje, które nie są już potrzebne, należy każdorazowo usuwać.

6.5 Usługi w chmurze, aplikacje internetowe i międzynarodowe przekazywanie danych

Jeżeli pracownicy korzystają z aplikacji internetowych służących do przetwarzania danych osobowych (takich jak internetowe aplikacje biurowe), pracodawcy powinni rozważyć umożliwienie pracownikom wyznaczenia określonych przestrzeni prywatności, do których pracodawca nie mógłby pod żadnym pozorem uzyskać dostępu, takich jak folder na prywatne wiadomości e-mail czy prywatne dokumenty.

Korzystanie z większości aplikacji w chmurze będzie skutkowało międzynarodowym przekazywaniem danych pracowników. Należy jednak zagwarantować, że przekazywanie danych osobowych państwu trzeciemu spoza UE odbywa się wyłącznie po zapewnieniu odpowiedniego stopnia ochrony oraz że udostępnianie danych poza obszarem UE/EOG i późniejsze uzyskiwanie dostępu do tych danych przez inne podmioty w ramach grupy ogranicza się do minimum niezbędnego do osiągnięcia zamierzonych celów.

* * *

Sporządzono w Brukseli dnia 8 czerwca 2017 r.

W imieniu Grupy Roboczej
Przewodnicząca
Isabelle FALQUE-PIERROTIN